✓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

چگونه از شبکه خود در برابر « مهندسي اجتماعي » دفاع كنيم

پسران افتاب

ممكن است شما يك تجهيزات ديواره آتش بسيار گران قيمتي بخريد. بهترين نرم افزار آنتي ويروس را نصب كرده باشيد و قوي ترين سيستم هاي كشف دخول سرزده (IDS) را اضافه كرده باشيد اما هنوز نقطه ضعفي در طراحي امنيتي شما وجود دارد كه از آن چشم پوشي كرده ايد.

در اين مقاله قصد داريم كه درباره بعضي از تاكتيك هاي مهندسي اجتماعي (Social Engineering) ، كه بسيار با اهميت نيز مي باشد بحث كنيم. در اين مقاله نحوه محافظت از نفوذگراني كه به وسيله سوءاستفاده از افراد و فريب آنها خيلي سريعتر در شبكه ما نفوذ مي كنند ، بحث خواهد شد.

اگر كاربري از سازمان شما كه دسترسي مجازي روي شبكه دارد فريب بخورد و كلمه عبور خود را در اختيار يك كاربر غير مجاز بگذارد ، آنگاه تمامي روشهاي محافظت در برابر حملات بي فايده خواهد بود.

هر سارقي مي داند كه براي وارد شدن به يك ساختمان ، داشتن يك كليد ، خيلي بهتر از شكاندن قفل با ديلم و يا وارد شدن به زور از

پنجره است.

در دنياي امنيت كامپيوتر به نحوه گرفتن اين كليد رمز ، «مهندسي اجتماعي» مي گويند. مهندسي اجتماعي نيازي به مسايل تكنيكي ندارد و بيشتر يك امر فردي مي باشد كه بستگي زيادي روي مهارت هاي فردي دارد. نفوذگر با استفاده از فريب و نيرنگ و يا ارعاب ، شخص را قانع مي كند كه پسورد و يا هر اطلاعات مفيد ديگري را در اختيار او قرار دهد.Kevin Mitnick كه يكي از ماهرترين نفوذگران در اين زمينه بود (كه به همين دليل نيز دستگير شد) ، كتابي دارد به نام Controlling the Human of Security كه در آن به اين موضوع پرداخته است.

مهندسي اجتماعي

مهندسي اجتماعي به صورت زير تعريف مي شود:

نوعي از دخول سرزده غير تكنيكي كه وابستگي زيادي به نحوه ارتباط افراد دارد و اغلب نيز با حيله گري انجام مي شود و باعث مي گردد كه بعضي از مسايل امنيتي در سازمان شكسته شود و يا لو رود.

بعضي از سناريو هاي مهندسي اجتماعي به صورت زير مي باشد:

- به يكي از كاربران تلفن بزنيد و بگوييد كه من يكي از مديران بخش شبكه هستم و براي حل بعضي از مشكلات بخش شبكه، نياز به نام كاربري و كلمه رمز شما دارم.

- به يكي از شركت هاي بخش آي تي زنگ بزنيد و وانمود كنيد كه يكي از مديران شركت مي باشيد و نام كاربري و كلمه رمز خود را گم كرده ايد و خيلي فوري به آن احتياج داريد.

- با يكي از كارمندان بخش كامپيوتر سازمان طرح دوستي بريزيد و در يك مكالمه عشقي از او اطلاعات بخش امنيتي شركت را دريافت كنيد.

وقتي كه نفوذگر مهارت هاي مهندسي اجتماعي و مهارت هاي كامپيوتري را با هم دارد به راحتي مي تواند در هر شبكه اي نفوذ كند.

بيشتر درخواستهايي كه از طريق اينترنت و به خصوص پست الكترونيكي دريافت مي شود كه در آن از جانب مدير و يا يكي از كارمندان بانك و يا شركت هاي كارت اعتباري از كاربر خواسته شده است كه به فلان سايت بروند و در آنجا اطلاعات كاربري خود را وارد كنند ،(در سايتي كه مربوط به هكر مي باشد) اين نيز يكي از روشهاي مهندسي اجتماعي مي باشد.

بعضي از مهندسي هاي اجتماعي ، روي مطالب تحقيقاتي شركت ها مي باشد. چنين فعاليت هايي به نام آشغال گردي (dumpster diving) معروف هستند(يعني در آشغالها و كاغذ هاي كاري دور انداخته شده يك شركت به دنبال اطلاعات مفيد گشتن) كه اين هم مي تواند نوعي مهندسي اجتماعي باشد.

