استراتژی حفاظت از اطلاعات

در شبکه‌های کامپیوتری

مدیریت فناوری اطلاعات و ارتباطات

بهمن ماه ۱۳۸۵

زکاه العلم نشره

مدیران و کارشناسان گرامی

مجموعه حاضر یک برنامه استراتژیک بر مبنای استاندارد ISO17799 درباره سیستم های امنیت اطلاعات و ارتباطات است که منجر به ارائه راه حل امنیتی برای مرکز دادهای معاونت اداری و مالی شده و با پیشنهاد خرید تجهیزات لازمه در چند فاز، پوشش امنیتی کافی برای توسعه نرم افزارهای کاربردی تحت وب و ارائه خدمات دولت الکترونیک در سطح سازمان (اینترنت) فراهم میکند.

گسترش تجارت الکترونیک و فعالیتهای مالی و اداری حساس در محیط اشتراکی شبکهای مرهون توجه به اهمیت و نقش این موضوع در سازمانها و شرکتهای جهانی بوده است، در جائی که شعب و نمایندگی های شرکت مادر یا نمایندگی های سیاسی کشورها در عصر جهانی شدن مجبورند در تعاملات متعددی، فارغ از محدودیتهای جغرافیایی حضور یابند.

این طرح زیر نظر مدیریت فناوری اطلاعات و ارتباطات معاونت اداری و مالی به انجام رسیده است هر چند به رغم تلاشهای صورت گرفته،نتیجه فعالیت می تواند دچار کاستی و ضعف کارشناسی باشد. امید است برای بهبود روند فعالیتی، این مجموعه را از نظرات صائب خود مطلع فرمائید.

فصل سوم : مزایای سرمایه گذاری در امنیت اطلاعات برای سازمانها

فصل چهارم : استانداردهای جهانی امنیت اطلاعات

فصل پنجم : امنیت در شبکه های کامپیوتری

قسمت دوم : استراتژی امنیت شبکه واحد فناوری اطلاعات وارتباطات

فصل اول : Data Center واحد فناوری ارتباطات و اطلاعات

فصل دوم : افق کاری Data Center واحد فناوری اطلاعات و ارتباطات

فازبندی و ارائه راهکار ارتقاء امنیت شبکه واحد فناوری ارتباطات و اطلاعات

فاز 1

با توجه به آنچه در مورد اهمیت اطلاعات موجود بر روی سرورهای بانک اطلاعاتی حوزه انفورماتیک اداری ومالی درپی می آید و نیز با عنایت به آنچه که مفصلا در مورد نیاز به وجود دستگاههای دیواره آتش **(Firewall)** و سیستمهای تشخیص حملات برای چنین مرکز داده حساسی در سازمان- که حاوی اطلاعات جامع و محرمانه مالی، اطلاعات کامل پرسنل سازمان و ... می باشد- توضیح داده خواهد شد، در این فاز برای این مرکز داده ابتدا یک دیواره آتش نرم افزاری بر روی سرور **Linux** تدوین می گردد. این دیواره آتش کاملا **Stateful** است و قابلیتهایی نظیر **Connection Tracking** را داراست. در مرحله بعد این دیواره آتش در کنار یک دیواره آتش سخت افزاری قرار می گیرد و بار اصلی بر روی دیواره آتش سخت افزاری قرار خواهد گرفت. چرا که چنین فایروالی دارای خاصیت **Content Filtering** می باشد و در لایه **Application** قابلیت فیلترینگ دارد. ضمن اینکه امکان ایجاد ارتباطات **SSL VPN** را برای وجود ارتباطی امن با کیفیت عالی فراهم می سازد. با توجه به نیاز مبرم به وجود چنین دستگاه **Firewall** سخت افزاری که فراهم کننده کلیه نیاز های لازم برای مرکز داده واحد است ، مشخصات دستگاه مطلوب برای نیل به چنین مقصودی در ذیل می آید:

Major Information		
Product Name	Product Part Number	Model
Cisco ASA 5540 Firewall	ASA5540-AIP20-K9	IPS Edition

Product Details	
Security License	Concurrent sessions
3DES/AES license	400000
Users/Nodes	Firewall Throughput
Unlimited	650 Mbps
VLANs	Network ports
200	4 Gigabit Ethernet, 1Fast Ethernet
Security contexts	High Availability
2 (Up to 50)	Active/Active, Active/Standby
IPsec VPN peers	SSL VPN peers
5000	2 (Up to2500)

Technical Specifications		
Memory	Minimum system flash	System bus
1024 MB	64 MB	Multibus architecture

Major Information	
Product Name	Product Part Number
500 SSL Vpn Users License	ASA5500-SSL-500

لازم به ذکر است دستگاه مزبورپس از راه اندازی و پیکر بندی کاملا دقیق، حاوی راه حلی جامع جهت برقراری اِمنیت در شبکه ها می باشد بدین ترتیب که در عین حال که یک دستگاه حرفه ای دیواره آتش می باشد و بصورت کاملا دقیق کنترل کننده ترافیک ورودی به شبکه داخلی و نحوه دسترسی به ناحیه ها و حوزه های مختلف کاری (مانند ناحیه DMZ و ...) خواهد بود، همزمان با پیکر بندی صحیح دارای بهترین نوع سیستمهای تشخیص و دفع حملات خواهد شد، که با شناسایی درست و به موقع حملات ورودی به شبکه؛ می تواند نسبت به ارسال اخطار و عملکرد مناسب جهت خنثی سازی آنها اقدام نماید.

لازم به ذکر است این سیستم پس از راه اندازی و پیکر بندی مناسب دارای کمترین اشتباه ممکن در مورد تشخیص اِینکه ترافیک ورودی به شبکه، حاوی جریان سالمی از اطلاعات ویا نوعی حمله می باشد خواهد بود و با قرار گرفتن مداوم الگو های بروز شده برای تشخیص حملات جدید بر روی دستگاه، می تواند نسبت به دفع کد های مخرب جدید و حملات تازه، موثر اقدام نماید.

ضمنا همانطور که در صورت سفارش ذکر گردیده است، با تهیه مجوز لازم از شرکت سازنده، می توان سرویس امنیتی و بسیار مهم SSL VPN را برای ایمنی اتصال به سرورهای WEB مرکز داده سازمان، بر روی این دستگاه راه اندازی نمود. با بکارگیری این روش انتقال داده ما بین سرورهای WEB مجموعه و سیستم کاربردارای امنیت کامل خواهد شد چراکه ابتدا اطلاعات رمز نگاری شده سپس انتقال داده می شوند و سپس در مقصد رمز گشوده شده و اطلاعات قابل دریافت خواهند بود. بنابر این به کمک این مکانیزم مسیر رفت و آمد اطلاعات ایمن خواهد شد.

فاز 2

در آینده در صورت افزایش تعداد کاربران شبکه داخلی حوزه انفورماتیک، نیاز به نسخه کاملی از یک سرور Antivirus **وجود خواهد داشت:**

Major Information	
Product Name	Product Detail
Symantec Antivirus Server	100 Users License Corporate Edition

فاز 3

در این فاز با توجه به اهمیت Redundancy و وجود تجهیزات Back up در مرکز داده سازمان، با سفارش دومین دیواره آتش، این وسیله نه تنها به صورت Back up عمل خواهد کرد، بلکه بصورت همزمان می توان امکان ایجاد Load Balancing را در هر دو وسیله داشته باشیم و با جریان ترافیک ورودی بر روی هر دو دستگاه ، این امکان بوجود می آید که احیانا در صورت وجود حجم بسیار زیاد و بالای ترافیک ورودی در آینده، بدون کوچکترین مشکلی دستگاهها به کار خود ادامه دهند.

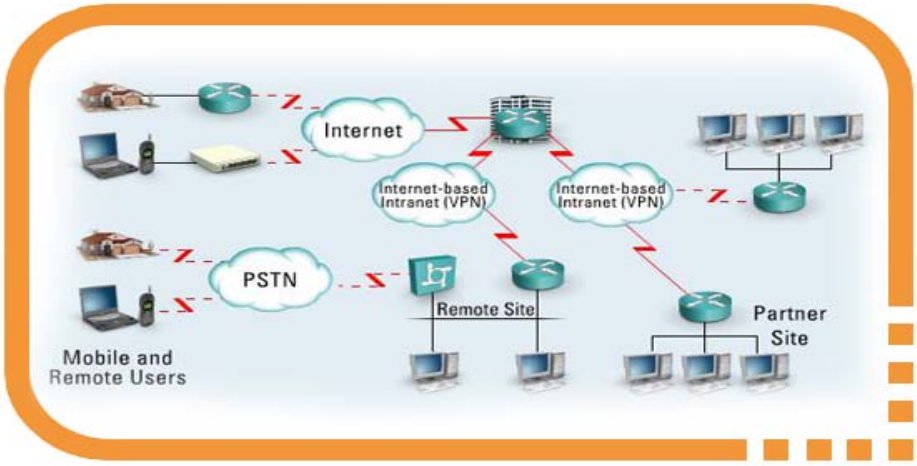
Major Information		
Product Name	Product Part Number	Model
Cisco ASA 5540 Firewall	ASA5540-AIP20-K9	IPS Edition

Product Details	
Security License	Concurrent sessions
3DES/AES license	400000
Users/Nodes	Firewall Throughput
Unlimited	650 Mbps
VLANs	Network ports
200	4 Gigabit Ethernet, 1Fast Ethernet
Security contexts	High Availability
2 (Up to 50)	Active/Active, Active/Standby
IPsec VPN peers	SSL VPN peers
5000	2 (Up to2500)

Technical Specifications		
Memory	Minimum system flash	System bus
1024 MB	64 MB	Multibus architecture

فصل اول : امنیت اطلاعات به چه منظور ؟

1_ 1 مقدمه



اطلاعات در سازمان ها و موسسات مدرن، بمنزله شاهرگ حیاتی محسوب می گردد. دستیابی به اطلاعات وعرضه مناسب و سریع آن، همواره مورد توجه سازمان هائی است که اطلاعات در آنها دارای نقشی محوری و سرنوشت ساز است. سازمان ها و موسسات می بایست یک زیر ساخت مناسب اطلاعاتی را برای خود ایجاد و در جهت انظباط اطلاعاتی در سازمان خود حرکت نمایند. اگر می خواهیم ارائه دهنده اطلاعات در عصر اطلاعات بوده و صرفا" مصرف کننده اطلاعات نباشیم، در مرحله نخست می بایست فرآیندهای تولید، عرضه و استفاده از اطلاعات را در سازمان خود قانونمد نموده و در مراحل بعد، امکان استفاده از اطلاعات ذیربط را برای متقاضیان (محلی، جهانی) در سریعترین زمان ممکن فراهم نمائیم . سرعت در تولید و عرضه اطلاعات ارزشمند، یکی از رموز موفقیت سازمان ها و موسسات در عصر اطلاعات است. پس از ایجاد انظباط اطلاعاتی، می بایست با بهره گیری از شبکه های کامپیوتری زمینه استفاده قانومند و هدفمند از اطلاعات را برای سایرین فراهم کرد. اطلاعات ارائه شده می تواند بصورت محلی (اینترانت) و یا جهانی(اینترنت) مورد استفاده قرار گیرد. فراموش نکنیم در این هنگامه اطلاعاتی، مصرف کنندگان اطلاعات دارای حق مسلم انتخاب می باشند و در صورتیکه سازمان و یا موسسه ای در ارائه اطلاعات سهوا" و یا تعمدا" دچار اختلال و یا مشکل گردد، دلیلی بر توقف عملکرد مصرف کنندگان اطلاعات تا بر طرف نمودن مشکل ما، وجود نخواهد داشت.

سازمان ها و موسسات می بایست خود را برای نبردی سخت در عرضه و ارائـه اطلاعـات آمـاده نمایند و در این راستا علاوه بر پتانسیل های سخت افزاری و نرم افزاری استفاده شده ، از تـدبیر و دوراندیشی فاصله نگیرند. در میدان عرضه و ارائه اطلاعات ، کسب موفقیت نه بدلیل ضعف دیگران بلکه بر توانمندی ما استوار خواهد بود.

مصرف کنندگان اطلاعات، قطعا" ارائه دهنـدگان اطلاعـاتی را برمـی گزینـد کـه نـسبت بـه تـوان و پتانسیل آنان اطمینان حاصل کرده باشند. آیا سازمان ما در عصر اطلاعات بـه پتانـسیل هـای لازم در این خصوص دست پیدا کرده است ؟ آیا در سازمان ما بستر و ساختار مناسب اطلاعاتی ایجـاد شده است ؟ آیا گردش امور در سازمان ما مبتنی بر یک سیستم اطلاعاتی مدرن است ؟ آیا سازمان ما قادر به تعامل اطلاعاتی با سایر سازمان ها است ؟ آیا در سازمان ما نقـاط تمـاس اطلاعـاتی بـا دنیای خارج از سازمان تدوین شده است ؟ آیا فاصله تولید و استفاده از اطلاعـات در سـازمان مـا به حداقل مقدار خود رسیده است ؟ آیا اطلاعات قابل عرضه سازمان ما، در سریعترین زمـان و بـا کیفیتی مناسب در اختیارمصرف کنندگان متقاضی قرار می گیرد ؟ حضور یک سـازمان در عرصـه جهانی، صرفا" داشتن یک وب سایت با اطلاعات ایستا نخواهد بود. امروزه میلیون ها وب سایت بر روی اینترنت وجود داشته که هر روز نیز به تعداد آنان افزوده مـی گـردد. کـاربران اینترنـت بـرای پذیرش سایت سازمان ما، دلایل موجه ای را دنبال خواهند کرد. در این هنگامه سـایت داشـتن و راه اندازی سایت، اصل موضوع که همانا ایجاد یک سـازمان مـدرن اطلاعـاتی اسـت، فرامـوش نگـردد. سازمان ما در این راستا چگونه حرکت کرده و مختصات آن در نقشه اطلاعاتی یک سازمان مـدرن چیست؟

بدیهی است ارائه دهندگان اطلاعات خود در سطوحی دیگر به مـصرف کننـدگان اطلاعـات تبـدیل و مصرف کنندگان اطلاعات، در حالات دیگر، خـود مـی توانـد بعنـوان ارائـه دهنـده اطلاعـات مطـرح گردند. مصرف بهینه و هدفمند اطلاعات در صورتیکه به افزایش آگاهی، تولید و ارائه اطلاعات خـتم شود، امری بسیار پسندیده خواهد بود. در غیر اینصورت، مصرف مطلق و همیشگی اطلاعات بدون جهت گیری خاص، بدترین نوع استفاده از اطلاعات بوده که قطعا" به سرانجام مطلوبی ختم نخواهد شد.

1_2 اهمیت امنیت اطلاعات و ایمن سازی کامپیوترها

حجم تولید اطلاعات در سطح جهان روندی کاملا" تصاعدی و شگفت انگیز را طی می نماید. استفاده از اطلاعات در صورتیکه به تولید و ارائه دانش و دانائی منتهی گردد، می تواند دستاوردهای مثبتی را برای یک جامعه بدنبال داشته باشد، درغیراینصورت فقط سرمایه ها ی ملی که مهمترین آن عنصر زمان است را ازدست خواهیم داد .یکی از ویژگی های مهم عصر اطلاعات، میزان تولید، ذخیره سازی و نشر اطلاعات در جهان است. اکثر کارشناسان و متخصصین فنآوری اطلاعات بر این باور می باشند که در عصر حاضر ما با اقیانوسی از اطلاعات مواجه بوده و می بایست در عوض پرتاب نمودن خود به درون این اقیانوس با نحوه شنا کردن درون آن آشنا شویم. با توجه به میزان رشد سی درصدی اطلاعات ذخیره شده در هر سال، ما شاهد تغییرات اساسی در اکولوژی انسانی می باشیم. همه چیز عمومی بوده و همه چیز در حال ثبت و ضبط است. سازمان ها و موسسات، نیازمند مدیریت هوشمندانه در امنیت اطلاعات می باشند.

