چهارمین
همایش ملی تجارت الکترونیکی
The 4th e-Commerce
CONFERENCE
تهران- ۳ و ۴ آذرماه ۱۳۸۶

امنیت و تجارت الکترونیکی

کبرا قاسمی شبانکاره[1]-وحید مختاری[2] -منصور امینی لاری[3]

چکیده:

با توجه به نقش اطلاعات به عنوان کالای با ارزش در تجارت امروز لزوم حفاظت از آن ضروری به نظر می رسد.برای دستیابی به این هدف هر سازمان بسته به سطح اطلاعات(از نظر ارزش اقتصادی)نیازمند به طراحی سیستم مدیریت امنیت اطلاعات است تا از این طریق بتواند از سرمایه های اطلاعاتی خود حفاظت نماید. مهمترین مزیت و رسالت شبکه های رایانه ای، اشتراک منابع سخت افزاری و نرم افزاری و دستیابی سریع و آسان به اطلاعات است.کنترل دستیابی و نحوه استفاده از منابعی که به اشتراک گذاشته شده اند، از مهمترین اهداف یک نظام امنیتی در شبکه است. در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، به یک راهبرد خاص پایبند باشد و بر اساس آن نظام امنیتی را اجرا نماید.

واژه های کلیدی : **امنیت اطلاعات/ اطلاعات/ امنیت/ فناوری/ حفاظت/ مدیریت /تجارت**

[1]- **دانشجوی کارشناسی مدیریت بازرگانی دانشگاه پیام نور خرامه**
[2]- **دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات دانشگاه شیراز**
[3]- **عضو هیئت علمی دانشگاه آزاد اسلامی واحد علوم وتحقیقات فارس**

مقدمه

اطلاعات در سازمانها، مؤسسات پیشرفته و جوامع علمی، شاهرگ حیاتی محسوب می گردد. گر چه بحث دسترسی به اطلاعات و از سوی دیگر امنیت و حفاظت از اطلاعات در سطح کشوری برای حکمرانان از زمانهای قدیم مطرح بوده و دستیابی به اطلاعات نظامی و کشوری گاه موجب نابودی قومی شده است اما با توسعه فناوری اطلاعات و استفاده از اطلاعات به عنوان یک ابزار تجاری و سرمایه سودآور، بحث امنیت اطلاعات بعد جدیدی به خود می گیرد. دستیابی به اطلاعات و عرضه مناسب و سریع آن همواره مورد توجه سازمانهایی است که اطلاعات در آن ها دارای نقش محوری و سرنوشت ساز است. اگر می خواهیم ارائه دهنده اطلاعات در عصر اطلاعات، و نه صرفاً مصرف کننده اطلاعات باشیم باید امکان استفاده از اطلاعات ذیربط را برای متقاضیان محلی و جهانی در سریعترین زمان ممکن فراهم سازیم. سرعت در تولید و عرضه اطلاعات باید بهره گیری از شبکه های رایانه ای، زمینه استفاده قانونمند و هدفمند از اطلاعات را برای دیگران فراهم کرد. به موازات حرکت به سمت یک سازمان پیشرفته و مبتنی بر فناوری اطلاعات، باید تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده شود.

مهم ترین مزیت و رسالت شبکه های رایانه ای، اشتراک منابع سخت افزاری و نرم افزاری و دستیابی سریع و آسان به اطلاعات است. کنترل دستیابی و نحوه استفاده از منابعی که به اشتراک گذاشته شده اند، از مهمترین اهداف یک نظام امنیتی در شبکه است. با گسترش شبکه های رایانه ای خصوصاً اینترنت، نگرش به امنیت اطلاعات و دیگر منابع به اشتراک گذاشته شده، وارد مرحله جدیدی گردیده است. در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، به یک راهبرد خاص پایبند باشد و بر اساس آن، نظام امنیتی را پیاده سازی و اجرا نماید.

مقاله حاضر در صدد بیان و توضیح مفهوم مدیریت امنیت اطلاعات و تشریح برخی راه کارهای ممکن می باشد.

تعاریف :

تعریف امنیت اطلاعات :

«امنیت اطلاعات»[1] به حفاظت از اطلاعات و به حداقل‌رساندن خطر افشای اطلاعات در بخش های غیرمجاز اشاره دارد. امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است. با توجه به تعاریف ارائه شده، امنیت به مجموعه‌ای از تدابیر، روش‌ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام‌های رایانه‌ای و ارتباطی اطلاق می‌شود.

