Web Site: http://www.MixofTix.net
Document # 7856-X-EHR-02

Material: Enterprise Security

موضوع		صفحه
فهرست	.....	1
گپ امنیتی!	.....	2
آزمون امنیت اطلاعات	.....	7
انواع حملات	.....	14
رمزنگاری	.....	31
آسیب پذیری SSL	.....	35
استاندارد BS7799 ، راهکاری اجتناب ناپذیر	.....	38

- گپ امنیتی!

وقتی از امنیت شبکه صحبت می کنیم، مباحث زیادی قابل طرح و بررسی هستند، موضوعاتی که هر کدام به تنهایی می توانند در عین حال جالب، پرمحتوا و قابل درک باشند. اما وقتی صحبت کار عملی به میان می آید، قضیه تا حدودی پیچیده می شود. ترکیب علم و عمل، احتیاج به تجربه دارد و نهایت هدف یک علم بعد کاربردی آن است.

وقتی دوره تئوری امنیت شبکه را با موفقیت پشت سر گذاشتید و وارد محیط کار شدید، ممکن است این سوال برایتان مطرح شود که " حالا باید از کجا شروع کرد؟ اول کجا باید ایمن شود؟ چه استراتژی را در پیش گرفت و کجا کار را تمام کرد؟ به این ترتیب " انبوهی از این قبیل سوالات فکر شما را مشغول می کند و کم کم حس می کنید که تجربه کافی ندارید (که البته این حسی طبیعی است).

پس اگر شما نیز چنین احساسی دارید و می خواهید یک استراتژی علمی - کاربردی داشته باشید، تا انتهای این مقاله را بخوانید.

همیشه در امنیت شبکه موضوع لایه های دفاعی، موضوع داغ و مهمی است. در این خصوص نیز نظرات مختلفی وجود دارد. عده ای فایروال را اولین لایه دفاعی می دانند، بعضی ها هم Access List رو اولین لایه دفاعی می دانند، اما واقعیت این است که هیچکدام از این‌ها، اولین لایه دفاعی محسوب نمی شوند. به خاطر داشته باشید که اولین لایه دفاعی در امنیت شبکه و حتی امنیت فیزیکی وجود یک خط مشی (Policy) هست. بدون policy، لیست کنترل، فایروال و هر لایه دیگر، بدون معنی می شود و اگر بدون policy شروع به ایمن سازی شبکه کنید، محصول وحشتناکی از کار در می آید.

با این مقدمه، و با توجه به این که شما policy مورد نظرتان را کاملا تجزیه و تحلیل کردید و دقیقا می دانید که چه می خواهید و چه نمی خواهید، کار را شروع می‌شود. حال باید پنج مرحله رو پشت سر بگذاریم تا کار تمام شود. این پنج مرحله عبارت اند از :

1- Inspection (بازرسی)

2- Protection (حفاظت)

3- Detection (ردیابی)

4- Reaction (واکنش)

5- Reflection (بازتاب)

در طول مسیر ایمن سازی شبکه از این پنج مرحله عبور می کنیم، ضمن آن که این مسیر، احتیاج به یک تیم امنیتی دارد و یک نفر به تنهایی نمی تواند این پروسه را طی کند.

1- اولین جایی که ایمن سازی را شروع می کنیم، ایمن کردن کلیه سندیت های (authentication) موجود است. معمولا رایج ترین روش authentication، استفاده از شناسه کاربری و کلمه رمز است.

مهمترین قسمت هایی که باید authentication را ایمن و محکم کرد عبارتند از :

- کنترل کلمات عبور کاربران، به ویژه در مورد مدیران سیستم.

- کلمات عبور سوییچ و روتر ها (در این خصوص روی سوییچ تاکید بیشتری می شود، زیرا از آنجا که این ابزار (device) به صورت plug and play کار می کند، اکثر مدیرهای شبکه از config کردن آن غافل می شوند. در حالی توجه به این مهم می تواند امنیت شبکه را ارتقا دهد. لذا به مدیران امنیتی توصیه میشود که حتما سوییچ و روتر ها رو کنترل کنند).

- کلمات عبور مربوط به SNMP.

- کلمات عبور مربوط به پرینت سرور.

- کلمات عبور مربوط به محافظ صفحه نمایش.

در حقیقت آنچه که شما در کلاس‌های امنیت شبکه در مورد Security Account and Password یاد گرفتید این جا به کار می رود.

2- گام دوم نصب و به روز رسانی آنتی ویروس ها روی همه کامپیوتر ها، سرورها و میل سرورها است. ضمن اینکه آنتی ویروس های مربوط به کاربران باید به صورت خودکار به روز رسانی شود و آموزش های لازم در مورد فایل های ضمیمه ایمیل ها و راهنمایی لازم جهت اقدام صحیح در صورت مشاهده موارد مشکوک نیز باید به کاربران داده شود.

3 – گام سوم شامل نصب آخرین وصله های امنیتی و به روز رسانی های امنیتی سیستم عامل و سرویس های موجود است. در این مرحله علاوه بر اقدامات ذکر شده، کلیه سرورها، سوییچ ها، روتر ها و دسک تاپ ها با ابزار های شناسایی حفره های امنیتی بررسی می شوند تا علاوه بر شناسایی و رفع حفره های امنیتی، سرویس های غیر ضروری هم شناسایی و غیرفعال بشوند.

4-در این مرحله نوبت گروه بندی کاربران و اعطای مجوزهای لازم به فایل ها و دایرکتوری ها است. ضمن اینکه اعتبارهای(account) قدیمی هم باید غیر فعال شوند.

گروه بندی و اعطای مجوز بر اساس یکی از سه مدل استاندارد Techniques Access Control یعنی DAC , MAC یا RBAC انجام می شود. بعد از پایان این مرحله، یک بار دیگر امنیت سیستم عامل باید چک شود تا چیزی فراموش نشده باشد.

5- حالا نوبت device ها است که معمولا شامل روتر، سوییچ و فایروال می شود. بر اساس policy موجود و توپولوژی شبکه، این ابزار باید config شوند. تکنولوژی هایی مثل NAT , PAT و filtering و غیره در این مرحله مطرح می شود و بر همین علت این مرحله خیلی مهم است. حتی موضوع مهم IP Addressing که از وظایف مدیران شبکه هست نیز می تواند مورد توجه قرار گیرد تا اطمینان حاصل شود که از حداقل ممکن برای IP Assign به شبکه ها استفاده شده است.

6- قدم بعد تعیین استراژی تهیه پشتیبان(backup) است. نکته مهمی که وجود دارد این است که باید مطمئن بشویم که سیستم backup و بازیابی به درستی کار کرده و در بهترین حالت ممکن قرار دارد.

7- امنیت فیزیکی. در این خصوص اول از همه باید به سراغ UPS ها رفت. باید چک کنیم که UPS ها قدرت لازم رو برای تامین نیروی الکتریکی لازم جهت کار کرد صحیح سخت افزار های اتاق سرور در زمان اضطراری را داشته باشند. نکات بعدی شامل کنترل درجه حرارت و میزان رطوبت،ایمنی در برابر سرقت و آتش سوزی است. سیستم کنترل حریق باید به شکلی باشد که به نیروی انسانی و سیستم های الکترونیکی آسیب وارد نکند. به طور کل آنچه که مربوط به امنیت فیزیکی می شود در این مرحله به کار می رود.

8- امنیت وب سرور یکی از موضوعاتی است که باید وسواس خاصی در مورد آن داشت.به همین دلیل در این قسمت، مجددا و با دقت بیشتر وب سرور رو چک و ایمن می کنیم. در حقیقت، امنیت وب نیز در این مرحله لحاظ می شود.

(توجه:هیچ گاه اسکریپت های سمت سرویس دهنده را فراموش نکنید)

9 – حالا نوبت بررسی، تنظیم و آزمایش سیستم های Auditing و Logging هست. این سیستم ها هم می تواند بر پایه host و هم بر پایه network باشد. سیستم های رد گیری و ثبت حملات هم در این مرحله نصب و تنظیم می شوند. باید مطمئن شوید که تمام اطلاعات لازم ثبت و به خوبی محافظت می شود. در ضمن ساعت و تاریخ سیستم ها درست باشد چرا که در غیر این صورت کلیه اقداما قبلی از بین رفته و امکان پیگیری های قانونی در صورت لزوم نیز دیگر وجود نخواهد داشت.

10- ایمن کردن Remote Access با پروتکل و تکنولوژی های ایمن و Secure گام بعدی محسوب می شود. در این زمینه با توجه به شرایط و امکانات، ایمن ترین پروتکل و تکنولوژی ها را باید به خدمت گرفت.

11 – نصب فایروال های شخصی در سطح host ها، لایه امنیتی مضاعفی به شبکه شما میدهد. پس این مرحله را نباید فراموش کرد.

12 – شرایط بازیابی در حالت های اضطراری را حتما چک و بهینه کنید. این حالت ها شامل خرابی قطعات کامپیوتری، خرابکاری کاربران، خرابی ناشی از مسایل طبیعی (زلزله - آتش سوزی – ضربه خوردن - سرقت - سیل) و خرابکاری ناشی از نفوذ هکرها، است. استاندارد های warm site و hot site را در صورت امکان رعایت کنید.

به خاطر داشته باشید که " همیشه در دسترس بودن اطلاعات "، جز، قوانین اصلی امنیتی هست.

13– و قدم آخر این پروسه که در حقیقت شروع یک جریان همیشگی هست، عضو شدن در سایت ها و بولتن های امنیتی و در آگاهی ازآخرین اخبار امنیتی است.

آزمون امنیت اطلاعات

متن زیر یک تست سریع و آموزنده می باشد که به برخی از سوالات شما در زمینه امنیت اطلاعات پاسخ می دهد. همانطور که خواهید دید به صورت پرسش و پاسخ بیان شده است.
باب امنیت اطلاعات اغلب پیچیده می باشد. بر همین اساس این مبحث به برخی از سوالاتی که ممکن است برای شما ایجاد شود ، پاسخ داده است و پیشنهاداتی را برای آن ارائه داده است تا به سادگی قبول کنید که سیستم های شما نیز ممکن است در معرض خطر قرار گیرد.

1-اگر امنیت اطلاعات را افزایش دهیم ، کارایی کاهش پیدا می کند. درست یا غلط ؟

درست – امنیت اطلاعات هزینه مربوط به خودش را دارد. افزایش امنیت اطلاعات ممکن است به روالهای موثر اضافی از جمله «تکنولوژی» و «سرمایه گذاری » نیاز داشته باشد.
افزایش امنیت اطلاعات ممکن است پیشرفت جریان کار را با کندی مواجهه کند و این امر ممکن است در کارایی افراد و شبکه شما نمود پیدا کند. امنیت اطلاعات ممکن است به معنی قفل کردن ایستگاههی کاری و محدود کردن دسترسی به اتاقهای کامپیوتر و سرور شما باشد. هر سازمانی باید هنگامی که به مقوله امنیت اطلاعات می پردازد به صورت اندیشمندانه ای بین خطرات (Risks) و کارآیی توازن برقرار کند.

2-حملاتی که توسط نفوذگران خارجی انجام می گیرد نسبت به حملات کارمندان داخلی هزینه بر تر و خسارت بار تر می باشد. درست یا غلط ؟

غلط– حملات کارمندان داخلی نوعا بسیار خسارت بار تر از حملات خارجی گزارش شده است. بر طبق آمارهای انستیتو امنیت کامپیوتر (Computer Security Institute) میانگین حملات خارجی 57000 دلار و میانگین هزینه حملات داخلی 2700000 دلار برآورد شده است.
کارمندان داخلی اطلاعات محرمانه بیشتری درباره سیستم های هدف در دسترس دارند از آن جمله می توان اطلاعاتی درباره فعالیت های دیده بانی (Monitoring) را نام برد (به خصوص نقاط ضعف این فعالیتها)

3-پیکربندی یک دیواره آتش (Firewall) به صورت کامل ما ر در مقابل حملات خارجی ایمن می کند. درست یا غلط ؟

غلط – آمارهای انستیو امنیت کامپیوتر نشان می دهد که 1/3 شرکتهایی که از دیواره آتش استفاده کرده اند هنوز از دست نفوذگران بد اندیش در امان نمانده اند. اولین کارکرد دیواره آتش بستن پورتهای مشخص می باشد به همین دلیل در بعضی از مشاغل نیاز است که بعضی از پورتها باز باشد. هر پورت باز می تواند یک خطری را برای سازمان ایجاد کند و یک معبر برای شبکه شما باشد.

ترافیکی که از میان یک پورت می گذرد را باید همیشه به صورت سختگیرانه ای دیده بانی (Monitor) کرد تا تمامی تلاشهایی که منجر به نفوذ در شبکه می شود شناسایی و گزارش شود.
یک دیواره آتش به تنهایی نمی تواند یک راه حل جامع باشد و باید از آن به همراه تکنولوژی های IDS (Intrusion Detection System) و روشهای ترکیبی استفاده کرد.

4-اگر دیواره آتش من به صورت مناسبی پیکر بندی شود دیگر نیازی به دیده بانی بیشتر ترافیک شبکه نمی باشد. درست یا غلط ؟

غلط – همیشه نفوذگران خبره می توانند یک دیواره آتش را در هم شکنند و به آن نفوذ کنند. به همین دلیل دیده بانی کلیدی برای هر برنامه امنیت اطلاعات می باشد. فراموش نکنید که دیواره آتش نیز ممکن است هک شود و IDS ها راهی می باشند برای اینکه بدانید چه سیستم هایی در شرف هک شدن می باشند.

5-دیواره های آتش باید به گونه ای پیکربندی شوند که علاوه بر ترافیک ورودی به شبکه ، ترافیک های خروجی را نیز کنترل کنند . درست یا غلط ؟

درست – بسیاری از سازمانها توجه زیادی به محدود کردن ترافیک ورودی خود دارند ، اما در مقایسه توجه کمتری در مسدود کردن ترافیک خروجی از شبکه را دارند. خطرات زیادی ممکن است در درون سازمان وجود داشته باشد. یک کارمند ناراضی یا یک نفوذگر که شبکه شما را در دست گرفته است ، ممکن است که بخواهد اطلات حساس و محرمانه شما را برای شرکت رقیب بفرستد.

6-امنیت اطلاعات به عنوان یک مبحث تکنولوژیکی مطرح است درست یا غلط ؟

غلط – امنیت اطلاعات یک پی آمد تجاری - فرهنگی می باشد. یک استراتژی جامع امنیت طلاعات باید شامل سه عنصر باشد: روالها و سیاستهای اداری ، کنترل دسترسی های فیزیکی ، کنترل دسترسی های تکنیکی . این عناصر – اگر به صورت مناسبی اجرا شود – مجموعا یک فرهنگ امنیتی ایجاد می کند. بیشتر متخصصین امنیتی معتقدند که تکنولوژیهای امنیتی فقط کمتر از 25 درصد مجموعه امنیت را شامل می شوند. حال آنکه در میان درصد باقیمانده آنچه که بیشتر از همه نمود دارد ،« افراد » می باشند. (کاربر انتهایی) افراد یکی از ضعیف ترین حلقه ها ، در هر برنامه امنیت اطلاعات می باشند.

7-هرگاه که کارمندان داخلی ناراضی از اداره اخراج شوند ، خطرات امنیتی از بین می روند. درست یا غلط ؟

غلط – به طور واضح غلط است. برای شهادت غلط بودن این موضوع می توان به شرکت Meltdown اشاره کرد که لشکری از کارمندان ناراضی اما آشنا به سرقتهای کامپیوتری برای خود ایجاد کرده بود. بر طبق گفته های FBI حجم فعالیتهای خرابکارانه از کارمندان داخلی افزایش یافته است. همین امر سازمانها را با خطرات جدی در آینده مواجهه خواهد کرد.