تمامی کامپیوترها از کامپیوترهای موجود در منازل تا کامپیوترهای موجود در سازمان ها و موسسات بزرگ، در معرض آسیب و تهدیدات امنیتی می باشند .با انجام تدابیر لازم و استفاده از برخی روش های ساده می توان پیشگیری لازم و اولیه ای را خصوص ایمن سازی محیط کامپیوتری خود انجام داد. علیرغم تمامی مزایا و دستاوردهای اینترنت، این شبکه عظیم به همراه فن آوری های مربوطه، دریچه ای را در مقابل تعداد زیادی از تهدیدات امنیتی برای تمامی استفاده کنندگان (افراد ، خانواده ها، سازمان ها، موسسات و ..) گشوده است.

با توجه به ماهیت حملات، می بایست در انتظار نتایج نامطلوب متفاوتی بود(از مشکلات و مزاحمت های اندک تا از کار انداختن سرویس ها و خدمات).در معرض آسیب قرار گرفتن داده ها و اطلاعات حساس، تجاوز به حریم خصوصی کاربران، استفاده از کامپیوتر کاربران برای تهاجم بر علیه سایر کامپیوترها، از جمله اهداف مهاجمانی است که با بهره گیری از آخرین فن آوری های موجود ، حملات خود را سازماندهی و بالفعل می نمایند. بنابراین، می بایست به موضوع امنیت اطلاعات، ایمن سازی کامپیوترها و شبکه های کامپیوتری، توجه جدی شده و از فرآیندهای متفاوتی در جهت مقاوم سازی آنان، استفاده گردد.

3_1 ضرورت توجه به امنیت اطلاعات

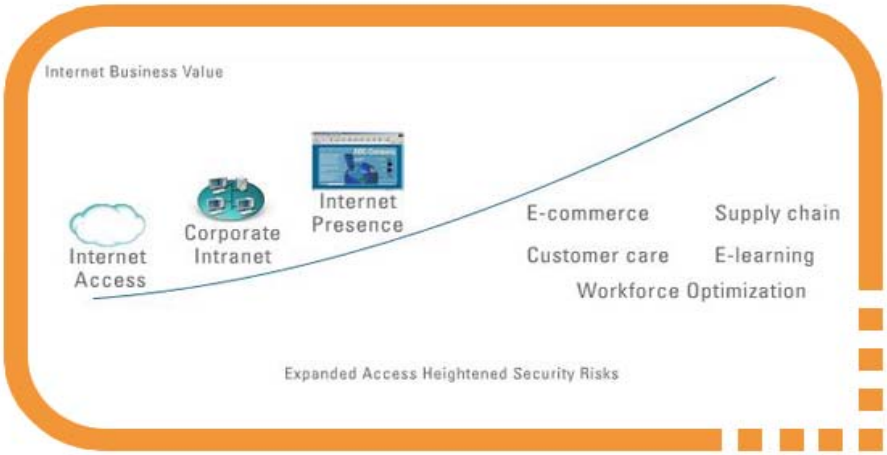
فن آوری اطلاعات دارای یک نقش حیاتی و تعیین کننده در اکثر سازمان های مدرن اطلاعاتی است. امروزه زیرساخت فن آوری اطلاعات سازمان ها در محیطی قرار گرفته اند که بطور فزاینده بر تعداد دشمنان و مهاجمانی که علاقه مند به حضور مستمر، مطمئن و سودمند سیستم های کامپیوتری نمی باشد، افزوده می گردد. حملات سیری کاملا" صعودی را داشته و متاسفانه اغلب سازمان ها قادر به واکنش مناسب در مقابل تهدیدات امنیتی جدید در زمان مطلوب و قبل از سوء استفاده از سیستم های کامپیوتر خود نمی باشد. کاهش مدت زمان لازم به منظور برخورد با تهدیدات امنیتی و افزایش بهره وری، از جمله خواسته های مشترک سازمان ها و کاربران می باشد. به منظور برخورد مناسب و ساخت یافته با تهدیدات امنیتی، "مدیریت خطرات امنیتی " و یا مدیریت ریسک امنیتی به یکی از نیازهای اولیه و اساسی مراکز فن آوری اطلاعات تبدیل شده است.

4_1 ایمن سازی اطلاعات

توفیق در ایمن سازی اطلاعات منوط به حفاظت از اطلاعات و سیستم های اطلاعاتی در مقابل حملات است. بدین منظور از سرویس های امنیتی متعددی استفاده می گردد. سرویس های انتخابی، می بایست پتانسیل لازم در خصوص ایجاد یک سیستم حفاظتی مناسب، تشخیص بموقع حملات و واکنش سریع را داشته باشند. بنابراین می توان محور استراتژی انتخابی را بر سه مولفه حفاظت، تشخیص و واکنش استوار نمود. حفاظت مطمئن، تشخیص بموقع و واکنش مناسب از جمله مواردی است که می بایست همواره در ایجاد یک سیستم امنیتی رعایت گردد. سازمان ها و موسسات، علاوه بر یکپارچگی بین مکانیزم های حفاظتی، می بایست همواره انتظار حملات اطلاعاتی را داشته و لازم است خود را به ابزارهای تشخیص و روتین های واکنش سریع، مجهز تا زمینه برخورد مناسب با مهاجمان و بازیافت اطلاعات در زمان مناسب فراهم گردد. یکی از اصول مهم استراتژی"دفاع در عمق"، برقراری توازن بین سه عنصر اساسی، انسان، تکنولوژی و عملیات، است. حرکت بسمت تکنولوژی اطلاعات بدون افراد آموزش دیده و روتین های عملیاتی که راهنمای آنان در نحوه استفاده وایمن سازی اطلاعات باشد، محقق نخواهد شد.

فصل دوم

خطرات ناشی از عدم توجه به امنیت اطلاعات در سازمانها



2_1 اهمیت امنیت اطلاعات برای یک سازمان

وجود یک حفره و یا مشکل امنیتی، می تواند یک سازمان را بـه روش هـای متفـاوتی تحـت تـاثیر قرار خواهد داد. آشنائی با عواقب خطرناک یک حفره امنیتی در یک سازمان و شناسـائی مهمتـرین تهدیدات امنیتی که می تواند حیات یک سازمان را با مشکل مواجه نماید، از جمله موارد ضروری به منظور طراحی و پیاده سازی یک مدل امنیتی در یک سازمان می باشد.

- ***پیشگیری از خرابی و عواقب خطرناک یک حفره امنیتی ، یکی از مهمترین دلایل پیاده سازی یک استراتژی امنیتی موثر و کارآ است .***

وجود حفره های امنیتی در یک سازمان، می تواند پیامدهای منفی متعددی را برای یک سازمان به دنبال داشته باشد :

- کاهش درآمد و افزایش هزینه
- خدشه به اعتبار و شهرت یک سازمان
- از دست دادن داده و اطلاعات مهم
- اختلال در فرآیندهای جاری یک سازمان
- پیامدهای قانونی به دلیل عدم ایجاد یک سیستم ایمن و تاثیر جانبی منفی بر فعالیت سایر سازمان ها
- سلب اعتماد مشتریان
- سلب اعتماد سرمایه گذاران

2_2 امنیت اطلاعات در سازمان ها طی سالیان اخیر

ماحصل بررسی انجام شده توسط موسسات و مراکز تحقیقاتی معتبر در خصوص امنیت اطلاعات، نشان دهنده این واقعیت مهم است که حملات مهاجمان بر روی درآمد و هزینه یک سازمان بطور مستقیم و یا غیرمستقیم تاثیر خواهد داشت (کاهش درآمد، افزایش هزینه).

- در سال 2003 ، ویروس ها و حملات از نوع **DOS** (برگرفته از **Service Denial of**) بیشترین تبعات منفی را برای سازمان ها به دنبال داشته اند.

- در سال 2004 ، سرقت اطلاعات بالاترین جایگاه را داشته و حملات از نوع **DOS** با اندکی کاهش نسبت به سال 2003 در رتبه دوم قرار گرفته اند .

- با این که هزینه پیاده سازی یک سیستم حفاظتی اندک نمی باشد ولی می توان آن را به عنوان بخشی از هزینه هائی درنظر گرفت که یک سازمان به دلیل عدم ایمن سازی،می بایست پرداخت نماید (برخورد با تبعات منفی).

موثرترین راهکار و یا راه حل امنیتی، ایجاد یک محیط چندلایه ای است. در یک محیط چند لایه، مهاجمان در هر لایه شناسائی و با آنان برخورد خواهد شد. موفقیت یک مهاجم نیز به عبور موفقیت آمیز از هر لایه بستگی دارد. راه هکار امنیتی چندلایه به "دفاع در عمق " نیز مشهور است. در این مدل، در هر لایه از استراتژی های تدافعی خاصی استفاده می گردد که با توجه به ماهیت پویای امنیت اطلاعات، می بایست به صورت ادواری توسط کارشناسان حرفه ای امنیت اطلاعات، بررسی و بهنگام گردند.

**** هر سازمان می بایست یک فریمورک و یا چارچوب امنیتی فعال و پویا را برای خود ایجاد و به درستی از آن نگهداری نماید .***

در سال 2004 ، هفتاد درصد سازمان ها حداقل یک مرتبه مورد تهاجم قرار گرفته اند.

در سال 2003 بالغ بر 666 میلیون دلار صرف برخورد با مشکلات امنیتی در سازمان ها شده است.

نیمی از سازمان ها به این موضوع اعتراف نموده اند که نمی دانند چه میزان از اطلاعات سازمان خود را به دلیل حملات از دست داده اند.

چهل و یک درصد سازمان ها اعلام داشته اند که دارای هیچگونه طرح و یا برنامه ای برای گزارش و یا پاسخ به تهدیدات امنیتی نمی باشند.

3_2 اشتباهات متداول مدیران سازمان ها

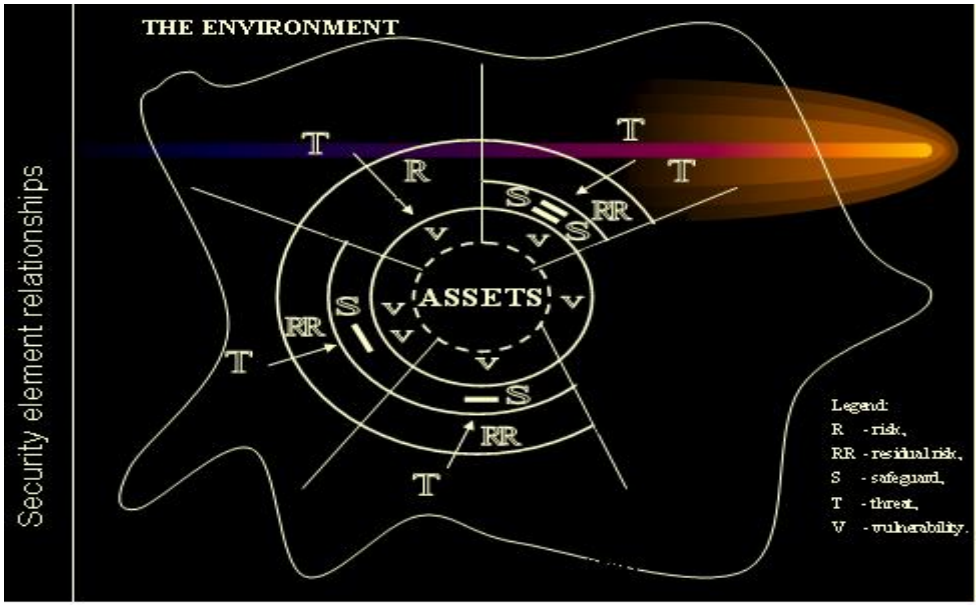
مدیران سازمان، به افرادی اطلاق می گردد که مسئولیت مدیریت، هدایت و توسعه سازمان را بر عهده داشته و با منابع متفاوت موجود در سازمان نظیر بودجه، سروکار دارند. امروزه استفاده از اینترنت توسط سازمان ها و موسسات، مزایای متعددی را بدنبال دارد. واژه " تجارت الکترونیکی" بسیار متداول و استراتژی تجارت الکترونیکی، از جمله مواردی است که در هر برنامه ریزی تجاری به آن توجه خاص می گردد. در صورتیکه سازمان ها و موسسات دارای یک استراتژی امنیتی مشخص شده ای نباشند، اتصال به شبکه جهانی تهدیدی در ارتباط با اطلاعات حساس خواهد بود. در ادامه به برخی از اشتباهات متداول که از ناحیه مدیران سازمان بروز و تاثیر منفی در ارتباط با امنیت اطلاعات در سازمان را بدنبال خواهد داشت، اشاره می گردد:

Human		Environment
Deliberate	**Accidental**	
Eavesdropping	Errors and omissions	Earthquake
Information modification	File deletion	Lightning
System hacking	Incorrect routing	Floods
Malicious code	Physical accidents	Fire
Theft		

4_2 فقدان آگاهی لازم در رابطه با تاثیر یک ضعف امنیتی برعملکرد سازمان

بسیاری از مدیران سازمان بر این باور می باشند که" این مسئله برای ما اتفاق نخواهد افتاد " و بر همین اساس و طرز فکر به مقوله امنیت نگاه می نمایند. بدیهی است در صورت بروز مشکل در سازمان، امکان عکس العمل مناسب در مقابل خطرات و تهدیدات احتمالی وجود نخواهد داشت. این مسئله می تواند بدلیل عدم آشنائی با ابعاد و اثرات یک ضعف امنیتی در سازمان باشد. در این رابطه لازم است به این نکته اشاره گردد که همواره مشکل برای دیگران بوجود نمی آید و ما نیز در معرض مشکلات فراوانی قرار خواهیم داشت. بنابراین لازم است همواره و بصورت مستمر مدیران سازمان نسبت به اثرات احتمالی یک ضعف امنیتی توجیه ودانش لازم در اختیار آنان قرار گیرد. در صورت بروز یک مشکل امنیتی در سازمان، مسئله بوجود آمده محدود به خود سازمان نشده و می تواند اثرات منفی متعددی در ارتباط باادامه فعالیت سازمان را بدنبال داشته باشد. در عصر اطلاعات و دنیای شدید رقابت، کافی است سازمانی لحظاتی آن چیزی باشد که نمی بایست باشد، همین امر کافی است که تلاش چندین ساله یک سازمان هرز و در برخی حالات فرصت جبران آن نیز وجود نخواهد داشت.

- تاثیر منفی بر سایر فعالیت های تجاری online سازمان
- عاملی برای توزیع اطلاعات غیر مفید و غیر قابل استفاده در یک چرخه تجاری
- عرضه اطلاعات حساس مشتریان به یک مهاجم و بمخاطره افتادن اطلاعات خصوصی مشتریان
- آسیب جدی وجهه سازمان و بدنبال آن از دست دادن مشتریان و همکاران تجاری



5_2 عدم تخصیص بودجه مناسب برای پرداختن به امنیت اطلاعات

مجاب نمودن یک مدیر سازمان مبنی بر اختصاص بودجه مناسب برای پرداختن به مقوله امنیت اطلاعات در سازمان از حمله مواردی است که چالش های خاص خود را خواهد داشت. مدیران، تمایل دارند بودجه را به حداقل مقدار خود برسانند، چرا که آنان یا اطلاعات محدودی در رابطه با تاثیر وجود ضعف های امنیتی در عملکرد سازمان را دارند و یا در برخی حالات بودجه، آنان را برای اتخاذ تصمیم مناسب محدود می نماید. اینترنت یک شبکه جهانی است که فرصت های جذاب و نامحدود تجاری را برای هر بنگاه تجاری فراهم می نماید، با رعایت امنیت اطلاعات و حفا ظت مناسب از داده های حساس، امکان استفاده از فرصت های تجاری بیشتری برای یک سازمان فراهم خواهد شد. با اختصاص یک بودجه مناسب برای پرداختن و بهاء دادن به مقوله امنیت اطلاعات در یک سازمان، پیشگیری های لازم انجام ودر صورت بروز مسائل بحرانی، امکان تشخیص سریع آنان و انجام واکنش های مناسب فراهم می گردد. بعبارت دیگر با در نظر گرفتن بودجه مناسب برای ایمن سازی سازمان، بستر مناسب برای حفاظت سیستم ها و داده های حساس در یک سازمان فراهم خواهد شد. قطعا" تولید و عرضه سریع اطلاعات در سازمان های مدرن و مبتنی بر اطلاعات، یکی از مهمترین شاخص های رشد در عصر حاضر بوده وهرآنچیزی که می تواند خللی در فرآیند فوق ایجاد نماید، باعث توقف و گاها" برگشت به عقب یک سازمان، می گردد.