تعریف مدیریت امنیت اطلاعات :

مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع سر راه رسیدن به این اهداف و ارائه راهکارهای لازم را بر عهده دارد. همچنین مدیریت امنیت وظیفه پیاده سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهده داشته و در نهایت باید تلاش کند تا سیستم را همیشه روزآمد نگه دارد. هدف مدیریت امنیت اطلاعات در یک سازمان، حفظ سرمایه های (نرم افزاری، سخت افزاری، اطلاعاتی و ارتباطی و نیروی انسانی) سازمان در مقابل هر گونه

[1] **Information Security**

تهدید (اعم از دسترسی غیرمجاز به اطلاعات، خطرات ناشی از محیط و سیستم و خطرات ایجاد شده از سوی کاربران) است .
و برای رسیدن به این هدف نیاز به یک برنامه منسجم دارد.
سیستم امنیت اطلاعات راهکاری برای رسیدن به این هدف می باشد.

تاریخچه امنیت اطلاعات :

برای اینکه نگاهی به تاریخچه امنیت اطلاعات داشته باشیم بد نیست به دوره ظهور یکی از نخستین ماشین های رمز نگاری توجه کنیم. در سال1918 میلادی مخترع آلمانی Arthur Scherblus به همراه دوست صمیمی خود Richard Ritter شرکت Scherblus&Ritter را تأسیس کردند، یک شرکت مهندسی متفاوت با زمینه فعالیت متنوع و نامحدود از توربین تا لوازم خانگی.فعالیت او منجر به ساخت یکی از نخستین ماشین های رمز نگاری و شناخته شده ترین سیستم رمز الکترو مکانیکی شد.ماشین جدید بر اساس تئوری ماشین های گردان Rotor Machine طراحی گردیده بود انیگما نامیده شد و در سال 1918 ثبت گردید. اولین مدل آن دارای وزنی حدود 12 کیلوگرم و ارزشی معادل 30 هزار دلار در سال 2003 بود. به علت قیمت قابل توجه دستگاه، توجه کمتری در بخش تجاری به آن شد.

ارتش آلمان نیز در ابتدا توجه زیادی به ارزش های انیگما نشان نمی داد زیرا هنوز نا امن بودن و ضعف سیستم های مورد استفاده در طول جنگ جهانی اول بر آنها اثبات نشده و همچنان تصور می شد اطلاع متفقین از برخی مکالمات محرمانه در طول جنگ به سبب سرقت اطلاعات مربوط توسط جاسوسان بوده است نه کشف پیام های رمز شده و شکست دستگاه های استفاده شده در طول جنگ اول جهانی.تا یک دهه پس از جنگ جهانی اول این تصور ادامه داشت تا اینکه در سال 1923 با افشای جزئیات چگونگی دستیابی به محتوای پیام های مخابره شده ارتش آلمان توسط ارتش انگلیس دوران بی توجه ای ارتش آلمان به انیگما پایان یافت. در کمتر از دو دهه بعد بیش از 30 هزار انیگما توسط ارتش آلمان خریداری شد. اشتباه جنگ اول جهانی تکرار شد و ارتش آلمان یک بار دیگر تمام ارتباطات خود را با اطمینان و خوش بینی کامل بر انیگما بنا نهاد، اشتباهی که به گواه تاریخ ، یکی از عوامل اصل شکست ارتش نازی و سقوط رایش سوم بود.

تا 13 سال پس از ساخت اولین نمونه انیگما، انیگما غیرقابل شکست و رمز آن غیر قابل کشف تصور می شد. تا اینکه در سال 1932 یک افسر ریاضیدان لهستانی به نام"Marian Reje Wski" روشی کاملاً ریاضی برای شکست انیگما ارائه کرد. این روش علاوه بر ایجاد امید در متفقین برای شکست انیگما یک دستاورد مهم در تاریخ رمزشناسی بود.

بی تردید در کنار تمام عوامل مؤثردر تغییر مسیر جنگ جهانی دوم جهانی و سقوط ارتش آلمان، شکست ماشین انیگما و کشف رمز آن تأثیر به سزا داشته است. تلاش های انجام شده در این حوزه در طول جنگ دوم جهانی هم از نقطه نظر ایجاد امنیت و هم از حیث روش ها و تکنیک های شکست ساختارهای امنیتی بسیار قابل توجه هستند.

تا اوایل دهه هفتاد، فعالیت های مربوط به دسترسی و محافظت از اطلاعات در سازمان ها و شرکت ها محدود به محل های نگهداری این اطلاعات شامل آرشیو اسناد و شبکه های محلی رایانه ای بود. در چنین محیط های حفاظت فیزیکی امنیت سیستم ها را اطلاعات را تا حد بسیار بالایی تأمین می کرد.