8-نرم افزارهای بدون کسب مجوز (Unauthorized Software) یکی از عمومی ترین رخنه های امنیتی کاربران داخلی می باشد. درست یا غلط ؟

درست – رخنه ها (Breaches) می تواند بدون ضرر به نظر بیاید ، مانند Screen Saver های دریافت شده از اینترنت یا بازی ها و ... نتیجه این برنامه ها ، انتقال ویروس ها ، تروجانها و ... می باشد. اگر چه رخنه ها می تواند خطرناکتر از این باشد. ایجاد یا نصب یک برنامه کنترل از راه دور که می تواند یک در پشتی (Backdoor) قابل سوءاستفاده ای را در شبکه ایجاد کند که به وسیله دیواره آتش نیز محافظت نمی شود.

بر طبق تحقیقاتی که توسط ICSA.net و Global Integrity انجام شده است بیش از 78 درصد گزارش ها مربوط به ایجاد یک رخنه در نرم افزار دریافتی از افراد یا سایتهای ناشناخته است.

9-خسارتهای ناشی از سایتهای فقط اطلاعاتی کمتر از سایتهای تجاری می باشد. درست یا غلط ؟

درست – درست است که خطرهای مالی در سایتهای فقط اطلاعاتی کمتر از سایتهای تجاری می باشد ولی خطر مربوط به شهرت و اعتبار، آنها را بیشتر تهدید می کند. سازمانها نیازمند این می باشند که مداوم سایت های اطلاع رسانی را بازبینی کنند تا به تهدید های احتمالی شبکه های خود خیلی سریع پی ببرند و در مقابل آنها واکنش نشان دهند تا از خسارتهایی که ممکن است شهرت آنها را بر باد دهد جلوگیری کنند.

10-رمزهای عبور می تواند جلو کسانی که دسترسی فیزیکی به شبکه را دارند ، بگیرد. درست یا غلط ؟

غلط – کلمات رمز نوعا خیلی کم می توانند جلو کارمندان داخلی و خبره را بگیرند. بسیاری از سازمانها تمامی تلاش خود را روی امور تکنیکی امنیت اطلاعات صرف می کنند و در برخورد با مسائل اداری و کنترل دسترسی فیزیکی لازم برای ایجاد یک محافظت مناسب ، با شکست مواجه می شوند.

11-یک نام کاربری و یک رمز عبور می تواند شبکه ما را از ارتباط با یک شبکه غیردوستانه (Unfriendly) محافظت کند. درست یا غلط ؟

غلط – یک ارتباط فیزیکی و یک آدرس شبکه همه آنچیزی می باشد که یک نفوذگر برای نفوذ در شبکه نیاز دارد.با یک ارتباط می توان تمامی ترافیک شبکه را جذب کرد (به این کار Sniffing می گویند) . مهاجم قادر است با استفاده از تکنیکهای Sniffing کل ترافیک حساس شبکه ، شامل ترکیباتی از **نام کاربری/رمز عبور** را جذب کند و در حملات بعدی از آنها استفاده کند.

12-هیچکسی در سازمان نباید به رمزهای عبور دسترسی داشته باشد به جز مدیر امنیت شبکه . درست یا غلط ؟

غلط – هیچ کس در سازمان نباید به کلمات رمز کاربران دسترسی داشته باشد ، حتی مدیر امنیتی شبکه! رمزهای عبور باید به صورت رمز شده (Encrypted) ذخیره شوند. برای کاربران جدید ابتدا با یک رمز عبور ساخته شده اجازه ورود به شبکه داده می شود و پس از آن باید روالی قرار داد تا کاربران بتوانند در هر زمانی کلمات رمز خود را تغییر دهند. همچنین باید سیاستهایی را برای مواردی که کاربران رمزهای عبور خود را فراموش کرده اند در نظر گرفت.

13- رمزگذاری باید برای ترافیک های داخلی شبکه به خوبی ترافیک خروجی شبکه انجام گیرد. درست یا غلط ؟

درست – به عنوان یک نکته باید گفت که فرآیند Sniffing (جذب داده هایی که روی شبکه رد و بدل می شود) به عنوان یک خطر امنیتی داخلی و خارجی مطرح می شود.

14-امنیت داده ها در طول انتقال آنها هدف رمزگذاری است . درست یا غلط ؟

غلط – رمزگذاری همچنین می تواند جامعیت (Integrity) ، تصدیق (Authentication) و عدم انکار (nonrepudiation) داده ها را نیز پشتیبانی کند.

نفوذ به ذهن یک نفوذگر

برای شناخت یک نفوذگر یا «هکر» در وهله اول باید در مورد آن کمی بحث کرد.

بسیاری از مردم که بدون انگیزه های بزهکارانه یا نیت تبهکارانه به سیستم ها نفوذ می کنند و با غرور خاصی بر چسب «هکر» را بر خود می زنند، بر این باورند که چون نیت و قصد بدی ندارند باید آنها را هکر نامید. در مقابل این افراد به کسانی که با قصد و نیت سودجویانه و خرابکارانه این کار را انجام می دهند، «کرکر» می گویند. هکرها افراد خبیث یا بدکاری نیستند که قصد خراب کردن سیستم ها یا دزدیدن کلمات عبور را داشته باشند. هکرهای واقعی، خود از این گونه افراد به شدت متنفرند.

کسانی که در مورد هکرهای کامپیوتری صحبت می کنند. روی این نکته تاکید دارند که برخی از افراد با نیت کاملاً مثبت و یا به قصد سرگرمی وارد یک سیستم می شوند و گاهی نیز عیوب آن را که ممکن است باعث تخریب سیستم شود به صاحب سیستم گوشزد می کنند. در مقابل عده ای نیز با قصد ایجاد اختلال در زمینه های مختلف مانند مسایل مالی، وارد سیستم ها، به ویژه سیستم های موجود در شرکت ها می شوند.

به علاوه همه هکرها بزهکار یا مجرم نیستند. اما چه خوب چه بد، آنها در یک نقطه با هم اشتراک دارند و آن اینکه برای شما مشکل ایجاد می کنند. در مجمع سالیانه هکرها، افراد به بیان مسایل متعددی از جمله شبکه هایی که با خطرات جدی مواجه شده اند، و همچنین ورود به پایگاه های اطلاعاتی و یافتن محصولات و غیره می پردازند. بعضی از آنها مانند «مارک مایفرت» اهل کالیفرنیای شمالی که 21 سال سن دارد، خود را «مسوول نفوذهای دزدی» یا نفوذهایی که به قصد دزدی انجام می شود، می داند . او ابتدا به صورت یک نوجوان بومی به هک کردن شبکه های اینترنتی می پردازد و پس از فراگیری، آن را به عنوان مشاوره امنیتی ارایه می کند.

هدف اصلی این مقاله ابتدا شناخت هکرها، به خصوص افرادی که قصد خرابکاری یا سوءاستفاده دارند و سپس ارایه راهکارهای مناسب برای حفاظت بیشتر از سیستم هاست. این افراد که غالباً هم مرد هستند، به عنوان خطری جدی برای امنیت شبکه ها و کاربران محسوب می شوند. «باب سالیوان»، گزارشگر با سابقه سایت MSNBC.Com که پنج سال پیش برای اولین بار گروه هکرهای کامپیوتری را کشف کرد، از آنان به عنوان «تبهکاران کامپیوتری» ، «یاغی حمله کننده» و «جنایتکاران آنلاین» یاد می کند. نکات مهمی که همواره باید در مورد این افراد به خاطر داشت، عبارتند از:

هکرها به طور عامل و خرابکاران کامپیوتری به طور خاص عاشق قدرت و کنترل هستند

«ریچارد فورد» به عنوان یک محقق بر این باور است که اغلب افراد این کار را بیش از آن که بدخواهی یا خرابکاری بدانند، نوعی سرگرمی مهیج که ره آورد فناوری نوین است قلمداد می کنند. «سیمسون کارفیل»، نویسنده چندین کتاب در زمینه امنیت شبکه می گوید: « برای عده ای، این کار نوعی پازل برای حل کردن و یک نوع بازی است. شاید هم برای کسب درآمد باشد، اما به هر حال باید دانست که میان این مفاهیم و فرآیند هک، تفاوت های بسیاری وجود دارد. «افراد مورد نظر یا همان نفوذگران سعی در کنترل هر چه بیشتر ماشین ها دارند. اغلب آنان برای تفریح و سرگرمی و شاید خنده دست به این عمل می زنند. هکرها به شرکت های مختلف حمله می کنند و در هر حال، افرادی که در این زمینه فعالیت می کنند، گاه به سودهای آنی و زودگذر هم دست پیدا می کنند.

خرابکاران با دزدی اطلاعات و کلاهبرداری، بزرگ ترین صدمات را به بعضی از شرکت ها وارد می آورند

اگر چه امروزه ضریب امنیت بهره گیری از فناوری روند صعودی دارد، اما در مقابل، سوء استفاده زیادی از اختلالات موجود در اینترنت توسط خرابکاران و سود جویان انجام می شود که خود ناشی از گسترش و بسط سریع این شبکه است.

بر اساس تحقیقات انجام شده و آمار به دست آمده توسط دانشگاه «کارنگی ملون» تعداد خرابکاری های کامپیوتری از جمله حمله ویروس ها، در سال 2001 دو برابر شد و به 53 هزار مورد رسید. در سه ماهه اول سال 2002 نیز در حدود 27 هزار خرابکاری کامپیوتری به ثبت رسیده است. تصور می شود شایع ترین عامل اختلالات کامپیوتری، حملات ویروس ها باشد، اما در تحقیقی که در آوریل سال 2002 توسط موسسه ایمنی کامپیوتر وابسته به FBI انجام گرفت، مشخص شد که علت اصلی خرابکاری ها، ویروس ها نیستند. نتایج به دست آمده از تحقیقاتی در مورد پانصد نفر حاکی از آن است که بر اثر حمله ویروس ها سالیانه حدود 17/08 میلیون دلار سرقت اطلاعات، 115/7 میلیون دلار کلاهبرداری های مالی، 50 میلیون دلار سوء استفاده افرادی خود و کارمندان داخلی، زیان به شرکت ها وارد می شود.

در تحقیق دیگری که به تازگی انجام شده و از طریق سایت واشنگتن پست در اختیار علاقه مندان قرار گرفت، حمله مهاجمان اینترنتی در سراسر جهان در شش ماه اول سال 2002 حدود 28 درصد افزایش داشته که بیشتر متوجه شرکت های فناوری امریکا، سرویس های پولی و موسسات انرژی بوده است.

بسیاری از شرکت ها اجازه گریختن از دست قانون را به مهاجمان می دهند

در تحقیقات مشابه انجام شده توسط FBI ، مشخص شد 34 درصد پاسخ دهندگان معتقدند که تخلفات کامپیوتری باید توسط مراجع ذی ربط و مجاری قانونی مورد پیگرد قرار بگیرند. شرکت هایی که مورد هجوم افراد سودجو قرار می گیرند، بیش از هر چیز، از تبلیغات منفی که ممکن است سابقه و شهرت آنان را تحت الشعاع قرار دهد می ترسند. «سالیوان» در مصاحبه با یکی از نفوذ گران کامپیوتری به نام «زیلتریو» که بیش از یک سال به دزیدن اطلاعات برخی موسسات مالی و حتی معاملات آنلاین مشغول بوده، به چگونگی عملکرد این افراد که گاهی سود زیادی هم از این طریق به دست می آورند، می پردازد. سالیوان که از طریق پست الکترونیکی با این شخص مصاحبه کرده، می گوید: «زیلتریو به عنوان یک مهاجم کامپیوتری شخصیت بسیار عجیب، و بهتر بگویم، مرموزی دارد. او پس از دزدیدن اطلاعات مورد نظر، به اخاذی از شرکت یا مؤسسه مربوطه پرداخته، تا جایی که بعضی از این شرکت ها تا مبلغ 150 هزار دلار به او پرداخت کرده اند.» سالیوان معتقد است زیلتریو و افرادی مانند او باید توسط FBI تحت تعقیب قرار گیرند.

هیچ کس در امان نیست

به طور کلی می توان گفت که هر شرکت یا هر نوع بنگاه تجاری که دارای وب سایت باشد می تواند هدف افراد سودجو و فرصت طلب قرار گیرد. امروزه بسیاری از خرابکاران یا مهاجمان اینترنتی از اسکنر شبکه برای یافتن سایت هایی استفاده می کنند که به دلیل فقدان تمهیدات امنیتی، وارد شدن به آنها کار چندان دشواری نیست. «کارفینگل» در مقاله ای تحت عنوان «امنیت وب، تجارت و امور محرمانه» ضمن بیان اهمیت به کارگیری سیستم ها و و سایت های امنیتی به خصوص در زمینه اطلاعات محرمانه، به تشریح چگونگی کار اسکنرهایی می پردازد که می توانند در چند لحظه صدها یا هزاران سایت مشابه را اسکن کنند. او به برخی نرم افزارهای امنیتی از جمله «دیواره آتش» (فایروال) اشاره می کند که علاوه بر جلوگیری از ورود افراد متفرقه به سایت، تعداد اسکن ها را نیز به ثبت می رسانند. گارفینگل که برای کامپیوتر و سایت شخصی خود از این نرم افزار استفاده می کند،خاطرنشان می کند که در روزهای اخیر از طریق این نرم افزار حدود 289 هزار اسکن ثبت شده که به احتمال زیاد 1044 مورد آن توسط مهاجمان و هکرها صورت گرفته است. وی در قسمتی از کتاب خود یادآور می شود که بالا بردن ضریب امنیتی سایت، به خصوص سایت هایی که حاوی اطلاعات با ارزش و محرمانه هستند امری ضروری و اجتناب ناپذیر است. به عبارت ساده تر باید گفت که مهاجمان و هکرها به محض این که با یک سایت حساس و آسیب پذیر مواجه می شوند، اسب خود را زین می کنند. «آی میفرت» می گوید: «این که به چه کسب و کار یا تجارتی مشغولید، تفاوتی نمی کند. به هر حال باید بدانید که امکان دارد شما نیز هر لحظه به عنوان هدف اصلی مورد توجه مهاجمان قرار بگیرید. « با توجه به مواردی که گفته شد، چگونه می توان امنیت لازم را ایجاد کرد؟ برخی از راهکارها برای دستیابی به این امر مهم به این شرح است:

1- در حد بضاعت خود از بهترین سیستم امنیتی استفاده کنید

اگر چه در این باره بسیار صحبت شده، اما شرکت ها به خصوص آنهایی که اطلاعات محرمانه و حساس دارند علاوه بر سیستم های امنیتی پایه، لازم است از سیستم های مزاحم یاب نیز استفاده کنند. این کار و انتخاب نوع نرم افزار مربوطه باید با توجه به موارد متعدد، از جمله حساسیت و آسیب پذیری سیستم شما انجام شود. هرگز از مساله نفوذ افراد سودجو به سیستم های امنیتی غافل نشوید.

2- راهبردها و سیاست های امنیتی برای شرکت ایجاد کنید

ایجاد سیاست های امنیتی جزء وظایف اصلی مدیران یک شرکت محسوب می شود. هرگز اجازه ندهید برخی از کارمندان اطلاعات محرمانه و مهم را از شرکت خارج کنند.

3- از پرسنل کارآمد در جهت ایجاد امنیت استفاده کنید

آموزش، ابزار مورد نیاز، منابع و سایر موارد را در اختیار کارکنان و افرادی که در قسمت های حساس کار می کنند قرار دهید. در بسیاری از مشاغل یا تجارت های کوچک، استفاده از سرویس های امنیتی آماده، بهترین گزینه است.

4- به تهدیدات شخص مهاجم توجه نکنید و تخلفات را گزارش کنید

چنانچه شما به عنوان قربانی و طعمه در نظر گرفته شده اید، ابتدا باید به توانایی ها و امکانات موجود توجه کامل داشته باشید. چنانچه با فردی برخورد کردید که مدعی است اطلاعاتی را از سایت شما به دست آورده که ممکن است برایتان خطرناک باشد، یا به عبارتی قصد اخاذی از شما را داشت، فکر نکنید او همه اطلاعات شما را در اختیار دارد؛ حتی ممکن است قصد شوخی با شما داشته باشد. بنابراین ممکن است به خاطر ترس از فاش شدن اطلاعات، خود به خود اطلاعات دیگری در اختیار او قرار دهید. در همین راستا سالیوان می گوید: « اگر شما نترسید و خونسردی تان را حفظ کنید، شخص مقابل هیچ کاری از دستش بر نمی آید.»