بعضي از هكر ها هم به صورت ماهرانه اي وانمود مي كنند كه مثلا آنها

مسوول تعمييرات ساختمان هستند و يا اينكه به عنوان يك سرايدار در شركت شما استخدام شوند ، از آنجاييكه بيشتر كارمندان كارهاي خودشان را از راه دور انجام مي دهند بنابراين هيچگاه به كسي اجازه ندهيد كه به محل فيزيكي سايت كامپيوتر شما نزديك شود. يك هكر مصمم ممكن است كه روزها و يا هفته ها را صرف كند تا اعتماد يك كارمند را به دست آورد كه از راههاي مختلفي اين كار مي تواند انجام شود (مخصوصا براي ما ايراني ها كه هر روز با يك نفر در ياهو مسنجر دوست مي شويم!)

مهندسي اجتماعي معكوس نيز يكي روشهايي مي باشد كه در آن نفوذگر بعضي از مشكلات را براي كامپيوتر كاربر ايجاد مي كند و خودش هم براي كمك مي آيد (مانند اينكه يك نفر آتشي درست كند و خودش هم براي خاموش كردن آن كمك كند) . همين امر باعث مي شود كه اعتماد كاربر را سريع تر جلب كند و اطلاعات لازم را سريع تر از او بگيرد. براي مثال مهندس اجتماعي (نفوذگر) ممكن است كه ميلي به همراه تروجاني كه به آن ضميمه شده است براي كاربر مورد نظرش ارسال كند و چون كاربر ، مهندس را مي شناسد و به آن اعتماد دارد بدون اينكه درباره فايل ضميمه احتياط كند به راحتي فايل ضميمه شده را اجرا مي كند و يا حتي آن را براي ديگران نيز ارسال مي كند.

چگونه شما مي توانيد در مقابل مهندسي اجتماعي ايمن شويد؟

دفاع در برابر مهندسي اجتماعي بايد به اندازه تمام تكنولوژيهاي امنيتي كه براي محافظت از شبكه اتان به كار مي برید ، اهميت داشته باشد.

اما متاسفانه معمولا اين نوع دفاع از طرف مديران شبكه رد مي شود. اينگونه فرض نكنيد كه كاربران خودشان بهتر مي دانند كه نبايد پسورد خود را به كس ديگري بدهند. علاوه بر آموزش كارمندان جزء ، حتي اعضاي تيم IT خود را كه روي امنيت سيستم هاي شما كار مي كنند نيز بايد آموزش ببينند.بيش از نيمي از كارمندان ، هيچ دليلي نمي بينند كه به فردي كه به نظر وجهه خوبي دارد پاسخ ندهند. حتي حرفه اي ها هم وقتي به يك فرد خشمگين برخورد مي كنند كه مدعي هست از مديران رده بالاي شركت مي باشد و به سرعت نياز به اطلاعاتي دارد ، دو دل هستند كه از فرد بخواهند كارت شناسايي خود را نشان دهد.

محافظت شبكه ها در برابر حملات مهندسي اجتماعي در درجه نخست ، به يك سري سياستهايي نياز دارد كه بايد بين تمامي افراد سازمان اجرا گردد. اين سياستها و روالها ، يك سري قوانيني براي پاسخگويي به سوالات مهم را به وجود مي آورد. البته فقط ابلاغ كردن اين سياستها كافي نمي باشد . موارد زير نيز بايد در نظر گرفته شود:

همه اعضاي مديريت بايد اين سياستها را بپذيرند و اين را بفهمند كه در هنگام خواستن كلمه عبور و يا اطلاعات مهم ديگر ، به طرز مناسبي ابتدا هويت خود را معرفي كنند.
اين سياستها بايد توسط تمامي اعضاي شبكه اجرا شود و به صورت مناسبي به آنها آموزش داده شود و دلايل اجراي اين سياستها نيز به آنها تفهيم گردد.
بايد با متخلفين و كساني كه از اين سياستها سرپيچي مي كنند برخورد

كرد و مجازاتهايي براي اين تخلفات قرار داد.