در واقع تا اوایل دهه 80 میلادی امنیت فقط با دیدگاه فنی مشاهده می شد و برقراری آن منوط به امنیت رایانه و دستگاه های جانبی می دانستند. اما با گذشت زمان متوجه شدند که بیشتر تجاوزات امنیتی از طریق مسائلی همچون ضعف های مدیریتی (از لحاظ امنیتی) و عوامل انسانی (به دلیل عدم آموزش) می باشد لذا از اواسط دهه 80 میلادی تا اواسط دهه 90 میلادی بحث مدیریت امنیت اطلاعات مطرح شد که آن را منوط به خط مشی امنیت اطلاعات و ساختارهای سازمانی می

دانستند. از اواسط دهه 90 میلادی پارامترهای دیگری چون تعریف استراتژیهای امنیتی و خط مشی امنیتی بر اساس نیازهای اصلی سازمان و مدیریت آن می باشد.
مؤلفه هایی چون استانداردهای امنیت اطلاعات، گواهی نامه های بین المللی، فرهنگ سازی امنیت اطلاعات در سازمان و پیاده سازی معیارهای ارزیابی دائمی و پویای امنیت اطلاعات را نیز شامل می شود. لازم به ذکر است که این مرحله هنوز ادامه دارد و در حال تکمیل شدن می باشد.

مفاهیم اصلی در امنیت اطلاعات :

امنیت داده ها به چهار مفهوم کلی قابل تقسیم است: 1ـ محرمانگی[1] 2ـ تمامیت[2] 3ـ اعتبار و سندیت[3] 4ـ دسترسی پذیری[4]

- ♣ محرمانگی: محرمانگی اطلاعات یعنی حفاظت از اطلاعات در مقابل دسترسی و استفاده غیرمجاز، داده های محرمانه تنها توسط افراد مجاز قابل دسترسی می باشد.
- ♣ تمامیت: در بحث امنیت اطلاعات، تمامیت به این معناست که داده ها نمی توانند توسط افراد غیرمجاز ساخته، تغییر یا حذف گردند. تمامیت، همچنین یکپارچگی داده ها در بخش های مختلف پایگاه داده ذخیره شده اند را تحت الشعاع قرار می دهند.
- ♣ اعتبار و سندیت: اعتبار و سندیت دلالت بر موثق بودن داده ها و نیز اصل بودن آنها دارد. به طریقی که اطمینان حاصل شود داده ها کپی یا جعلی نیستند.
- ♣ دسترسی پذیری: دسترس پذیری به این معنی می باشد که داده ها، پایگاه های داده و سیستمهای حفاظت امنیت، در زمان نیاز به اطلاعات در دسترس باشند.

مزایای سرمایه گذاری در امنیت اطلاعات :

- ♣ کاهش احتمال غیر فعال شدن سیستم ها و برنامه ها
- ♣ استفاده موثر از منابع انسانی و غیر انسانی در یک سازمان
- ♣ کاهش هزینه از دست دادن داده
- ♣ افزایش حفاظت از مالکیت معنوی

Confidentially[1]
Integrity[2]
Authenticity[3]
Availability[4]

حفره امنیتی:

تعریف حفره امنیتی: عبارت است از نقاط ضعف موجود در سیستم حفاظت، از لحاظ سخت افزاری یا نرم افزاری که توسط مهاجمان مورد سوء استفاده قرار می گیرد و نفوذ به سیستم حفاظتی را ساده می نماید.

پیامدهای منفی یک حفره امنیتی چیست؟

- ♣ کاهش درآمدوافزایش هزینه
- ♣ خدشه به اعتبار و شهرت یک سازمان
- ♣ ازدست دادن اطلاعات مهم پیامدهای قانونی
- ♣ سلب اعتماد مشتریان و سرمایه گذاران

مدیریت خطرات امنیتی :

رویکرد پیشگیرانه چیست؟

- ♣ شناسایی تهدیدات موجود در یک سازمان: مدیر سازمان یا مشاور امنیی سازمان هدیدا پیش روی سازمان را باید بررسی کند.
- ♣ اولویت بندی خطرات: چون این کار هزینه بر است سازمان بایسی خطرا اساسی که به پیکره سازمان لطمه وارد می کنند را شناسایی و در اولویت قرار دهد.
- ♣ نحوه مدیریت در یک سطح قابل قبول
- ♣ کاهش خطر آسیب پذیری: سازمان باید تدابیر لازم را در جهت کاهش نفوذ پذیری اتخاذ نماید.

