درس اول : نماي كلي

وبلاگ درس به درس تا اخذ مدرك

http://www.certification.mihanblog.ir/
ali.esmaiely@gmail.com

شبكه، دو يا چند كامپيوتر است كه براي ارتباط با هم به يكديگر متصل شده اند. اين نگاهي بسيار ساده به شبكه است، ولي بستري است براي نشان دادن تصويري بسيار بزرگتر كه همان محيط تجاري و شبكه امروزي است.

شركتها كامپيوترها را به هم متصل ميكنند تا اطلاعات و منابع را بع اشتراك بگذارند و كارآيي و توليد را با هزينه پايين تري فراهم كنند. سرورها كامپيوترهايي هستند كه داراي قدرت پردازش و فضاي ذخيره سازي زيادي ميباشند و بدين ترتيب ميتوانند درخواست هاي كلاينت هاي شبكه را پاسخگو باشند. چاپگرها نمونه اي از منابعي ميباشند كه ميتوان به شبكه اضافه كرد و از طريق سرورها مديريت كرد.

كامپيوترهاي كلاينت ميتوانند طوري به سرورها متصل شوندكه كارمندان شركت بتوانند داده ها را ذخيره و بازيابي كنن و اطلاعات را روي چاپگرها چاپ كنند. از سرورها بك آپ تهيه ميشود تا زماني كه داده ها از دست رفت، داده ها از رسانه بك آپ بازيابي شوند. بدين ترتيب كارمندان قادرند ابزارهاي لازم براي انجام كار خود را در اختيار داشته باشند و در محيطي كارآ، كم هزينه و قابل اطمينان انجام دهند كه داده هاي شبكه شركت در امنيت كامل قرار دارند و به نحوي از مشكلات سخت افزاري يا اشتباهات كاربري در امانند.

براي بالا بردن بازدهي كارمندان، دسترسي اينترنت نيز ايجاد ميشود. بدين ترتيب كارمندان ميتوانند با افراد شركت هاي ديگر از طريق پيامرساني، ايميل يا روشهاي ديگر، ارتباط برقرار كنند. شركت هاي ديگر نيز به اينترنت متصل ميشوند و داده هاي حساس رد و بدل ميشود. اينترنت روشي سريع و ارزان را براي كسب و كار فراهم ميكند و به همين علت شركت ها سعي دارند تا خدمات تجاري بيشتري را از طريق اينترنت انجام دهند.

وقتي كسب و كار راه اندازي شد، داده هاي حساس ذخيره شده و رد و بدل ميشود. افرادي وجود دارند كه به هر علتي بخواهند در اين كسب و كار اختلال ايجاد كنند، داده ها دزديده و نابود كنند يا ارتباطات را تحت اختيار خود در آورند.

بعنوان يك كارمند بخش كامپيوتر در شركت كوچك، يا عضوي از سيستم اطلاعاتي (IS) در شركت هاي بزرگتر يا حتي بعنوان يك كاربر معمولي كه از اينترنت استفاده ميكنيد تا به گشت و گذار و ارتباط با دوستان و فايل بپردازيد، بايد با يك سري مباني امنيت اطلاعات آشنا باشيد. حتي اگر كار خيلي مهمي نداشته باشيد، با اتصال به اينترنت، داده هاي حساس روي سيستم شما در معرض خطر قرار دارند. سيستم شما ميتواند وسيله اي براي حمله و تخريب ديگر سيستم ها شود و يا به ويروسي آلوده شود كه كارها را مختل ميكند.

اگر در اين گروه قرار داريد، يا ميخواهيد كاري در اين زمينه انجام دهيد، بايد نحوه محافظت از دارايي هاي شركت خود را آموزش ببينيد، به كاربران ابزار لازم براي كارهايشان را ارائه كنيد و اتصالات مخابراتي با ديگر شركت ها و منابع داده برقرار كنيد. در هر حال، يكي از اولين قدم هاي شما در راه آموزش امنيت اطلاعات، اصطلاحات و مفاهيم آن است.