خلاصه این که، بدون ترس از تهیدات شخص مقابل، قبل از هر چیز به نیرو اعتماد به نفس خود تکیه کنید.

5- با قانون مبارزه با جرایم کامپیوتری همگام شوید

این قانون به قضات اجازه می دهد تا با توجه به موارد گوناگون مانند قصد و نیت هکرها، نوع تخلف صورت گرفته، و یا حقوق افراد، حکم مربوط را صادر کنند. البته این قانون نیز همانند دیگر قوانین، در ابتدا دارای نقایص و نقاط ضعفی است اما با گذشت زمان و اضافه شدن تبصره های لازم بسیار مفید خواهد بود.

6- آموزش رعایت موازین اخلاقی به مردم، به خصوص جوانان

امروزه مردم به خصوص نسل جوان بیش از پیش نیازمند درک اصول و راهبردهای اخلاقی و چگونگی پایبندی به آنها هستند. در این بین نقش والدین و به خصوص معلمان در تبیین اصول و موازین اخلاقی کار با کامپیوتر و تعیین موارد خوب یا بد، بسیار حساس و با اهمیت است. سرمایه گذاری و برنامه ریزی در این زمینه و تأکید بر آن چه گفته شد، نوید بخش فردایی بهتر خواهد بود که در آن جنایت کامپیوتری تا حد زیادی کاهش یابد.

انواع حملات

Distributed Denial of Service (DDoS)

Spoofing Back Door

Man in the Middle Replay

TCP/IP Hijacking Weak Keys

Mathematical Password Guessing

Brute Force Dictionary

Software Exploitation Birthday

Malicious Code Viruses

Virus Hoaxes Trojan Horses

Logic Bombs Worms

Social Engineering Auditing

System Scanning

حملات از نوع DoS

هدف از حملات DoS ، ایجاد اختلال در منابع و یا سرویس هائی است که کاربران قصد دستیابی و استفاده از آنان را دارند (از کار انداختن سرویس ها) . مهمترین هدف این نوع از حملات ، سلب دستیابی کاربران به یک منبع خاص است . در این نوع حملات، مهاجمان با بکارگیری روش های متعددی تلاش می نمایند که کاربران مجاز را به منظور دستیابی و استفاده از یک سرویس خاص ، دچار مشکل نموده و بنوعی در مجموعه سرویس هائی که یک شبکه ارائه می نماید ، اختلال ایجاد نمایند . تلاش در جهت ایجاد ترافیک کاذب در شبکه ، اختلال در ارتباط بین دو ماشین ، ممانعت کاربران مجاز به منظور دستیابی به یک سرویس ، ایجاد اختلال در سرویس ها ، نمونه هائی از سایر اهدافی است که مهاجمان دنبال می نمایند . در برخی موارد و به منظور انجام حملات گسترده از حملات DoS به عنوان نقطه شروع و یک عنصر جانبی استفاده شده تا بستر لازم برای تهاجم اصلی ، فراهم گردد . استفاده صحیح و قانونی از برخی منابع نیز ممکن است ، تهاجمی از نوع DoS را به دنبال داشته باشد .

مثلا" یک مهاجم می تواند از یک سایت FTP که مجوز دستیابی به آن به صورت anonymous می باشد ، به منظور ذخیره نسخه هائی از نرم افزارهای غیرقانونی ، استفاده از فضای ذخیره سازی دیسک و یا ایجاد ترافیک کاذب در شبکه استفاده نماید . این نوع از حملات می تواند غیرفعال شدن کامپیوتر و یا شبکه مورد نظر را به دنبال داشته باشد . حملات فوق با محوریت و تاکید بر نقش و عملیات مربوط به هر یک از پروتکل های شبکه و بدون نیاز به اخذ تائیدیه و یا مجوزهای لازم ، صورت می پذیرد . برای انجام این نوع حملات از ابزارهای متعددی استفاده می شود که با کمی حوصله و جستجو در اینترنت می توان به آنان دستیابی پیدا کرد . مدیران شبکه های کامپیوتری می توانند از این نوع ابزارها ، به منظور تست ارتباط ایجاد شده و اشکال زدائی شبکه استفاده نمایند . حملات DoS تاکنون با اشکال متفاوتی ، محقق شده اند . در ادامه با برخی از آنان آشنا می شویم .

Smurf/smurfing: این نوع حملات مبتنی بر تابع Reply پروتکل Internet Control Message Protocol) ICMP) ،بوده و بیشتر با نام ping شناخته شده می باشند .(Ping ، ابزاری است که پس از فعال شدن از طریق خط دستور ، تابع Reply پروتکل ICMP را فرامی خواند) . در این نوع حملات ، مهاجم اقدام به ارسال بسته های اطلاعاتی Ping به آدرس های Broadcast شبکه نموده که در آنان آدرس مبداء هر یک از بسته های اطلاعاتی Ping شده با آدرس کامپیوتر قربانی ، جایگزین می گردد .بدین ترتیب یک ترافیک کاذب در شبکه ایجاد و امکان استفاده از منابع شبکه با اختلال مواجه می گردد.

Fraggle: این نوع از حملات شباهت زیادی با حملات از نوع Smurf داشته و تنها تفاوت موجود به استفاده از User Datagram Protocol) UDP) در مقابل ICMP ، برمی گردد . در حملات فوق ، مهاجمان اقدام به ارسال بسته های اطلاعاتی UDP به آدرس های Broadcast (مشابه تهاجم Smurf) می نمایند . این نوع از بسته های اطلاعاتی UDP به مقصد پورت 7 (echo) و یا پورت 19 (Chargen) ، هدایت می گردند.

Ping flood: در این نوع تهاجم ، با ارسال مستقیم درخواست های Ping به کامپیوتر قربانی ، سعی می گردد که سرویس ها بلاک و یا فعالیت آنان کاهش یابد. در یک نوع خاص از تهاجم فوق که به ping of death ، معروف است ، اندازه بسته های اطلاعاتی به حدی زیاد می شود که سیستم (کامپیوتر قربانی) ، قادر به برخورد مناسب با اینچنین بسته های اطلاعاتی نخواهد بود .

SYN flood: در این نوع تهاجم از مزایای three-way handshake مربوط به TCP استفاده می گردد . سیستم مبداء اقدام

به ارسال مجموعه ای گسترده از درخواست های SYN (synchronization) نموده بدون این که acknowledgment ACK ( ) نهائی آنان را ارسال نماید. بدین ترتیب half-open TCP sessions (ارتباطات نیمه فعال) ، ایجاد می گردد . با توجه به این که پشته TCP ، قبل از reset نمودن پورت ، در انتظار باقی خواهد ماند ، تهاجم فوق ، سرریز بافر اتصال کامپیوتر مقصد را به دنبال داشته و عملا" امکان ایجاد ارتباط وی با سرویس گیرندگان معتبر ، غیر ممکن می گردد .

Land : تهاجم فوق، تاکنون در نسخه های متفاوتی از سیستم های عامل ویندوز ، یونیکس ، مکینتاش و IOS سیسکو،مشاهده شده است . در این نوع حملات ، مهاجمان اقدام به ارسال یک بسته اطلاعاتی SYN (TCP/IP synchronization) که دارای آدرس های مبداء و مقصد یکسان به همراه پورت های مبداء و مقصد مشابه می باشد ، برای سیستم های هدف می نمایند . بدین ترتیب سیستم قربانی، قادر به پاسخگوئی مناسب بسته اطلاعاتی نخواهد بود .

Teardrop : در این نوع حملات از یکی از خصلت های UDP در پشته TCP/IP برخی سیستم های عامل (TCPپیاده سازی شده در یک سیستم عامل) ، استفاده می گردد. در حملات فوق ، مهاجمان اقدام به ارسال بسته های اطلاعاتی fragmented برای سیستم هدف با مقادیر افست فرد در دنباله ای از بسته های اطلاعاتی می نمایند . زمانی که سیستم عامل سعی در بازسازی بسته های اطلاعاتی اولیه fragmented می نماید، قطعات ارسال شده بر روی یکدیگر بازنویسی شده و اختلال سیستم را به دنبال خواهد داشت . با توجه به عدم برخورد مناسب با مشکل فوق در برخی از سیستم های عامل ، سیستم هدف ، Crash و یا راه اندازی مجدد می گردد .

Bonk : این نوع از حملات بیشتر متوجه ماشین هائی است که از سیستم عامل ویندوز استفاده می نمایند . در حملات فوق ، مهاجمان اقدام به ارسال بسته های اطلاعاتی UDP مخدوش به مقصد پورت 53 DNS ، می نمایند بدین ترتیب در عملکرد سیستم اختلال ایجاد شده و سیستم Crash می نماید .

Boink : این نوع از حملات مشابه تهاجمات Bonk می باشند. با این تفاوت که در مقابل استفاده از پورت 53 ، چندین پورت ، هدف قرارمی گیرد .

یکی دیگر از حملات DoS ، نوع خاص و در عین حال ساده ای از یک حمله DoS می باشد که با نام Distributed DoS) DDoS) ، شناخته می شود .در این رابطه می توان از نرم افزارهای متعددی به منظور انجام این نوع حملات و از درون یک شبکه ، استفاده بعمل آورد. کاربران ناراضی و یا افرادی که دارای سوء نیت می باشند، می توانند بدون هیچگونه تاثیری از دنیای خارج از شیکه سازمان خود ، اقدام به ازکارانداختن سرویس ها در شبکه نمایند. در چنین حملاتی ، مهاجمان نرم افزاری خاص و موسوم به Zombie را توزیع می نمایند . این نوع نرم افزارها به مهاجمان اجازه خواهد داد که تمام و یا بخشی از سیستم کامپیوتری آلوده را تحت کنترل خود درآورند. مهاجمان پس از آسیب اولیه به سیستم هدف با استفاده از نرم افزار نصب شده Zombie ، تهاجم نهائی خود را با بکارگیری مجموعه ای وسیع از میزبانان انجام خواهند داد. ماهیت و نحوه انجام این نوع از حملات ، مشابه یک تهاجم استاندارد DoS بوده ولی قدرت تخریب و آسیبی که مهاجمان متوجه سیستم های آلوده می نمایند ، متاثر از مجموع ماشین هائی (Zombie) است که تحت کنترل مهاجمان قرار گرفته شده است .

به منظور حفاظت شبکه ، می توان فیلترهائی را بر روی روترهای خارجی شبکه به منظور دورانداختن بسته های اطلاعاتی مشمول حملات DoS ، پیکربندی نمود .در چنین مواردی می بایست از فیلتری دیگر که امکان مشاهده ترافیک (مبداء از طریق اینترنت) و یک آدرس داخلی شبکه را فراهم می نماید ، نیز استفاده گردد .

حملات از نوع Back door

door Back ، برنامه ای است که امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی ، فراهم می نماید . برنامه نویسان معمولا" چنین پتانسیل هائی را در برنامه ها پیش بینی تا امکان اشکال زدائی و ویرایش کدهای نوشته شده در زمان تست بکارگیری نرم افزار ، فراهم گردد. با توجه به این که تعداد زیادی از امکانات فوق ، مستند نمی گردند ، پس از اتمام مرحله تست به همان وضعیت باقی مانده و تهدیدات امنیتی متعددی را به دنبال خواهند داشت .

برخی از متداولترین نرم افزارها ئی که از آنان به عنوان back door استفاده می گردد ، عبارتند از :

Back Orifice : برنامه فوق یک ابزار مدیریت از راه دور می باشد که به مدیران سیستم امکان کنترل یک کامپیوتر را از راه دور (مثلا" از طریق اینترنت) ، خواهد داد. نرم افزار فوق ، ابزاری خطرناک است که توسط گروهی با نام Cult of the Dead Cow Communications ، ایجاد شده است . این نرم افزار دارای دو بخش مجزا می باشد : یک بخش سرویس گیرنده و یک بخش سرویس دهنده . بخش سرویس گیرنده بر روی یک ماشین اجراء و زمینه مانیتور نمودن و کنترل یک ماشین دیگر که بر روی آن بخش سرویس دهنده

اجراء شده است را فراهم می نماید .

NetBus : این برنامه نیز نظیر Back Orifice ، امکان دستیابی و کنترل از راه دور یک ماشین از طریق اینترنت را فراهم می نماید.. برنامه فوق تحت سیستم عامل ویندوز (نسخه های متفاوت از NT تا 95 و 98) ، اجراء و از دو بخش جداگانه تشکیل شده است : بخش سرویس دهنده (بخشی که بر روی کامپیوتر قربانی مستقر خواهد شد) و بخش سرویس گیرنده (برنامه ای که مسولیت یافتن و کنترل سرویس دهنده را برعهده دارد) . برنامه فوق ، به حریم خصوصی کاربران در زمان اتصال به اینترنت ، تجاوز و تهدیدات امنیتی متعددی را به دنبال خواهد داشت .

SubSeven (Sub7) ، این برنامه برنامه نیز تحت ویندوز اجراء شده و دارای عملکردی مشابه Back Orifice و NetBus می باشد . پس از فعال شدن برنامه فوق بر روی سیستم هدف و اتصال به اینترنت ،هر شخصی که دارای نرم افزار سرویس گیرنده باشد ، قادر به دستیابی نامحدود به سیستم خواهد بود .

نرم افزارهای Back Orifice، Sub7 ،NetBus دارای دو بخش ضروری سرویس دهنده و سرویس گیرنده، می باشند . سرویس دهنده بر روی ماشین آلوده مستقر شده و از بخش سرویس گیرنده به منظور کنترل از راه دور سرویس دهنده ، استفاده می گردد.به نرم افزارهای فوق ، " سرویس دهندگان غیرقانونی " گفته می شود .
برخی از نرم افزارها از اعتبار بالائی برخوردار بوده ولی ممکن است توسط کاربرانی که اهداف مخربی دارند ، مورد استفاده قرار گیرند :

VNC Virtual Network Computing) : نرم افزار فوق توسط آزمایشگاه T&AT و با هدف کنترل از راه دور یک سیستم ، ارائه شده است . با استفاده از برنامه فوق ، امکان مشاهده محیط Desktop از هر مکانی نظیر اینترنت ، فراهم می گردد . یکی از ویژگی های جالب این نرم افزار ، حمایت گسترده از معماری های متفاوت است .

PCAnywhere : نرم افزار فوق توسط شرکت Symantec ، با هدف کنترل از راه دور یک سیستم با لحاظ نمودن فن آوری رمزنگاری و تائید اعتبار ، ارائه شده است . با توجه به سهولت استفاده از نرم افزار فوق ، شرکت ها و موسسات فراوانی در حال حاضر از آن و به منظور دستیابی به یک سیستم از راه دور استفاده می نمایند .

Terminal Services : نرم افزار فوق توسط شرکت مایکروسافت و به همراه سیستم عامل ویندوز و به منظور کنترل از راه دور یک سیستم ، ارائه شده است .

همانند سایر نرم افزارهای کاربردی ، نرم افزارهای فوق را می توان هم در جهت اهداف مثبت و هم در جهت اهداف مخرب بکارگرفت.
بهترین روش به منظور پیشگیری از حملات Back doors ، آموزش کاربران و مانیتورینگ عملکرد هر یک از نرم افزارهای موجود می باشد. به کاربران می بایست آموزش داده شود که صرفا" از منابع و سایت های مطمئن اقدام به دریافت و نصب نرم افزار بر روی سیستم خود نمایند . نصب و استفاده از برنامه های آنتی ویروس می تواند کمک قابل توجهی در بلاک نمودن عملکرد اینچنین نرم افزارهائی (نظیر : Back Orifice, NetBus, and Sub7) را به دنبال داشته باشد . برنامه های آنتی ویروس می بایست به صورت مستمر بهنگام شده تا امکان شناسائی نرم افزارهای جدید ، فراهم گردد .

