نما

مجله الکترونیکی مرکز اطلاعات و مدارک علمی ایران

شماره چهارم دوره چهارم. اول مرداد ١٣٨٤

مديريت سيستمهاي امنيت اطلاعات

عادله اسعدي شالي

دانشجوي دوره كارشناسي ارشد رشته كتابداري و اطلاع رساني دانشگاه تهران

كتابدار دانشگاه آزاد تبريز

چكيده

با توجه به نقش اطلاعات به عنوان كالاي با ارزش در تجارت امروز لزوم حفاظت از آن ضروري بنظر مي رسد. براي دستيابي به اين هدف هر سازمان بسته به سطح اطلاعات(از نظر ارزش اقتصادي) نيازمند به طراحي سيستم مديريت امنيت اطلاعات دارد تا از اين طريق بتواند از سرمايه هاي اطلاعاتي خود حفاظت نمايد. اين مقاله سعي دارد به بررسي چگونگي و روند ايجاد يك سيستم امنيت اطلاعات بپردازد.

مقدمه

گرچه بحث دسترسي به اطلاعات و از سوي ديگر امنيت و حفاظت از اطلاعات در سطح كشوري براي حكمرانان از زمانهاي قديم مطرح بوده و دستيابي به اطلاعات نظامي و كشوري گاه موجب نابودي قومي مي شده است اما با توسعه فناوري اطلاعات و استفاده از اطلاعات به عنوان يك ابزار تجاري و سرمايه سود آور، بحث امنيت اطلاعات بعد جديدي به خود مي گيرد. در تجارت امروز، اطلاعات نقش سرمايه يك شركت[١] را ايفا مي كند و حفاظت از اطلاعات سازمان يكي از اركان مهم بقاي آن مي باشد. جهاني شدن اقتصاد منجر به ايجاد رقابت در سطح جهاني شده و بسياري از شركتها براي ادامه حضور خود در عرصه جهاني، ناچار به همكاري با ساير شركتها هستند. به اين ترتيب، طبقه بندي و ارزش گذاري و حفاظت از منابع اطلاعاتي سازمان (چه در مورد سيستم اطلاعاتي و چه اعضاي سازمان) بسيار حياتي و مهم بشمار مي رود. سيستم مديريت اطلاعات ابزاري است در جهت طراحي پياده سازي و كنترل امنيت نرم افزار و سخت افزار يك سيستم اطلاعاتي(Pipkin, 2000).

مديريت امنيت اطلاعات

مديريت امنيت اطلاعات بخشي از مديريت اطلاعات است كه وظيفه تعيين اهداف امنيت و بررسي موانع سر راه رسيدن به اين اهداف و ارائه راهكارهاي لازم را بر عهده دارد. همچنين مديريت امنيت وظيفه پياده سازي و كنترل عملكرد سيستم امنيت سازمان را بر عهده داشته و در نهايت بايد تلاش كند تا سيستم را هميشه روزآمد نگه دارد. هدف مديريت امنيت اطلاعات در يك سازمان، حفظ سرمايه هاي (نرم افزاري، سخت افزاري، اطلاعاتي و ارتباطي و نيروي انساني) سازمان در مقابل هر گونه تهديد (اعم از دسترسي غيرمجاز به اطلاعات، خطرات ناشي از محيط و سيستم و خطرات ايجاد شده از سوي كاربران) است (دشتي، ١٣٨٤: ١٥٩). و براي رسيدن به اين هدف نياز به يك برنامه منسجم دارد. سيستم امنيت اطلاعات راهكاري براي رسيدن به اين هدف مي باشد.