6_2 اتکاء کامل به ابزارها و محصولات تجاری

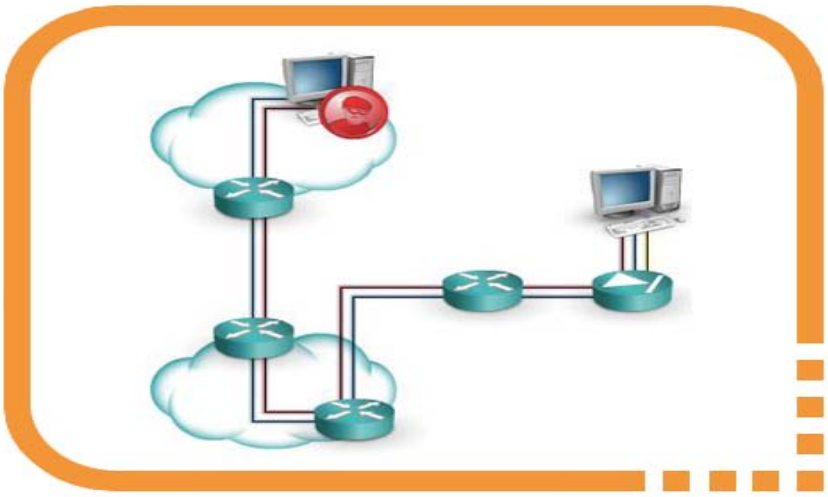
اگر از یک سازمان سوال شود که چگونه خود را در مقابل حملات حفاظت نموده اید؟ اغلب آنان در پاسخ خواهند گفت:" ما از یک فایروال شناخته شده و یک برنامه ویروس یاب بر روی سرویس دهنده استفاده می کنیم، بنابراین ما در مقابل حملات ایمن خواهیم بود". توجه داشته باشید که امنیت یک فرآیند است نه یک محصول که با خریداری آن خیال خود را در ارتباط با امنیت راحت نمائیم. مدیران سازمان لازم است شناخت مناسب و اولیه ای از پتانسل های عمومی یک فایروال و یا برنامه های ویروس یاب داشته باشند (قادر به انجام چه کاری می باشند و چه کاری را نمی توانند انجام دهند. مثلا" اگر ویروس جدیدی نوشته و در شبکه توزیع گردد، برنامه های ویروس یاب موجود قادر به تشخیص و برخورد با آن نخواهند بود. این نوع برنامه ها صرفا" پس از مطرح شدن یک ویروس و آنالیز نحوه عملکرد آن می بایست بهنگام شده تا بتوانند در صورت بروز وضعیتی مشابه با آن برخورد نمایند). ابزارهائی همچون فایروال و یا برنامه های ویروس یاب، بخشی از فرآیند مربوط به ایمن سازی اطلاعات حساس در یک سازمان بوده و با بکارگیری آنان نمی توان این ادعا را داشت که آنان سازمان را بطور کامل در مقابل تهاجمات، حفاظت خواهند نمود.

7_2 یک مرتبه سرمایه گذاری در ارتباط با امنیت

امنیت مفهمومی فراگیر و گسترده بوده که نیازمند هماهنگی و سرمایه گذاری در دو بعد تکنولوژی وآموزش است. هرروز ما شاهد ظهور تکنولوژی های جدیدی می باشیم. ما نمی توانیم درمواجهه با یک تکنولوژی جدید بصورت انفعالی برخورد و یا عنوان نمائیم که ضرورتی به استفاده از این تکنولوژی خاص را نداریم. بکارگیری تکنولوژی عملا" صرفه جوئی در زمان و سرمایه مادی را بدنبال داشته و این امر باعث ارائه سرویس های مطلوبتر وارزانتر به مشتریان خواهد شد. موضوع فوق هم از جنبه یک سازمان حائز اهمیت است و هم از نظر مشتریان، چراکه ارائه سرویس مطلوب با قیمت تمام شده مناسب یکی از مهمترین اهداف هر بنگاه تجاری محسوب شده و مشتریان نیز همواره بدنبال استفاده از سرویس ها و خدمات با کیفیت و قیمت مناسب می باشند. استفاده از تکنولوژی های جدید و سرویس های مرتبط با آنان، همواره تهدیدات خاص خود را بدنبال خواهد داشت.

بنابراین لازم است به این موضوع توجه شود که امنیت یک سرمایه گذاری پیوسته را طلب می نماید، چراکه با بخدمت گرفتن تکنولوژی ها ی نو بمنظور افزایش بهره وری در یک سازمان، زمینه پرداختن به امنیت می بایست مجددا" و درارتباط با تکنولوژی مربوطه بررسی و در صورت لزوم سرمایه گذاری لازم در ارتباط با آن صورت پذیرد. تفکر اینکه، امنیت یک نوع سرمایه گذاری یکبار مصرف است، می تواند از یکطرف سازمان را در استفاده از تکنولوژی ها ی نو با تردید مواجه سازد واز طرف دیگر با توجه به نگرش به مقوله امنیت (یکبار مصرف)، بهاء لازم به آن داده نشده و شروع مناسبی برای پیاده سازی یک سیستم امنیتی و حفاظتی مناسب را نداشته باشیم.

8_2 میزان خسارات مالی حملات انجام شده



* انگیزه اصلی نفوذ دیگر تفریح نیست بلکه وارد کردن خسارت است.
* تهدیدات دیگر فقط ازجانب نوجوانان نیست بلکه از جانب سازمان های هدف مند است.

♦ ا بزارهای بهتر با کارآیی بالاتر که بکار گرفتن شان نیاز به دانش فنی بالا ندارد در دسترس همه است، تعداد نتایجی که google بر میگرداند:

2،460،000 یافته برای کلید واژه " hack password"
101،000 یافته برای کلید واژه "SQL attack tool "
176،000 یافته برای کلید واژه "DOS attack tool"

سرعت شیوع حملات به شدت ا فزایش و فاصله زمانی بین آ نها به شدت کاهش یافته است. حملات بصورت متمرکز انجام میشود. دستور حمله و کنترل آن از یک نقطه انجام می شود.

* SQL – slammer در عرض 11 دقیقه 75،000 کامپیوتر را آلوده کرد.
* Ms Blaster، So bigf ، welchia در تاریخ 11 ، 18، 19 آگوست 2003 منشر شد.

میزان خسارات مالی حملات انجام شده

- سال 1996–980 میلیون دلار
- سال 1997_ 2 میلیارد دلار
- سال 1998_ 4،7 میلیارد دلار
- سال 1999_ 23 میلیارد دلار
- سال 2000_ 30 میلیارد دلار
- سال 2001_ 40 میلیارد دلار
- سال 2002_ 130 میلیارد دلار
- سال 2003_ 204 میلیارد دلار(200 برابر سال 1996)
- سال 2004_ 290 میلیارد دلار
- سال 2005_ 320 میلیارد دلار
- سال 2006_ 390 میلیارد دلار

فصل سوم

مزایای سرمایه گذاری در امنیت اطلاعات برای سازمانها

3_1 مزایای سرمایه گذاری در امنیت اطلاعات

سازمان ها و موسسات تجاری با پیاده سازی یک استراتژی امنیتی از مزایای زیر بهره مند خواهند شد :

- کاهش احتمال غیرفعال شدن سیستم ها و برنامه ها (از دست دادن فرصت ها)
- استفاده موثر از منابع انسانی و غیرانسانی در یک سازمان (افزایش بهره وری)
- کاهش هزینه از دست دادن داده توسط ویروس های مخرب و یا حفره های امنیتی (حفاظت از داده های ارزشمند)
- افزایش حفاظت از مالکیت معنوی

* هزینه پیشگیری از یک مشکل امنیتی، همواره کمتر از هزینه بازسازی خرابی متاثر از آن است.

* یک مشکل امنیتی که باعث از بین رفتن اطلاعات مشتریان می شود، می تواند پیامدهای قانونی را برای یک سازمان به دنبال داشته باشد.

2_3 عملیات

منظورازعملیات، مجموعه فعالیت های لازم بمنظور نگهداری وضعیت امنیتی یک سازمان است.
در این رابطه لازم است ، به موارد زیر توجه گردد :

- پشتیبانی ملموس و بهنگام سازی سیاست های امنیتی
- اعمال تغییرات لازم با توجه به روند تحولات مرتبط با تکنولوژی اطلاعات، در این رابطه می بایست داده های مورد نظر جمع آوری تا زمینه تصمیم سازی مناسب برای مدیریت فراهم گردد (تامین اطلاعات ضروری برای مدیریت ریسک)
- مدیریت وضعیت امنیتی با توجه به تکنولوژی های استفاده شده در رابطه ایمن سازی اطلاعات (نصب Patch امنیتی، بهنگام سازی ویروس ها، پشتیبانی لیست های کنترل دستیابی)
- ارائه سرویس های مدیریتی اساسی و حفاظت از زیرساخت های مهم (خصوصا" زیر ساخت هائی که برای یک سازمان ختم به درآمد می گردد)
- ارزیابی سیستم امنیتی
- هماهنگی و واکنش درمقابل حملات جاری
- تشخیص حملات و ارائه هشدارو پاسخ مناسب بمنظور ایزوله نمودن حملات و پیشگیری ازموارد مشابه
- بازیافت و برگرداندن امور به حالت اولیه (بازسازی)

از دیگررویه های[1] استاندارد عملیاتی می توان به نکات زیر اشاره کرد:

- ♦ آموزش به کاربران سایت‌های عملیاتی در رابطه با خطرات که از ناحیه انتخاب کلمات عبور نامناسب, متوجه اطلاعات و سیستم‌های عملیاتی خواهد شد.
- ♦ ایجاد دانش عمومی پایه امنیت اطلاعات و سیستم‌ها بین کاربران و مدیران سیستم
- ♦ تهیه رویه‌های اجرایی جهت حفظ امنیت فیزیکی سیستم‌های سخت‌افزاری
- ♦ اطلاع رسانی به کاربران و راهبران (مدیران سیستم) توسط تیم کنترلی و نظارتی امنیت سازمان
- ♦ مراجعه تیم کنترلی و نظارتی سازمان به سایت‌های خبری مرتبط با امنیت اطلاعات و سیستم‌ها و شرکت در فعالیت‌های مرتبط
- ♦ تهیه رویه‌هایی جهت منهدم نمودن مدارک و کاغذهای باطله تولید شده در سایت‌های عملیاتی
- ♦ تهیه رویه و فرم اتصال دستگاه‌های جدید به شبکه سایت‌های عملیاتی
- ♦ تهیه رویه جهت مشاهده دوره‌ای logهای سیستم و سرورهای سایت‌های عملیاتی توسط تیم نظارتی و کنترلی سازمان و نگهداری آنها در محل‌های مناسب

متوقف نمودن سرویس‌های اضافی سرورهای سایت‌های عملیاتی

- ♦ استخدام و بکارگیری کارشناسان خبره در امر امنیت اطلاعات و سیستم‌ها و شبکه
- ♦ تهیه و تدوین سیاست‌های میزان استفاده کاربران از سیستم‌ها و اطلاعات حساس و دریافت تاییده از آنها

- ♦ تعیین محدوده دسترسی کاربران به اطلاعات سیستم‌های کاربردی با توجه به نقش آنها در گردش کار

- ♦ جلوگیری از انتقال اطلاعات سازمان و سایت‌های عملیاتی به روی کامپیوترهای منازل مدیران
- ♦ ایجاد تعهدات حقوقی برای مدیران سیستم‌ها (پیمانکاران) در سایت‌های عملیاتی

[1] Procedure

- بررسی مکانیزم تهیه و نگهداری فایل‌های پشتیبان در سایت‌های عملیاتی توسط تیم نظارتی و کنترلی سازمان

- بررسی میزان دسترسی کاربران سیستم‌های کاربردی به اطلاعات و سیستم بر اساس گروه کاری آنها در سیستم و درصورت لزوم بازنگری و اصلاح آنها
- نگهداری یک نسخه از اسامی رمزهای سایت‌های عملیاتی در سازمان در پاکت‌های مهرو موم
- سازماندهی تیم‌های تخصصی درزمینه امنیت اطلاعات در سازمان شامل : کمیته امنیت اطلاعات, تیم اجرایی (جهت نظارت بر عملکرد راهبران و کاربران در سایت‌های عملیاتی) و تیم عملیاتی محیط ویندوز
  استفاده از خدمات مشاور و افراد دارای گواهینامه‌های خاص امنیت اطلاعات و سیستم‌ها
- ایمن‌سازی فیزیکی سایت‌های عملیاتی
- حضور فعال کارشناسان سازمان در مراکز, گروه‌ها و انجمن‌های امنیتی داخل و خارج کشور
- تهیه نرم‌افزارهای تشخیص حملات[۲] جهت تشخیص نقاط ضعف از جمله : اشکالات مجوزهای فایل[۳], سیاست‌های تعیین رمز عبور[4] و ...
- تهیه رویه‌های انتخاب کلمات عبور و نظارت بر نگهداری و تغییرات بعدی آنها

[2] Intrusion Detection System (IDS)
[3] File permission
[4] Password policy

فصل چهارم

استانداردهای جهانی امنیت اطلاعات

4_1 اصول مهم مباحث امنیتی

تا مدتها " امنیت اطلاعات " متعارف و متعادل با " محرمانگی اطلاعات " تلقی می شد. اما پس از دهه 90 با ظهور شبکه های محلی و جهانی، سیستم چند کاربره، سخت افزار های پیشرفته و اتکای بشر به دنیای مجازی، جنبه های دیگری از امنیت اطلاعات در سیتم های کامپیوتری ظاهر گردید. تلاش حمله کنندگان با هدف تغییر غیر مجاز اطلاعات و یا از کار اندازی سرویس دهی سیستم ها، هم اکنون از نمو نه ها ی بارز و جهانی مشکلات امنیت در فناوری اطلاعات است. تفکر امنیت در شبکه برای دستیابی به سه عامل مهم است که با یک دیگر مثلث امنیتی را تشکیل می دهند. این عوامل عبارتند از راز داری و امانت داری **(Confidentiality)** ، یکپارچگی **(Integrity)** و در نهایت در دسترس بودن همیشگی **(Availability)**. این سه عامل **(CIA)** اصول اساسی امنیت اطلاعات – در شبکه و یا بیرون آن – را تشکیل می دهند بگونه ای که تمامی تمهیدات لازمی که برای امنیت شبکه اتخاذ میشود و یا تجهیزاتی که ساخته می شوند، همگی ناشی از نیاز به اعمال این سه پارامتر در محیط های نگهداری و تبادل اطلاعات است.

1. **محرمانگی (Confidentiality)** : جلوگیری از دسترسی غیر مجاز و فاقد صلاحیت به اطلاعات را محرمانگی گویند . این اصل به اعتقاد بسیاری از صاحبنظران از مهمترین جنبه های امنیتی برای سازمان های نظامی و دولتی است. رمز نگاری مناسب ترین روش برای حفظ محرمانگی اطلاعات در حال حاضر است.

2. **صحت (Integrity)** : حفاظت از داده ها و اطلاعات در مقابل تغییرات غیر مجاز سهوی و عمدی را صحت و یا جامعیت اطلاعات گویند. اگر چه سیستم های امنیتی نمی توانند به تنهایی درستی داده های ورودی توسط کاربران به سیستم را ارزیاب ینمایند. ولی می توانند اعمال درست همه تغییرات درخواستی بر روی داده ها را تضمین کنند.

3. در دسترس بودن **(Availability)** : قابلیت استفاده از همیشکی و مداوم سیستم های کامپیوتری توسط کاربران مجاز را در دسترس بودن گویند. نفی خدمت معمولا رایجترین حملاتی است که برای از کاراندازی سیستم ها و توقف سرویس دهی آنها صورت می گیرد.