طرح مقابله با حوادث امنیتی و ترمیم خرابیها

طرح مقابله با حوادث امنیتی، با هدف پیشگیری، تشخیص و مقابله با حوادث امنیتی فضای تبادل اطلاعات، ارائه می‌گردد. محتوای این طرح، حداقل شامل موارد زیر می‌باشد:

1- دسته‌بندی حوادث
2- سیاست‌های مربوط به هر یک از سرویس‌های مقابله با حوادث امنیتی
3- ساختار و شرح وظایف مربوط به تیم مقابله با حوادث امنیتی دستگاه
4- سرویس‌های پیشگیری و مقابله با حوادث که توسط تیم مقابله با حوادث امنیتی دستگاه ارائه می‌گردد
5- روالهای اجرائی مربوط به هر یک از سرویس‌ها
6- متدولوژی مقابله با حوادث امنیتی
   - آماده‌سازی تیم
   - تشخیص و تحلیل حوادث
   - محدودسازی، ترمیم و ریشه‌کنی حوادث
   - فعالیت‌های بعد از حوادث
   - چک لیست مقابله با حوادث
7- الگوی مقابله با حوادث امنیتی

برنامه آگاهی‌رسانی امنیتی

برنامه آگاهی‌رسانی امنیتی، با هدف برنامه‌ریزی نحوه آگاهی رسانی به کاربران شبکه دستگاه ارائه می‌گردد و باید حاوی موارد ذیل باشد:

1- اهداف آگاهی‌رسانی

2- راهبردها

3- برنامه اجرائی آگاهی‌رسانی

4- مفاد دوره‌های آگاهی‌رسانی از قبیل:

- اعلام حیطه حریم خصوصی کاربران
- اعلام وظایف، مسئولیتها و مواردی که کاربران باید پاسخگو باشند
- اعلام مواردی که کاربران باید نسبت به آن حساسیت داشته باشند (از قبیل اعلام حوادث به تیم مقابله با حوادث)
- ارائه اطلاعات در زمینه آسیب‌پذیری سیستم‌ها و مواردی که کاربران باید دقت بیشتری لحاظ نمایند

برنامه آموزش پرسنل تشکیلات امنیت

برنامه آموزش امنیتی، با هدف توانمند سازی پرسنل تشکیلات امنیت دستگاه ارائه می‌گردد و باید حاوی موارد ذیل باشد:

5- اهداف آموزش

6- راهبردها

7- برنامه اجرائی آموزش

8- مفاد دوره‌های آموزشی

تشکیلات تامین امنیت فضای

تبادل اطلاعات دستگاه

اجزاء و ساختار تشکیلات امنیت

بر اساس استانداردهای مدیریت امنیت اطلاعات و ارتباطات، هر دستگاه به منظور تامین امنیت اطلاعات و ارتباطات خود، لازم است تشکیلات تامین امنیت به شرح زیر، ایجاد نماید.

اجزاء تشکیلات امنیت :

تشکیلات امنیت شبکه، متشکل از سه جزء اصلی به شرح زیر می باشد:

- در سطح سیاستگذاری: کمیته راهبری امنیت فضای تبادل اطلاعات دستگاه
- در سطح مدیریت اجرائی: مدیر امنیت فضای تبادل اطلاعات دستگاه
- در سطح فنی: واحد پشتیبانی امنیت فضای تبادل اطلاعات دستگاه

علاوه بر موارد فوق، واحدهای "مشاوره و طراحی" و "نظارت و بازرسی" نیز لازم است. لیکن این واحدها الزاما در داخل دستگاه و چارت سازمانی، تشکیل نخواهند شد.

ساختار تشکیلات امنیت :

ساختار تشکیلات امنیت شبکه دستگاه، عبارتست از:

Position	Last month	Virus	Percentage of reports
1	1	W32/Netsky-P	16.7%
2	2	W32/Zafi-B	11.4%
3	3	W32/Nyxem-D	7.5%
4	10	W32/Mytob-AS	6.3%
5	New	W32/Mytob-P	5.3%
5	New	W32/Mytob-M	5.3%
7	4	W32/Netsky-D	3.7%
8	Re-entry	W32/MyDoom-O	3.6%
9	6	W32/Mytob-FO	2.9%
10	7	W32/Mytob-C	2.1%
Others			35.2%

اعضاء تشکیلات امنیت فضای تبادل اطلاعات دستگاه:

اعضاء تشکیلات امنیت شبکه دستگاه، عبارتند از:

1- اعضاء کمیته راهبری امنیت:

- مدیر دستگاه (رئیس کمیته)
- نماینده ویژه مدیر دستگاه
- مدیر حراست دستگاه
- مدیر فن آوری اطلاعات دستگاه
- مدیر امنیت شبکه دستگاه (دبیر کمیته)

2- مدیر امنیت :

مدیریت واحد پشتیبانی امنیت شبکه را به عهده دارد و توسط مدیر فن‌آوری اطلاعات دستگاه تعیین می‌شود.

3- تیم‌های پشتیبانی امنیت :

شامل تیم‌های زیر بوده و اعضاء آن مستقیما توسط مدیر امنیت شبکه دستگاه تعیین می‌شوند:

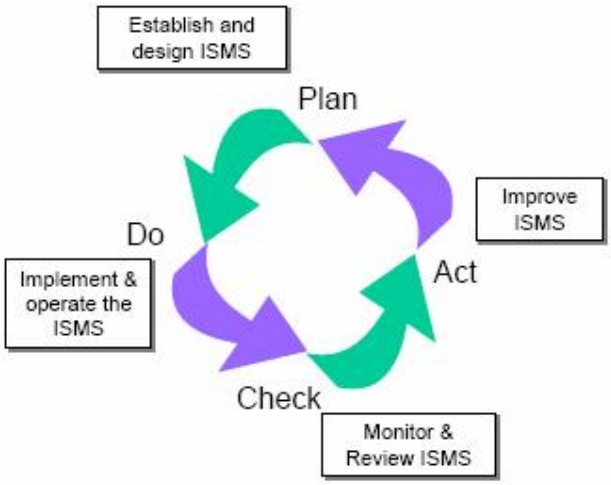
- تیم پشتیبانی حوادث

- تیم نظارت و بازرسی
- تیم نگهداری امنیت
- تیم مدیریت تغییرات
- تیم بررسی پاسخگوئی به نیازهای امنیتی

بخش دوم

در این بخش از استاندارد برای تامین امنیت اطلاعات و ارتباطات سازمان ، مطابق شکل (1) یک چرخهٔ ایمن سازی شامل 4 مرحلهٔ طراحی، پیاده سازی، تست و اصلاح ارائه شده و جزئیات هر یک از مراحل به همراه لیست و محتوای مستندات موردنیاز جهت ایجاد سیستم مدیریت امنیت اطلاعات سازمان، ارائه شده است.

شکل(1) : مراحل ایمن سازی بر اساس استاندارد BS7799:2002



استاندارد ISO/IEC 17799 موسسه بین‌المللی استاندارد

در سال 2000 ، بخش اول استاندارد BS7799:2 بدون هیچگونه تغییری توسط موسسهٔ بین المللی استاندارد بعنوان استاندارد ISO/IEC 17799 منتشر شد.

راهنمای فنی ISO/IEC TR13335 موسسه بین‌المللی استاندارد

این گزارش فنی در قالب 5 بخش مستقل در فواصل سالهای 1996 تا 2001 توسط موسسهٔ بین المللی استاندارد منتشر شده است . اگر چه این گزارش فنی به عنوان استاندارد ISO منتشر نشد و عنوان Technical Report بر آن نهاده شد، لیکن تنها مستندات فنی معتبری است که جزئیات و تکنیکهای مورد نیاز مراحل ایمن سازی اطلاعات و ارتباطات را تشریح نموده و در واقع مکمل استانداردهای مدیریتی BS7799 و ISO/IEC 17799 می باشد.

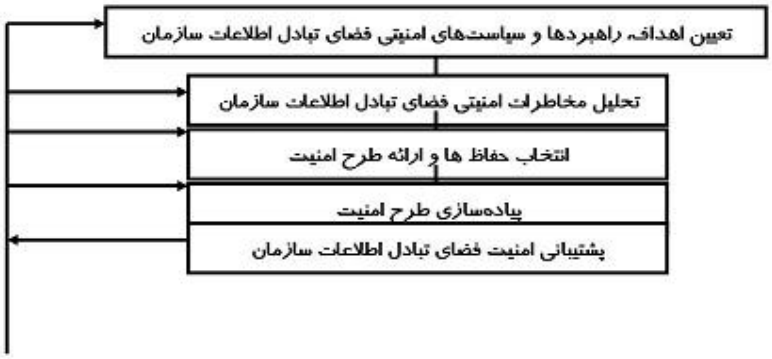
بخش اول

در این بخش که در سال 1996 منتشر شد، مفاهیم کلی امنیت اطلاعات از قبیل سرمایه، تهدید، آسیب پذیری، ریسک، ضربه و ... روابط بین این مفاهیم و مدل مدیریت مخاطرات امنیتی، ارائه شده است.

بخش دوم

این بخش که در سال 1997 منتشر شد ، مراحل ایمن سازی و ساختار تشکیلات تامین امنیت اطلاعات سازمان ارائه شده است . بر اساس این گزارش فنی ، چرخهٔ ایمن سازی مطابق شکل (2) به 5 مرحله شامل تدوین سیاست امنیتی سازمان، تحلیل مخاطرات امنیتی، تعیین حفاظها و ارائهٔ طرح امنیت، پیاده سازی طرح امنیت و پشتیبانی امنیت اطلاعات، تفکیک شده است.

شکل(2): مراحل ایمن سازی بر اساس گزارش فنی ISO/IEC 13335



بخش سوم

در این بخش که در سال 1998 منتشر شد، تکنیکهای طراحی، پیاده سازی و پشتیبانی امنیت اطلاعات از جمله محورها و جزئیات سیاستهای امنیتی سازمان، تکنیکهای تحلیل مخاطرات امنیتی، محتوای طرح امنیتی، جزئیات پیاده سازی طرح امنیتی و پشتیبانی امنیت اطلاعات، ارائه شده است.

بخش چهارم

در این بخش که در سال 2000 منتشر شد، ضمن تشریح حفاظهای فیزیکی، سازمانی و حفاظهای خاص سیستم‌های اطلاعاتی، نحوهٔ انتخاب حفاظهای مورد نیاز برای تامین هریک از مولفه‌های امنیت اطلاعات، ارائه شده است.

بخش پنجم

در این بخش که در سال 2001 منتشر شد، ضمن افزودن مقولهٔ ارتباطات و مروری بر بخشهای دوم تا چهارم این گزارش فنی، تکنیکهای تامین امنیت ارتباطات از قبیل شبکه‌های خصوصی مجازی، امنیت در گذرگاه‌ها، تشخیص تهاجم و کدهای مخرب، ارائه شده است.

مستندات ISMS

بر اساس استانداردهای مدیریت امنیت اطلاعات و ارتباطات، هر دستگاه (سازمان) باید مجموعه مستندات مدیریت امنیت اطلاعات و ارتباطات را به شرح زیر، برای خود تدوین نماید:

- اهداف، راهبردها و سیاستهای امنیتی فضای تبادل اطلاعات دستگاه
- طرح تحلیل مخاطرات امنیتی فضای تبادل اطلاعات دستگاه
- طرح امنیت فضای تبادل اطلاعات دستگاه
- طرح مقابله با حوادث امنیتی و ترمیم خرابیهای فضای تبادل اطلاعات دستگاه
- برنامهٔ آگاهی رسانی امنیتی به پرسنل دستگاه
- برنامهٔ آموزش امنیتی پرسنل تشکیلات تامین امنیت فضای تبادل اطلاعات دستگاه

در این بخش، به بررسی مستندات فوق خواهیم پرداخت.

اهداف،راهبردها و سیاست‌های امنیتی

اولین بخش از مستندات ISMS دستگاه، شامل اهداف، راهبردها و سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه می‌باشد. در این مستندات، لازم است موارد زیر، گنجانیده شوند:

اهداف امنیت فضای تبادل اطلاعات دستگاه

در این بخش از مستندات، ابتدا سرمایه‌های فضای تبادل اطلاعات دستگاه، در قالب سخت‌افزارها، نرم‌افزارها، اطلاعات، ارتباطات، سرویسها و کاربران تفکیک و دسته‌بندی شده و سپس اهداف کوتاه‌مدت و میان‌مدت تامین امنیت هر یک از سرمایه‌ها، تعیین خواهد شد. نمونه‌ای از این اهداف، عبارتند از:

نمونه‌هائی از اهداف کوتاه مدت امنیت:

- جلوگیری از حملات و دسترسی‌های غیرمجاز، علیه سرمایه‌های فضای تبادل اطلاعات دستگاه
- مهار خسارتهای ناشی از ناامنی موجود در فضای تبادل اطلاعات دستگاه
- کاهش رخنه‌پذیریهای سرمایه‌های فضای تبادل اطلاعات دستگاه

نمونه‌هائی از اهداف میان مدت امنیت:

- تامین صحت عملکرد، قابلیت دسترسی و محافظت فیزیکی برای سخت‌افزارها، متناسب با حساسیت آنها.
- تامین صحت عملکرد و قابلیت دسترسی برای نرم‌افزارها، متناسب با حساسیت آنها.
- تامین محرمانگی، صحت و قابلیت دسترسی برای اطلاعات، متناسب با طبقه‌بندی اطلاعات از حیث محرمانگی.
- تامین محرمانگی، صحت و قابلیت دسترسی برای ارتباطات، متناسب با طبقه‌بندی اطلاعات از حیث محرمانگی و حساسیت ارتباطات.
- تامین قابلیت تشخیص هویت، حدود اختیارات و پاسخگوئی، حریم خصوصی و آگاهی‌رسانی امنیتی برای کاربران شبکه، متناسب با طبقه‌بندی اطلاعات قابل دسترس و نوع کاربران.

راهبردهای امنیت فضای تبادل اطلاعات دستگاه

راهبردهای امنیت فضای تبادل اطلاعات دستگاه، بیانگر اقداماتی است که به منظور تامین اهداف امنیت دستگاه، باید انجام گیرد. نمونه‌ای از راهبردهای کوتاه‌مدت و میان‌مدت امنیت فضای تبادل اطلاعات دستگاه، عبارتند از:

نمونه‌هائی از راهبردهای کوتاه مدت امنیت:

- شناسائی و رفع ضعفهای امنیتی فضای تبادل اطلاعات دستگاه
- آگاهی‌رسانی به کاربران فضای تبادل اطلاعات دستگاه
- کنترل و اعمال محدودیت در ارتباطات شبکه داخلی دستگاه

نمونه‌هائی از راهبردهای میان مدت امنیت:

- رعایت استانداردهای مدیریت امنیت اطلاعات
- تهیه طرحها و برنامه‌های امنیتی فضای تبادل اطلاعات دستگاه، بر اساس استانداردهای فوق
- ایجاد و آماده‌سازی تشکیلات تامین امنیت فضای تبادل اطلاعات دستگاه
- اجرای طرحها و برنامه‌های امنیتی فضای تبادل اطلاعات دستگاه

سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه

سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه، متناسب با دسته‌بندی انجام شده روی سرمایه‌های فضای تبادل اطلاعات دستگاه، عبارتند از:

- سیاست‌های امنیتی سرویس‌های فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی سخت‌افزارهای فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی نرم‌افزارهای فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی اطلاعات فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی ارتباطات فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی کاربران فضای تبادل اطلاعات دستگاه

طرح تحلیل مخاطرات امنیتی

پس از تدوین اهداف، راهبردها و سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه و قبل از طراحی امنیت فضای تبادل اطلاعات، لازم است شناخت دقیقی از مجموعه فضای تبادل اطلاعات موجود دستگاه بدست آورد. در این مرحله، ضمن کسب شناخت نسبت به اطلاعات، ارتباطات، تجهیزات، سرویس‌ها و ساختار شبکه ارتباطی دستگاه، ضعفهای امنیتی موجود در بخشهای مختلف، شناسائی خواهند شد تا در مراحل بعدی، راهکارهای لازم به منظور رفع این ضعفها و مقابله با تهدیدها، ارائه شوند. روش تحلیل مخاطرات امنیتی، باید در مجموعه راهبردهای امنیتی فضای تبادل اطلاعات دستگاه، مشخص شده باشد.