دستاوردهای پیاده سازی فرایند مدیریت خطرات امنیتی:

- ♣ زمان پاسخ به تهدیدات: در صورت بروز تهدید امنیتی سرعت العمل سازمان نقش بسزایی در کاهش هزینه ها دارد.
- ♣ مدیریت قانونمند
- ♣ هزینه های مدیریت زیرساخت
- ♣ مدیریت و اولویت بندی خطرات

سیستم امنیت اطلاعات :

می توان گفت یکی از وظایف مهم مدیریت امنیت یا مشاور امنیتی سازمان ایجاد یک سازمان امنیت اطلاعات است که در راستای اهداف سازمان باشد. برای ایجاد این سیستم نیاز است که اطلاعات سازمان از حیث اقتصادی بررسی شود همچنین بررسی خطرات پش روی سازمان و تخمین میزان خسارت ناشی از آن خطر، بررسی تهدیدات احتمالی و راهکارهای مختلف برای انتخاب بهترین سیستم امنیت اطلاعات ضروری می باشد در مراحلی که برای ایجاد یک سیستم امنیت اطلاعات به کار می رود توجه به مراحل زیر حائز اهمیت می باشد:

- آشنایی با منابع اطلاعاتی موجود در سازمان: منابعی که سازمان در اختیار دارد شامل افراد شاغل در سازمان، امکانات و منابع مادی، اطلاعات موجود در سازمان. طراح سیستم باید آشنایی کامل نسبت به منابع سازمان، الگوها و نرم افزارهای سیستم اطلاعاتی سازمان، امکانات موجود در سازمان و فرآیند تولید داشته باشد که این آشنایی موجب درک بهتر وضعیت سازمان و میزان نیاز به امنیت را برای طراح سیستم مشخص می کند
- ارزیابی ارزش اطلاعات: قیمت گذاری اطلاعات به دو شکل قابل تخمین(محسوس) و غیر قابل تخمین (غیر محسوس) قابل محاسبه است. اطلاعات موجود در سازمان مورد ارزیابی قرار گرفته و هزینه تولید آن به هر دو شکل باید محاسبه شود. علاوه بر این ضروری است ارزش هزینه تولید و هزینه تولید دوباره اطلاعات در صورت تهدید امنیتی و از بین رفتن اطلاعات محاسبه شود هزینه بازتولید اطلاعات شامل نیروی انسانی، ماشین، تجهیزات و زمانی است که صرف جمع آوری و ورود و هماهنگی اطلاعات خواهد و همچنین مقایسه آن با هزینه ایجاد امکانات حفظ اطلاعات مثل تهیه پشتیبان مناسب و بارگزاری به موقع اطلاعات و همچنین هزینه نرسیدن به موقع اطلاعات در هر یک از این مدل ها موجب می شود مدیریت امنیت اطلاعات سیستمی متناسب با ارزش اطلاعات سازمان طراحی کند.
- هزینه فاش شدن اطلاعات: در واقع در این مرحله مشخص می کنیم با فاش شدن چه اطلاعاتی صدمات بیشتری به سرمایه های سازمان وارد می شود. به این ترتیب سطوح مختلف ارزش اطلاعاتی و سازماندهی و طبقه بندی اطلاعات و هزینه افشای هر یک از سطوح اطلاعاتی باید به دقت در طراحی سیستم مورد توجه قرار گیرد.
- تهدیدات سیستم اطلاعاتی: تهدیدات پیش روی سازمان یا به صورت عمدی مثل حملات ویروس ها، هکرها و یا به صورت غیر عمدی مثل اشتباهات انسانی ، بلایای طبیعی می باشد.

آشنایی با خطرهای تهدید کننده سیستم اطلاعاتی سازمان:

تهدیدات موجود در پیش روی امنیت سیستم های اطلاعاتی را می توان به سه دسته اصلی تقسیم کرد: افشای اطلاعات محرمانه (افشا)، صدمه به یکپارچگی اطلاعات (دستکاری) و موجود نبودن اطلاعات (تطبیق خدمات). بارزترین تهدید امنیت اطلاعات افشا می باشد .

دیگر خطرهای تهدید کننده به شرح زیر است:

- اشتباه های انسانی: که بیشترین میزان خسارات از این طریق به سیستم اطلاعاتی وارد می شود. عدم ارائه آموزشهای مناسب و عدم آگاهی و روزآمدسازی اطلاعات توسط کاربران و تولیدکننده گاه اطلاعات و گاه بی توجهی آنها در کار موجب تحمیل هزینه های سنگین بر سازمان می شود. که با آموزش مناسب بخش مهمی از مسایل مربوط به کاربران اطلاعاتی حل خواهد شد.
- بلایای طبیعی: مانند سیل، زلزله، طوفان و صاعقه.
- ایرادات سیستمی: مشکلات نرم افزاری و سخت افزاری سیستم که مشکلات سخت افزاری شامل توپولوژی[1] نامناسب شبکه اطلاعاتی، مشکلات مربوط به تجهیزات ارتباطات شبکه(کابلها و مسیریابها) و قطع و وصل برق و غیره بوده و از مشکلات نرم افزاری می توان به سیستمهای legacy[2]، حفره های موجود در سیستم نرم افزار که امکان حمله های هکرها[3] را بیشتر می کند، اشاره کرد.
- فعالیتهای خرابکارانه: مجموعه فعالیتهایی که توسط انسان یا ماشین در جهت حمله به سیستم اطلاعاتی و تهدید منابع و امکانات و در راستای تخریب، تغییر و یا فاش کردن اطلاعات یک سیستم انجام می شود. فعالیتهای خلاف شامل سرقت امکانات سخت افزاری و نیز فعالیتهایی که به جرایم سایبرنتیکی[4] معروفند می شود .
- اتخاذ سیاستهای امنیتی: بر اساس استاندارد BS7799[5] مواردی که یک سازمان برای پیاده سازی یک سیستم امنیتی اعمال می کند به شرح زیر می باشد:
  1. تعیین سیاست امنیتی اطلاعات
  2. اعمال سیاستهای مناسب
  3. بررسی فوری وضعیت امنیت اطلاعاتی بعد از اعمال سیاست امنیتی
  4. بازرسی و تست امنیت شبکه اطلاعاتی
  5. بهبود روشهای امنیت اطلاعاتی سازمان

تاریخچه استاندارد امنیت اطلاعات:

استانداردهای امنیت به دو دسته اصلی تقسیم می گردد که دسته اول در رابطه با امنیت از لحاظ فنی در زمینه هائی نظیر امضاء دیجیتال، رمزنگاری کلید عمومی، رمزنگاری متقارن، توابع درهم ساز، توابع رمزنگاری احراز اصالت پیام و غیره کاربرد دارند، و دسته دوم در رابطه با امنیت ازلحاظ مدیریتی است که قسمت های مختلف مدیریت سازمان را در بر می گیرند. که استاندارد مدیریتی BS7799 یکی از این استانداردها می باشد(نسخه جدید آن ISO/IEC 27001 می باشد)

1-چگونگی اتصال کامپیوترهای متصل به هم از لحاظ سخت افزاری

2-سیستمهای قدیمی که دوره استفاده مفید آنها به پایان رسیده و امکان ویرایش آنها نیز وجود ندارد

3-مهاجمینی که با گشودن اطلاعات رمز گذاری شده سعی در افشای اطلاعات، حذف یا تغییردر اطلاعات موجود دارند

1-کنوانسیون بین‌المللی جرایم رایانه‌ای بوداپست (2001) مجموعه این جرایم را موارد زیر تعریف نموده است: نفوذ غیرمجاز به سیستمهای رایانه‌ای، شنود غیرمجاز اطلاعات و ارتباطات رایانه‌ای، اخلال در داده‌های رایانه‌ای، اخلال در سیستمهای رایانه‌ای، جعل رایانه‌ای، کلاه‌برداری رایانه‌ای، سوءاستفاده از ابزارهای رایانه‌ای، هرزه‌نگاری کودکان و تکثیر غیرمجاز نرم‌افزارهای رایانه‌ای و نقض حقوق ادبی و هنری

2-این استاندارد به چگونگی پیاده سازی امنیت در ابعاد مختلف یک سازمان می پردازد که در ادامه به شرح آن خواهیم پرداخت

استاندارد **BS7799**

تاریخچه این استاندارد که اولین استاندارد مدیریت امنیت اطلاعات است و نام کاملش British Standard 7799 استاندارد انگلیس است به زمان تأسیس مؤسسه Commercial Computer Security Center و بخش UK Department of Trade and Industry در سال 1987 برمیگردد.

این مرکز برای تعیین و تعریف معیارها و استانداردهایی بین المللی برای ارزیابی میزان امنیت تجهیزات تولید شده توسط تولید کنندگان تجهیزات امنیتی و اعطای نشان ها و تأییده های بین المللی و همچنین کمک به کاربران این گونه تجهیزات تأسیس شد.

نسخه اول این استاندارد (BS7799-1) در سال 1995 و در یک بخش و با عنوان BS7799-1: Code of Practice for Information Security Management منتشر گردید و نسخه دوم آن (BS7799-2) که در سال 1999 ارائه شد، علاوه بر تغییر نسبت به نسخه اول، متشکل از دو بخش مستقل ارائه گردید. در فوریه 1998، قسمت دوم این استاندارد با عنوان سیستم مدیریت امنیت اطلاعات یا Information Security Management System که حالادیگر آن را به اختصار ISMS می نامند، منتشر شد. هدف از تدوین این استاندارد ارائه پیشنهاداتی در زمینه مدیریت امنیت اطلاعات برای کسانی است که مسئول طراحی، پیاده سازی یا پشتیبانی مسائل امنیتی در یک سازمان می باشند. این استاندارد متشکل از 35 هدف امنیتی و 127 اقدام بازدارنده برای تامین اهداف تعیین شده می‌باشد. طراحان استاندارد BS7799 اعتقاد دارند که ممکن است کنترل ها و راهکارهای مطرح شده برای همه سازمان ها قابل استفاده نباشد ویا نیاز به کنترلهای بیشتری داشته باشند. در سال 2000 میلادی بخش اول استاندارد BS7799-2 بدون هیچگونه تغییری توسط موسسه بین المللی استاندارد بعنوان استاندارد ISO/IEC 17799 منتشر گردید. وده گروه کنترلی آن شامل سر فصل های ذیل است:

- ♣ سیاست های امنیتی
- ♣ امنیت سازمان
- ♣ کنترل و طبقه بندی داراییها
- ♣ امنیت پرسنلی
- ♣ امنیت فیزیکی و پیرامونی
- ♣ مدیریت ارتباطات و بهره برداری
- ♣ کنترل دسترسی
- ♣ روشهای نگهداری و بهبود اطلاعات
- ♣ مدیریت تداوم فعالیت سازمان
- ♣ سازگاری با موارد قانونی

این استاندارد مجددا در سال 2002و 2005 میلادی بازنویسی شد و با دو نام BS ISO/IEC 17799:2005 و BS 7799-1:2005 در یک سند انتشاریافت. این نسخه متشکل از 39 هدف امنیتی و 134 اقدام بازدارنده است. تغییرات آن نسبت به استاندارد قبل عبارت است از:

الف- افزایش یک فصل جدید و تغییر نمودن بعضی از فصول گذشته

ب- تغییر وحذف شدن بعضی از کنترلهای قدیمی و افزایش تعداد کنترل‌ها به 134عدد

فایده های استاندارد **BS7799** :

استاندارد BS7799 مبنایی مطمئن برای ایجادیک سیستم ایمن می باشد. در زیر به چندی از فایده های اجرای آن اشاره شده است:

- اطمینان از تداوم تجارت و کاهش صدمات توسط ایمن ساختن اطلاعات و کاهش تهدیدها
- اطمینان از سازگاری با استاندارد امنیت اطلاعات و محافظت از داده ها
- قابل اطمینان کردن تصمیم گیری ها و محک زدن سیستم مدیریت امنیت اطلاعات
- ایجاد اطمینان نزد مشتریان و شرکای تجاری
- امکان رقابت بهتر با سایر شرکت ها
- ایجاد مدیریت فعال و پویا در پیاده سازی امنیت داده ها و اطلاعات
- بخاطر مشکلات امنیتی اطلاعات و ایده های خود را در خارج سازمان پنهان نسازید

سیستم مدیریت امنیت اطلاعات :[1]

هدف سیستم مدیریت امنیت اطلاعات اطمینان از تداوم کسب و کار از طریق جلوگیری و به حداقل رساندن اثرات حوادث امنیتی است. اطمینان از ذخیره مطمئن اطلاعات، و حفاظت از آن توسط یک سیستم مدیریت موجب افزایش رقابت با سازمان های دیگر می گردد.

سه اصل در یک سیستم جامع امنیتی به شرح زیر می باشد:

1. سیاستها و دستورالعملهای امنیتی: ارائه طرحها و راهکارهای مناسب جهت محافظت از سیستم‌های اطلاعاتی و داده‌های آن.
2. تکنولوژی و محصولات امنیتی: ابزارهای مورد استفاده برای اعمال دستورالعملها، کنترل و نظارت می‌باشد.
3. عوامل اجرایی: مدیران سیستم‌ها و شبکه‌ها، پرسنل و کاربران عادی در این قسمت جای دارند.

ISMS در ایران: متأسفانه تا کنون هیچ سازمان ایرانی موفق به کسب گواهینامه ISMS نشده است. با توجه به اینکه ایران در صدر جدول جرایم رایانه ای خاورمیانه است پرداخت به این موضوع دارای اهمیت ویژه‌ای است. از میان بیشترین سازمان ها دارای گواهینامه ISMS متعلق به کشور ژاپن است و پس از آن کشور انگلیس قرار دارد. سازمان هایی از کشورهای مصر، عربستان و قطر نیز موفق به دریافت گواهینامه ISMS شده اند.