سياستهاي امنيتي شما بايد شفاف باشد و موارد زير را نيز بايد شامل گردد:

سياستهاي كلمات رمز محكم: طول كوتاه، تغييرات كلمه رمز در طول يك مدت مشخص ، عدم استفاده از كلمات موجود در لغتنامه ها، كلمات رمز قابل حدس مانند شماره تلفن ، شماره شناسنامه و يا تاريخ تولد و ...
ممنوع كردن لو دادن پسورد : براي گرفتن كلمات عبور يكي از اعضاي سازمان ، البته فقط براي كسي كه به طور واقع به آن احتياج دارد، روالي در نظر گرفته شود .
كاربران هنگامي كه از كامپيوتر خود به مدت طولاني استفاده نمي كنند و يا آن را ترك مي كنند ، سيستم خود را log off كنند و از Screensaver هايي كه به وسيله كلمات عبور محافظت مي شود ، استفاده كنند.
يك مقداري هم امنيت فيزيكي در نظر گرفته شود تا مهمانان و بيگانگاني كه وارد شركت مي شوند ، به سيستم هاي داخلي دسترسي نداشته باشند.
يك روالي براي معرفي هويت كاربران به گروه IT و كاركنان بخش IT به كاربران معمولي مشخص گردد.
سياستهاي مديريتي انهدام كاغذهاي كاري (تكه تكه كردن ، خرد كردن،

سوزاندن و ...) ، ديسكها و ديگر رسانه هايي كه اطلاعاتي را نگهداري مي كنند قرار داده شود زيرا كه اين اطلاعات مي تواند به يك نفوذگر براي به دست گرفتن سيستم هاي ما كمك كند.

سياهه محافظت و پيشگيري در برابر مهندسي اجتماعي

براي اينكه از موفقيت يك مهندس اجتماعي در دستيابي به اطلاعاتي كه به آنها نياز دارد جلوگيري كنيم و يا اينكه وقوع يك مهندسي اجتماعي را كشف كنيم موارد زير را مي توان در نظر گرفت:

- ابزارهاي شبكه و كامپيوترهاي خود را به صورت فيزيكي محافظت كنيد
- سياستهاي امنيتي را در تمامي كاركنان سازمان گسترش دهيد و به صورت جزيي روشهاي مهندسي اجتماعي را به آنها معرفي كنيد.
- به تمامي كاركنان سازمان نحوه شناختن مهندسان اجتماعي را آموزش دهيد
- تمامي كاغذهاي اداري و رسانه هاي مغناطيسي را كه اطلاعات محرمانه اي را نگهداري مي كنند در جاي مناسبي بايگاني كنيد و پس از مدتي كه غير قابل استفاده شدند ، آنها را نابود كنيد.

يك تمرين خوب براي ايجاد يك پايگاه داده از انواع اين گونه حملات اين مي باشد كه تمامي حملات مهندسي اجتماعي كه در سازمان شما

رخ داده است را در جايي بايگاني كنيد و مكاني را براي هماهنگي و پاسخگويي و جمع آوري اين گونه حملات در سازمان ايجاد كنيد. براي مثال اگر به يكي از منشي ها تلفني زده مي شود از طرف فردي كه وانمود مي كند مدير بخش IT مي باشد ، بايد جايي وجود داشته باشد تا اين منشي گزارش اين تلفن را به آنجا ابلاغ كند. اين كار به شما امكان مي دهد كه با الگوهاي اينگونه حملات آشنا شويد و خودتان را براي آينده قوي تر كنيد و همين امر باعث مي شود كه شما بفهميد ، افرادي وجود دارند كه به اطلاعات شبكه شما نياز دارند و قصد دست يافتن بدانها را دارند.

خلاصه

مهندسي اجتماعي يكي از ساده ترين و عمومي ترين راههاي نفوذ در شبكه هاي مي باشد. سازمانهاي بسياري وجود دارند كه براي امنيت شبكه خود پولهاي فراواني خرج مي كنند ولي هنوز حاضر نيستند براي مقابله با « سوءاستفاده از فاكتورهاي انساني» پولي خرج كنند.

ابتدا بايد براي پيشگيري از اين گونه حملات، سياستهايي را تدوين و اجرا كرد. اما مهمترين مرحله براي پيشگيري، آموزش كاركنان سازمان مي باشد.

امنيت اطلاعات بايد براي تمامي شركتهايي كه به نوعي از شبكه هاي كامپيوتري استفاده مي كنند ، بخش مهمي از برنامه هاي آنان باشد. بايد مراقب تمامي حملاتي باشيم كه عليه شبكه هاي ما اتفاق مي افتد

به خصوص اگر به صورت «مهندسي اجتماعي» باشد.

منبع:پرشین هک