4_2 استانداردی برای حفاظت از شبکه ها حالا دیگر امنیت دارید

امنیت از دیرباز یکی از اجزای اصلی زیرساخت‌های فناوری اطلاعات به شمار می‌رفته است. تهدید های امنیتی تنها منحصر به تهدیدات الکترونیکی نیستند، بلکه هر شبکه باید از نظر فیزیکی نیز ایمن گردد. خطرات الکترونیکی غالباً شامل تهدیدات هکرها و نفوذگران خارجی و داخلی در شبکه‌ها می باشند. در حالی که امنیت فیزیکی شامل کنترل ورود و خروج پرسنل به سایت‌های شبکه و همچنین روال‌های سازمانی نیز هست. برای پیاده سازی امنیت در حوزه‌های فوق، علاوه بر ایمن‌سازی سخت‌افزاری شبکه، نیاز به تدوین سیاست‌های امنیتی در حوزه فناوری اطلاعات در یک سازمان نیز می باشد. در این راستا لازم است از روال‌های استانداردی استفاده شود که به واسطه آن‌ها بتوان ساختار یک سازمان را برای پیاده سازی فناوری اطلاعات ایمن نمود استاندارد امنیت اطلاعات BS7799 استانداردی جهانی و پویاست که با ارائه کنترل های مختلف سعی در پیاده سازی قالبی مطمئن برای سازمان ها دارد. اجرای این کنترل ها علاوه بر نظم بخشیدن به سازمان ها، امنیت اطلاعات و دارایی های مختلف سازمان ها را تضمین خواهد کرد.

4_3 استاندارد BS7799

BS7799 استانداردی انگلیسی و ارهنمایی برای حفاظت اطلاعات و تجهیزات سازمان می باشد.

BS7799 در دو قسمت ISO/IEC 17799:2000 و BS7799-2 1999 آمده است.

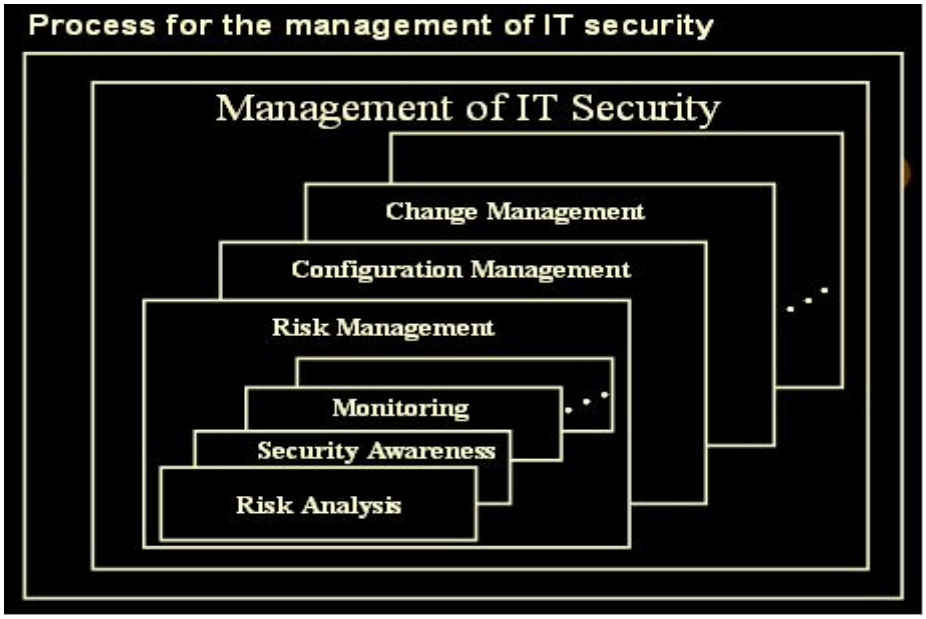
بخش اول: کدهای استانداردی است که راهنمای اولیه برای حفاظت دارایی و اطلاعات یک سازمان می باشد که باید اجرا شود. محدوده این استاندارد صوت،اینترنت، تلفن ها، نمابر و . . . را در بر می گیرد.

بخش دوم: شرایط استاندارد مدیریتی برای مدیریت و امنیت اطلاعات (ISMS) می باشد. با کمک این بخش به سازمانها پیمودن مراحل مختلف این قالب مدیریتی آموزش داده می شود. این قالب، افراد، سیستم IT و پروسه های مختلف را در بر می گیرد. ISMS یا Information Security Management System برای حصول موارد زیر ایجاد می شود.

- دارایی های با ارزش که نیاز به حفاظت دارند مشخص خواهند شد.
- سازمان را برای مد یریت خطرها آماده می کند.
- کنترل های مختلف را برای این حفاظت ایجاد می کند.
- -میزان اطمینان مورد نیاز را مشخص می کند.

کنترل هایی که در BS7799-2:1999 لحاظ شده است به قرار زیر است :

1- سیاست های امنیتی
2- امنیت سازمان
3- دسته بندی دارایی های با ارزش و کنترل آنها
4- امنیت افراد
5- امنیت فیزیکی و محیط کار
6- امنیت ارتباطات و مدیریت اجرا
7- کنترل دسترسی ها
8- سیستم نگهداری و ارتقاء
9- نقشه ادامه Bussiness شرکت
10- سازگاری با موارد قانونی



4_4 چرا BS7799 ؟

بیشتر صحبتها امروزه در مورد BS7799-2 است که در سال 1999 منتشر شده است. دلیل محبوبیت این استاندارد در سالهای اخیر اهمیت بسیارزیاد حفاظت اطلاعات می باشد.امروزه دسته بندی و درجه بندی اهمیت دارایی های با ارزش سازمان توسط مدیریت سازمان مشخص می شود. هر چقدر این دسته بندی و اطلاعات کامل تر باشند پیشبرد اهداف امنیتی یک سازمان آسان ترصورت خواهد پذیرفت. BS7799-2 یکی از معدود روشهایی است که اطلاعات و امنیت آنها را با جزئیات کامل بیان می کند. در واقع چگونگی مدیریت امنیت اطلاعات توسط BS7799 بیان شده است. با توجه به آنچه که ذکر شد این استاندارد، استاندارد های لازم الاجرا درسازمان صدا و سیما می باشد. چرا که هرارگانی ناگزیراست که این استاندارد را در بدنه خود پیاده سازی کنند تا بتوان در آن سازمان آثار امنیت جامعه را دید.

4_5 سازگاری BS779 !

سازگاری با BS7799 سازمان را مجبورمیسازد سیستم امنیت اطلاعات را اجرا نموده و مستند نماید همچنین بندهای کنترلی مختلف در آن سازمان اجرا خواهند شد.

چه مواردی جهت این سازگاری لازم هستند؟

اولین قدم برای رسیدن به این مهم برقراری و نگهداری مستندات ISMS می باشد.

1- دارایی های با ارزش حفاظت شوند
2- سازمان به سمت مدیریت خطرات پیش برود
3- کنترلهای موجود در استاندارد لحاظ شود
4- درجه امنیت مورد نیاز سازمان تعیین شود

سازگاری با BS7799 اجرای شش مرحله را طلب می کند.

مرحله اول : سیاست های امنیت اطلاعات سازمان مشخص می شود.

مرحله دوم : ناحیه اجرای استاندارد مشخص می شود. سازمان مشخص می کند کدام کنترل ها برای سازمان ضروری می باشند. حاصل این کنترل های انتخاب شده به نیازمندیهای سازمان، دارایی های نیازمند به ایمنی ،مکان و تکنولوژی بستگی دارد.

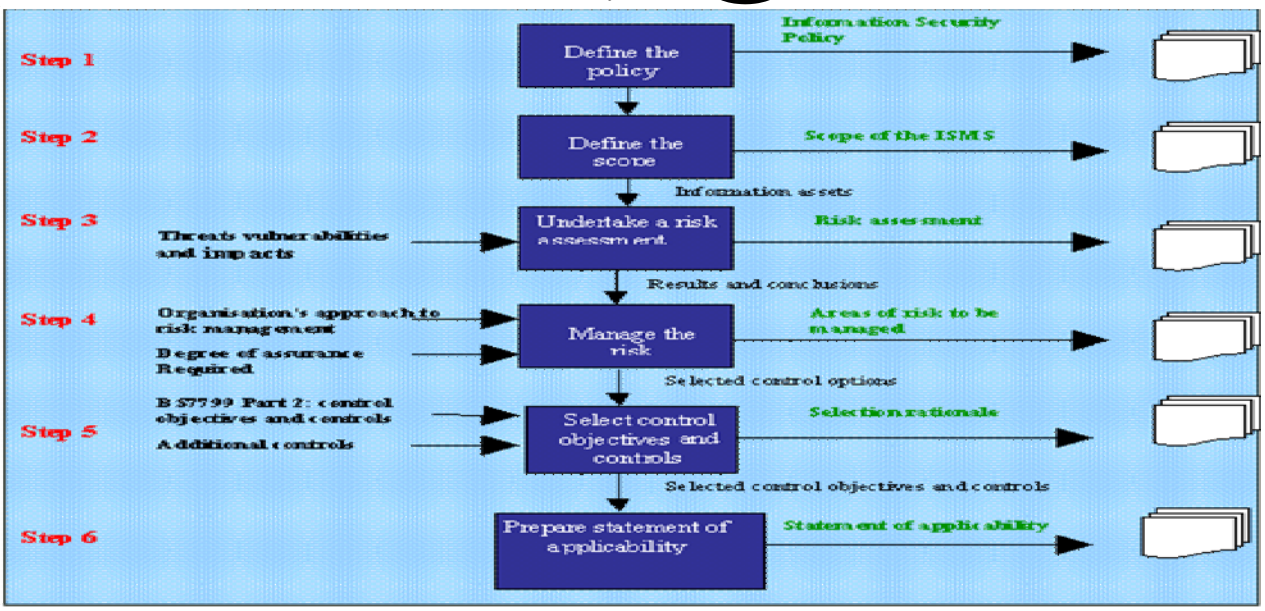
مرحله سوم : ارزیابی خطرات: هدف از این ارزیابی مشخص کردن تهدیدها و مخاطرات دارایی ها می باشد. نتیجه این ارزیابی درجه خطر را مشخص می نماید.

مرحله چهارم : مدیریت خطرها می باشد. محدوده مدیریت خطر توسط سیاستهای امنیتی اطلاعات و همچنین میزان امنیت مورد نیاز سازمان مشخص خواهد شد.

مرحله پنجم : انتخاب کنترل ها در بند 4 استانداردBS7799 لحاظ شده است که باید اجرا شوند.

مرحله ششم : امکان پذیری اجرا مدنظر قرار گیرد

یک سازمان نیاز به مستند کردن کنترلهای انتخاب شده دارد. بعضی از این کنترلها به دلیل ماهیت سازمان نیاز به اجرا ندارند که باید مشخص شوند.



6_4 نحوه عملکرد استاندارد BS 7799

درراستای تحقق دومین هدف پیدایش این استاندارد که به آن اشاره شد، یعنی کمک به کاربران سرفصل‌هایی برای نحوه پیاده سازی امنیت در یک سازمان که در حقیقت یک کاربر سیستم های امنیتی می باشد، تعیین شده است که عبارتند از:

- تعیین مراحل ایمن سازی و نحوه شکل گیری چرخه امنیت
- جزییات مراحل ایمن سازی و تکنیک‌های فنی مورد استفاده در هر مرحله
- لیست و محتوای طرح ها و برنامه های امنیت اطلاعات مورد نیاز سازمان
- ضرورت و جزییات ایجاد تشکیلات سیاستگذاری، اجرایی و فنی تامین امنیت
- کنترل‌های امنیتی مورد نیاز برای هر یک از سیستم های اطلاعاتی و ارتباطی
- تعریف سیاست‌های امنیت اطلاعات
- تعریف قلمرو سیستم مدیریت امنیت اطلاعات و مرزبندی آن متناسب با نوع نیازهای سازمان
- انجام و پذیرش برآورد مخاطرات، متناسب با نیازهای سازمان
- پیش بینی زمینه ها و نوع مخاطرات بر اساس سیاست‌های امنیتی تدوین شده
- انتخاب هدف‌های کنترل و کنترل‌های مناسب که قابل توجیه باشند، از لیست کنترل‌های همه جانبه
- تدوین دستورالعمل های عملیاتی

4_7 تشکیلات اجرائی امنیت

برای پیاده سازی یک سیستم امنیتی پویا، وجود تشکیلات امنیتی متناسب با نیازهای امنیتی سازمان لازم و ضروری می باشد. گروه‌های کاری لازم برای اینکه امور امنیتی یک شبکه به نحو احسن اداره شود عبارتند از:

- سیاست امنیت
- مرکز هماهنگی واطلاع رسانی
- تشخیص و مقابله باحوادث
- تشخیص و مقابله با حوادث خاص
- بازرسی امنیتی
- نصب و پیکر بندی
- نگهداری و پشتیبانی

4_8 سیاست امنیت

وظایف این قسمت تدوین سیاست امنیتی و بازنگری و اصلاح سیاست امنیتی در صورت پیشنهاد گروه مدیریت امنیتی می‌باشد. قسمت سیاست امنیتی هماهنگی تشکیل جلسات گروه سیاستگذاری امنیتی را از قسمت مدیریت امنیتی دریافت کرده و طبق آن عمل می کند و نتایج حاصله را به مدیریت امنیتی تحویل می دهد.

4_9 مرکز هماهنگی واطلاع رسانی

مرکز هماهنگی تمامی گزارش‌ها را از بخش‌های مختلف جمع آوری کرده و در واقع نقش رابط بین قسمت‌ها را بازی می‌کند. این مرکز بیشتر مانند واسط اصلی بین قسمت‌ها و بخش مدیریتی عمل می کند و تغییرات و پیشنهادات گروه مدیریتی را به گروه‌های کاری منعکس می‌کنند. وظایف این قسمت دریافت اطلاعات و گزارش از گروه‌های پائین‌تر، پردازش و دسته‌بندی آن‌ها، ثبت اطلاعات، ارسال نتایج به گروه مدیریت امنیتی، دریافت تغییرات (تغییر سیاست امنیتی) از گروه مدیریت امنیتی، ثبت اطلاعات و ارسال آن برای گروه‌های پائین‌تر، تشکیل بانک‌اطلاعاتی حاوی آسیب‌پذیری‌ها و پیکربندی امن تجهیزات و سرویس‌های شبکه، نگهداری آمار و گزارش حملات انجام شده و واکنش گروه‌های مرتبط وارائه مشاوره در زمینه خرید تجهیزات، آنالیز ریسک و ... می باشد.

4_10 تشخیص و مقابله باحوادث

وظیفه این قسمت شناسایی و مقابله با حملات و دسترسی‌های غیرمجاز می‌باشد و دارای بخش آماده‌سازی به منظور تعیین روند و سیاست سازمانی جهت شناسایی، تعیین منابع اطلاعاتی جهت شناسایی تهاجم، تهیه بانک‌اطلاعاتی حاوی الگوهای حملات شناخته شده، مدیریت مکانیزم های ثبت اطلاعات، پشتیبانی سیستم و دریافت گزارشات و توصیه‌های گروه هماهنگی و اطلاع رسانی، بخش کشف تهاجم به منظور نظارت بر فعالیت‌های شبکه، نظارت بر فعالیت‌های سیستم، بازرسی فایل‌ها و دایرکتوری‌ها، جستجوی اتصالات غیرقانونی به شبکه، بازرسی منابع فیزیکی و دریافت و پردازش گزارشات کاربران، بخش پاسخگویی به تهاجم به منظور آنالیز گزارش، انتقال اطلاعات حادثه وروند آن به بخش‌های لازم، به‌کارگیری سریعترین راهکارها جهت قطع حمله، جلوگیری از وقوع دوباره حمله، بازیابی سیستم به حالت عادی و تعیین خسارت و در انتها بخش تحقیقات به منظور شناخت انواع حملات، دریافت گزارش مقابله ناموفق و تشخیص و مقابله با ویروس‌ها می‌باشد.

4_11 تشخیص و مقابله با حوادث خاص

این قسمت با اجزای آماده‌سازی، کشف و پاسخگویی وظایف مقابله با خطرات ناشی از حوادث و پیشگیری از برخی حوادث محتمل را به عهده دارد. این قسمت گزارش‌های مربوط به مقابله با تهاجم یا ویروس یا حادثه خاص را به قسمت مرکز هماهنگی برای ارسال به قسمت مدیریتی منتقل می‌کند و سیاست ها و موارد اضافه‌شده در برابر حوادث را به عنوان نتیجه دریافت می‌نماید.