راه کار های امنیتی:

راه کارهای امنیت اطلاعات به دو دسته تقسیم می شود:

الف) فناوری های امنیت اطلاعات کنشگرایانه یا کنشی[1]: انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی است. در واقع جواب سؤال چه کار باید انجام دهیم تا ...؟ می باشد، که به شرح زیر است:

ISMS [1]

1. رمزنگاری[2] : نوعی نوشتن پنهان، و علم حفاظت، اعتمادپذیری و تأمین تمامیت داده‌ها است، که شامل سه مرحله رمزگذاری[3]، رمزگشایی[4] و تحلیل رمز[5] است. کدگذاری واژه ها به صورت پنهان را رمزگذاری گویند و بازیابی متن آشکار(پیام) از متن رمزی را رمز گشایی می نامند. مدل های رمز گذاری و رمز گشایی توسط دو روش انجام می گردد: 1- مدل متقارن: که استفاده از کلیدهای یکسانی برای رمزگذاری و رمز گشایی است. 2- مدل نامتقارن: استفاده از کلیدهای متفاوت برای رمزگذاری و رمز گشایی است. بازیابی متن آشکار بدون کلید مناسب را تحلیل رمز گویند.
2. امضا های رقومی[6]: معادل «امضای دست‌نوشت» و همان هدف را دارد، نشانه منحصر به فرد یک شخص است، بنابراین نباید قابل جعل باشد.
3. شبکه‌های مجازی خصوصی[7]: فناوری شبکه‌های مجازی خصوصی، عبور و مرور شبکه را رمزگذاری می‌کند. بنابراین این فناوری برای تضمین صحت و امنیت داده‌ها، به رمزنگاری وابسته است. این شبکه بسیار امن، برای انتقال داده‌های
حساس (از جمله اطلاعات تجاری الکترونیکی) از اینترنت به عنوان رسانه انتقال بهره می‌گیرد.
4. نرم‌افزارهای آسیب‌نما[8] : برنامه‌هایی برای بررسی نقاط ضعف یک شبکه یا سیستم یا سایت هستند. بین معنا که میزبان های روی شبکه ر فواصل نامنظم پویش می شوند، به محض خاتمه یافتن بررسی یک میزبان از داده های آن نمونه برداری می شود، در واقع یک عکس فوری[9] گرفته می شود.
5. پویشگرهای ضد ویروس[10]: برنامه‌های نرم‌افزاری هستند که برای بررسی و حذف ویروس‌های رایانه‌ای، طراحی شده‌اند. کارهایی که انجام می دهند عبارتند از: 1) ممانعت از فعالیت ویروس، 2) حذف ویروس، 3) تعمیر آسیبی که ویروس عامل آن بوده است، و 4) گرفتن ویروس در زمان کنترل و بعد از فعال‌شدن آن.
6. پروتکل‌های امنیتی[11]: شیوه های استاندارد که تبادل اطلاعات را میان سیستم ها، کنترل و هدایت می‌کنند.
7. سخت افزارهای امنیتی[12]: ابزارهای فیزیکی مانند امنیت سرورها، امنیت کابلها و غیره که کاربرد امنیتی دارند..
8. جعبه‌های توسعه نرم‌افزار امنیتی[13](SDKs): ابزارهای برنامه‌نویسی مانند «Java security manager» و «Microsoft.net SDKs» که در ایجاد برنامه‌های امنیتی و ساختن برنامه‌های کاربردی امنیتی کاربرد دارند.

ب) فناوری های امنیت اطلاعات وا کنشی[14]: انجام عکس العمل لازم پس از وقوع یک مشکل خاص امنیتی است. در واقع پاسخ سؤال(اکنون که ... چه کار باید انجام دهیم؟) که به شرح زیر است:

Proactive [1]
Cryptography [2]
encryption[3]
decryption[4]
cryptanalysis[5]
digital signtures[6]
virtual private networks [7]
scanners vulnerability [8]
snapshot[9]
Anti- virus scanner [10]
security protocols [11]
Security hardware[12]
security software development kits[13]
Reactive[14]