سيستم امنيت اطلاعات

يكي از وظايف مديريت امنيت بررسي و ايجاد يك سيستم امنيت اطلاعات است كه متناسب با اهداف سازمان باشد. براي طراحي اين سيستم بايد عوامل مختلفي را در نظر گرفت. محاسبه ارزش اطلاعات از نظر اقتصادي، بررسي خطرات و محاسبه خسارتهاي احتمالي و تخمين هزينه- سودمندي استفاده از سيستم امنيت اطلاعات، بررسي تهديدات احتمالي و بررسي راهكارهاي مختلف و انتخاب سودمندترين روش براي طراحي سيستمهاي امنيت اطلاعات ضروري بنظر ميرسد(Pipkin, 2000).

مجموعه مراحلي كه در طراحي يك سيستم امنيت اطلاعات در نظر گرفته مي شود به شرح زير مي باشد:

- آشنايي با منابع اطلاعاتي موجود در سازمان: مجموعه منابعي كه يك سازمان در اختيار دارد شامل افرادي كه در سازمان شاغل هستند، امكانات و سرمايه هاي مادي، اطلاعاتي و كه حوضه هاي كاري را مشخص مي كند و سازمان را از ساير سازمان ها جدا مي كند، ساختارها يك سازمان مثل نيروي برق، ارتباطات و تبادلات اطلاعاتي و غيره ... مي

باشد. بعلاوه طراح سيستم بايد با مجموعه الگوريتمها و نرم افزارهاي سيستم اطلاعاتي سازمان، امكانات موجود در سازمان و فرايند توليد و بازيابي اطلاعات و كاربران اين اطلاعات آشنايي كامل داشته باشد. آشنايي با منابع مربوط به حوضه اطلاعات يك سازمان موجب درك وضعيت و ميزان نياز به امنيت و چگونگي اعمال راهكارهاي امنيتي مناسب با آنها خواهد شد.

- ارزيابي ارزش اطلاعات: قيمت گذاري اطلاعات به دو شكل قابل تخمين(محسوس) و غير قابل تخمين (غير محسوس) قابل محاسبه است[۲]. اطلاعات موجود در سازمان مورد ارزيابي قرار گرفته و هزينه توليد آن به هر دو شكل بايد محاسبه شود. علاوه بر اين ضروري است ارزش هزينه توليد و هزينه توليد دوباره اطلاعات در صورت تهديد امنيتي و از بين رفتن اطلاعات محاسبه شود هزينه بازتوليد اطلاعات شامل نيروي انساني، ماشين، تجهيزات و زماني است كه صرف جمع آوري و ورود و هماهنگي اطلاعات خواهد و همچنين مقايسه آن با هزينه ايجاد امكانات حفظ اطلاعات مثل تهيه پشتيبان مناسب و بارگزاري به موقع اطلاعات و همچنين هزينه نرسيدن به موقع اطلاعات در هر يك از اين مدل ها موجب مي شود مديريت امنيت اطلاعات سيستمي متناسب با ارزش اطلاعات سازمان طراحي كند(Pipkin, 2000).
- هزينه فاش شدن اطلاعات: مورد ديگري كه بايد بدقت مورد بررسي قرار گيرد هزينه فاش سازي اطلاعات است اينكه چه اطلاعاتي با فاش شدن صدمات بيشتري به سرمايه هاي سازمان وارد خواهد كرد و به اين ترتيب تعيين سطوح مختلف ارزش اطلاعاتي و سازمان دهي و طبقه بندي اطلاعاتي و هزينه افشا سازي هر يك از سطوح اطلاعاتي مسئله اي است كه نبايد در طراحي سيستم هاي اطلاعاتي مورد غفلت قرار گيرد(Pipkin, 2000).
- تهديدات سيستم اطلاعاتي: مجموعه تهديداتي كه متوجه سيستم اطلاعاتي مي باشد به دو صورت كلي مي باشد برخي به صورت عمدي ايست مثل كلاهبرداري هاي اينترنتي، حملات ويروسها و هكرها، و يا به صورت غير عمدي صورت مي گيرد مثل اشتباهات انساني، مشكل سخت افزاري و نرم افزاري و بلاياي طبيعي.