در تحلیل مخاطرات امنیتی، به مواردی پرداخته می‌شود که بصورت بالقوه، امکان دسترسی غیرمجاز، نفوذ و حمله کاربران مجاز یا غیرمجاز فضای تبادل اطلاعات دستگاه، به منابع (سرمایه‌های) فضای تبادل اطلاعات دستگاه و منابع کاربران این فضا را فراهم می‌نمایند.

در این مستند، لازم است مخاطرات امنیتی فضای تبادل اطلاعات، حداقل در محورهای "معماری شبکه"، "تجهیزات شبکه"، "سرویس‌دهنده‌های شبکه"، "مدیریت و نگهداری شبکه" و "تشکیلات و روشهای مدیریت امنیت شبکه"، بررسی شوند.

معماری شبکه ارتباطی

در این بخش، لازم است معماری شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- ساختار شبکه ارتباطی
- ساختار آدرس‌دهی و مسیریابی
- ساختار دسترسی به شبکه ارتباطی

تجهیزات شبکه ارتباطی

در این بخش، لازم است تجهیزات شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- محافظت فیزیکی
- نسخه و آسیب‌پذیریهای نرم‌افزار
- مدیریت محلی و از راه دور
- تصدیق هویت، تعیین اختیارات و ثبت عملکرد سیستم، بویژه در دسترسی‌های مدیریتی

- ثبت وقایع
- نگهداری و به‌روزنمودن پیکربندی
- مقابله با حملات علیه خود سیستم، بویژه حملات ممانعت از سرویس

مدیریت و نگهداری شبکه ارتباطی

در این بخش، لازم است مدیریت و نگهداری شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- تشکیلات و روشهای مدیریت و نگهداری شبکه ارتباطی
- ابزارها و مکانیزم‌های مدیریت و نگهداری شبکه ارتباطی

سرویس‌های شبکه ارتباطی

در این بخش، لازم است سرویس‌های شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- سیستم عامل سرویس‌دهنده
- سخت‌افزار سرویس‌دهنده، بویژه رعایت افزونگی در سطح ماجول و سیستم
- نرم‌افزار سرویس
- استفاده از ابزارها و مکانیزم‌های امنیتی روی سرویس‌دهنده‌ها

تشکیلات و روشهای تامین امنیت شبکه ارتباطی

در این بخش، لازم است تشکیلات و روشهای امنیت شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- طرح‌ها، برنامه‌ها و سایر مستندات امنیتی
- تشکیلات امنیت، روالهای اجرائی و شرح وظایف پرسنل امنیت

طرح امنیت

پس از تحلیل مخاطرات امنیتی شبکه ارتباطی دستگاه و دسته‌بندی مخاطرات امنیتی این شبکه، در طرح امنیت، ابزارها و مکانیزم‌های موردنیاز به منظور رفع این ضعفها و مقابله با تهدیدها، ارائه می‌شوند. در طرح امنیت، لازم است کلیه ابزارها ومکانیزم‌های امنیتی موجود، بکار گرفته شوند. نمونه‌ای از این ابزارها عبارتند از:

1- سیستم‌های کنترل جریان اطلاعات و تشکیل نواحی امنیتی

- فایروال‌ها
- سایر سیستم‌های تامین امنیت گذرگاه‌ها

2- سیستم‌های تشخیص و مقابله یا تشخیص و پیشگیری از حملات،شامل:

- سیستم‌های مبتنی بر ایستگاه
- سیستم‌های مبتنی بر شبکه

3- سیستم فیلترینگ محتوا (بویژه برای سرویس E-Mail)

4- نرم‌افزارهای تشخیص و مقابله با ویروس
5- سیستم‌های تشخیص هویت، تعیین حدود اختیارات و ثبت عملکرد کاربران
6- سیستم‌های ثبت و تحلیل رویدادنامه‌ها
7- سیستم‌های رمزنگاری اطلاعات
8- نرم‌افزارهای نظارت بر ترافیک شبکه
9- نرم‌افزارهای پویشگر امنیتی
10- نرم‌افزارهای مدیریت امنیت شبکه

ویژگیهای اصلی سیستم امنیتی شبکه ارتباطی دستگاه، عبارتند از:

- چندلایه بودن سیستم امنیتی
- توزیع‌شده بودن سیستم امنیتی
- تشکیل نواحی امنیتی جهت کنترل دقیق دسترسی به سرویس‌های شبکه
- یکپارچگی مکانیزم‌های امنیتی، بویژه در گذرگاههای ارتباطی شبکه
- تفکیک زیرساختار مدیریت امنیت شبکه (حداقل بخش اصلی سیستم امنیتی شبکه)
- انتخاب اجزاء سیستم امنیتی شبکه، از Brandهای مختلف، بنحوی که ضعفهای امنیتی یکدیگر را پوشش داده و مخاطره باقیمانده را کاهش دهند
- انتخاب محصولاتی که دارای تائیدیه‌های معتبر، از موسسات ارزیابی بین‌المللی می‌باشند

در حال حاضر، وضعیت امنیت فضای تبادل اطلاعات کشور، بویژه در حوزه دستگاههای دولتی، در سطح نامطلوبی قرار دارد. از جمله دلایل اصلی وضعیت موجود، می‌توان به فقدان زیرساخت‌های فنی و اجرائی امنیت و عدم انجام اقدامات موثر در خصوص ایمن‌سازی فضای تبادل اطلاعات دستگاه‌های دولتی اشاره نمود.

بخش قابل توجهی از وضعیت نامطلوب امنیت فضای تبادل اطلاعات کشور، بواسطه فقدان زیرساخت‌هائی از قبیل نظام ارزیابی امنیتی فضای تبادل اطلاعات، نظام صدور گواهی و زیرساختار کلید عمومی، نظام تحلیل و مدیریت مخاطرات امنیتی، نظام پیشگیری و مقابله با حوادث فضای تبادل اطلاعات، نظام مقابله با جرائم فضای تبادل اطلاعات و سایر زیرساخت‌های امنیت فضای تبادل اطلاعات در کشور می‌باشد. از سوی دیگر، وجود زیرساخت‌های فوق، قطعا تاثیر بسزائی در ایمن‌سازی فضای تبادل اطلاعات دستگاههای دولتی خواهد داشت.

صرفنظر از دلایل فوق، نابسامانی موجود در وضعیت امنیت فضای تبادل اطلاعات دستگاه‌های دولتی، از یکسو موجب بروز اخلال در عملکرد صحیح دستگاه‌ها شده و کاهش اعتبار این دستگاه‌ها را در پی خواهد داشت، و از سوی دیگر، موجب اتلاف سرمایه‌های ملی خواهد شد. لذا همزمان با تدوین سند راهبردی امنیت فضای تبادل اطلاعات کشور، توجه به مقوله ایمن‌سازی فضای تبادل اطلاعات دستگاه‌های دولتی،

ضروری به نظر می‌رسد. این امر علاوه بر کاهش صدمات و زیانهای ناشی از وضعیت فعلی امنیت دستگاه‌های دولتی، نقش موثری در فرآیند تدوین سند راهبردی امنیت فضای تبادل اطلاعات کشور خواهد داشت.

سیستم مدیریت امنیت اطلاعات (ISMS)

با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال 1995، نگرش سیستماتیک به مقوله ایمن‌سازی فضای تبادل اطلاعات شکل گرفت. بر اساس این نگرش، تامین امنیت فضای تبادل اطلاعات سازمانها، دفعتا مقدور نمی‌باشد و لازم است این امر بصورت مداوم در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح، انجام گیرد. برای این منظور لازم است هر سازمان بر اساس یک متدولوژی مشخص، اقدامات زیر را انجام دهد:

1- تهیه طرح‌ها و برنامه‌های امنیتی موردنیاز سازمان
2- ایجاد تشکیلات موردنیاز جهت ایجاد و تداوم امنیت فضای تبادل اطلاعات سازمان
3- اجرای طرح‌ها و برنامه‌های امنیتی سازمان

در حال حاضر، مجموعه‌ای از استانداردهای مدیریتی و فنی ایمن‌سازی فضای تبادل اطلاعات سازمان‌ها ارائه شده‌اند که استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس، استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد و گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد از برجسته‌ترین استانداردها و راهنماهای فنی در این زمینه محسوب می‌گردند.

در این استانداردها، نکات زیر مورد توجه قرار گرفته شده است:

1- تعیین مراحل ایمن‌سازی و نحوه شکل‌گیری چرخه امنیت اطلاعات و ارتباطات سازمان
2- جزئیات مراحل ایمن‌سازی و تکنیکهای فنی مورد استفاده در هر مرحله
3- لیست و محتوای طرح‌ها و برنامه‌های امنیتی موردنیاز سازمان
4- ضرورت و جزئیات ایجاد تشکیلات سیاستگذاری، اجرائی و فنی تامین امنیت اطلاعات و ارتباطات سازمان
5- کنترل‌های امنیتی موردنیاز برای هر یک از سیستم‌های اطلاعاتی و ارتباطی سازمان

مروری بر استانداردهای مدیریت امنیت اطلاعات

استانداردهای مدیریتی ارائه شده در خصوص امنیت اطلاعات و ارتباطات سازمان‌ها، عبارتند از:

- استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس
- استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد
- گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد

در این بخش، به بررسی مختصر استانداردهای فوق خواهیم پرداخت.

استاندارد BS7799 موسسه استاندارد انگلیس

استاندراد BS7799 اولین استاندارد مدیریت امنیت اطلاعات است که نسخه اول آن (BS7799:1) در سال 1995 منتشر شد. نسخه دوم این استاندارد (BS7799:2) که در سال 1999 ارائه شد، علاوه بر تغییر نسبت به نسخه اول، در دو بخش ارائه گردید. آخرین نسخه این استاندارد، (BS7799:2002) نیز در سال 2002 و در دو بخش منتشر گردید.

بخش اول

در این بخش از استاندارد، مجموعه کنترل‌های امنیتی موردنیاز سیستم‌های اطلاعاتی و ارتباطی هر سازمان، در قالب ده دسته‌بندی کلی شامل موارد زیر، ارائه شده است:

1- تدوین سیاست امنیتی سازمان

در این قسمت، به ضرورت تدوین و انتشار سیاست‌های امنیتی اطلاعات و ارتباطات سازمان ، بنحوی که کلیه مخاطبین سیاست‌ها در جریان جزئیات آن قرار گیرند، تاکید شده است. همچنین جزئیات و نحوه نگارش سیاست‌های امنیتی اطلاعات و ارتباطات سازمان، ارائه شده است.

2- ایجاد تشکیلات تامین امنیت سازمان

در این قسمت، ضمن تشریح ضرورت ایجاد تشکیلات امنیت اطلاعات و ارتباطات سازمان، جزئیات این تشکیلات در سطوح سیاستگذاری، اجرائی و فنی به همراه مسئولیت‌های هر یک از سطوح، ارائه شده است.

3- دسته‌بندی سرمایه‌ها و تعیین کنترل‌های لازم

در این قسمت، ضمن تشریح ضرورت دسته‌بندی اطلاعات سازمان، به جزئیات تدوین راهنمای دسته‌بندی اطلاعات سازمان پرداخته و محورهای دسته‌بندی اطلاعات را ارائه نموده است.

4- امنیت پرسنلی

در این قسمت، ضمن اشاره به ضرورت رعایت ملاحظات امنیتی در بکارگیری پرسنل، ضرورت آموزش پرسنل در زمینه امنیت اطلاعات و ارتباطات، مطرح شده و لیستی از مسئولیت‌های پرسنل در پروسه تامین امنیت اطلاعات و ارتباطات سازمان، ارائه شده است.

5- امنیت فیزیکی و پیرامونی

در این قسمت، اهمیت و ابعاد امنیت فیزیکی، جزئیات محافظت از تجهیزات و کنترلهای موردنیاز برای این منظور، ارائه شده است.

6- مدیریت ارتباطات

در این قسمت، ضرورت و جزئیات روالهای اجرائی موردنیاز، بمنظور تعیین مسئولیت هر یک از پرسنل، روالهای مربوط به سفارش، خرید، تست و آموزش سیستم‌ها، محافظت در مقابل نرم‌افزارهای مخرب، اقدامات موردنیاز در خصوص ثبت وقایع و پشتیبان‌گیری از اطلاعات، مدیریت شبکه، محافظت از رسانه‌ها و روالها و مسئولیت‌های مربوط به درخواست، تحویل، تست و سایر موارد تغییر نرم‌افزارها ارائه شده است.

7- کنترل دسترسی

در این قسمت، نیازمندیهای کنترل دسترسی، نحوه مدیریت دسترسی پرسنل، مسئولیت‌های کاربران، ابزارها و مکانیزم‌های کنترل دسترسی در شبکه، کنترل دسترسی در سیستم‌عاملها و نرم‌افزارهای کاربردی، استفاده از سیستم‌های مانیتورینگ و کنترل دسترسی در ارتباط از راه دور به شبکه ارائه شده است.

8- نگهداری و توسعه سیستم‌ها

در این قسمت، ضرورت تعیین نیازمندیهای امنیتی سیستم‌ها، امنیت در سیستم‌های کاربردی، کنترلهای رمزنگاری، محافظت از فایلهای سیستم و ملاحظات امنیتی موردنیاز در توسعه و پشتیبانی سیستم‌ها، ارائه شده است.

9- مدیریت تداوم فعالیت سازمان

در این قسمت، رویه‌های مدیریت تداوم فعالیت، نقش تحلیل ضربه در تداوم فعالیت، طراحی و تدوین طرح‌های تداوم فعالیت، قالب پیشنهادی برای طرح تداوم فعالیت سازمان و طرح‌های تست، پشتیبانی و ارزیابی مجدد تداوم فعالیت سازمان، ارائه شده است.

10- پاسخگوئی به نیازهای امنیتی

در این قسمت، مقررات موردنیاز در خصوص پاسخگوئی به نیازهای امنیتی، سیاست‌های امنیتی موردنیاز و ابزارها و مکانیزم‌های بازرسی امنیتی سیستم‌ها، ارائه شده است.

رمزنگاری

1- معرفی و اصطلاحات

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی است و برای قرنها بمنظور محافظت از پیغامهایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل می‌شده، استفاده شده است تا پیغامهای آنها محرمانه بماند.

هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند.

اغلب این مساله باید تضمین شود که یک پیغام فقط میتواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند. روشی که تامین کننده این مساله باشد "رمزنگاری" نام دارد. رمزنگاری هنر نوشتن بصورت رمز است بطوریکه هیچکس بغیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند.

رمزنگاری مخففها و اصطلاحات مخصوص به خود را دارد. برای درک عمیق‌تر به مقداری از دانش ریاضیات نیاز است. برای محافظت از دیتای اصلی (که بعنوان ***plaintext*** شناخته می‌شود)، آنرا با استفاده از یک کلید (رشته‌ای محدود از بیتها) بصورت رمز در می‌آوریم تا کسی که

دیتای حاصله را می‌خواند قادر به درک آن نباشد. دیتای رمزشده (که بعنوان ***ciphertext*** شناخته می‌شود) بصورت یک سری بی‌معنی از بیتها بدون داشتن رابطه مشخصی با دیتای اصلی بنظر می‌رسد. برای حصول متن اولیه دریافت‌کننده آنرا رمزگشایی می‌کند. یک شخص ثالث (مثلا یک هکر) می‌تواند برای اینکه بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمزنوشته ***(cryptanalysis)*** کند. بخاطرداشتن وجود این شخص ثالث بسیار مهم است.

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده‌اند. کلید، یک رشته از ارقام دودویی (صفر و یک) است که بخودی‌خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده‌سازی تغییر می‌کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند.

