عنوان مقاله : استانداردهاي امنيت اطلاعات (ISO/IEC 17799 و BS 7799)

گروه مطالعاتی : امنیت

گروه کاری : امنیت

ارائه دهنده: افسانه كربلائي زاده

تاریخ ارائه: ۸۳/۱۱/۱۳

سرپرست گروه کاری: طیبه میرزائی

تاریخ اصلاح: ۸۳/۱۱/۱۵

اصلاح کننده : افسانه كربلائي زاده

مرجع: اینترنت

مقدمه :

استانداردهاي ISO/IEC 17799 و BS 7799 كه بصورت واحد بر روي امنيت يک سازمان اعمال ميگردند، استانداردهايي مي باشند كه مجموعه اي فراگير از كنترلها شامل بر بهترين متد سنجش در امنيت اطلاعات بوده و شامل بر كليه جزئيات امنيتي هستند. اين استانداردها به دو بخش عمده تقسيم ميگردد: الف) يک مجموعه قانونمند از متد سنجش امنيتي (ISO/IEC 17799) و ب) يک نظام نامه براي مديريت امنيت اطلاعات (BS 7799-2). بطور اساسي يک استاندارد امنيت اطلاعات عمومي مورد تاييد بين المللي است.

هدف از ايجاد اين استانداردها اين بوده است كه بمانند يک منبع منفرد براي تعريف محدوده اي از كنترلهاي مورد نياز براي اغلب موقعيتهايي كه سيستمهاي اطلاعاتي وجود داشته و در تجارت و صنعت كاربرد دارد ، بكار برده شوند. ضرورتاً تسهيلاتي براي رسيدن به انجام تجارت در محيطي قابل اطمينان فراهم مي آورد.

تاريخچه :

- اولين نسخه آن توسط وزارت تجارت و صنعت انگلستان (DTI) براي بررسي ارائه گرديد.
- تحت يک عنوان مشخص و بصورت بازنگري شده با عنوان نسخه اول BS 7799 در فوريه سال ۱۹۹۵ منتشر گرديد.
- نسخه ارائه شده بصورت فراگير اهداف اوليه را تحت پوشش قرار نميداد و داراي مشكلات ذيل بود :
  - به اندازه كافي انعطاف پذير نبود.
  - كليدهاي كنترلي را خيلي ساده بيان كرده بود.
  - تحت فشار مشكلات ديگري انتشار داده شده بود (مانند مشكل سال ۲۰۰۰).
- تجديد نظر زيادي مي بايست صورت مي پذيرفت كه در نتيجه نسخه دوم BS 7799 در ماه مي سال ۱۹۹۹ منتشر گرديد.
- شماهاي رسمي و نظام نامه ارائه گواهينامه و اعتبارنامه هاي آن در همان سال منتشر گرديد.
- در همان سال ابزاري كه از اين استاندارد حمايت مينمودند پديدار گرديدند.
- همزمان مؤسسه ISO با سرعت زيادي در اين راه پيشقدم گرديد.
- قسمت دوم استاندارد BS 7799 در سال ۲۰۰۲ ميلادي ارائه و متعاقب آن مجموعه ابزارمند استاندارد ISO 17799 در همان سال منتشر گرديد.

الف) استاندارد ISO/IEC 17799 :

ايـن اسـتاندارد در ده بخـش و بـيش از ۱۲۷ نـوع متـد جهـت سـنجش امنيـت سيستم سازماندهي گرديده است. هر بخش بر روي يک سرفصل يا محدوده عملکرد مجزا تعريف شده است. ده عنوان و اهداف آن عبارتند از:

۱) طرح تداوم خدمات تجاري :
اهداف ايـن بخـش شـامل جلـوگيري از منقطـع شـدن فعاليتهـاي تجـاري و فراينـدهاي بحراني اقتصادي بر اثر حوادث ناگوار و يا ناتواني در ارائه خدمات در سطح وسـيع مـي باشد.

۲) کنترل بر نحوه دستيابي به سيستم :
اهداف اين بخش شامل :
۲-۱) کنترل دسترسي به اطلاعات.
۲-۲) جلوگيري از دستيابي غير مجاز به سيستم اطلاعاتي.
۲-۳) ايجاد تضمين در نحوه خدمت رساني حمايت شده شبکه.
۲-۴) جلوگيري از دستيابي غير مجاز به رايانه ها.
۲-۵) بازرسي و نظارت بر فعاليتهاي غير مجاز.
۲-۶) اطمينـان حاصـل کـردن از امنيـت اطلاعـات در زمـاني کـه در شـبکه از تجهيـزات شبکه بيسيم و يا تلفن سيار استفاده مي گردد.

۳) پشتيباني کردن و توسعه دادن سيستم :
اهداف اين بخش شامل :
۳-۱) اطمينان از امکانات امنيتي ايجاد شده در درون سيستمهاي قابل کنترل.
۳-۲) ممانعت از گم شدن ، تغيير و سؤاستفاده از داده هاي کاربران در سيستم هاي کاربردي.
۳-۳) حمايت از جنبه هاي محرمانگي ، صحت و تماميت اطلاعات.
۳-۴) اطمينان از پروژه هاي IT و فعاليتهاي حمايتي آن که در يک چارچوب امن هدايت خواهند شد.
۳-۵) پشتيباني امنيتي از داده ها و نرم افزارهاي کاربردي.