انواع خطرهاي تهديد كننده سيستم اطلاعاتي

اشتباه‌هاي انساني: كه بيشترين ميزان خسارات از اين طريق به سيستم اطلاعاتي وارد مي شود. عدم ارائه آموزشهاي مناسب و عدم آگاهي و روزآمدسازي اطلاعات توسط كاربران و توليدكننده گاه اطلاعات و گاه بي توجهي آنها در كار موجب تحميل هزينه هاي سنگين بر سازمان مي شود. كه با آموزش مناسب بخش مهمي از مسايل مربوط به كاربران اطلاعاتي حل خواهد شد. بي دقتي و بي توجهي كارمندان نسبت به مسايل امنيتي نيز گاه موجب بروز مشكلات مي شود شخصي به عنوان منشي دفتر فني به كارمندان زنگ زده و مي گويد براي رفع مشكل امنيتي نياز به اسم كاربري و كلمه عبور كارمندان بخش دارد احتمال اينكه از هر ۱۰۰ كارمند تعدادي به اين سوال جواب دهند زياد است. ممكن است پنجره اي باز شود و بگويد كه اتصال شما به شبكه قطع شده براي وصل شدن اسم كاربري و كلمه رمز خود را وارد كنيد (احترامي، ۱۳۸۳: ۱۳۸). اينها مثالهايي هستند كه در صورت سهل نگاري كاربران شركت اطلاعات به راحتي در اختيار جاسوسان اطلاعاتي قرار مي گيرد. نوع ديگر از خطراتي كه توسط كاربران متوجه سازمان است شكل عمدي داشته و در اين حالت سازمان بايد با تعيين دقيق حدود اطلاعات و نيز دقت در انتخاب كاربران اطلاعاتي صدمات آن را تا حد امكان كاهش دهد. در جهاني كه اطلاعات سرمايه اي براي رقابت سازمانها و شركتها مي باشد، با داشتن امكانات و تجهيزات امنيتي نمي توان مطمئن بود كه سيستم امن است، ممكن است مشاور يك شركت براي رقيب نيز نقش مشاوره داشته باشد در اين صورت احتمال فاش شدن اطلاعات سازمان شما وجود دارد. كارمندان خوب، وجود روابط مناسب و خوب در محيط كاري تا اندازه زيادي موجب كاهش اين خطرات مي شود(Pipkin, 2000).

۱. خطرات ناشي از عوامل طبيعي: سيل، زلزله، آتش سوزي، طوفان، صاعقه و غيره... جز عواملي هستند كه هر سيستمي را تهديد مي كنند. استفاده از تجهيزات مناسب و ساختمان مقاوم در مقابل بلاياي طبيعي و طراحي نظام بازيابي مجدد اطلاعات تا حدي مي تواند مشكلات ناشي از آن را كاهش دهد.

۲. ايرادات سيستمي: مشكلات نرم افزاري و سخت افزاري سيستم ممكن است تهديدي براي امنيت اطلاعات سيستم محسوب شود. امروزه سيستمهاي سخت افزاري و نرم افزاري نسبت به قبل بهتر شده است مشكلات سخت افزاري شامل توپولوژي نامناسب شبكه اطلاعاتي، تجهيزاتي كه با هم هماهنگ نيستند، مشكلات مربوط به تجهيزات ارتباطات شبكه(كابلها و مسيريابها) و قطع و وصل برق و غيره بوده و از مشكلات نرم افزاري مي توان به سيستمهاي legacy،[۳] holl هاي موجود در سيستم نرم افزار كه امكان حمله هاي هكرها را بيشتر مي كند، عدم هماهنگي ميان نرم افزار و سخت افزار اشاره كرد(Pipkin, 2000).