1. دیوار آتش[1]: اولین خط دفاعی برای دفع مزاحم می باشد. دیوار آتش یک فیلتر بین سازمان داخلی (امین) واینترنت(غیر امین) نصب می شود و هدف آن جلوگیری از ارتباطات غیرمجاز در درون یا بیرون شبکه داخلی میزبان است.
2. کنترل دسترسی[2]: مجموعه سیاست‌های مربوط به دادن اجازه یا عدم اجازه برای دسترسی یک کاربر خاص به قسمت های مختلف اطلاق می‌شود.
3. کلمات عبور[3]: کلمه یا عبارتی است که فرد برای دریافت مجوز دسترسی به اطلاعات باید وارد نماید
4. زیست‌سنجی[4]: علم سنجش و تحلیل‌داده‌های زیستی است. در امنیت اطلاعات، از تحلیل ویژگی‌های بدن انسان (مانند اثر انگشت، قرنیه و شبکیه چشم، الگوهای صدا، الگوهای چهره، و اندازه‌های دست) ً به‌منظور تعیین اعتبار استفاده می شود.
5. نظام‌های آشکارساز نفوذی[5](IDS):یک سیستم دفاعی است که فعالیت‌های مخاطره آمیز را در یک شبکه تشخیص می‌دهد. از ویژگی‌های مهم آن، توانایی در تأمین نمایی از فعالیت‌های غیرعادی، و اعلام هشدار به مدیران و مسدود نمودن ارتباط مشکوک است.
6. واقعه‌نگاری[6]: به ثبت نظام‌مند رویدادهای مشخص به ترتیب وقوع آن‌ها برای فراهم‌کردن امکان تعقیب و پیگیری داده‌ها در تحلیل‌های آتی اطلاق می‌شود.
7. دسترسی از راه دور[7]: دسترسی به یک سیستم یا برنامه، بدون نیاز به حضور فیزیکی در محل می باشد، که خطر جعل هویت در آنها بیشتر است به همین دلیل معمولا کنترل شده نیستند.

نتیجه گیری

اگر چه اغلب سازمان ها تمایل به داشتن شبکه های ایمن ذارند، ارائه تعریف واحدی از امنیت که همه نیازهای شبکه را تأمین نماید ممکن نیست. در عوض هر سازمان باید ارزش اطلاعات خود را ارزیابی کندو سپس یک خطی مشی امنیتی برای مواردی که باید مورد محافظت قرار گیرد مشخص نماید. سیستم امنیت اطلاعات شاید پرهزینه و وقت گیر به نظر آید اما با توجه به اهمیت اطلاعات در بقای سازمان وجود چنین سیستمی بسیار ضروری می نماید. اعمال چنین سیستمی برای هر سازمان لازم بوده و بسته به سطح اطلاعات و ارزش اطلاعات سامان گستردگی متنوعی خواهد داشت، اما هرگز محو نخواهد شد. در کل لارم است سازمان ها سه شرط زیر را در طراحی سیستم امنیت اطلاعاتی خود مدتظر داشته باشند:

1. اطمینان از سلامت اطلاعات چه در زمان ذخیره و چه بهنگام باز یابی و ایجاد امکان برای افرادی که مجاز به استفاده از اطلاعات هستند.
2. دقت:اطلاعات چه از نظر منبع ارسالی و چه در هنگام ارسال و بازخوانی آن باید از دقت و صحت برخورار باشد و ایجاد امکاناتی در جهت افزایش این دقت ضرورت خواهد داشت.

Firewall [1]
Access control[2]
passwords[3]
biometrics[4]
intrusion detection systems[5]
logging [6]
remote accessing 7

3. قابلیت دسترسی: اطلاعات برای افرادی که مجاز به استفاده از آن می باشند باید در دسترس بوده و امکان استفاده در موقع لزوم برای این افراد مقدور باشد.

فهرست منابع:

1. اسدی مریم، فناوری امنیت اطلاعات با یک دیدگاه طبقه بندی http://www.ICTna.ir، تاریخ انتشار 1385/1/11
2. آشنایی با سیستم مدیریت امنیت اطلاعات http://www.amnafzar.net
3. حاجیان بهروز ، امنیت اطلاعات در طول جنگ جهانی دوم http://www.IRITN.com ، تاریخ انتشار 1384/4/18
4. کریم بیگی آرش ، مدیریت امنیت اطلاعات، http://www.ICTna.ir
5. مورل جی،شیلدز، تجارت الکترونیک و برنامه ریزی منابع سازمان، مترجم پارسائیان علی، حنفی زاده پیام، انتشارات ترمه
6. اسعدی شالی عادله، مدیریت سیستم های امنیت اطلاعات،مجله الکترونیکی پژوهشگاه اطلاعات و مدارک علمی ایران،شماره چهارم دوره چهارم،تاریخ انتشار1384/5/1 http://www.irandoc.ac.ir
7. ده نکته برای حفظ امنیت http://ircert.com
8. دکتر سعیدی سرمد، دکتر میرانی حمید رضا، تجارت الکترونیک، انتشارات پرسمان
9. دلیلی حمید، امنیت اطلاعات در کار الکترونیکی، http://bashgah.net
10. راستی مهدی ،امضا دیجیتالی و کاربرد آن در حفظ امنیت شبکه، http://www.ICTna.ir، تاریخ انتشار 1384/1/7
11. چرا و چگونه؟ http://www.dnv.ir
12. مرور کلی DNV http://www.dnv.ir
13. Brandel Mary، 8 تکنولوژی خطرناک برای امنیت اطلاعات سازمان ها و شرکت ها، مترجم سید حسین محتسبی، www.ITIran.ir ، 86/7/8