چه چيزي در خطر است؟

شايد فكر كنيد كه حملات خرابي زيادي به بار نمي آورند. ولي با توجه به مقاله اي كه در فوريه ۲۰۰۱ در Newsfactor.com منتشر شد، ذكر شده كه مطالعات روي ۳۰۰۰ كسب كار در ايالات متحده نشان داده است كه هكرها و مشكلات امنيتي از هر دلار درآمد، ۶ سنت را به خود اختصاص ميدهند كه زيان بسيار بزرگي است.

ارزشگذاري دارايي ها

براي هر شركتي، اطلاعات با ارزش ميباشند. اگر هر سازنده نوشيدني هاي غير الكلي، فرمول كوكاكولا را در اختيار داشتند، همه ميتوانستند شركت كوكاكولا راه اندازي كنند و اين شركت نميتوانست محصولات خود را بفروشد. براي يك سازنده هواپيما، اين اطلاعات ممكن است طراحي يك

جت جديد باشد كه صنعت هوايي را دگرگون خواهد كرد. هر نوع شركت و هر نوع صنايعي، اطلاعاتي دارد كه بايد از آنها محافظت كند.

ولي اطلاعات شركت شما چقدر مهم و با ارزش است؟ سوالات زير شما را به درك روشنتري از ارزش ميرسانند :

- اگر داده هاي شركت فاش شود، چه صدمه اي به دارايي هاي شركت ميرسد؟
- ارزش دارايي هاي شركت شما چقدر است؟
- صدمه به سود و سهم بازار چقدر است؟
- ارزش حريم خصوصي چقدر است؟

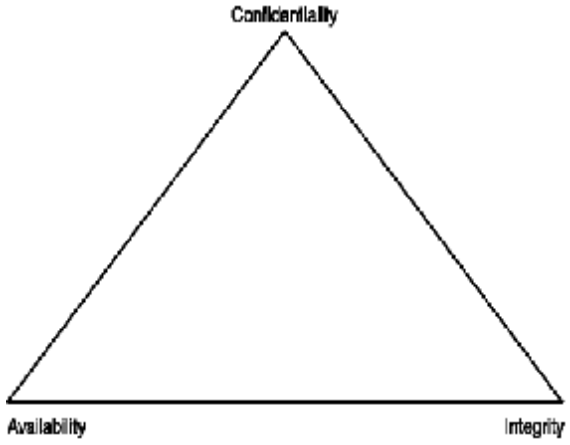
براي هر شركتي، ارزش اطلاعات متفاوت است. براي بسياري از شركت ها، اطلاعات يكي از مهمترين دارايي ها ميباشند. اگر قسمتي از سخت افزار ايراد پيدا كند يا قسمتي از ساختمان شركت آسيب ببيند، صدمات هزينه بالايي دربر خواهند داشت، ولي ميتوان آنها را جايگزين كرد و در بسياري از موارد تعميرات انجام داد. ولي اگر داده ها و اطلاعات از بين بروند، براي هميشه از بين رفته اند و ديگر جايگزين نميشوند. بدين ترتيب صدمه جبران ناپذيري وارد ميشود. همچنين بدانيد كه ارزش اطلاعات در طول زمان متغير است. ارزش بر دو نوع است : ارزش واقعي و ارزش مورد توقع.

- ارزش واقعي : فرض كنيد كه براي شركتي كار ميكنيد سازنده چاي است. اگر شركت شما فرمولي در دست داشته باشد كه تركيب خاصي از چاي باشد و فروش سالانه اين چاي ۵ ميليون دلار باشد، پس ميتوان گفت كه ارزش اين فرمول، ۵ ميليون دلار است. پنج سال بعد، ديگر اين چاي چنان محبوبيتي ندارد و قهوه بيشتر در بين مردم رايج شده است. بدين ترتيب درآمد حاصل از اين چاي در سال به ۲ ميليون دلار تنزل مي يابد. پس ارزش اين فرمول نيز به همين ترتيب كاهش مي يابد. پس اطلاعات تغيير نميكنند، بلكه ارزش اطلاعات است كه تغيير ميكند.
- ارزش مورد توقع : شركت چايسازي كه شما برايشان كار ميكنيد، داراي مديران و گروه بازاريابي هوشمندي است. تيم مديريت تصميم ميگيرد تا با يك شركت توزيع قرارداد ببندد تا چاي خود را در تمام دنيا بيشتر پخش كند. تيم بازاريابي نيز برنامه اي دارند تا در رويارويي تجاري، ارزش قهوه را در برابر چاي پايين تر آورند. دسترسي به برنامه هاي تيم مديريت و بازاريابي ممكن است ارزشمند باشد، ولي اين ارزش هنوز قطعي نيست و فقط پيش بيني ميشود. بدون توجه به نوع ارزش اطلاعات، وظيفه شما اين است كه از آنها حفاظت كنيد. هرچه ارزش هاي قطعي و مورد توقع بالاتر باشند، بيشتر هدف دزدي قرار ميگيرند.