۳. فعاليتهاي خرابكارانه: مجموعه فعاليتهايي كه توسط انسان يا ماشين در جهت حمله به سيستم اطلاعاتي و تهديد منابع و امكانات و در راستاي تخريب، تغيير و يا فاش كردن اطلاعات يك سيستم انجام مي شود. فعاليتهاي خلاف شامل سرقت سخت امكانات سخت افزاري و نيز فعاليتهايي كه به جرايم سايبرنتيكي[٤] معروفند مي شود. راهكارهاي لازم براي حفاظت از مجموعه امكانات سازمان(جه امكانات و تجهيزات مربوط به سيستم اطلاعاتي و چه سيستم هاي ديگر سازمان) براي هر سازمان ضروري ايست. براساس آمار ارائه شده در سال ۱۹۹۸، ٤٨درصد و بيشترين تهديداتي كه

متوجه فناوري اطلاعات شده است مربوط به حمله ويروسها بوده است در حالي كه دزدي رايانه اي[٥] و كلاهبرداري رايانه اي[٦] به ترتيب با ١٩و ١٣ درصد، هكرها با ١٢ درصد و استفاده نامناسب از اطلاعات و ارائه اطلاعات نامناسب با ٨ درصد در رتبه هاي بعدي قرار دارند(Bainbridge, 287). كلاهبرداران اطلاعاتي از طريق دست آوردن اطلاعات شخصي و شماره حسابهاي افراد از هويت آنها براي اعمال خلاف استفاده كرده و يا دست به دزدي از حسابهاي آنها مي زنند. هكرها با گشودن اطلاعات رمز گذاري شده سعي در افشا اطلاعات، حذف يا تغيير در اطلاعات موجود دارند. ويروسها با حمله به كامپيوترها مشكلاتي براي سيستم نرم افزاري رايانه ها ايجاد مي كنند[٧] و موجب اختلال در كارايي سيستم مي شوند. مجموعه اين جرايم در كل موجب فاش شدن غير مجاز اطلاعات، قطع ارتباط و اختلال در شبكه، تغيير و دستكاري غير مجاز اطلاعات يا يك پيغام ارسال شده مي شود و سيستم هاي اطلاعاتي بايستي تدابير امنيتي لازم براي جلوگيري از اين آسيبها اعمال كنند.

- اتخاذ سياستهاي امنيتي: بر اساس استاندارد BS7799 [8]i مواردي كه يك سازمان براي پياده سازي يك سيستم امنيتي اعمال مي كند به شرح زير مي باشد:

١. تعيين سياست امنيتي اطلاعات
٢. اعمال سياستهاي مناسب
٣. بررسي بلادرنگ وضعيت امنيت اطلاعاتي بعد از اعمال سياست امنيتي
٤. بازرسي و تست امنيت شبكه اطلاعاتي
٥. بهبود روشهاي امنيت اطلاعاتي سازمان(دشتي، ١٣٨٤: ١٥٩).

در پيش گرفتن سياست امنيتي بايد با توجه بدين نكات باشد:

١. ايجاد امنيت از نظر فيزيكي: همانگونه كه در بخشهاي قبل اشاره شد امنيت تجهيزات و امكانات مادي در ايجاد يك كانال امن براي تبادل اطلاعات بسيار موثر است. انتخاب لايه كانال ارتباطی امن، انتخاب توپولوژی مناسب براي شبكه، امنيت فيزيكي، محل‌های امن برای تجهيزات، منابع تغذيه شبكه و حفاظت تجهيزات در مقابل عوامل محيطی مواردي است كه در امنيت يك سيستم اطلاعاتي بسيار موثرند(بهاري، ١٣٨٤).
٢. سطح بندي صحيح اطلاعات با توجه به ارزش اطلاعات و امكان دسترسي به موقع به اطلاعات براي كاربران هر سطح.
٣. آموزش كاربران اطلاعاتي سازمان در چگونگي استفاده از تجهيزات سخت افزاري و نرم افزاري سازمان و نيز آموزش راههايي كه نفوذ گران براي كسب اطلاعات سازمان استفاده مي كنند[٩] و هشدار به كارمندان در حفاظت از اطلاعات سازمان. از سوي ديگر ايجاد حس تعهد نسبت به شغل و سازمان در كارمندان از طريق اعمال مديريت صحيح.
٤. رمز گذاري اطلاعات و استفاده از امضا ديجيتال[١٠] در ارسال اطلاعات موجب افزايش ضريب اطمينان در تجارت الكترونيك خواهد شد.
٥. تغير مداوم در الگوريتم هاي استفاده شده براي رمز گذاري در كاهش احتمال كشف رمز توسط نفوذ گران و كلاهبرداران اطلاعاتي بسيار موثر است.
٦. استفاده از انواع امكانات امنيتي (البته با توجه نتايج ارزيابي سطح امنيتي مورد نياز) از جمله استفاده از پراكسي كه نقش ايجاد ديواره آتش (Firewall) فيلتر كردن (Filtering)، ثبت كردن (Logging) و تصديق هويت (Authentication) را در شبكه بر عهده دارد; نيز استفاده از نرم افزارهاي مقابله با ويروسها.
٧. استفاده از تست نفوذ پذيري: رويه اي است كه در آن ميزان امنيت اطلاعات سازمان شما مورد ارزيابي قرار مي گيرد. يك تيم مشخص با استفاده از تكنيك هاي هك يك حمله واقعي را شبيه سازي مي كنند تا به اين وسيله سطح امنيت يك شبكه يا سيستم را مشخص كنند. تست نفوذپذيري به يك سازمان كمك مي كند كه ضعف هاي شبكه و ساختارهاي اطلاعاتي خود را بهتر بشناسد و در صدد اصلاح آنها بر آيد. اين امر به يك سازمان كمك مي كند تا در زمينه تشخيص، توانايي پاسخ و تصميم مناسب در زمان خود، بر روي امنيت نيروها و شبكه خود يك ارزيابي واقعي داشته باشد. نتيجه اين تست يك گزارش مي باشد كه براي اجرايي شدن و بازرسي هاي تكنيكي مورد استفاده قرار مي گيرد (شريفي، ١٣٨٣).
٨. با استفاده از يك سيستم پشتيبان گيري اطلاعات از احتمال از بين رفتن اطلاعات جلوگيري نمايد. سيستم پشتيبان گيري مناسبي را كه سازگار با سيستم اطلاعاتي سازمان است انتخاب نموده و تستهاي مربوط به بازيابي اطلاعات را به صورت آزمايشي روي سيستم اعمال نماييد.
٩. بطور مرتب تجهيزات و سيستم اطلاعاتي سازمان را بازرسي نماييد و هر گونه مشكل را گزارش نموده و سعي در رفع آن نماييد. همچنين بطور مرتب سيستم اطلاعاتي و امنيتي سازمان را به روز رساني كنيد و آموزش كارمندان را به صورت مستمر ادامه دهيد(دشتي، ١٣٨٤: ١٦٠).

نتيجه گيري

سيستم امنيت اطلاعات شايد پر هزينه و وقت گير به نظر آيد اما با توجه به اهميت اطلاعات در بقاي سازمان وجود چنين

سيستمي بسيار ضروري مي نمايد. اعمال چنين سيستمي برا ي هر سازمان لازم بوده و بسته به سطح اطلاعات و ارزش اطلاعات سازمان گستردگي متنوعي خواهد داشت. اما هرگز محو نخواهد شد. و در كل لازم است سازمانها سه شرط زير را در طراحي سيستم امنيت اطلاعاتي خود مد نظر داشته باشند:

١. اطمينان از سلامت اطلاعات چه در زمان ذخيره و چه به هنگام بازيابي و ايجاد امكان براي افرادي كه مجاز به استفاده از اطلاعات هستند.

٢. دقت: اطلاعات چه از نظر منبع ارسالي و چه در هنگام ارسال و بازخواني آن بايد از دقت و صحت برخوردار باشد و ايجاد امكاناتي در جهت افزايش اين دقت ضرورت خواهد داشت.