4_12 بازرسی امنیتی

بخش بازرسی امنیتی وظایف بازرسی تجهیزات امنیتی، بازبینی log ها و پیغام‌ها و سیستم‌های پشتیبان و بازرسی شبکه برای ایجاد امنیت در شبکه را برعهده دارد. در این نوع بازرسی‌ها باید اجزا و شبکه به صورت خودکار مورد بررسی قرار گیرند.

4_13 نصب و پیکربندی

این قسمت وظایف پیکربندی امن تجهیزات و سرویس‌های شبکه و نصب و پیکربندی سیستم امنیتی شبکه را به عهده دارد.

4_14 نگهداری و پشتیبانی

این قسمت وظایف محافظت و پشتیبانی از کلیه تجهیزات و اطلاعات امنیتی، نگهداری و ثبت تجهیزات، گزارش هشدارهای خودکار، عیب‌یابی شبکه و ارائه سرویس لازم و آمارگیری شبکه را به‌عهده دارد.

15_4 تکنولوژی

سازمان ها و موسسات می بایست سیاست ها و فرآیندهای لازم بمنظور استفاده از یک تکنولوژی را مشخص تا زمینه انتخاب و بکارگیری درست تکنولوژی در سازمان مربوطه فراهم گردد. در این رابطه می بایست به مواردی همچون:

- سیاست امنیتی
- اصول ایمن سازی اطلاعات
- استانداردها و معماری ایمن سازی اطلاعات
- استفاده ازمحصولات مربوط به ارائه دهندگان شناخته شده و خوش نام
- راهنمای پیکربندی
- پردازش های لازم برای ارزیابی ریسک سیستم های مجتمع و بهم مرتبط توجه گردد.

دفاع در چندین محل. مهاجمان اطلاعاتی(داخلی و یا خارجی) ممکن است، یک هدف را از چندین نقطه مورد تهاجم قرار دهند. در این راستا لازم است سازمان ها و موسسات از روش های حفاظتی متفاوت در چندین محل (سطح) استفاده، تا زمینه عکس العمل لازم در مقابل انواع متفاوت حملات ، فراهم گردد. در این رابطه می بایست به موارد زیر توجه گردد :

◄ دفاع از شبکه ها و زیر ساخت. در این رابطه لازم است شبکه های محلی و یا سراسری حفاظت گردند. (حفاظت در مقابل حملات اطلاعاتی از نوع عدم پذیرش خدمات)

◄ حفاظت یکپارچه و محرمانه برای ارسال اطلاعات در شبکه (استفاده از رمزنگاری و کنترل ترافیک بمنظور واکنش در مقابل مشاهده غیرفعال)

◄ دفاع در محدوده های مرزی. (بکارگیری فایروال ها و سیستم های تشخیص مزاحمین بمنظور واکنش در مقابل حملات اطلاعاتی از نوع فعال)

◄ دفاع در محیط های محاسباتی (کنترل های لازم بمنظور دستیابی به میزبان ها و سرویس دهنده بمنظور واکنش لازم در مقابل حملات از نوع خودی، توزیع و مجاور)

16_4 امنیت در فناوری اطلاعات

موضوع امنیت در فناوری از اطلاعات همراه با رشد صنعت کامپیوتر گسترش یافته است در دو دهه اول که کامپیوتر ها به کار گرفته شدند، موضوع امنیت به شکل و پیچیدگی امروز مطرح نبود. بعد از بکار گیری کامپیوترها در زمینه های امنیت ملی و کاربردهای تجاری، حساسیت موضوع دو چندان شد. امروزه تعداد بیشماری سیستم کامپیوتری وظیفه سرویس دهی به گروه کثیری از کاربران و پردازش حجم زیادی از اطلاعات را با حساسیت های مختلف، بر عهده دارند. از طرفی،همزمان با روند فناوری اطلاعات، تهدید های متنوع و گوناگونی بسیار زیادی نیز بوجود آمده که امنیت اطلاعات و منابع آنها در سازما نها را به خطرمی ندارند.

فصل پنجم

امنیت در شبکه های کامپیوتری

5_1 شبکه های کامپیوتری

بر روی هر شبکه کامپیوتری روزانه اطلاعات متفاوتی جابجا می گردد و همین امر می تواند موضوعی مورد علاقه برای مهاجمان باشد. در این نوع حملات، مهاجمان اقدام به استراق سمع و یا حتی تغییر بسته های اطلاعاتی در شبکه می نمایند. مهاجمان به منظور نیل به اهداف مخرب خود از روش های متعددی به منظور شنود اطلاعات، استفاده می نمایند. شبکه های کامپیوتری اهداف مناسب و جذابی برای مهاجمان اطلاعاتی می باشند، یک شبکه با ضریب عملکرد بالا به سختی مورد دستبرد قرارمی گیرد در حالیکه یک شبکه با ضریب عملکرد پایین می تواند نسبتاً به راحتی مختل شود. اگر هکرها تشخیص دهند که شبکه شما ضریب عملکرد بالایی دارد، که فایده رویکرد لایه بندی شده نیز هست، احتمالاً شبکه شما را رها می کنند و به سراغ شبکه هایی با امنیت پایین تر می روند و این دقیقاً همان چیزیست که شما می خواهید.

بنابراین لازم است، تدابیر لازم در خصوص حفاظت سیستم ها و شبکه ها در مقابل انواع متفاوت حملاتی اطلاعاتی اندیشیده گردد در صورتیکه قصد ارائه و یا حتی مصرف بهینه و سریع اطلاعات را داشته باشیم، می بایست زیر ساخت مناسب را در این جهت ایجاد کنیم. شبکه های کامپیوتری، بستری مناسب برای عرضه، ارائه و مصرف اطلاعات می باشند(دقیقا" مشابه نقش جاده ها در یک سیستم حمل و نقل). عرضه، ارائه و مصرف یک کالا نیازمند وجود یک سیستم حمل و نقل مطلوب خواهد بود. در صورتیکه سازمان و یا موسسه ای محصولی را تولید ولی قادر به عرضه آن در زمان مناسب (قبل از اتمام تاریخ مصرف) برای متقاضیان نباشد، قطعا" از سازمان ها ئی که تولیدات خود را با بهره گیری از یک زیر ساخت مناسب، بسرعت در اختیار متقاضیان قرار می دهند، عقب خواهند افتاد.

شاید بهمین دلیل باشد که وجود جاده ها و زیرساخت های مناسب ارتباطی، بعنوان یکی از دلایل موفقیت برخی از کشورها در عصر انقلاب صنعتی، ذکر می گردد. فراموش نکنیم که امروزه زمان کهنه شدن اطلاعات از زمان تولید اطلاعات بسیار سریعتر بوده و می بایست قبل از اتمام تاریخ مصرف اطلاعات با استفاده از زیر ساخت مناسب (شبکه های ارتباطی) اقدام به عرضه آنان نمود. برای عرضه اطلاعات می توان از امکاناتی دیگر نیز استفاده کرد ولی قطعا" شبکه های کامپیوتری بدلیل سرعت ارتباطی بسیار بالا دارای نقشی کلیدی و منحصر بفرد می باشند. مثلا" می توان مشخصات کالا و یا محصول تولید شده در یک سازمان را از طریق یک نامه به متقاضیان اعلام نمود ولی در صورتیکه سازمانی در این راستا از گزینه پست الکترونیکی استفاده نماید، قطعا" متقاضیان مربوطه در زمانی بسیار سریعتر نسبت به مشخصات کالای تولیده شده، آگاهی پیدا خواهند کرد.

2-5 امنیت اطلاعات در شبکه های کامپیوتری

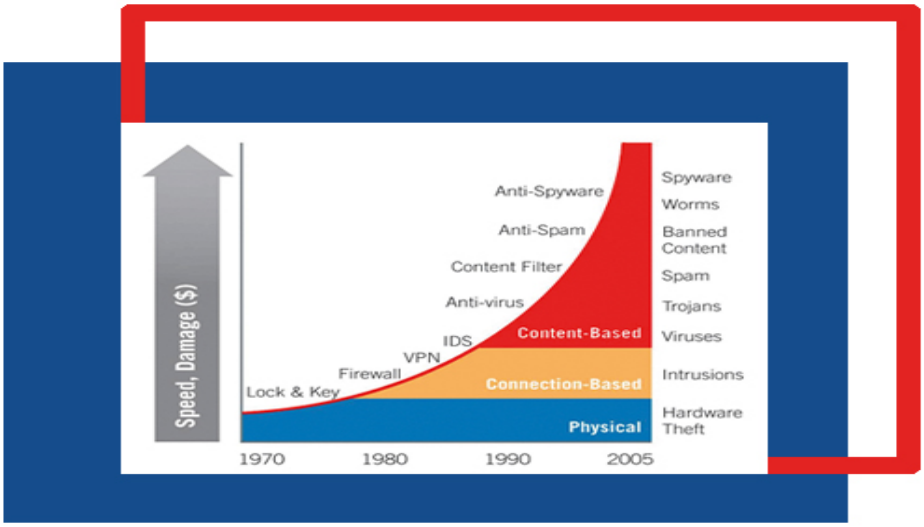
همزمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه های کامپیوتری و به دنبال آن اینترنت (بزرگترین شبکه جهانی)، حیات کامپیوترها و کاربران آنان دستخوش تغییرات اساسی شده است. استفاده کنندگان کامپیوتر به منظور استفاده از دستاوردها و مزایای فن آوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مولفه های تاثیر گذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می باشند. امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری از جمله این مولفه ها بوده که نمی توان آن را مختص یک فرد و یا سازمان در نظر گرفت.

پرداختن به مقوله امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری در هر کشور، مستلزم توجه تمامی کاربران صرفنظر از موقعیت شغلی وسنی به جایگاه امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری بوده و می بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد. بموازات حرکت بسمت یک سازمان مدرن و مبتنی بر تکنولوژی اطلاعات، می بایست تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده گردد. مهمترین مزیت و رسالت شبکه های کامپیوتری، اشتراک منابع سخت افزاری و نرم افزاری است. کنترل دستیابی و نحوه استفاده از منابع به اشتراک گذاشته شده، از مهمترین اهداف یک سیستم امنیتی در شبکه است. با گسترش شبکه های کامپیوتری خصوصا" اینترنت ، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته شده، وارد مرحله جدیدی شده است.

در این راستا، لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، پایبند به یک استراتژی خاص بوده و بر اساس آن سیستم امنیتی را اجراء و پیاده سازی نماید. عدم ایجاد سیستم مناسب امنیتی، می تواند پیامدهای منفی و دور از انتظاری را بدنبال داشته باشد. استراتژی سازمان ما برای حفاظت و دفاع از اطلاعات چیست؟ در صورت بروز مشکل امنیتی در رابطه با اطلاعات در سازمان، بدنبال کدامین مقصر می گردیم ؟ شاید اگر در چنین مواردی، همه مسائل امنیتی و مشکلات بوجود آمده را به خود کامپیوتر نسبت دهیم، بهترین امکان برون رفت از مشکل بوجود آمده است، چراکه کامپیوتر توان دفاع کردن از خود را ندارد. آیا واقعا" روش و نحوه برخورد با مشکل بوجود آمده چنین است ؟در حالیکه یک سازمان برای خرید سخت افزار نگرانی های خاص خود را داشته و سعی در برطرف نمودن معقول آنها دارد، آیا برای امنیت و حفاظت از اطلاعات نباید نگرانی بمراتب بیشتری در سازمان وجود داشته باشد ؟

3_5 دشمنان، انگیزه ها، انواع حملات اطلاعات

امنیت از دیرباز یکی از اجزای اصلی زیرساخت‌های فناوری اطلاعات به شمار می‌رفته است. تهدیدهای امنیتی تنها منحصر به تهدیدات الکترونیکی نیستند، بلکه هر شبکه باید از نظر فیزیکی نیز ایمن گردد. خطرات الکترونیکی غالباً شامل تهدیدات هکرها و نفوذگران خارجی و داخلی در شبکه‌ها می باشند. در حالی که امنیت فیزیکی شامل کنترل ورود و خروج پرسنل به سایت‌های شبکه و همچنین روال‌های سازمانی نیز هست. برای پیاده سازی امنیت در حوزه‌های فوق، علاوه بر ایمن‌سازی سخت‌افزاری شبکه، نیاز به تدوین سیاست‌های امنیتی در حوزه فناوری اطلاعات در یک سازمان نیز می باشد. در این راستا لازم است از روال‌های استانداردی استفاده شود که به واسطه آن‌ها بتوان ساختار یک سازمان را برای پیاده سازی فناوری اطلاعات ایمن نمود. بمنظور دفاع موثر و مطلوب در مقابل حملات به اطلاعات و سیستم های اطلاعاتی، یک سازمان می بایست دشمنان، پتانسیل و انگیزه های آنان و انواع حملات را بدرستی برای خود آنالیز تا از این طریق دیدگاهی منطقی نسبت به موارد فوق ایجاد و در ادامه امکان برخورد مناسب با آنان فراهم گردد.



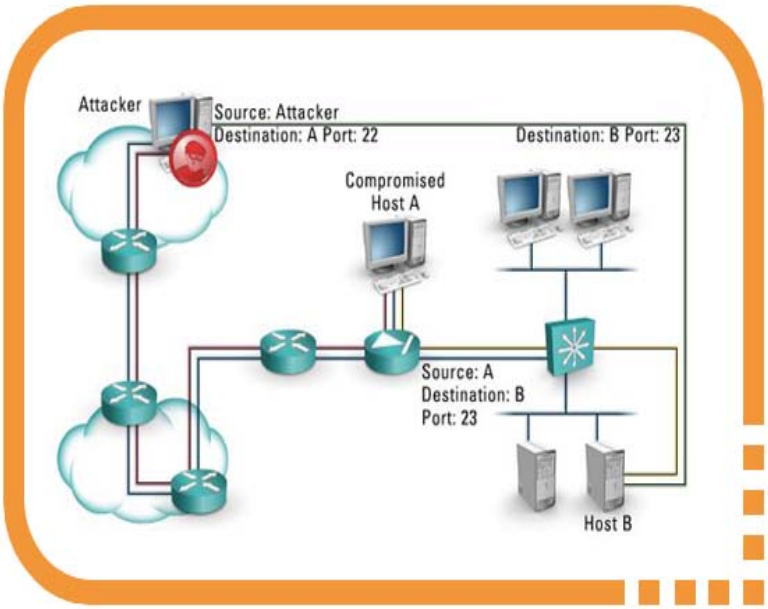
5_4 تهدیدهای امنیتی شبکه

تهدیدهای بالقوه برای امنیت شبکه‌های کامپیوتری به صورت عمده عبارتند از:

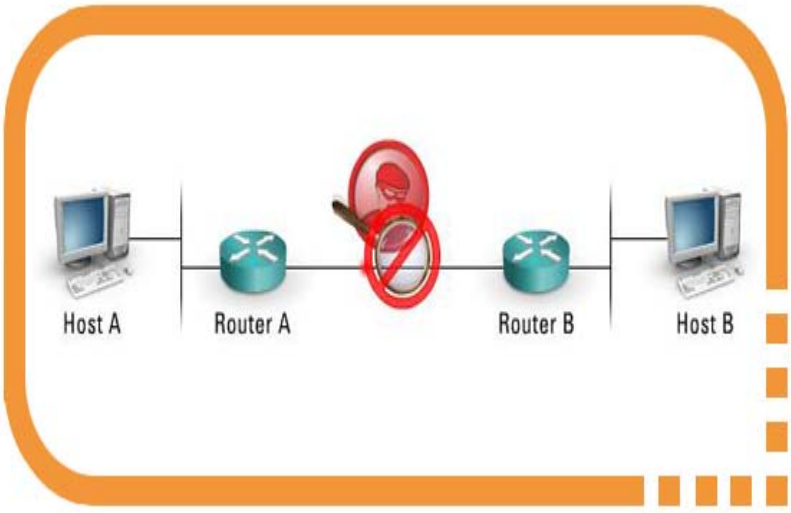
- فاش شدن غیرمجاز اطلاعات در نتیجه استراق‌سمع داده‌ها یا پیام‌های در حال مباد له روی شبکه
- قطع ارتباط و اختلال در شبکه به واسطه یک اقدام خرابکارانه
- تغییر و دستکاری غیر مجاز اطلاعات یا یک پیغام ارسال‌شده برای جلوگیری از این صدمات باید سرویس‌های امنیتی زیر در شبکه‌های کامپیوتری ارائه شود و زمانی که یکی از سرویس‌های امنیتی نقص شود بایستی تمامی تدابیر امنیتی لازم برای کشف و جلوگیری رخنه در نظر گرفته شود
- محرمانه ماندن اطلاعات
- احراز هویت فرستنده پیغام
- سلامت داده‌ها در طی انتقال یا نگهداری
- کنترل دسترسی و امکان منع افرادی که برای دسترسی به شبکه قابل اعتماد نمی باشد.
- در دسترس بودن تمام امکانات شبکه برای افراد مجاز و عدم امکان اختلال در دسترسی