هدف امنيت

مثلث C-I-A در شكل زير عبارت معمولي است كه در امنيت داده ها بسيار مورد استفاده قرار ميگيرد. اين عبارت اختصار سه كلمه زير است :

- محرمانگي (Confidentiality) : اطمينان از اينكه داده ها فقط توسط افراد مجاز قابل دسترسي باشند.
- صحت (Integrity) : اطمينان از اينكه داده ها فقط توسط افراد مجاز ويرايش ميشوند.
- دسترسي (Availability) : اطمينان از اينكه اطلاعات هنگام نياز افراد مجاز قابل دسترسي باشند.



CERTIFICATION

وقتي تلاش براي فراهم كردن محرمانگي داده ها، صحت داده ها و قابليت دسترسي آنها با امنيت فيزيكي تركيب ميشود، ميتوانيد راه حل امنيتي بسيار موثري داشته باشيد.

در ادامه دروس، روش هاي دفاع در مقابل تهديدات شناخته شده، تشريح خواهند شد. كار يك متخصص IS (امنيت اطلاعات) اين است كه داده هاي بسيار قابل دسترسي و قابل اطمينان را فقط براي كساني كه بايد به آنها هنگام نياز دسترسي داشته باشند، فراهم كند.

مديريت ريسك

اطلاعات شركت شما با ارزش است و بايد در زمان و مكان مورد نياز براي استفاده كاربران مجاز قابل دسترسي باشد. بعنوان متخصص امنيت، كار شما به حداقل رساندن شانس شكسته شدن مثلث CIA است.

مديريت ريسك، كه در شكل زير نمايش داده شده است، روال كاملي را نشان ميدهد كه براي معرفي، كنترل و پيش بيني وقايع غير منتظره بكار ميرود. چون غير ممكن است كه خطر را كاملاً از بين ببريم، پس هدف مديريت ريسك را كاهش خطر و حفاظت از مثلث C-I-A تعريف ميكنيم. اين كار با شناسايي ريسك، معرفي تهديدات و حفره هاي امنيتي و سپس كاهش آنها انجام ميشود.

با شناسايي ريسك ها و ايجاد جايگزين براي آنها ميتوانيد خطر را كاهش دهيد. جايگزين كردن يعني انجام كاري كه خطر و دردسر كمتري داشته باشد. پس، برنامه ريزي شما در راه كاهش خطر خواهد بود. براي شركت چاي، برنامه جايگزين را ميتوان محدود كردن تعداد كپي هاي فرمول و كم كردن جاهايي است كه فرمول در آنها ذخيره شده است. ميتوان تعداد افراد و نحوه دسترسي افراد به فرمول را نيز تغيير داد.

براي كاهش خطر، ابتدا بايد ميزان خطر و نقاط ضعف را مشخص كرد.