دیتای اولیه اغلب قبل از رمزشدن بازچینی می‌شود؛ این عمل عموما بعنوان scrambling شناخته می‌شود. بصورت مشخص‌تر، hash functionها بلوکی از دیتا را (که می‌تواند هر اندازه‌ای داشته باشد) به طول از پیش مشخص‌شده کاهش می‌دهد. البته دیتای اولیه نمی‌تواند از hashed value بازسازی شود. Hash functionها اغلب بعنوان بخشی از یک سیستم تایید هویت مورد نیاز هستند؛ خلاصه‌ای از پیام (شامل مهم‌ترین قسمتها مانند شماره پیام، تاریخ و ساعت، و نواحی مهم دیتا) قبل از رمزنگاری خود پیام، ساخته و hash می‌شود.

یک چک تایید پیام (Message Authentication Check) یا MAC یک الگوریتم ثابت با تولید یک امضاء برروی پیام با استفاده از یک کلید متقارن است. هدف آن نشان دادن این مطلب است که پیام بین ارسال و دریافت تغییر نکرده است. هنگامی که رمزنگاری توسط کلید عمومی برای تایید هویت فرستنده پیام استفاده می‌شود، منجر به ایجاد امضای دیجیتال (digital signature) می‌شود.

2- الگوریتم‌ها

طراحی الگوریتمهای رمزنگاری مقوله‌ای برای متخصصان ریاضی است. طراحان سیستمهایی که در آنها از رمزنگاری استفاده می‌شود، باید از نقاط قوت و ضعف الگوریتمهای موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم‌گیری داشته باشند. اگرچه رمزنگاری از اولین کارهای شانون (Shannon) در اواخر دهه 40 و اوایل دهه 50 بشدت پیشرفت کرده است، اما کشف رمز نیز پابه‌پای رمزنگاری به پیش آمده است و الگوریتمهای کمی هنوز با گذشت زمان ارزش خود را حفظ کرده‌اند. بنابراین تعداد الگوریتمهای استفاده شده در سیستمهای کامپیوتری عملی و در سیستمهای برپایه کارت هوشمند بسیار کم است.

2-1 سیستمهای کلید متقارن

یک الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند. بیشترین شکل استفاده از رمزنگاری که در کارتهای هوشمند و البته در بیشتر سیستمهای امنیت اطلاعات وجود دارد data encryption algorithm یا DEA است که بیشتر بعنوان DES شناخته می‌شود. DES یک محصول دولت ایالات متحده است که امروزه بطور وسیعی بعنوان یک استاندارد بین‌المللی شناخته می‌شود. بلوکهای 64بیتی دیتا توسط یک کلید تنها که معمولا 56 بیت طول دارد، رمزنگاری و رمزگشایی می‌شوند. DES از نظر محاسباتی ساده است و براحتی می‌تواند توسط پردازنده‌های کند (بخصوص آنهایی که در کارتهای هوشمند وجود دارند) انجام گیرد.

این روش بستگی به مخفی‌بودن کلید دارد. بنابراین برای استفاده در دو موقعیت مناسب است: هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا جایی که کلید بین دو سیستم مبادله می‌شوند که قبلا هویت یکدیگر را تایید کرده‌اند عمر کلیدها بیشتر از مدت تراکنش طول نمی‌کشد. رمزنگاری DES عموما برای حفاظت دیتا از شنود در طول انتقال استفاده می‌شود.

کلیدهای DES چهل بیتی امروزه در عرض چندین ساعت توسط کامپیوترهای معمولی شکسته می‌شوند و بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی اعتبار استفاده شود. کلید 56بیتی عموما توسط سخت‌افزار یا شبکه‌های بخصوصی شکسته می‌شوند. رمزنگاری DESسه‌تایی عبارتست از کدکردن دیتای اصلی با استفاده از الگوریتم DES که در سه مرتبه انجام می‌گیرد. (دو مرتبه با استفاده از یک کلید به سمت جلو (رمزنگاری) و یک مرتبه به سمت عقب (رمزگشایی) با یک کلید دیگر) مطابق شکل زیر:

این عمل تاثیر دوبرابر کردن طول مؤثر کلید را دارد؛ بعدا خواهیم دید که این یک عامل مهم در قدرت رمزکنندگی است.

الگوریتمهای استاندارد جدیدتر مختلفی پیشنهاد شده‌اند. الگوریتمهایی مانند Blowfish و IDEA برای زمانی مورد استفاده قرار گرفته‌اند اما هیچکدام پیاده‌سازی سخت‌افزاری نشدند بنابراین بعنوان رقیبی برای DES برای استفاده در کاربردهای میکروکنترلی مطرح نبوده‌اند. پروژه استاندارد رمزنگاری پیشرفته دولتی ایالات متحده (AES) الگوریتم Rijndael را برای جایگزینی DES بعنوان الگوریتم رمزنگاری اولیه انتخاب کرده است. الگوریتم Twofish مشخصا برای پیاده‌سازی در پردازنده‌های توان-پایین مثلا در کارتهای هوشمند طراحی شد.

در 1998 وزارت دفاع ایالات متحده تصمیم گرفت که الگوریتمها Skipjack و مبادله کلید را که در کارتهای Fortezza استفاده شده بود، از محرمانگی خارج سازد. یکی از دلایل این امر تشویق برای پیاده‌سازی بیشتر کارتهای هوشمند برپایه این الگوریتمها بود.

برای رمزنگاری جریانی (streaming encryption) (که رمزنگاری دیتا در حین ارسال صورت می‌گیرد بجای اینکه دیتای کدشده در یک فایل مجزا قرار گیرد) الگوریتم RC4 سرعت بالا و دامنه‌ای از طول کلیدها از 40 تا 256 بیت فراهم می‌کند. RC4 که متعلق به امنیت دیتای RSA است، بصورت عادی برای رمزنگاری ارتباطات دوطرفه امن در اینترنت استفاده می‌شود.

2-2 سیستمهای کلید نامتقارن

سیستمهای کلید نامتقارن از کلید مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. بسیاری از سیستمها اجازه می‌دهند که یک جزء (کلید عمومی یا public key) منتشر شود در حالیکه دیگری (کلید اختصاصی یا private key) توسط صاحبش حفظ شود. فرستنده پیام، متن را با کلید عمومی گیرنده کد می‌کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری میکند. بعبارتی تنها با کلید اختصاصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی‌تواند از متن کدشده به متن اصلی دست یابد، بنابراین پیام کدشده برای هرگیرنده‌ای بجز گیرنده مورد نظر فرستنده بی‌معنی خواهد بود. معمولترین سیستم نامتقارن بعنوان RSA شناخته می‌شود (حروف اول پدیدآورندگان آن یعنی Rivest ، Shamir و Adlemen است). اگرچه چندین طرح دیگر وجود دارند. می‌توان از یک سیستم نامتقارن برای نشاندادن اینکه فرستنده پیام همان شخصی است که ادعا می‌کند استفاده کرد که این عمل اصطلاحا امضاء نام دارد. RSA شامل دو تبدیل است که هرکدام احتیاج به بتوان‌رسانی ماجولار با توانهای خیلی طولانی دارد:

- امضاء، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند؛
- رمزگشایی عملیات مشابه‌ای روی متن رمزشده اما با استفاده از کلید عمومی است. برای تایید امضاء بررسی می‌کنیم که آیا این نتیجه با دیتای اولیه یکسان است؛ اگر اینگونه است، امضاء توسط کلید اختصاصی متناظر رمزشده است.

به بیان ساده‌تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شا-

شرکت RSA Security اعلام کرد که پس از 3 ماه تلاش مداوم , تیمی از ریاضیدانان اروپا و آمریکای شمالی توانستند آخرین معمای رمزنگاری این شرکت را حل کنند. این تیم که از 8 متخصص تشکیل شده بود از 100 ایستگاه کاری (Workstation) برای شکستن این رمز استفاده کردند و جایزه 10 هزار دلاری را از آن خود کردند.

این مسابقات را شرکت RSA برای تست استحکام الگوریتم های طولانی به کار گرفته شده برای امنیت الکترونیکی برگزار می کند. هدف از این رقابت , تشویق به تحقیق در زمینه تئوری اعداد محاسباتی و دشواری عملی فاکتورگیری از اعداد صحیح بزرگ است.

کالیسکی – یکی از مدیران آزمایشگاههای RSA – معتقد است که اطلاعات دریافت شده طی این رقابتها , منابع بسیار ارزشمندی برای جامعه رمزنگاری است و می تواند به سازمانها کمک کند تا معیارهای رمزنگاری مناسبی را برای دست یابی به سطح امنیتی مورد نظر انتخاب کنند.

شرکت کنندگان در این مسابقه سعی داشتند تا دو عدد اولی را که مورد استفاده قرار می گیرند تا 8 عدد اصلی کد رمزنگاری 576 بیتی RSA را تولید کنند , بیایند. RSA-576 یک نمونه کوچک از کلیدهای رمزنگاری است که برای امن کردن تراکنشهای اینترنت و بی سیم توصیه می شود. کلیدها معمولا حداقل 1024 بیتی (310 رقم دهدهی) هستند اما RSA-576 , 576 بیتی (174 رقم دهدهی) است. اعداد بزرگتر امنیت بیشتری را تامین می کنند. رقابت بعدی بر روی RSA-640 خوهد بود.

آسیب پذیری SSL

آسیب پذیری از کاراندازی سرویس در کتابخانه SSL مایکروسافت وجود دارد. آسیب پذیری مربوط به نحوه اداره پیغامهای بدشکل SSL در کتابخانه مایکروسافت SSL می باشد. این آسیب پذیری ممکن است باعث شود که سیستم آسیب دیده اتصالات SSL دریافت شده بر روی ویندوز 2000 و XP را متوقف نماید. در ویندوز سرور 2003، آسیب پذیری ممکن است باعث شود که سیستم آسیب دیده مجددا راه اندازی گردد.

توضیحاتی درباره آسیب پذیری SSL

محدوده آسیب پذیری چیست؟

آسیب پذیری ازکار اندازی سرویس در کتابخانه SSL مایکروسافت، بر روی نحوه اداره کتابخانه SSL مایکروسافت تاثیر می گذارد. این آسیب پذیری منجر به توقف اتصالات SSL بر روی ماشینهای آسیب دیده، ویندوز 2000 و XP می گردد. سیستمهای آسیب دیده ویندوز سرور 2003 به طور اتوماتیک راه اندازی مجدد می گردند.

آسیب پذیری ازکار اندازی سرویس، مانع از اجرای کد یا افزایش اجازه های دسترسی حمله گر نمی شود، بلکه مانع از پذیرش تقاضاهای وارد شونده توسط سیستم آسیب دیده می شود.

چه چیزی باعث آسیب پذیری می شود؟

پردازه بکار رفته توسط کتابخانه SSL برای کنترل پیغامهای ورودی، باعث آسیب پذیری می شود.

*کتابخانه **SSL** از مایکروسافت چیست؟*

کتابخانه SSL از مایکروسافت، از تعدادی از پروتکلهای ارتباطی امن پشتیبانی می نماید. این پروتکلها عبارتند از: Transport Layer Security 1.0 (TLS 1.0)، Secure Socket Layer 3.0 (SSL 3.0)، نسخه قدیمی تر و کم کاربردتر Secure Socket Layer 2.0 (SSL 2.0)، و پروتکل Private Communication Technology 1.0 (PCT 1.0).

این پروتکلها، ارتباط رمزنگاری شده ای را بین سیستم سرور و کاربر ایجاد می نمایند. SSLکمک به حفاظت از اطلاعات به هنگام اتصال کاربران در شبکه های عمومی مانند اینترنت می نماید. پشتیبانی SSL نیازمند گواهینامه SSL، که باید بر روی سرور نصب شود، می باشد.

حمله گر چگونه از آسیب پذیری استفاده می نماید؟

در ویندوز 2000 و XP، حمله گری که به طور موفقیت آمیزی از آسیب پذیری استفاده نموده است، می تواند باعث توقف اتصالات SSL شود. در ویندوز سرور 2003، حمله گر ممکن است باعث شود که سیستم آسیب دیده به طور اتوماتیک راه اندازی مجدد شود. در آن زمان، سیستم آسیب دیده به تقاضاهای تصدیق اصالت پاسخ نمی دهد. پس از راه اندازی مجدد سیستم، سیستم آسیب دیده با عملکرد خاصی بازیابی می گردد. به هرحال، این سیستم هنوز در معرض حمله ازکاراندازی سرویس می باشد، مگر اینکه بروزرسانیهایی اعمال گردد.

اگر حمله گری از این آسیب پذیری استفاده نماید، رویداد سیستمی خطا ثبت می شود. شماره رویداد (event ID) 5000 در log رویداد سیستم ثبت می شود، و ارزش SymbolicName آن، "SPMEVENT_PACKAGE_FAULT" می باشد و شرح آن به صورت ذیل است:

"بسته امنیتی NAME استثنایی را ایجاد نموده است" که در آن NAME ارزش "Schannel" یا " Microsoft Unified Secuirty Protocol Provider" می باشد.

چه کسی می تواند از آسیب پذیری استفاده نماید؟

هر کاربر بدون نامی که بتواند پیغام SSL را به سیستم آسیب دیده ارسال نماید، می تواند از این آسیب پذیری استفاده کند.

حمله گر چگونه می تواند از آسیب پذیری استفاده نماید؟

حمله گر برای استفاده از این آسیب پذیری برنامه ای ایجاد می نماید، که می تواند با سرور آسیب پذیر از طریق سرویس فعال شده با SSL ارتباط برقرار کندو پیغام TCP خاصی را ارسال نماید. سیستم آسیب پذیر در صورت دریافت چنین پیغامی، به نحوی شکست می خورد که حمله ازکاراندازی سرویس روی می دهد.

حمله گر، همچنین می تواند به جزء آسیب دیده از طریق دیگری دسترسی پیدا کند. مثلا حمله گر می تواند بر روی سیستم آسیب پذیر به طور محاوره ای یا به کمک برنامه دیگری که پارامترها را به جزء آسیب پذیر می فرستد، Login نماید(به طور محلی و یا از راه دور).

چه سیستمهایی در معرض این آسیب پذیری می باشند؟

همه سیستمهایی که SSL را فعال نموده اند، در معرض آسیب پذیری می باشند. اگرچه SSL به IIS به کمک HTTPS و پورت 443 دسترسی پیدا می کند، هر سرویسی که SSL را بر روی بستر آسیب دیده پیاده سازی می نماید، در معرض آن می باشد. سیستمهای IIS 4.0، IIS 5.0، IIS 5.1، Exchange Server 5.5، Exchange Server 2000، Exchange Server 2003، Analysis Services 2000 و هر برنامه ای که از SSL استفاده می نماید، از این نوع است.

کنترل کننده دامنه ویندوز 2000 که بر روی دامنه دایرکتوری فعال نصب می باشند، و Enterprise Root Certification Authority بر روی آن نصب می باشد، نیز در معرض آن می باشند.

Windows Server 2003	Windows XP	Windows 2000	Windows NT 4.0	Windows ,98, 98 SE ME	Impact of Vulnerability	Vulnerability Identifiers
Important	Important	Important	None	None	Of Denial Service	SSL Vulnerability

تخفیف عوامل در آسیب پذیری SSL

- تنها سیستمهایی که SSL را فعال نموده اند، فقط سیستمهای سرور، در معرض آن می باشند. به هر حال SSL به طور عمومی بر روی وب سرورها بکار می رود تا از برنامه های تجارت الکترونیکی، بانکداری online، و سایر برنامه هایی که نیاز به اتصال امن دارند، پشتیبانی نماید.
- بهترین تمرینات برای دیوار آتش، و پیکربندی پیش فرض استاندارد برای دیوار آتش، از شبکه ها در برابر حملات نشات گرفته از خارج از آنها محافظت می نماید.
- ویندوز NT 4.0 ، در معرض این آسیب پذیری نمی باشد.