ضمنا از موارد مهم حملات فنی در شبکه می توان به این موارد اشاره نمود:

- IP Spoofing

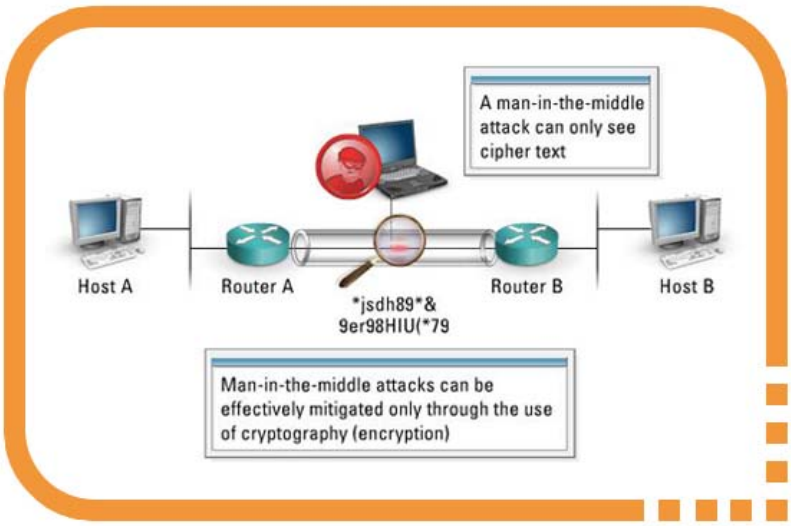


- Sniffing

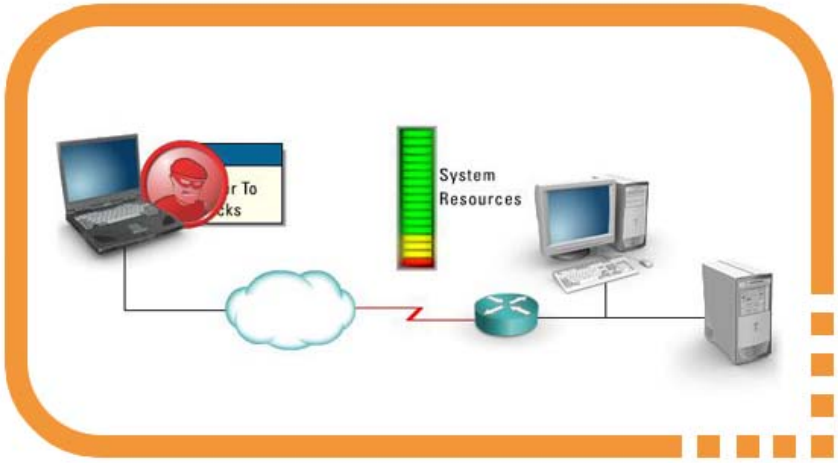


♦ Session Hijacking

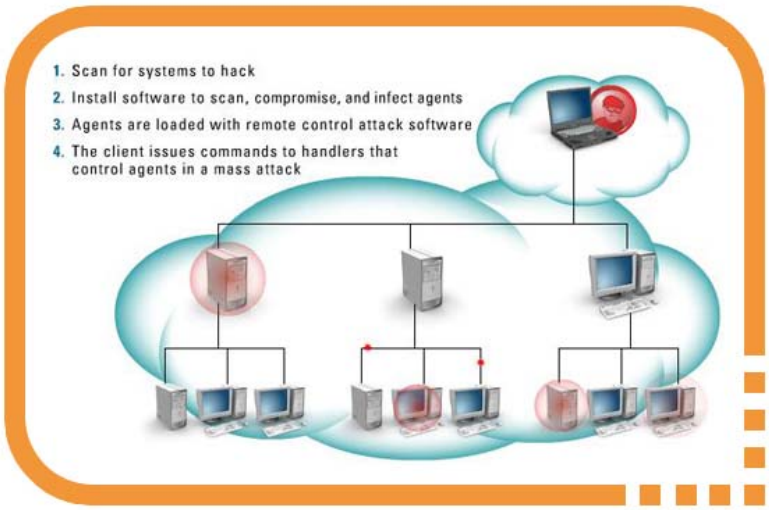
♦ Man In The Middle Attack



♦ Denail Of Service(DOS)



- Distributed Denial Of Service(DDOS)



- Types Of Trojans,Spywares,Worms & Viruses
- Application Layer Attacks such as Buffer Overflow ,SQL Injection …

5_5 سیاست های امنیتی

همانطور که در قبل به مقوله امنیتی در شبکه ها اشاره شد،امنیت شبکه یک مسأله مهم برای ادارات و شرکتهای دولتی و ازمان های کوچک و بزرگ است. یک سیستم امنیتی فیزیکی و شخصی بمنظور کنترل و هماهنگی در دستیابی به هر یک از عناصر حیاتی در محیط های مبتنی بر تکنولوژی اطلاعات، نیز ایجاد گردد. ایمن سازی اطلاعات از جمله مواردی است که می بایست موفقیت خود را در عمل و نه در حرف نشان دهد. بنابراین لازم است که پس از تدوین سیاست ها و دستورالعمل های مربوطه، پیگیری مستمر و هدفمند جهت اجرای سیاست ها و دستورالعمل ها ، دنبال گردد. سازمان های بزرگ وکوچک نیازمند ایجاد سیاست های امنیتی لازم در خصوص استفاده از کامپیوتر و ایمن سازی اطلاعات و شبکه های کامپیوتری می باشند.

5_6 استراتژی

دفاع درعمق، عنوان یک استراتژی عملی بمنظور نیل به تضمین و ایمن سازی اطلاعات در محیط های شبکه امروزی است.استراتژی فوق، یکی ازمناسبترین وعملی ترین گزینه های موجود است که متاثر از برنامه های هوشمند برخاسته از تکنیک ها و تکنولوژی های متفاوت تدوین می گردد. استراتژی پیشنهادی، بر سه مولفه متفاوت ظرفیت های حفاظتی، هزینه ها و رویکردهای عملیاتی تاکید داشته و توازنی معقول بین آنان را برقرارمی نماید.

5_7 ایمن‌کردن شبکه

مدیریت ضعیف، فقدان آموزش و نبود ابزارها و کنترل‌های کافی باعث آسیب‌پذیری سیستم در برابر حملات می‌شوند. ارتباطات گسترده، دسترسی نفوذگرها° به سیستم را افزایش می‌دهد. تا موقعی که استانداردها به طور وسیع مورد استفاده قرار بگیرند، امنیت شبکه باید به صورت سیستم به سیستم مدیریت شود. برای مقابله با تهدیدات بالقوه به یک سیستم لازم نیست ابزارهای مختلفی به کار گرفته شود. بسیاری از کنترل‌هایی که با یک نوع خطر مقابله می‌کنند برای مقابله با اشکال دیگر تهدید نیز مناسبند.

5_8 کنترل‌های امنیت شبکه

برای حفاظت داده‌ها در شبکه‌های اختصاصی و عمومی و جلوگیری از دسترسی غیرمجاز باید کنترل‌های مناسب را اعمال نمود. مهمترین ابزار کنترل ود سترسی در شبکه ها ابزارهای دیواره آتش و یا firewall ها هستند که در کنار سیستم های تشخیص حملات یکی از موثرترین و کارآمدترین ابزارهای کنترل امنیت شبکه می باشد. هر کاربر باید آگاه باشد که با اتصال رایانه به شبکه چنانچه کنترل‌های لازم اعمال نشود، ممکن است اطلاعات خصوصی مورد دسترسی غیرمجاز قرار گیرد. باید جزئیات چگونگی حفاظت از داده‌ها در اختیار کاربران متصل به شبکه قرار گیرد.برای محافظت از داده‌های حساس که از شبکه‌های عمومی مانند اینترنت عبور می‌کند، توجه ویژه‌ای لازم است.

5_9 نظارت بر شبکه

آسیب‌پذیری‌های شبکه به دودسته کلی تقسیم می‌شوند:

- سرقت اطلاعات هنگام انتقال
- عدم تشخیص پیام‌های نامناسب و سرنمای[6] پیام‌های دریافتی هنگامی که اطلاعات از یک سیستم به سیستم دیگر منتقل می‌شود ممکن است اطلاعات در راه دزدیده شود.

5_10 ابزارهای نظارت

با استفاده از وسایل نظارتی می‌توان از افشا، دستکاری یا از بین بردن اطلاعات پیشگیری کرد:

1- نصب کنترل‌های استفاده و ذخیره روی وسایلی که بر اطلاعات انتقال‌یافته روی شبکه نظارت دارند یا آن را ثبت می‌کنند.
2- حصول اطمینان از اینکه کارمندان درک می‌کنند که استفاده از تجهیزات ICT به معنای رضایت از نظارت اعمال‌شده بر آنهاست.
3- اطمینان ازتداوم کنترل کیفیت‌ها با نگهداری ازفعالیت‌های ثبت‌شده.

- دفاع لایه ای، بهترین محصولات مربوط به ایمن سازی اطلاعات دارای نقاط ضعف ذاتی، مربوط به خود می باشند. بنابراین همواره زمان لازم در اختیار مهاجمان اطلاعاتی برای نفوذ در سیستم های اطلاعاتی وجود خواهد داشت.بدین ترتیب لازم است قبل از سوءاستفاده اطلاعاتی متجاوزان، اقدامات مناسبی صورت پذیرد. یکی از روش های موثر پیشگیری در این خصوص، استفاده از دفاع لایه ای در مکان های بین مهاجمان و اهداف مورد نظر آنان، می باشد. هر یک از مکانیزم های انتخابی، می بایست قادر به ایجاد موانع لازم درارتباط با مهاجمان اطلاعاتی (حفاظت) و تشخیص بموقع حملات باشد. بدین ترتیب امکان تشخیص مهاجمان اطلاعاتی افزایش و از طرف دیگر شانس آنها بمنظور نفوذ در سیستم و کسب موفقیت، کاهش خواهد یافت. استفاده از فایروال های تودرتو (هر فایروال در کنار خود از یک سیستم تشخیص مزاحمین ، نیز استفاده می نماید) در محدوده های داخلی و خارجی شبکه، نمونه ای از رویکرد دفاع لایه ای است. فایروال های داخلی ممکن است امکانات بیشتری را دررابطه با فیلتر سازی داده ها و کنترل دستیابی به منابع موجود ارائه نمایند.

جدول زیر رویکردهای دیگر بمنظور تحقق دفاع لایه ای را نشان می دهد.

نوع تهاجم	سطح اول دفاع	سطح دوم
غیر فعال	لایه ارتباطی و شبکه	برنامه های مبتنی بر امنیت
فعال	دفاع در محدوده های بسته (حفاظتی)	دفاع محیط محاسباتی
مجاور	امنیت فیزیکی و شخصی	کنترل و بررسی دقیق
خودی	امنیت فیزیکی و شخصی	نظارت و پیشگیری فنی
توزیع	نرم افزارهای مطمئن	کنترل های یکپارچگی

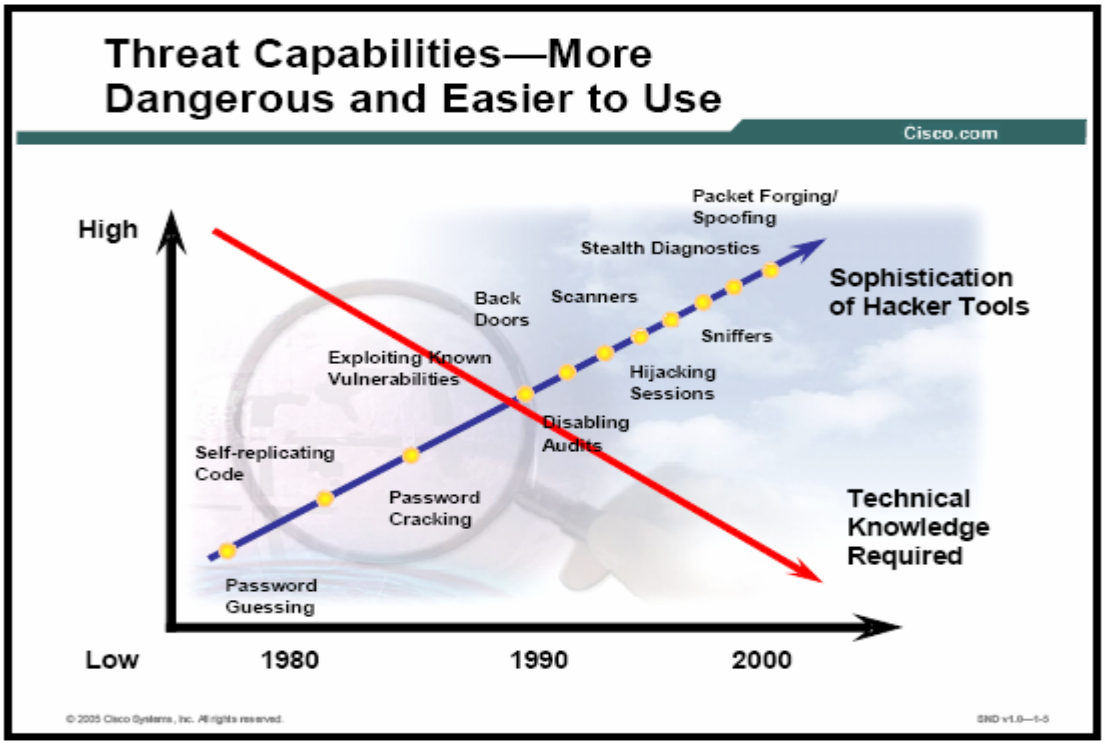
امنیتی هر یک از عناصر موجود در ایمن سازی اطلاعات (چه چیزی حفاظت شده و نحوه برخورد با تهاجم اطلاعاتی در محلی که از عنصر مربوطه استفاده شده، به چه صورت است ؟). پس از سنجش میزان اقتدار امنیتی هر یک از عناصر مربوطه، می توان از آنان در جایگاهی که دارای حداکثر کارآئی باشند، استفاده کرد. مثلا" می بایست از مکانیزم های امنیتی مقتدر در محدوده های مرزی شبکه استفاده گردد.

- استفاده از مدیریت کلید مقتدر و زیر ساخت کلید عمومی، که قادر به حمایت از تمام تکنولوژی های مرتبط با ایمن سازی اطلاعات بوده و دارای مقاومت مطلوب در مقابل یک تهاجم اطلاعاتی باشد.
- بکارگیری زیرساخت لازم بمنظور تشخیص مزاحمین، آنالیز و یکپارچگی نتایج بمنظور انجام واکنش های مناسب در رابطه با نوع تهاجم. زیر ساخت مربوطه می بایست به پرسنل عملیاتی، راهنمائی لازم در مواجه با سوالاتی نظیر: آیا من تحت تهاجم اطلاعاتی قرار گرفته ام ؟ منبع تهاجم چه کسی می باشد ؟ به چه فرد دیگری تهاجم شده است ؟ را ارائه نماید.