٣. قابليت دسترسي: اطلاعات براي افرادي كه مجاز به استفاده از آن مي باشند بايد در دسترس بوده و امكان استفاده در موقع لزوم براي اين افراد مقدور باشد(Pipkin, 2000).

يادداشتها

[١] در حدود ٤٠ درصد منافع كشور آمريكا از طريق فناوري اطلاعات بدست مي آيد.

[٢] ارزش محسوس از طريق قيمت خريد اطلاعات و ارزش اطلاعات بوسيله صاحبان آنها يا توليدكنندگان آنها ارزش گذاري مي شود

[٣] سيستمهاي قديمي كه دوره استفاده مفيد آنها به پايان رسيده و امكان ويرايش آنها نيز وجود ندارد

[۴] كنوانسيون بين‌المللي جرايم رايانه‌اي بوداپست (٢٠٠١) مجموعه اين جرايم را موارد زير تعريف نموده است: نفوذ غيرمجاز به سيستمهاي رايانه‌اي، شنود غيرمجاز اطلاعات و ارتباطات رايانه‌اي، اخلال در داده‌هاي رايانه‌اي، اخلال در سيستمهاي رايانه‌اي، جعل رايانه‌اي، كلاه‌برداري رايانه‌اي، سوءاستفاده از ابزارهاي رايانه‌اي، هرزه‌نگاري كودكان و تكثير غيرمجاز نرم‌افزارهاي رايانه‌اي و نقض حقوق ادبي و هنري

[5] Theft

[6] Fraud

[٧] به تازگي برخي از ويروسها موجب تخريب سيستم سخت افزاري رايانه ها نيز مي شوند

[٨] اين استاندارد به چگونگي پياده سازي امنيت در ابعاد مختلف يك سازمان مي پردازد

[٩]علاوه بر آموزش چگونگي استفاده از نرم افزار، بايد به كاربران در زمينه چگونگي انتخاب كلمات رمز و حفا ظت از آنها آموزش هاي لازم ارائه شود در زمينه انتخاب و محافظت از كلمات عبور مي توانيد به مقاله اي با آدرس اينترنتي http://ircert.com/articles/Security_Tips.htm

[١٠] امضا ديجيتال از طريق كد گذاري متن ارسالي با يك كد خصوصي توسط فرستنده اعمال مي شود و نيز يك كد عمومي نيز براي گيرنده در نظر گرفته شده است كه از اين طريق مي تواند به متن دسترسي داشته باشد. مزيت امضا ديجيتال در اين است كه گيرنده از طريق تطبيق مقدار hash هاي توليد شده توسط فرستنده و گيرنده امكان تصديق عدم آسيب و تغير در متن ارسالي را به گيرنده مي دهد. براي مطالعه بيشتر در اين زمينه مي توانيد به منبع زير مراجعه نماييد:

صالحي، سهيل. " راهنماي سريع هكر پروف" تهران: ناقوس، ١٣٨١.

منابع:

احترامي، بابك (١٣٨٣). " نقطه ضعف اصلي" مجله شبكه، ش ٥٢ : ١٣٨.

بهاري، مهدي(١٣٨٤). " امنيت تجهيزات شبكه"

قابل دسترس از طريق: http://ircert.com/articles/Security_Tips.htm

دشتي، افسانه(١٣٨٤)." استانداردهاي امنيت" مجله شبكه، ش ٥٤ : ١٥٨.

شريفي، امير حسين(١٣٨٣)."مقدمه اي بر مفاهيم تست نفوذپذيري"

قابل دسترس از طريق: http://www.websecurity.ir/ShowArt.asp?ID=90

صالحي، سهيل(١٣٨١). " راهنماي سريع هكر پروف" تهران: ناقوس.

Bainbridge, David (2000). "introduction to computer law" Harlow: Longman.

"Internet Fraud. " [Online] Available from < http://www.usdoj.gov/criminal/fraud/text/Internet.htm

Pipkin, Donald. L. (2000)." Information security" new jersey: Prentice Hall.