۴) ايجاد امنيت فيزيکي و محيطي:
اهداف اين بخش شامل ممانعت از دسترسـي غيـر مجـاز ، آسيبرسـاني و دخالـت در بنيادهاي اقتصادي و اطلاعات ؛ ممانعت از گم شدن ، آسيب ديـدن و مـصالحه بـر سـر دارايي ها براي تعليق فعاليتهاي اقتـصادي مؤسـسه ؛ ممانعـت از مـورد مـصالحه قـرار گرفتن يا سرقت اطلاعات و همچنين امکانات پردازش اطلاعات ميگردد.

۵) مورد قبول واقع شدن:
اهداف اين بخش شامل :
۵-۱) اجتناب از بروز هرگونـه رخنـه اي کـه مجرمانـه بـوده ويـا قـوانين مـدني ، قـوانين موضوعي ، قوانين تنظيمي يا قراردادهاي الزام آور و هر نوع نياز امنيتي را مـورد هـدف قرار دهد.
۵-۲) ايجاد اطمينان از همخواني سيستمها با سياسـتهاي امنيتـي و اسـتانداردهاي سازماني.
۵-۳) به حد اکثر رساندن تاثيرات کارا و به حد اقـل رسـاندن فراينـدهاي اخـلال کننـده سيستم مراقبت امنيتي وارد شده بر سيستم يا صادر شده از سيستم.

۶) امنيت شخصي:
اهداف اين بخش شامل كاهش خطرات ناشي از خطاهاي انساني ، دزدي ، تقلب يا سؤاستفاده از امكانات ؛ ايجاد اطمينان از اينكه كاربران از تهديدات امنيتي موجود بر روي اطلاعات واقف و نگران بوده و در روشهاي كاري معمول خود ، در جهت حمايت از سياستهاي امنيتي ، شراكت خواهند داد ؛ به حداقل رساندن خسارتهاي ناشي از بروز حوادث امنيتي و سؤ عمل و همچنين درس گرفتن از اين رخدادهاي امنيتي مي باشد.

۷) ايجاد امنيت سازماني:
اهداف اين بخش شامل :
۷-۱) مديريت امنيت اطلاعات در محدوده شركت.
۷-۲) پشتيباني از امكانات امنيت فرايندهاي اطلاعاتي سازماني و دستيابي به داراييهاي اطلاعاتي به واسطه عوامل ثالث (Third Party).
۷-۳) پشتيباني از امنيت اطلاعات در زماني كه وظيفه پردازش اطلاعات شركت ، بصورت Outsource به سازمان ديگري سپرده شده باشد.

۸) مديريت رايانه و عمليات:
اهداف اين بخش شامل :

۸-۱) ايجاد اطمينان از عمليات موجود و امنيتي بر روي امكانات پردازش اطلاعات.
۸-۲) به حداقل رساندن خطرات ناشي از ناتواني هاي سيستم.
۸-۳) حمايت از تماميت اطلاعات و نرم افزار.
۸-۴) پشتيباني از در دسترس بودن و تماميت پردازش اطلاعات و ارتباطات.
۸-۵) ايجاد اطمينان از امن نگهداشتن اطلاعات در شبكه ها و حمايت از زيربناي پشتيباني كننده.
۸-۶) ممانعت از آسيب رسيدن به دارايي ها و تعليق فعاليتهاي اقتصادي.
۸-۷) ممانعت از گم شدن ، تغيير دادن و سؤاستفاده از اطلاعات در حال مبادله مابين سازمانها.

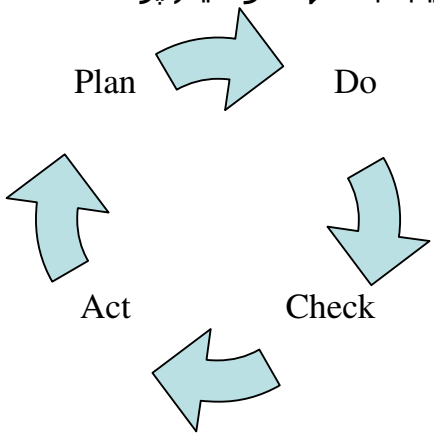
۹) كنترل و طبقه بندي داراييها:
اهداف اين بخش شامل پشتيباني مناسب حمايتي از داراييهاي مشترک و اطمينان از اينكه داراييهاي اطلاعاتي در يک سطح مناسب امنيتي دريافت مي گردد مي باشد.

۱۰) امنيت اطلاعاتي:
اهداف اين بخش شامل ايجاد مديريت هدفمند و حمايتي براي امنيت اطلاعات ميگردد.