5_11 ارزیابی سطح امنیت یک شبکه با استفاده از Penetration Test

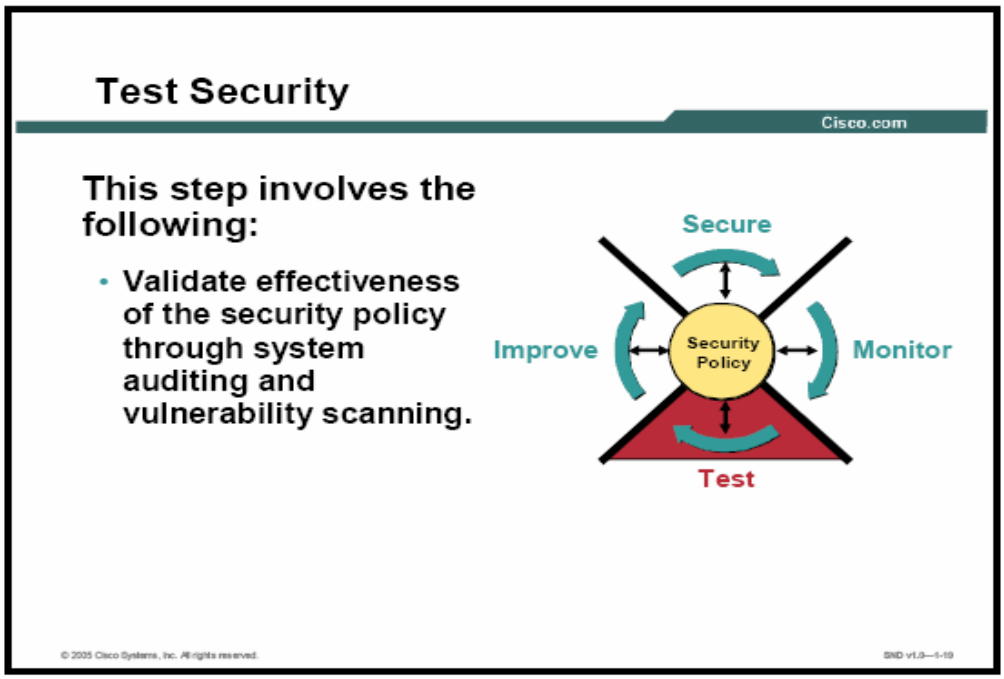
امروزه امنیت شبکه های کامپیوتری و توجه به رخنه‌های امنیتی در سیستم‌های شبکه‌ای و عجین شدن آنها با تجارت و فعالیت‌های اصلی سازمان در مقایسه با گذشته اهمیت فراوانی یافته است. نفوذ، تخریب، از کاراندازی و سرقت اطلاعات خسارتهای فراوانی را متوجه سازمانها می‌نماید که اغلب جبران آنها مشکل یا غیر ممکن است.

امروزه نفوذ، تخریب و سرقت اطلاعات به دانش زیادی نیاز ندارد



در این میان سازمان‌ها در جهت افزایش سطح ایمنی شبکه‌های خود اقدام به نصب ابزارهای متعددی مانند دیواره‌های آتش، سیستمهای تشخیص حملات، ضد ویروسها، سیستمهای تعیین اعتبار، شبکه-های خصوصی مجازی و پیاده سازی سیاستهای امنیتی می‌نمایند. این موارد همگی در افزایش ضریب ایمنی شبکه‌ها موثر بوده و ریسک تهدیدات الکترونیکی را تا حد چشمگیری کاهش می‌دهند.

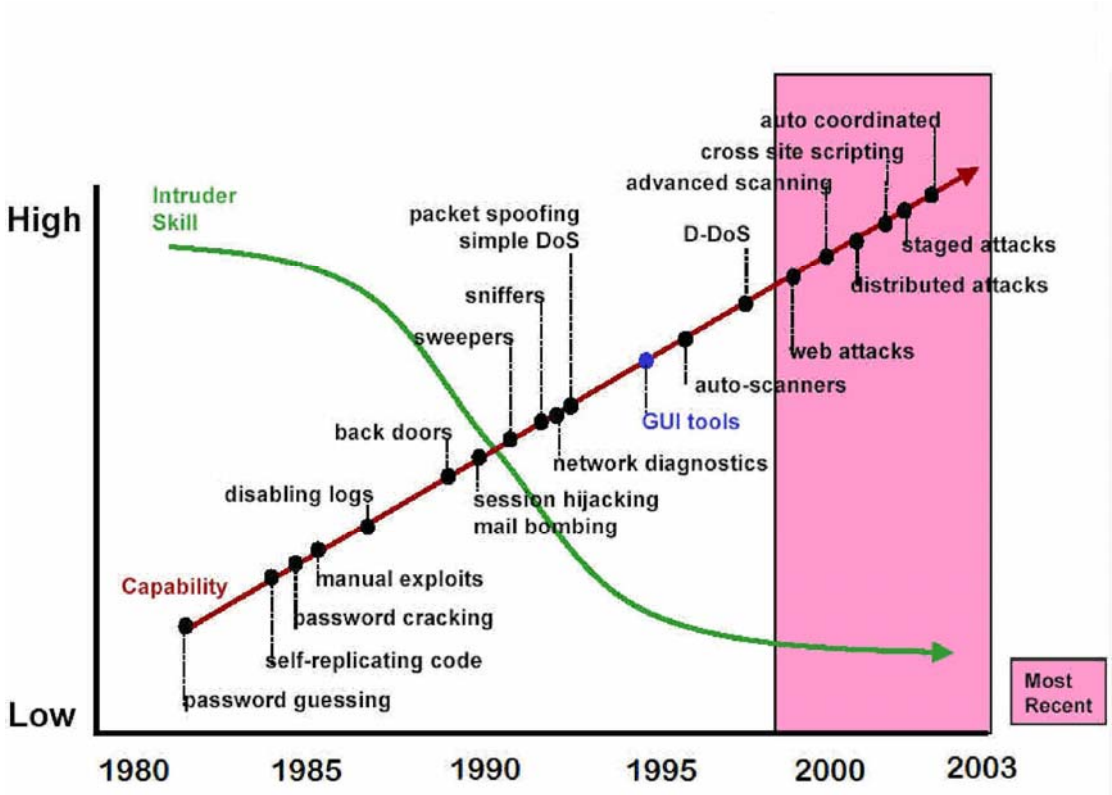
نکته حائز اهمیت این است که در حین انجام تنظیمات به دلیل خطای انسانی، کامل نبودن تنظیمها، عدم هماهنگی ابزارها و سیاستهای امنیتی و ... امکان دارد آسیب پذیری‌هایی در شبکه بوجود آمده و یا آسیب پذیری‌هایی دور از توجه مدیران شبکه وجود داشته باشند که مرتفع نگردیده‌اند. اگر چرخه 3 از پروسه امنیت شبکه را که تست سطح امنیت شبکه میباشد بررسی نماییم متوجه میگردیم که فرایند مذکور با توجه به رشد و گسترش شبکه‌ها ، امری پویا بوده و نیاز به تکرار در بازه‌های زمانی مشخصی دارد. بطور مثال اتصال یک شبکه جدید به شبکه فعلی، راه اندازی یک سرویس جدید، اتصال به مسیرهای ارتباطی جدید و ... همگی یک شبکه را با مخاطرات امنیتی جدیدی مواجـــه می‌نماید.



تست نفوذپذیری یا Penetration Test شامل مراحلی است که بصورت گام به گام و با استفاده از ابزارهای ulnerability/Security scanner و روشهای دستی آسیب پذیری‌های شبکه را کشف و راه‌کارهای قابل پیاده سازی در جهت رفع موارد فوق ارائه میدهد.

12_5 وابستگی سیستم ها به یک بستر خاص جهت برقراری امنیت

امروزه با توجه به رشد و توسعه صنعت نرم افزار و ابداع ابزار متنوع جهت بکار گیری این صنعت در جهت دلخواه ، انتخاب بهترین ابزار و تکنولوژی در راستای نیل به اهداف ، امری مهم و قابل توجه است. این مساله چه در مرحله طراحی و چه در مرحله اجرا می بایست رعایت گردد.بمانند مثال انتخاب Platform اجرا از میان .NET ویا Java وبه دنبال آن انتخاب زبان برنامه نویسی C# ، C++ ویا J2EE می بایست بر اساس نوع نیازها و اهداف مورد نظر و از پیش تعیین شده انجام گردد تا بتوان بهترین کارایی و بالاترین میزان بهره وری را از این صنعت بدست آورد.در این میان نکته حائز اهمیت و قابل تامل ، بر قراری امنیت در این مبحث می باشد. مساله امنیت در مقوله IT امروزه به یکی از مهمترین مسائل جهانی تبدیل شده است. با رشد چشمگیر صنعت IT از یکسو شاهد بهبود کارایی وسرعت در شبکه ها و سیستمها و از سوی دیگر همزمان شاهد پیشرفت وسیع متد ها و راهکارهای حمله و نفوذ به همین شبکه ها و سیستمها هستیم. امروزه با برخورداری از حداقل دانش و تعدد نرم افزارهای نفوذ و حمله ، می توان به راحتی به یکی از دهها متد حمله و نفوذ به شبکه ها و سیستمها دست یافت. نمودار ذیل این موضوع را به وضوح نشان می دهد.



اما از طرف دیگر بر قراری امنیت و جلو گیری از این همه راهکارهای حمله و نفوذ، (به خصوص آنکه هر روزه به تعداد وتنوع این روشها اضافه می گردد،) احتیاج به وجود متخصصین زبده امنیت ، دستگاههایی چون دیواره های آتش، سیستمهای تشخیص حملات و همچنین امنیت سطح Application را بیش از پیش ضروری جلوه می دهد.

در این مبحث،در لایه Application نکته حائز اهمیت آنست که فارغ از اینکه چه بستری برای طراحی و اجرا و چه زبان برنامه نویسی انتخاب شده است،می بایست تمامی نکات امنیتی مربوط به آنچه که انتخاب شده رعایت گردد. با دید ایمن سازی Application ، دیگر این مهم نیست که شما از میان Platform های جهانی و استاندارد، چه بستری را انتخاب می کنید؛ بلکه آنچه که مهم است رعایت دقیق اصول امنیتی مربوط به آن Platform است.مثلا در مرحله اجرا اگر زبان برنامه نویسی C# انتخاب شده است، برنامه نویس می بایست کاملا مسلط و آشنا به نکات امنیتی و ریزه کاریهای کد کردن و برنامه نویسی مربوط به آن زبان باشد.هرگاه این مساله کاملا رعایت گردد،امنیت لازم برقرار می شود. این مساله یک قانون کلی بوده و فارغ از وابستگی به نوع خاصی از زبان برنامه نویسی می باشد.در Web Application ، اینکه بستر راه اندازی IIS از Microsoft است ویا Apache از Linux ، در بحث برقراری امنیت مساله مهمی نیست، بلکه آنچه مهم است پیکر بندی دقیق و رعایت اصول ایمنی بستر منتخب است.

دلیل آنچه که در بالا ذکر شد را می توان با نگاهی دقیق به اتفاقات جهان نرم افزاری پیرامون ما ، درک نمود: بیشترین کاربرد امنیت در بحث شبکه و نرم افزار را می توان در سیستمهای بانکهای جهانی جستجو کرد.بعنوان نمونه CommerzBank آلمان، ترکیبی از Platform های مختلف از شرکتهای متفاوت را استفاده نموده است مانند بانک اطلاعاتی Sql Srv، وب سرور های IIS و Apache و... همچنین بسیاری از شرکتهای بین المللی نیز از بستر های Net. و... استفاده می کنند که در ذیل مشاهده می شود . همانطور که می بینیم آنچه مهم است رعایت اصوت امنیتی هر آنچه که انتخاب شده است می باشد.

پیوست

Partnering with 30 states and employing over 3,800 people, **ACS State** generated a thick-client Visual Basic interface for their mainframe Medicaid enrollment application (which is marketed to State organizations). ACS licenses the enhanced application to the governments of Iowa, Montana, West Virginia, and Wyoming, as well as Washington D.C.

AgFirst Farm Credit Bank, the premier agricultural lender in the eastern United States and Puerto Rico, providing more than $10 billion in loans to more than 79,000 farmers, ranchers and agribusinesses is leveraging Visual Studio .NET to significantly re-engineer and graphically enable an existing ALLTEL Loan Applications systems. It also integrates the ALLTEL application with AgFirst's PeopleSoft General Accounting application and a SQL Server data warehouse - all within Microsoft .NET. When completed, the new integrated system will extend to hundreds of concurrent users.

A leader in the life insurance industry providing innovative products and services to over eight million customers for more than 75 years, **AIG American General** wanted an easier solution for users to execute mainframe task in their call center. The provider leveraged to re-engineer and graphically-enable their core CICS policy management system. By also seamlessly integrating mainframe data into Microsoft Word templates, AIG American General reduced training time and increased agent productivity, as well as decreased development time for incorporating new functions.

The nations largest publicly held personal lines insurer, providing insurance products to more than 16 million households, **Allstate** wanted to sell insurance products and offer policyholder self-service via the Internet. The provider employed its new Web-based Good Hands Network, built with Microsoft Active Server Pages and residing on BizTalk Server. Implemented in a matter if months, the Good Hands Network allows Allstate policyholders to get a quote and buy coverage for cars, homes, condos or apartments. The site also allows customers to look up over 35 million policies, request changes in coverage, report claims, and check claim status.

Serving more than 900,000 customers in 11 of Arizona's 15 counties, **Arizona Public Service** generates, sells and delivers electricity and energy-related products and services. The utilities provider wanted to enable technicians in the field to receive work orders in their trucks directly from mainframe-based dispatch and records system, and allow the technicians to view and revise work orders remotely in areas where no wireless coverage is available. ClientBuilder provided a stand-alone intelligent front-end interface for a laptop in each truck with connectivity to multiple wireless IP networks.The project enabled faster dispatch of service technicians to high-priority repair sites, eliminated manual data entry of work order information from the field, and provided the ability to use most cost effective wireless network across the entire state.

The Canada Life Assurance Company, Canada's first domestic life insurance company with total assets under administration in excess of $64 billion, wanted to extend policy administration via the Internet for group life products to agents, group administrators, and ultimately to the employees/insured. The provider employed AS/400 data via a SQL server. The project immediately translated into lower policy administration costs, increased competitiveness, and improved market penetration with group products and programs. The new application

Convergys Corporation, a member of the S&P 500 and the global leader in integrated billing, employee care, and customer care services provided through outsourcing or licensing, wanted to add functionality to their website, providing customer's employees with a cash withdrawal capability from 401K savings plans. By moving away from UNIX boxes to NT boxes, Convergys saved 40% on future development costs.

Do it Best Corp., which currently distributes over 68,000 hardware and building products to 4,300 retail stores worldwide, is using robust Microsoft COM components directly from mainframe VSE logic. These components reside on the company's application server, and form the backbone of Infoplus, Do it Best Corp.'s new online application that allows distributors to view inventories and order products in real-time.

Electric Insurance Company (EIC), a direct writer of private passenger automobile and homeowner's insurance and a GE benefit provider for over 35 years, utilized a mainframe rating engine for both traditional and Internet lines of business. To eliminate the need to maintain two separate copies of the rating systems, the insurer licensed modern Web-based rating engine to seamlessly serve both lines of business. The tool wraps data from the Internet engine as a .NET Web service message and allows the mainframe to query this Web service whenever a user needs to access rating functionality

Automatic Switch Company (ASCO), a subsidiary of **Emerson Electric**, needed to provide manufacturers with real-time access to inventory and order entry. The company AS/400 functionality via Active Server Pages deployed on BizTalk Server. By providing customers with real-time access to inventory and order entry logic, ASCO immediately streamlined vital operations and significantly improved the customer experience.

Federal-Mogul, a global supplier of automotive components, modules, sub-systems and systems, booked over $5.4 billion in revenues in 2002. For its aftermarket division, the company wanted to build a new graphical interface for the North America Business System (NABS) mainframe application. ClientBuilder enabled the manufacturer to quickly develop a more modern Visual Basic interface for the mainframe application, and in the process, allow the company to reduce dependence on IBM technology. By using ClientBuilder to leverage mainframe functionality within the .NET architecture, Federal-Mogul is greatly improving operational efficiency and enhancing customer service.

First Health Services Corporation, one of the nation's leading healthcare management and information services companies specializing in public sector health care clients, needed to dramatically overhaul the presentation and workflow of its core mainframe call center application. It delivers an easy-to-use Windows-based graphical user interface with intuitive graphics and "point-and-click" navigation, integrates an automated call tracking and reporting system to eliminate manual logs, as well as connects to a new SQL database. and most importantly, improved the call center's ability to provide quality customer service. First Health customers include the State of Virginia and West Virginia Medical Institute.