کارهایی که می توان برای آسیب پذیری SSL انجام داد؟

مایکروسافت راه حلهای ذیل را توصیه نموده است. اگر چه توصیه های ذیل، آسیب پذیریها را اصلاح نمی نمایند، بردارهای شناخته شده حملات را بلوکه می کنند.

- *پورتهای 443 و 636 را در دیوار آتش بلوکه نمایید.* پورت 443 برا دریافت ترافیک SSL بکار می رود. پورت 636 برای دریافت اتصالات LDAP SSL (LDAPS) استفاده می شود. بلوکه کردن آنها در دیوار آتش، به سیستمهایی که در پشت دیوار آتش می باشند، کمک می کند تا از این آسیب پذیری در امان باشند. به هرحال پورتهایی که در ذیل آمده اند، بیشترین بردارهای حمله می باشند. مایکروسافت توصیه می کند که همه اتصالات ورودی از اینترنت را بلوکه نماید تا مانع از استفاده حملات از سایر پورتها گردد.

تاثیر راهکار فوق: اگر پورت 443 یا 636 بلوکه گردند، سیستمهای آسیب دیده دیگر نمی توانند اتصالات خارجی SSL یا LDAPS را دریافت نمایند

- استاندارد BS7799 ، راهکاری اجتناب ناپذیر

پیشرفت علوم کامپیوتری و درنتیجه ، پیشرفت شبکه های سخت افزاری و نرم افزاری، امکان دسترسی آسان و سریع را به منابع اشتراک گذاشته شده سازمان ها و شرکت ها پدید آورده است. سیستم های خود پرداز بانکی ، کارتهای اعتباری ، امکانات کامپیوتری بر روی تلفن های همراه و . . . همگی مثال های بارزی از تاثیر امکانات کامپیوتری بر جامعه کنونی ایران هستند. با نظر به این تحولات نکاتی نظیر خطر آشکار شدن رمز عبور، خطر ویروسی شدن سیستم ها ، ازبین رفتن اطلاعات و . . . جلوه گری خاصی می کنند.

آیا به راستی برای امنیت سازمان یا شرکت خود چه کرده اید؟ آیا پس از نابود شدن اطلاعات و یا رسوخ افراد بیگانه به سیستم اطلاعاتی سازمان و به تاراج بردن اطلاعات به یاد ایمن سازی خواهید افتاد؟ آیا فکر نمی کنید پیشگیری بهتر از درمان است؟
BS7799 استانداری مطمئن برای ایمن سازی اطلاعات شرکت شماست. این استاندارد از مدل PDCA تبعیت می کند.PDCA الگویی با چهار مرحله زیر است.

PLAN
این فاز در واقع مرحله مشخص شدن **تعاریف اولیه** پیاده سازی ISMS می باشد. تهیه سیاست های امنیتی ،مقاصد ،تعریف پردازش های مختلف درون سازمانی و روتین های عملیاتی و . . . در این مرحله تعریف و پیاده سازی می شوند.

DO
پیاده سازی و اجرای سیاست های امنیتی ،کنترل ها و پردازش ها در این مرحله انجام می شوند. درواقع این مرحله اجرای کلیه تعاریف فاز اول را طلب می کند.

Check
این مرحله را می توان فاز **ارزیابی** نیز نامید. در این مرحله ارزیابی موفقیت پیاده سازی سیاست های مختلف امنیتی، همچنین تجربه های عملی و گزارش های مدیریتی گردآوری خواهند شد. مرور نتایج ما را در جهت پیدا کردن دیدی بهتر رهنمون می سازد.

ACT
اجرای موارد ترمیمی و بازنگری در نحوه مدیریت اطلاعات،همچنین **تصحیح** موارد مختلف در این فاز انجام می شود.

پس از پایان عملیات فاز چهار دوباره به فاز اول یعنی مرحله PLAN بازگشته و با تعریف سیاستهای جدید مورد نیاز مراحل بعدی را پی می گیریم. باتوجه به تعریفی که در بالا ملاحظه می شود عملیات فوق پروسه ای چرخشی و پویا می باشد که با تغییرات درون سازمانی امکان تصحیح در مدیریت اطلاعات همواره وجود دارد.

ISMS چیست؟
سیستم مدیریت امنیت اطلاعات یا Information Security Management System سیستمی برای پیاده سازی کنترل های امنیتی می باشد که با برقراری زیرساخت های مورد نیاز ایمنی اطلاعات را تضمین می نماید. مدل PDCA ساختاری است که در پیاده سازی ISMS بکار برده می شود و ISMS زیربنای BS7799 می باشد.

BS7799 حفاظت از اطلاعات را در سه مفهوم خاص یعنی قابل اطمینان بودن اطلاعات (Confidentiality) و صحت اطلاعات (Integrity) و در دسترس بودن اطلاعات (Availability) تعریف می کند.

Confidentiality : تنها افراد مجاز به اطلاعات دسترسی خواهند یافت.
Integrity : کامل بودن و صحت اطلاعات و روشهای پردازش اطلاعات مورد نظر هستند.
Availability : اطلاعات در صورت نیاز بطور صحیح در دسترس باید باشد.

استاندارد BS7799 دارای 10 گروه کنترلی می باشد که هرگروه شامل چندین کنترل زیرمجموعه است بنابراین در کل 127 کنترل برای داشتن سیستم مدیریت امنیت اطلاعات مدنظر قراردارد. این ده گروه کنترلی عبارتند از :

1- سیاستهای امنیتی
2- امنیت سازمان
3- کنترل و طبقه بندی دارایی ها
4- امنیت فردی
5- امنیت فیزیکی
6- مدیریت ارتباط ها
7- کنترل دسترسی ها
8- روشها و روالهای نگهداری و بهبود اطلاعات
9- مدیریت تداوم کار سازمان
10- سازگاری با موارد قانونی

در زیر چند زیرکنترل از کنترل شماره A.9.4 استاندارد BS7799 آورده شده است.زیر کنترل های مذکور تماما مربوط به اجرای موارد امنیتی مورد نیاز در شبکه های کامپیوتری می باشند.

مشخص کردن سیاست های امنیتی در استفاده از شبکه (A.9.4.1)

کاربران تنها به سرویس های مورد نیازشان در شبکه دسترسی داشته باشند و دسترسی آنها به سایر قسمت ها باید محدود و یا حتی ممنوع شود. با انجام اینکار منابع مختلف سازمان کلاسه بندی شده و سطح دسترسی افراد به این منابع تعیین می شوند.

مشخص کردن مسیرهای مختلف جهت استفاده راه دور از اطلاعات (A.9.4.2)

مسیرهای مختلف ترمینال کردن و دسترسی راه دور به سرورها نظیر خطوط Leased Line و خطوط تلفنی و . . . مشخص شده و محدودیتهای لازم بر روی آنها اعمال خواهد شد.

احراز هویت کاربران خارج از سازمان (A.9.4.3)

دسترسی کاربران خارج از سازمان توسط تعریف نام کاربری و کلمه عبور مشخص و محدود می شود لذا لیست کاربران خارج از سازمان خود را تهیه کرده و با مشخص کردن نام کاربری و کلمه عبور دسترسی آنها را محدود نمایید.

احرار هویت تعریف نام کاربر و کلمه عبور جهت دسترسی به منابع خارج سازمان(A.9.4.4)

دسترسی کاربران درون سازمان به منابع خارج سازمان نظیر سرور در یکی از شعب شرکت شما نیازمند تعیین یک سری محدودیت ها می باشد. لذا برای این منظور با مشخص کردن اینگونه منابع و تعیین افراد مجاز به آنها ایمنی اطلاعات خارج از سازمان را نیز بهبودبخشید.

حفاظت از پورت های شاخص شبکه در دستور کار قرار گیرد(A.9.4.5)

با توجه به اینکه 99٪ از شبکه ها از پروتکل TCP/IP برای ارتباطات کامپیوتری خود استفاده می کنند لزوم اعمال کنترل های امنیتی برای دسترسی به این پورت ها را در دستور خود قرار دهید . به عنوان مثال FTP یا File Transfer Protocol پروتکلی برای انتقال اطلاعات روی شبکه های کامپیوتری می باشد که از پورت های 20 و 21 استفاده می کند. اگر انتقال اطلاعات از طریق این پورت ها در سازمان شما صورت نمی گیرد و این پورت ها روی سرور شبکه شما باز می باشند اقدام به بستن این پورت ها نمایید زیرا با باز بودن اینگونه پورت ها امکان سوء استفاده از منابع سازمانتان همواره وجود دارد.

تفکیک و کلاسه کردن در شبکه (A.9.4.6)

تفکیک سرویس های مختلف اطلاعاتی ، کاربران و سیستم اطلاعات و درنتیجه آن تعیین دسترسی به هریک از گروه های اطلاعاتی و سرویس های تفکیک شده از جمله اقداماتی است که برای بهبود وضعیت ایمنی اطلاعات شبکه انجام می شود.

کنترل ارتباطهای شبکه (A.9.4.7)

امکان ارتباط کاربران به منابع به اشتراک گذارده شده شبکه کامپیوتری مستقر در سازمان با تعیین و تعریف سیاست های کنترلی دسترسی افراد و محدود کردن این دسترسی ها برای گروه های کاری مختلف از جمله اقداماتی هستند که مدنظر قرار می گیرند.

کنترل های مسیر یابی شبکه (A.9.4.8)

Routerهای مختلف در سازمان هاو تعیین مسیرهای شبکه و تبدیل آدرس های مختلف شبکه برای ایجاد ارتباط Segment ها امری روزمره و طبیعی است.با کنترل مسیرهای مختلف منتهی به منابع اطلاعاتی قادر به محدود کردن و ایجاد ایمنی بیشتر خواهید شد.

استاندارد امنیت اطلاعات BS7799 استانداردی جهانی و پویاست که با ارائه کنترل های مختلف سعی در پیاده سازی قالبی مطمئن برای شرکت ها دارد. با اجرای این کنترل ها نه تنها به شرکت خود نظم می بخشیم بلکه امنیت اطلاعات و دارایی های مختلف شرکت را برقرار خواهید ساخت.

استاندارد BS7799 پرسنل،تکنیک ها و ایده ها را ایمن خواهد ساخت.

داشتن حجم بالای اطلاعات در سازمان نیازمند پیاده سازی استانداردی مطمئن در زمینه امنیت می باشد. اهمیت این قضیه در برخی سازمان ها حساس تر می باشد. شرکت های بیمه ، بانک ها و پیمانکاران مختلف نمونه اینگونه سازمان ها هستند. همچنین شرکت های ساختمانی و شرکت های مشاوره ای نیازمند حفاظت از اطلاعات سایر سازمان ها می باشند این اطلاعات در قالب طراحی ، نقشه ها و اطلاعات عمومی و . . . هستند.

هدف اصلی و نگرش به استاندارد BS7799 در سه قالب جلوگیری ، حفاظت و ثبت اطلاعات ، خلاصه می شود. استاندارد انواع مختلف اطلاعات مربوط به سازمان، نظیر امضای الکترونیکی، اسناد مکتوب و . . . را شامل می شود اما بحث پیاده سازی سیاست کنترلی مشخص برای افراد مختلف درون سازمانی و برون سازمانی از اهمیت بالاتری برخوردار است. نحوه اطمینان به پرسنل و روالهای مختلف برای برخورد با افرادی که از شرکت می روند شامل این استاندارد می شود.

BS7799 نتیجه تلاش برای رسیدن به یک قالب مشترک امنیتی جهت شرکت های مختلف با زمینه کاری مختلف می باشد.امروزه استاندارد ISO راهنمایی خاص را برای رسیدن به این منظور به نام ISO/IEC 17799:2000 ارائه داده است که در واقع تمرینی جدی و عالی برای پیاده سازی امنیت اطلاعات می باشد.این رهنمودها با دقت خاصی در استاندارد BS7799-2:2002 گردآوری شده است که نتیجه پیاده سازی آن اخذ گواهینامه امنیت اطلاعات می باشد. پیاده سازی این استاندارد سبب خواهد شد تا امکان سوء استفاده از اطلاعات ، ازبین رفتن آن و سایر خطرات به حداقل برسد.

امنیت اطلاعات برای جلوگیری از دسترسی های غیر مجاز به اطلاعات ایجاد شده است. BS7799 حفاظت از اطلاعات را در سه مفهوم خاص یعنی قابل اطمینان بودن اطلاعات (Confidentiality) و صحت اطلاعات (Integrity) و در دسترس بودن اطلاعات (Availability) تعریف می کند.

Confidentiality : تنها افراد مجاز به اطلاعات دسترسی خواهند یافت.

Integrity : کامل بودن و صحت اطلاعات و روشهای پردازش اطلاعات مورد نظر هستند.

Availability : اطلاعات در صورت نیاز بطور صحیح در دسترس باید باشد.

در زیر چند کنترل امنیتی مؤثر مدون در استاندارد BS7799 مورد بحث و بررسی قرار خواهد گرفت.

A.8.6 امنیت ابزارهای انتقال اطلاعات

برای جلوگیری از آسیب دیدگی دارایی ها و حفاظت از اطلاعات ابزارهای انتقال اطلاعات نظیر کامپیوتر ها ، فلاپی دیسک ها ، CD ها و . . . کنترلهای زیر در مستندات BS7799 گنجانده شده است.

***مدیریت ابزارهای انتقال اطلاعات (کنترل A.8.6.1)**

کلیه ابزارهای انتقال اطلاعات نظیر Tape ها ، فلاپی دیسکت ها ، نسخه های پرینت گرفته شده اطلاعات و . . . نیاز به حفاظت و کنترل دارند. داشتن جداولی از این ابزارها ، مشخص کردن نوع اطلاعات روی آنها و همچنین اشخاص مجاز به دسترسی به آن امری لازم است. همچنین محل نگهداری این ابزارها و ایجاد شرایط محیطی امن و کنترل شده باید در دستور کار قرار گیرد.

***ازرده خارج کردن اطلاعات (کنترل A.8.6.2)**

در صورتیکه که نیاز به اطلاعات روی ابزار انتقال ندارید نگه داری و امنیت آن کاری دشوار و بیهوده می باشد لذا اقدام به از بین بردن اطلاعات روی آنها نمائید. بطور مثال با هفت بار فرمت هارددیسک و یا با شکستن CD حاوی اطلاعات قدیمی و بدون مصرف قادر به از بین بردن اینگونه اطلاعات خواهید شد.

***امنیت اطلاعات در هنگام حمل (کنترل A.8.6.3)**

برای جلوگیری از سوء استفاده از اطلاعات و همچنین کاهش ریسک نیاز به تعریف و ایجاد سیاست های امنیتی در هنگام حمل اطلاعات هستید.لذا با زدن برچسب روی ابزارهای انتقال اطلاعات و همچنین مشخص کردن مبدا و مقصد و نیز افراد مجاز به دسترسی قادر به ایجاد امنیت و کنترل اطلاعات خواهید شد.

***امنیت اطلاعات سیستم (کنترل A.8.6.4)**

باتوجه به تنوع اطلاعات در شرکت و وجود شبکه های کامپیوتری امکان دسترسی افراد مختلف به اطلاعات وجود دارد. لذا با دسته بندی اطلاعات و تعریف حق دسترسی افراد امنیت اطلاعات خود را بیش از پیش خواهید کرد.

A.8.7 رد و بدل کردن اطلاعات و نرم افزار بین شرکتهای مختلف

برای جلوگیری از تغییرات ، ازبین رفتن و سوءاستفاده از اطلاعات زمانیکه بین شرکت ها ردوبدل می شوند نیاز به ایجاد سیاستهای کنترلی می باشد.

***قرارداد انتقال اطلاعات بین شرکت ها (A.8.7.1)**

برای جلوگیری از سوء استفاده اطلاعات در هنگام ردوبدل شدن آنها بین شرکتها و تعیین حریم استفاده از آنها توسط شرکت مقصد نیاز به عقد قرارداد بین شرکت مبدا و مقصد اطلاعات می باشد.