- خطر يعني امكان آسيب ديدن. از ديدگاه امنيت اطلاعات، خطر اين است كه اطلاعات شركت شما بدست نيروهاي بيگانه بيافتد و بدين ترتيب شركت شما در زمان و هزينه و سود ضرر كند. در مورد شركت چاي خطر اين است كه فرمول اختصاصي شركت فاش شود و شركت هاي ديگر شروع به ساخت محصول مشابه كنند. بدين ترتيب سهم شركت شما از بازار كاهش خواهد يافت. ولي اگر فرمول عمومي باشد و شركت شما فقط روش توليد ارزانتر را بداند، در اينجا فرمول ارزشي ندارد، بلكه خط توليد است كه ارزشمند ميشود.
- تهديد از ديدگاه امنيت اطلاعات، هر فعاليتي است كه باعث خطر احتمالي براي اطلاعات شما باشد. تهديدات بصورت هاي مختلفي وجود دارند، ولي هر تهديدي، خطري براي مثلث CIA ميباشد. در مثال شركت چاي، شركت هاي ديگر ممكن است فرمول را بدزدند يا كارمندي اين فرمول را به شركت ديگري بفروشد.
- حفره، ضعفي در امنيت اطلاعات شماست كه ميتواند توسط تهديدي گشوده شود. اين ضعف ميتواند در امنيت سيستم ها و شبكه، فرآيند ها و روالهاي شما باشد. در مورد شركت چاي، فرمول چاي داده ارزشمند است. افرادي بايد به اين فرمول دسترسي داشته باشند تا چاي را بسازند و خود فرمول نيز در بايد در جايي ذخيره شود. برخي از حفره ها ممكن است در محل نگهداري فرمول باشند، يا تعداد افرادي كه به فرمول دسترسي دارند و محل دسترسي به فرمول.

جمع بندي

از ديدگاه امنيت اطلاعات، شما وظيفه داريد تا از مثلث C-I-A محافظت كنيد، ولي نميتوانيد اين كار را به هر قيمتي انجام دهيد و هميشه نياز به حفاظت از اطلاعات وجود ندارد. براي مثال، اگر شركت شما در كار فروش آب معدني است و اين آب با فرآيند معكوس اوزموسيس خالص ميشود، فرآيند شما شناخته شده است، پس وجهه كاري خوبي ندارد كه از اين فرمول حفاظت كنيد. ولي اگر شركت شما فرآيندي انقلابي در اين زمينه ايجاد كرده كه منجر به كاهش هزينه و زمان خالص سازي آب به نصف ميشود، اين اطلاعات ارزش حفاظت دارند. در مورد نوع حفاظت مورد استفاده نيز محدوديت وجود دارد، پس شما بايد دانش خود را در تركيب با ارزش، تهديدات، حفره ها و خطرات بكار ببريد تا برنامه اي بسيار دقيق و قوي ايجاد كنيد. براي انجام اين كار، برنامه زير را در پيش بگيريد :

- اطلاعات را ارزش گذاري كنيد.
- تا ميتوانيد خطرات را شناسايي كنيد و تهديدات و حفره هاي مربوطه را مشخص كنيد.
- جايگزيني براي خطرات يافت شده، معين كنيد.
- دقت داشته باشيد كه هميشه موارد وجود دارد كه شما در نظر نمي گيريد.

در مورد توانايي شما براي جايگزين كردن خطر نيز محدوديت هايي وجود دارد و گاهي هزينه مشكلي در سر راه كاهش خطر است كه از عواقب خطر بالاتر است. براي مثال، در شركت چاي، فايل داده را كه شامل تركيبات مورد استفاده براي ساخت چاي است، در اختيار شماست، ولي اين اطلاعات ارزش نگهداري و هزينه و زمان را ندارند، زيرا ليستي شناخته شده از تركيبات است. ولي اگر دستور تهيه بهترين چاي را در اختيار شما قرار دهند و شركت شما تنها سازنده اين چاي باشد، ارزش هزينه و زمان و تلاش براي حفاظت را خواهد داشت. هر برنامه خطري متفاوت است، زيرا هر شركتي داراي مجموعه متفاوتي از شرايط، بودجه و نيروي كار قابل استفاده براي كاهش خطر است. برخي از سوالاتي كه ميتوانيد براي مشخص كردن بهتر شرايط كاري شركت ميتوانيد داشته باشيد، بصورت زير است :

كدام اطلاعات نياز به امنيت دارند؟

ارزش اطلاعات چقدر است؟
شانس فاش شدن اطلاعات چقدر است؟
فاش شدن اطلاعات براي شركت به چه قيمتي تمام ميشود؟
نحوه دسترسي به اطلاعات چگونه است؟
چند نفر به اطلاعات دسترسي دارند؟
آيا اطلاعات براحتي ايمن ميشوند؟