GE Capital Bank

As **GE Capital Bank - Sweden**, a national division of GE Consumer Finance, was developing a new .NET application to support both the call center and online banking systems, the financial services provider needed to incorporate functionality from a licensed mainframe application. GE Capital Bank licensed ServiceBuilder for Visual Studio .NET to generate both .NET components and Web services for the new banking application. ServiceBuilder will work from the third-party vendor's mainframe, generating the components and Web services for deployment on BizTalk Server. By rapidly exposing proven mainframe logic within the .NET architecture, GE Capital Bank is slashing application development costs and delivering superior functionality to both the call center and directly to the consumer.

As a member of the Blue Cross Blue Shield Association, **Hawaii Medical Services Association (HMSA)** is the largest provider of healthcare in the state. Building out a new call center application on BizTalk Server with an ASP.NET graphical front-end, HMSA required direct access to core IMS logic. To satisfy the IT requirements, HMSA licensed Visual Studio .NET to rapidly expose IMS logic within the new Membership and Claims Inquiry Application.

HMSA
Blue Cross Blue Shield of Hawaii
Choices for a Healthier Hawaii

Maintaining a force of more than 1,400 agents, **Kansas City Life Insurance Company** serves 48 states and the District of Columbia. The provider is employing Active Server Pages to build a corporate portal that will be available to agents, as well as internal associates and call center employees. Unable to access logic residing within their CSC system administration package, CyberLife, via 3270 data streams, the provider needed ServiceBuilder to offer direct access to the CSC application logic, and then integrate that logic into the new .NET portal. ServiceBuilder is enabling Kansas City Life to

slash development costs, as they deliver their new portal in record time.

Kraft Foods markets many of the world's leading food brands in over 150 countries. After purchasing SAP to run the majority of daily accounting processing volume, Kraft Foods - Italy needed to provide existing mainframe applications with access to SAP data. SAP provides application programming interfaces for Microsoft .NET. When a mainframe user needs data, It goes to .NET, retrieves the information from SAP, and then updates the mainframe. By allowing the mainframe to quickly access necessary information, Kraft is reducing IT costs, enhancing operational efficiency, and enhancing client service.

MACSF, a large French insurance company, wanted to enhance operational efficiency by providing better integration between mainframe and desktop functionality. To accomplish this, when a user wants to quickly print a letter to a client, ServiceBuilder populates mainframe data into a Microsoft Word template. Also, ServiceBuilder allows the mainframe to consume data from a desktop application that calculates travel reimbursements, making accounting's life that much easier. By allowing the mainframe to both publish data and consume information from Microsoft .NET, ServiceBuilder is enabling MACSF to realize better employee productivity and reduced operational costs.

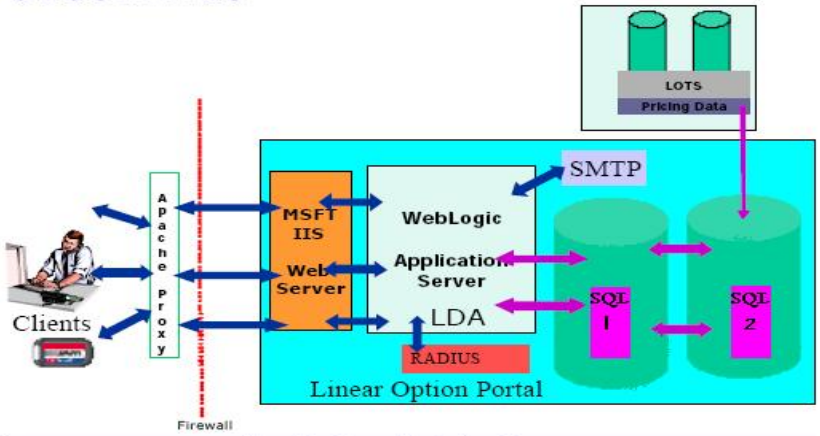
Serving more than 400,000 customers, **Memphis Light, Gas and Water** wanted to enable workers to interact and retrieve functionality from the mainframe through a Web-based solution, as well as automate the tedious form letters process.. By providing integration with Microsoft Word to generate form letters based on requests like employee verification, It automates the form letter process, including creation and mailing, as well as, significantly improves productivity and efficiency in the workplace.

While building the Juvenile Probation Information Program, an internal Web-based application for juvenile probation personnel to track juveniles who have been through the county's juvenile detention facilities, the **Sacramento County Probation Department** needed to integrate core mainframe functionality within the new system. built with Active Server Pages, and the host system. By doing so, It helped the county streamline operational efficiency, better manage juvenile offenders, and create a safer working environment for county personnel.

Financial Indemnity Company, a subsidiary of **Unitrin**, wanted to quickly Web-enable the FIC Specialty Lines policy submission and endorsement process.. FIC also pulls data from Oracle, SQL Server, and ClientAccess databases. FIC reduces endorsement turnaround time and costs to enable to agents to be more responsive to customers, enhances its offerings competitively, as well as fulfills "Easy to Do Business With" branding.

With over 30,000 enrolled, The **University of Central Florida** needed to provide students with quick access to department offerings, grade postings, class availability, registration, schedules, fee invoicing, and financial aid. They also wanted to provide the entire university staff, 4,000 employees (counselors to professors), with relevant information, such as class rolls, departmental accounts, budget allocation, benefits, authorized signature files, transaction audits, vacation days and more. UCF extended the life of its existing legacy applications by combining multiple mainframe and AS/400 systems - linked to a SQL server - within a new university Intranet. The new system immediately improved quality of life for both students and administrators alike.

COMMERZBANK
SECURITIES



Application Architecture

Portal Login

Portal: access status, updates - customized view for clients.

The Technology:

XML	SQL Server 2000
W2K	Apache
Java	WebLogic
MS IIS	RSA SecureID

قسمت دوم : استراتژی امنیت شبکه واحد فناوری اطلاعات وارتباطات

فصل اول : Data Center واحد فناوری ارتباطات و اطلاعات

Data Center ها مراکز تجمیع داده ها و بانک های اطلاعاتی می باشند، Data Center ها با در اختیارداشتن اتصالات پرسرعتی به اینترنت، و همچنین دراختیار داشتن سرورهای قوی ومتعدد، امکان راه‌اندازی سرورهای وب و ذخیره بانک های اطلاعاتی را برای سازمان ها ممکن ساخته اند.

Data Center واحد فناوری ارتباطات و اطلاعات مشتمل بر 4 سرور

1. **SQL server**
2. **Citrix serve**
3. **Web server**
4. **Active directory server**

می باشد. که هر سروردارای سرویس دهی لازم و مخصوص به خود است، توضیحات تکمیلی مربوط به هر سرور در ذیل ذکر می گردد.

SQL server 1_1

اطلاعات جزو سرمایه ها و دارایی های هر سازمان به حساب می آیند. امروزه اهمیت اطلاعات هم به عنوان یک منبع مهم تاکتیکی واستراتژیک در سازمان ها مطرح می باشد و هم به عنوان یک منبع عمده برای ارزش افزوده احتمالی، شناخته شده است. از آنجاییکه داده هاواطلاعات پارامترهای اولیه سیستم ها محسوب می گردند از اهمیت بسزایی برخوردارمی باشند، از اینروسازمانها به دنبال رویه ها و راهکارهای مناسب برای رسیدن به حفظ امنیت اطلاعات در سطح بالا می باشند. توفیق در ایمن سازی اطلاعات منوط به حفاظت از اطلاعات و سیستم های اطلاعاتی در مقابل حملات است. بد ین منظور باید ازسرویس های امنیتی متعددی استفاده گردد. سرویس های انتخابی، می بایست پتانسیل لازم در خصوص ایجاد یک سیستم حفاظتی مناسب، تشخیص بموقع حملات و واکنش سریع را داشته باشند.

درراستای تامین امنیت اطلاعات درسازمان صدا وسیما، علاوه برایجاد یکپارچگی بین مکانیزم های حفاظتی، می بایست همواره انتظار حملات اطلاعاتی را داشته و لازم است خود را به ابزارهای تشخیص و روتین های واکنش سریع، مجهز نماییم تا زمینه برخورد مناسب با مهاجمان و بازیافت اطلاعات در زمان مناسب فراهم گردد، در صورت تامین نشدن امنیت لازم برای Data center ، پیامدهای مخربی برای چرخه کاری سازمان بوجود می آید و تلاش چندین ساله سازمان هرز رفته ومعمولا" فرصت جبران آن نیز وجود نخواهد داشت .

Data center واحد فناوری اطلاعات و ارتباطات حامل داده ها و اطلاعات پردازش شده مربوط به سیستم های تدوین شده این واحد می باشد. لذا با توجه به اهمیت بالای داده ها از حساسیت بالایی بر خوردار می باشند. از اینرونقصان یا ازبین رفتن داده ها را می توان به منزله فلج شدن سیستم کاری تلقی کرد.

در ذیل به پاره ای از پیامد های ناشی از نقصان سیستم امنیتی **Data center** اشاره می گردد:

1. از دست دادن داده و اطلاعات مهم
2. اختلال در فرآیندهای جاری یک سازمان
3. پایین آمدن ضریب اعتماد به اطلاعات سیستم ها
4. وارد شدن اطلاعات نادرست عاملی برای توزیع اطلاعات غیر مفید و غیر قابل استفاده در یک چرخه کاری
5. عرضه اطلاعات حساس سازمان به افراد ناشناس و فرصت طلبان و بمخاطره افتادن اطلاعات سیستم ها
6. آسیب جدی به وجهه سازمان و بدنبال آن از دست دادن مشتریان و همکاران تجاری، و سلب اعتماد سازمانهای طرف قرارداد.

بانک های اطلاعاتی مربوط سیستم ها :

1. دبیرخانه
2. حضور و غیاب
3. پرسنلی (ساماندهی)
4. آگهی بازرگانی

داده های مربوط به پرسنلی (ساماندهی)

کلیه بانک های اطلاعاتی مربوط به مشخصات پرسنل واقع در طرح ساماندهی از بدو تشکیل تا به امروز را شامل می گردد، البته قابل ذکر است که کلیه داده های اطلاعاتی پرسنل رسمی سازمان تا پایان سال 84، در این بانک اطلاعاتی موجود است ، بنابراین این بانک اطلاعاتی، یکی از مهمترین منابع داده ای سازمان می باشد.

داده های مربوط به حضور و غیاب :

1. اطلاعات مربوط به تردد پرسنل
2. اطلاعات تائید انجام کار
3. مرخصی پرسنل

❖ **سیستم حضور و غیاب در واحد های ذیل در سطح حوزه معاونت اداری و مالی مورد استفاده قرار گرفته است .**

1. منابع انسانی (امور کارکنان)
2. ، اداره کل تمور حقوقی
3. اداره کل بودجه
4. انبار
5. دریافت و کنترل کالا
6. بازنشستگی
7. فناوری اطلاعات و ارتباطات

داده های مربوط به آگهی بازرگانی :

سیستم آگهی در واحد بازرگانی مورد استفاده قرار گرفته است، و بانک های مربوط به این سیستم در ذیل ذکر شده است .

1. اطلاعات مربوط به آگهی ها
2. اطلاعات مربوط به کنداکتورهای پخش

اشاره به این نکته لازم است که داده های بانکهای اطلاعاتی سیستم های فوق الـذکر، پایـه و بدنـه اصلی چرخه کاری سیستم های سازمان است، از اینـرواز اهمیـت فـوق العـاده ای بـرای سـازمان برخوردار می باشد. همچنین به دلیل اهمیت و حـساسیت داده هـا، برقـراری شـرایط امنیتـی لازم، امری واجب و اجتناب ناپذیر است.

Web server 2_1

امروزه با نسل جدیدی از برنامه ها مواجه می باشـیم کـه از زیرسـاخت اینترنـت و اینترانـت بـه عنوان بستری مناسب بمنظور سرویس دهی استفاده می نمایند. web، امکان دسترسی مستقیم و سهل الوصول کاربران به برنامه های کاربردی را امکان پذیر ساخته است. با اسـتفاده از ایـن سـرویس، در حال حاضر سیستم های تدوین شده بر روی وب سایت www.office.irib.ir حوزه معاونت فنـاوری اطلاعات وارتباطات برای دسترسی کاربران و کارمندان حوزه بر روی web server قرار گرفته اسـت .

Active directory server 3_1

در این سرور حق دسترسی کاربران به سیستم ها به صورت گروه های مجزا و بر اساس واحدهای کاری در سطح حوزه اداری و مالی با توجه به حوزه کاری تعریف شده برای سرور می باشد. برقراری امنیت لازم جهت حفاظت از این سرور امری حتمی و لازم الاجرا می باشد، چرا که در صورت دسترسی نامجاز افراد به این سرورامکان تغییر سطوح دسترسی و نهایتا" دسترسی کامل به اطلاعات حیاتی متمرکز بر روی بانکهای اطلاعاتی حیاتی متمرکز است.

فصل دوم : افق کاری Data Center واحد فناوری اطلاعات و ارتباطات :

با توجه به اینکه مدیریت و تامین امنیت اطلاعات بر روی داده های متمرکز سهل الوصول و هوشمندانه تراست در این خصوص واحد فناوری اطلاعات وارتباطات در راستای نیل به هدف در این زمینه در نظر دارد بانک های اطلاعاتی مربوط به سیستم های اداری ومالی کل سازمان مانند سیستمهای بودجه ، بانکهای طرف قرارداد سازمان،کلیه اطلاعات پرسنلی ، سیستم وام و... را در Data Center این واحد متمرکز نماید. بدیهی است مهمترین این سیستمها، سیستمهای حاوی اطلاعات مالی سازمان می باشد. از اینرو شرحی مختصر از بانک های اطلاعاتی مربوط به سیستم های بانک و بودجه در ذیل ذکر می گردد.

بانک های اطلاعاتی سیستم بانک

بانک های اطلاعاتی سیستم بانک، داده های مربوط به چرخه کاری سیستم بانک را شامل می گردد،داده های مربوط به حساب های بانکی اعم از تراکنشهای روزانه و مانده حسابها و بقیه آیتم های موجود در برنامه حسابهای بانکی سازمان بسیار محرمانه بوده و از نظر طبقه بندی اطلاعات در رده فوق محرمانه می باشد، این اطلاعات مربوط به تمامی شعب بانک تجارت، ملی و ملت طرف قرار داد سازمان می باشد. تمامی حسابهای مربوط به معاونتها، ادارات کل، شهرستانها و حسابداری کل سازمان در این بانک اطلاعاتی وجود دارد.

به عنوان مثال : تراکنش های حسابداری کل به میزان مشخصی بابت پرداخت نقدی چک به بانک تجارت گلوبندک و مانده حساب آن تماما" در بانک اطلاعاتی این مرکز گزارش گیری می شود. که این دسترسی به صورت کلی صرفا برای معاونت محترم اداری و مالی سازمان مورد نیاز می باشد.در صورت لزوم درآینده، جهت مدیران مالی واحد ها بر طبق اعلام ودستورکتبی، معاونت محترم اداری و مالی این امکان به افراد فوق داده می شود تا تنها بتوانند ریز حساب مختص به آن واحد را داشته باشند.

بانک های اطلاعاتی سیستم بودجه

شامل بانک اطلاعاتی بودجه سالیانه اختصاص یافته تهران و کلیه مراکز شهرستانها وجداول هزینه و بودجه به تفکیک فصول در هریک از زیر شاخه های امور، بخش و برنامه می باشد. با استفاده از این اطلاعات امکان گزارشگیری،نمایش و مقایسه بودجه تخصیص یافته سالانه حوزه های ریاست، معاونت، رادیو ها، سیما و شبکه ها و در نهایت مراکز شهرستانها برای مدیران ارشد سازمان مهیامی باشد. بدیهی است چنین اطلاعاتی کاملا محرمانه بوده و امکان رویت آن تنها برای افراد ذی صلاح مبایست فراهم باشد. بنابراین حفظ و نگاهداری مطمئن از این اطلاعات جز وظایف اصلی مرکز داده انفورماتیک اداری و مالی می باشد.

آنچه ذکر شد نمونه هایی از بانکهای اطلاعاتی مهم و حساس در این مرکز داده است ؛ از آنجا که تولید ، توزیع و جریان چنین اطلاعاتی در سازمان ، وظیفه واحد فناوری اطلاعات وارتباطات معاونت اداری و مالی می باشد، بنابراین سرمایه گذاری در این بخش جهت ایمن سازی ساختار شبکه و در نهایت ایمن نمودن مرکز داده این واحد، امری مهم و الزامی به نظر می رسد.