***امنیت اطلاعات در ترانزیت (A.8.7.2)**

همانطور که در کنترل های قبلی اشاره شد امنیت اطلاعات در هنگام انتقال اطلاعات از شرکت مبدا به شرکت مقصد و تعیین دسترسی افراد مختلف به آن امری ضروری است.

***امنیت تجارت الکترونیک (A.8.7.3)**

فعالیت های مختلف تجارت الکترونیکی نیازمند تدارک یک سری سیاست های امنیتی و پیاده سازی این سیاستها می باشد. نکات مختلف نظیر جلوگیری از فعالیت افراد تبهکار، حق تغییر اطلاعات،امضای الکترونیکی و . . . باید درنظر گرفته شوند.

***امنیت نامه های الکترونیکی یا e-mail (A.8.7.4)**

سیاست های خاصی برای جلوگیری از سوءاستفاده افراد غیر مجاز برای استفاده از نامه های الکترونیکی باید تدوین شوند.ایجاد ایمیل شخصی برای افراد مختلف و آموزش صحیح آنها برای استفاده از ایمیلو همچنین آشنایی آنها با مفاهیم مختلف ایمیل از جمله وظایفی است که مدیر شبکه در دستور کار خود قرار می دهد.

***امنیت سیستم های موجود در شرکت (A.8.7.5)**

برای استفاده صحیح از دستگاه های مختلف داخل شرکت نیاز به تعریف سیاست های مختلف و کتابچه های راهنما می اشد. کامپیوتر های مختلف در سازمان ، دستگاههای فکس و . . . از جمله امکاناتی است که در حین ساده کردن کارها نقاط استراتژیک اطلاعاتی هستند.

***صحت اطلاعات (A.8.7.6)**

برای رسیدن به اطلاعاتی کارساز و مفید نیاز به پردازش روی اطلاعات خام و اولیه می باشد.حفاظت از این اطلاعات خام گردآوری شده کاری بسیار مهم می باشد که باید در دستور کار قرارگیرد. نتیجه گیری درست از اطلاعات اولیه غلط بسیار بعید می نماید.

***مبادله سایر فرم های اطلاعات(A.8.7.7)**

برای سایر اشکال اطلاعات در شرکت ایجاد سیاست های حفاظتی امری ضروری می باشد. ابزارهای صوتی و ارتباطات ویدئویی از جمله این اشکال هستند.

کنترل های بالا تنها بخشی از 127 کنترل مدون در استاندارد BS7799 می باشد که اجرای آنها شما را چند قدم به ایجاد امنیت واقعی نزدیک تر می سازد. درست است که امنیت 100٪ اطلاعات کاری دشوار است ولی نزدیک تر شدن به آن نیازمند کمی تلاش و مدیریت می باشد.

به وجود آمدن خطوط پرسرعت اینترنتی و دسترسی آسان تر به این شاهراه اطلاعاتی توسط خطوط Leased و همچنین ارزان شدن تکنولوژی مبتنی بر ارتباط بی سیم ، شرکت ها و سازمان ها را به تدریج مجبور به رعایت نکات مربوط به ایمنی اطلاعات و نیز نصب انواع IDS، FireWall و همچنین HoneyPot ساخته است. دراین راستا داشتن سیاست امنیتی مؤثر و ایجاد روالهای درست امری اجتناب ناپذیر می نماید.

برای داشتن سازمانی با برنامه و ایده آل ، هدفمند کردن این تلاش ها برای رسیدن به حداکثر ایمنی امری است که باید مدنظر قرار گیرد.

استاندارد BS7799 راهکاری است که اطلاعات سازمان و شرکت را دسته بندی و ارزش گذاری کرده و با ایجاد سیاستهای متناسب با سازمان و همچنین پیاده سازی 127 کنترل مختلف، اطلاعات سازمان را ایمن می سازد. این اطلاعات نه تنها داده های کامپیوتری و اطلاعات سرور ها بلکه کلیه موارد حتی نگهبان سازمان یا شرکت رادر نظر خواهد گرفت.

آیا امنیت 100٪ امکانپذیر است؟

با پیشرفت علوم کامپیوتری و همچنین بوجود آمدن ابزارهای جدید Hack و Crack و همچنین وجود صدها مشکل ناخواسته در طراحی نرم افزارهای مختلف و روالهای امنیتی سازمان ها ، همیشه خطر حمله و دسترسی افراد غیرمجاز وجود دارد. حتی قوی ترین سایتهای موجود در دنیا در معرض خطر افراد غیرمجاز و سودجو قرار دارند. ولی آیا چون نمی توان امنیت 100٪ داشت باید به نکات امنیتی و ایجاد سیاستهای مختلف امنیتی بی توجه بود؟

فوائد استاندارد BS7799 و لزوم پیاده سازی

استاندارد BS7799 قالبی مطمئن برای داشتن یک سیستم مورد اطمینان امنیتی می باشد. در زیر به تعدادی از فوائد پیاده سازی این استاندارد 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

مراحل ایجاد سیستم مدیریت امنیت اطلاعات (ISMS)

ایجاد و تعریف سیاست ها:

در این مرحله ایجاد سیاستهای کلی سازمان مدنظر قراردارد. روالها از درون فعالیت شرکت یا سازمان استخراج شده و در قالب سند و سیاست امنیتی به شرکت ارائه می شود. مدیران کلیدی و کارشناسان برنامه ریز نقش کلیدی در گردآوری این سند خواهند داشت.

تعیین محدوده عملیاتی :

یک سازمان ممکن است دارای چندین زیرمجموعه و شاخه های کاری باشد لذا شروع پیاده سازی سیستم امنیت اطلاعات کاری بس دشوار است . برای جلوگیری از پیچیدگی پیاده سازی ، تعریف محدوده و Scope صورت می پذیرد. Scope می تواند ساختمان مرکزی یک سازمان یا بخش اداری و یا حتی سایت کامپیوتری سازمان باشد. بنابراین قدم اول تعیین Scope و الویت برای پیاده سازی استاندارد امنیت اطلاعات در Scope خواهد بود. پس از پیاده سازی و اجرای کنترل های BS7799 و اخذ گواهینامه برای محدوده تعیین شده نوبت به پیاده سازی آن در سایر قسمت ها می رسد که مرحله به مرحله اجرا خواهند شد.

برآورد دارایی ها و طبقه بندی آنها:

برای اینکه بتوان کنترل های مناسب را برای قسمت های مختلف سازمان اعمال کرد ابتدا نیاز به تعیین دارایی ها می باشیم. در واقع ابتدا باید تعیین کرد چه داریم و سپس اقدام به ایمن سازی آن نماییم. در این مرحله لیست کلیه تجهیزات و دارایی های سازمان تهیه شده و باتوجه به درجه اهمیت آن طبقه بندی خواهند شد.

ارزیابی خطرات:

با داشتن لیست دارایی ها و اهمیت آن ها برای سازمان ، نسبت به پیش بینی خطرات اقدام کنید. پس از تعیین کلیه خطرات برای هر دارایی اقدام به تشخیص نقاط ضعف امنیتی و دلایل بوجود آمدن تهدیدها نمایید و سپس با داشتن اطلاعات نقاط ضعف را برطرف سازید و خطرات و تهدیدها و نقاط ضعف را مستند نمایید.

مدیریت خطرات :

مستندات مربوط به خطرات و تهدید ها و همچنین نقاط ضعف امنیتی شما را قادر به اتخاذ تصمیم درست و مؤثر برای مقابله با آنها می نماید.

انتخاب کنترل مناسب :

استاندارد BS7799 دارای 10 گروه کنترلی می باشد که هرگروه شامل چندین کنترل زیرمجموعه است بنابراین در کل 127 کنترل برای داشتن سیستم مدیریت امنیت اطلاعات مدنظر قراردارد. با انجام مراحل بالا شرکت یا سازمان شما پتانسیل پیاده سازی کنترل های مذکور را خواهد داشت.

این ده گروه کنترلی عبارتند از :

1- سیاستهای امنیتی
2- امنیت سازمان
3- کنترل و طبقه بندی دارایی ها
4- امنیت فردی
5- امنیت فیزیکی
6- مدیریت ارتباط ها
7- کنترل دسترسی ها
8- روشها و روالهای نگهداری و بهبود اطلاعات
9- مدیریت تداوم کار سازمان
10- سازگاری با موارد قانونی

تعیین قابلیت اجرا:

جمع آوری لیست دارایی ها، تعیین تهدیدها ، نقاط ضعف امنیتی و در نهایت ایجاد جدول کنترل ها مارا در به دست آوردن جدولی موسوم به SOA یا Statement Of Applicability یاری می رساند. این جدول لیستی نهایی از کلیه کنترل های مورد نیاز برای پیاده سازی را ارائه می دهد. با مطالعه این جدول و مشخص کردن کنترل های قابل اجرا و اعمال آنها ،سازمان یا شرکت خودرا برای اخذ استاندارد BS7799 آماده خواهید ساخت.

نتیجه آنکه برای رسیدن به یک قالب درست امنیتی ناچار به استفاده از روال های صحیح کاری و همچنین پیاده سازی استاندارد امنیت هستیم و استاندارد BS ISO/IEC 17799:2000 انتخابی درست برای رسیدن به این منظور می باشد.

آیا دارایی های سازمان شما مورد ارزیابی قرار می گیرند؟

BS7799 استانداردی است که شما را قادر به ارزیابی اطلاعات و محافظت از آن می کند در واقع اطلاعات ، کلید موفقیت و رشد هر سازمانی است.

امروزه اطلاعات مهمترین دارایی هرسازمانی می باشد که نظیر سایر وسایل موجود در سازمان دارای ارزش بوده و درنتیجه باید بطور مناسب حفاظت گردد.
دسترسی غیرمجاز و رخنه به اطلاعات روی دیسک ها ، کامپیوترها و استفاده غیرمجاز از آنها تبدیل به معضل شده است و این دسترسی توسط کارمندان یک سازمان،کاربران اینترنت و یا توسط عوامل دیگر صورت می گیرند لذا سازمان ها و شرکت ها ناگزیر به دنبال پیاده سازی موارد امنیتی می باشند.
برای پیاده سازی امنیت تنها توجه به مسائل تکنیکی کافی نیست بلکه ایجاد سیاستهای کنترلی و استاندارد کردن آن و همچنین ایجاد روالهای صحیح درصد امنیت اطلاعات را بالا خواهد برد.

فوائد اجرا و گرفتن گواهینامه BS7799 به شرح زیرمی باشد:

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.

استاندارد BS7799 پرسنل،تکنیک ها و ایده ها را ایمن خواهد ساخت.

امروزه داشتن حجم بالای اطلاعات در سازمان نیازمند پیاده سازی استاندارد مناسب در زمینه امنیت می باشد. اهمیت این قضیه در برخی سازمان ها حساس تر می باشد. شرکت های بیمه ، بانک ها و پیمانکاران مختلف نمونه اینگونه سازمان ها هستند. همچنین شرکت های ساختمانی و شرکت های مشاوره ای نیازمند حفاظت از اطلاعات خود و یا بهتر بگوییم اطلاعات سایر سازمان ها می باشند این اطلاعات در قالب طراحی ، نقشه ها و اطلاعات عمومی و . . . هستند. هدف اصلی و نگرش به استاندارد BS7799 در سه قالب جلوگیری ، حفاظت و ثبت اطلاعات می باشد. استاندارد انواع مختلف اطلاعات مربوط به سازمان نظیر امضای الکترونیکی، اسناد مکتوب و . . . را شامل می شود اما بحث پیاده سازی سیاست کنترلی مشخص برای افراد مختلف درون سازمانی و برون سازمانی از اهمیت بالاتری برخوردار است. نحوه اطمینان به پرسنل و روالهای مختلف برای برخورد با افرادی که از شرکت می روند شامل این استاندارد می شود.
BS7799 نتیجه تلاش برای رسیدن به یک قالب مشترک پیاده سازی استاندارد امنیت برای سازمان های مختلف با زمینه کاری مختلف می باشد. امروزه استاندارد ISO راهنمایی خاص را برای رسیدن به این منظور به نام ISO/IEC 17799:2000 ارائه داده است که در واقع تمرینی جدی و عالی برای پیاده سازی امنیت اطلاعات می باشد. این رهنمودها با دقت خاصی در استاندارد BS7799-2:2002 گردآوری شده است که نتیجه پیاده سازی آن اخذ گواهینامه امنیت اطلاعات می باشد. پیاده سازی این استاندارد سبب خواهد شد تا امکان سوء استفاده از اطلاعات ، ازبین رفتن آن و سایر خطرات به حداقل برسد.امنیت اطلاعات برای جلوگیری از دسترسی های غیر مجاز به اطلاعات ایجاد شده است. BS7799 حفاظت از اطلاعات را در سه مفهوم خاص یعنی قابل اطمینان بودن اطلاعات (Confidentiality) ، صحت اطلاعات (Integrity) و در دسترس بودن اطلاعات (Availability) تعریف می نماید.

Confidentiality : تنها افراد مجاز ، به اطلاعات دسترسی خواهند یافت.

Integrity : کامل بودن ، صحت اطلاعات و روشهای پردازش اطلاعات مورد نظر هستند.
Availability : اطلاعات در صورت نیاز بطور صحیح در دسترس باید باشد.

ISO/IEC 17799 Information Technology-Code of practice for information security

کنترلهای زیر موارد پایه ای برای پیاده سازی سیستم امنیت اطلاعات هستند:

1- سیاستهای امنیتی
2- امنیت سازمان
3- کنترل و طبقه بندی دارایی ها
4- امنیت فردی
5- امنیت فیزیکی
6- مدیریت ارتباط ها
7- کنترل دسترسی ها
8- روشها و روالهای نگهداری و بهبود اطلاعات
9- مدیریت تداوم کار سازمان
10- سازگاری با موارد قانونی

BS7799-2:2002 ISMS-Specification with guidance for use

هدف اصلی و اولیه سیستم مدیریت امنیت اطلاعات حفاظت از اطلاعات می باشد. ساختار این پردازش بر پایه رده بندی دارایی های سازمان و درجه اهمیت آن ها بنا نهاده شده است. این دارایی ها ممکن است امضای الکترونیکی ، اسناد مکتوب و یا دارایی های فیزیکی نظیر کامپیوترها و شبکه و یا هرچیز با ارزش دیگری باشد. دراین تعریف حتی افراد مختلف سازمان هم دارایی محسوب می شوند.

تصویر بالا وظایف اصلی و پایه ای را در ISMS یا سیستم مدیریت امنیت اطلاعات نشان می دهد.با دقت در این عکس پویا بودن این سیستم کاملا مشهود است.
BS7799-2002 شامل لیستی از کنترل ها می باشد که نیاز واقعی سازمان به داستن استانداردی کامل و پویا را برطرف می کند.

مراحل اخذ گواهینامه امنیت اطلاعات

سیستم ISMS برای هر سازمان و شرکت برپایه خطرات مختلف محتمل در آن شرکت پیاده سازی می شود که نیازمند به بازرسی های مداوم توسط شخص خبره و آشنا به مفاهیم استانداردBS7799 دارد.پس از پیاده سازی و بازرسی های دقیق برای اجرای بدون نقص 127 کنترل مصوب در استاندارد شخص گواهی دهنده (Certification Body) جهت بازرسی نهایی و تعیین صلاحیت برای دادن گواهینامه امنیت مراجعه کرده و سازمان را مورد ارزیابی دقیق قرار می دهد.برای گرفتن گواهینامه اجرای دقیق کلیه کنترل هایی که قابل پیاده سازی هستند نیاز است.

ISMS سیستم مدیریتی کامل و مجتمع می باشد.

این استاندارد در ردیف ISO 9001:2000 و ISO 14001:1996 برای پشتیبانی و نظارت در صحت اجرا و پیاده سازی می باشد.

چه کسی قادر به گرفتن این گواهینامه است؟

این استاندارد به سازمان ها ، اداره ها ، سایت ها و کلیه زیرمجموعه های اداری قابل اعطاء می باشد. سازمان ها با اندازه هاو پیچیدگی های مختلف قادر هستند با پیاده سازی این کنترل ها گواهینامه معتبر و بین المللی BS7799 اخذ کنند.