بدون در نظر گرفتن اينكه چگونه ميخواهيد ريسك را جايگزين كنيد، بايد تا ميتوانيد ريسك هاي قوي را پيدا كنيد و يك برنامه جايگزيني بسازيد كه تك تك آنها را در بر گيرد. وقتي ريسك را شناختيد و هزينه اي براي آن در نظر گرفتيد (زمان و پول) تا اطلاعات را ايمن كنيد، ميتوانيد آنرا با ارزش اطلاعات مقايسه كنيد تا تشخيص دهيد كه چه ميزان از امنيت معقول است. براي هر وضعيتي، مديريت ريسك و تهديدات متفاوت خواهد بود. در مثال شركت چاي، ممكن است موارد زير را در نظر داشته باشيد :

- ارزش فرمول چاي ۵ ميليون دلار است، زيرا فروش آن ۵ ميليون دلار است.
- خطر اين است كه رقبا ممكن است فرمول چاي را بدست آورند.
- تهديدات را ميتوان كسي از بيرون در نظر گرفت كه فرمول چاي را يافته و به آن دسترسي پيدا ميكند يا كارمندي كه به فرمول دسترسي دارد، آنرا به رقبا ميفروشد.
- حفره ها را ميتوان ذخيره سازي فرمول در پنج مكان مختلف و دسترسي افراد زيادي به فرمول در نظر گرفت.
- براي جايگزيني ريسك، فرمول را ميتوان در يك محل ذخيره كرد و آنرا قابل دسترسي كرد، ولي اين كار عملي نيست. جايگزين بهتر اين ميتواند باشد كه تعداد محل هاي ذخيره سازي را به سه محل كاهش دهيم و دسترسي را به ۲۵ نفر محدود كنيم.

قطعاً تهديدات، حفره ها، خطرات و جايگزين هاي ديگري نيز وجود دارند كه ميتوانيد آنها را مشخص كنيد. شناسايي هر چه بيشتر اين موارد نياز به يك متخصص خوب امنيتي دارد.

تمرين : ايجاد برنامه مديريت ريسك

شما متخصص امنيت يك شركت كوچكيد كه شمع هاي كوچكي را توليد و پخش ميكند. شركت شما اين شمع ها را به فروشگاه ها ميدهد. همچنين فروش اينترنتي نيز دارد. موادي كه براي ساخت شمع از آنها استفاده ميكنيد، از فروشندگان مختلفي از طريق اينترنت خريداري ميشوند. شركت شما نيروي فروش راه دوري دارد كه بين المللي كار ميكند و به شبكه داخلي شما از طريق اينترنت دسترسي دارد. همچنين كارمنداني داريد كه ميتوانند از منزل به شبكه شركت دسترسي پيدا كنند.

CERTIFICATION

شرکت هر سال ۱۲ میلیون دلار فروش دارد که ۳ میلیون دلار آن از فروشگاه ها، ۲ میلیون دلار از طریق اینترنت و ۶ میلیون دلار از فروش مواد سازنده شمع حاصل میشود.

در این تمرین شما باید :

- ارزش بخشهاي مختلف کسب و کار را تعریف کنید.
- تهدیدات را تا جاي ممکن شناسايي کنید.
- حفره ها را تا جاي ممکن شناسايي کنید.
- ریسك ها را تا جاي ممکن شناسايي کنید.
- يك برنامه مدیریت ریسك ارائه کنید.

براي این تمرین جواب کاملي وجود ندارد. هدف از طراحي این تمرین این است که در مورد ریسك هاي ممکن و جایگزین کردن آنها فکر کنید. با ادامه این دروس، یاد خواهید گرفت که براي این سوال راه حلهاي بهتر و دقیق تري ارائه کنید. جوابي را که هم اکنون میدهید، یادداشت کنید و پس از اتمام این دوره، به این تمرین برگردید تا ببینید چقدر دانش و تخصص پیدا کردید.

Security+ Certification Training Kit / Microsoft Corporation.
ISBN 0-7356-1822-4
1. Electronic data processing personnel--Certification.
2. Computer security--Examinations--Study guides. I. Microsoft Corporation.

CERTIFICATION