ب) استاندارد BS 7799-2 :

يک استاندارد خاص طراحي شده براي يک سيستم مديريت امنيت اطلاعات يا ISMS (Information Security Management Systems) مي باشد. ISMS جهت مونيتورينگ ، كنترل امنيت و كاهش درجه خطرپذيري خطا در امنيت اطلاعات مورد استفاده قرار مي گيرد. سري استاندارد مديريتي BS 7799-2 توضيحات لازم در مورد چگونگي بكارگيري امنيت اطلاعات و بر اساس عملكرد استاندارد ISO/IEC 17799

ارائه مي دهد و همچنين چگونگي ايجاد ، سپس هدايت و نهايتاً مديريت يک ISMS را بيان مينمايد. جزئيات يک ISMS در چرخه چهار مرحله حياتي Plan - Do - Check - Act خلاصه ميشود که بترتيب به آنها خواهيم پرداخت.



Plan:

اين فاز به زير شاخه هاي Scope , Policy , Risk Assessment و Risk Treatment تقسيم ميشود .

Scope : در اين بخش هدف ISMS تعريف و تدوين ميگردد. تعيين اهداف بستگي تام به نياز شبکه ما دارد که مي تواند مربوط به يک بخش خاص از سايتهاي سازمان بوده و يا مربوط به ارائه يک سرويس خاص مثل E-Banking باشد.

Policy : در اين بخش به سؤالات مهمي مانند :

- چرا امنيت اطلاعات براي ما مهم است ؟
- آيا مقابله با ويروس خاصي مد نظر است ؟
- آيا تنها در صدد تهيه و جمع آوري يک سري اطلاعات مانند Confidentiality ، Integrity و Availability مي باشيم؟
- چه سطحي از خطا براي ما قابل قبول است؟
- آيا تنظيمات خاصي مد نظر مي باشد؟
- محدوديت خاصي وجود دارد؟
- و .....

تمام پاسخهاي جمع آوري شده را بايد در بخش Policy جمع آوري کرده و مورد پردازش قرار دهيم.

Risk Assessment : در اين بخش با توجه به بدست آوردن Policy ، اکنون ما مي دانيم که چه چيزي را ميبايست مورد محافظت قرار داده و سطح قابل قبول خطا براي ما چقدر خواهد بود. در اين بخش خطرهاي مهم و جدي را شناسايي کرده و بر آنها اشراف داريم. بنابراين بايد يک روش مناسب که براي سازمان ما قابل قبول باشد را انتخاب ، و هدف از ISMS را تعيين نماييم.

Risk Treatment : بعد از کامل نمودن ارزيابي خطا , استاندارد BS 7799-2 از ما ميخواهد تا در خصوص مديريت خطا تصميم گيري کنيم .

نسخه جديد اين استاندارد، يهني BS 7799-2:2002 در مورد از بين بردن خطا استانداردهاي زيادي دارد که بر پايه سه سوال اساسي ذيل دسته بندي مي شوند :

۱) آيا خطا را مي پذيريد و به توانائي خود براي شناسائي و از بين بردن خطا اعتماد کامل داريد ؟

۲) از پذيرش خطا اجتناب مي کنيد و محصولات خود را بيمه مي کنيد ؟

۳) آيا مي خواهيد کنترل مناسبي روي شبکه داشته باشيد ؟

: Do

در این فاز ما ملزم به کنترل خطا مي باشيم. در ايـن مرحلـه مـا بـه يـک فراينـد نيازمنديم تا خطا را شناسائي و به ما اعلام کند. همچنين نيازمند به آمـوزش پرسـنل در خـصوص مـسائل امنيتـي خـواهيم بـود تـا پـس از آموزشــهاي مربوطـه، بـه عنـوان متخصصين امنيتي منحصراً بتوانند امنيت شبکه را بعهده بگيرند .

: Check

در فـاز Check بايـد از کنتـرل شــبکه در مواقـع لازم مطمـئن شـويم و هـر گونـه مشاهده اي را آرشيو کنيم. استانداردها دامنه متنوعي از فعاليتهاي قابـل بررســي را مشخص کرده اند که در ذيل به آنها اشاره ميشود:

Intrusion Detection
Incident Handling
Routine Checks
Self – Policing Procedures
Learning From Others (e.g. CERT)
Internal ISMS Audit
Management Review

دو فعاليـت بررســي شــونده Internal ISMS Audit و Management Review لازم الاجراء بوده و بقيه موارد اختياري مي باشند.

: Act

خروجي فاز Check فعاليتهاي اين بخش را تشکيل مي دهد که در سه بخـش خلاصه ميشود :

Corrective Action
Preventive Action
Improvements

چهار فاز فوق الـذکر در بـازه هـاي زمـاني مشخـصي کـه حـساسيت اطلاعـات سازمان مشخص مي نمايد مي بايست تکرار گردد. ذکر ايـن نکتـه ضـروري اسـت کـه لزوماً ممکن است در اجراي استانداردهاي امنيتي خريد تجهيزات جديد پيشنهاد نگردد و با بازنگري تجهيزات موجود ، گرفتن گواهي هاي استاندارد امکانپذير باشد.