بسم الله الرحمن الرحيم

سیستم مدیریت امنیت اطلاعات

Information Security Management System

(ISMS)

آرامش در زندگی بدون امنیت امکان پذیر نیست .

همیشه باید نگران باشید.

IT یک سکه دوروست : هم فرصت است و هم تهدید ! اگر به همان نسبتی که به توسعه و همه گیری اش توجه و تکیه میکنیم به "امنیت" آن توجه نکنیم میتواند به سادگی و در کسری از ثانیه تبدیل به یک تهدید و مصیبت بزرگ شود.

نیاز روزافزون به استفاده از فناوریهای نوین در عرصه اطلاعات و ارتباطات، ضرورت استقرار یک نظام مدیریت امنیت اطلاعات را بیش از پیش آشکار می‌نماید .

مقدمه

امروزه شاهد گسترش حضور کامپیوتر در تمامی ابعاد زندگی خود می باشیم . کافی است به اطراف خود نگاهی داشته باشیم تا به صحت گفته فوق بیشتر واقف شویم . 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 و سنی 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. وجود ضعف امنیتی در شبکه های کامپیوتری و اطلاعاتی ، عدم آموزش و توجیه صحیح تمامی کاربران صرفنظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات ، عدم وجود دستورالعمل های لازم برای پیشگیری از نقایص امنیتی ، عدم وجود سیاست های مشخص و مدون به منظور برخورد مناسب و بموقع با اشکالات امنیتی ، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملا" زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می دهد.

.

به طور کلی می توان فرایند امن سازی را در ۴ شاخه ی اصلی طبقه بندی کرد :

۱- امنیت در رایانه ها

۲- امنیت در شبکه ها

۳- امنیت در سازمان ها

۴-امنیت کاربران

ISMS چیست ؟

برگرفته از کلمات زیر و به معنای "سیستم مدیریت امنیت اطلاعات" است .
Information Security Management System

ISMS به مدیران این امکان را می دهد تا بتوانند امنیت سیستم های خود را با به حداقل رساندن ریسک های تجاری کنترل کنند.

سیستم مدیریت امنیت اطلاعات (ISMS) راهکار حل مشکلات امنیتی در سیستم‌های اطلاعاتی است، یک سیستم جامع امنیتی بر ۴ پایه بنا می‌شود:

- **بررسی و تحلیل سیستم اطلاعاتی**
- **سیاستها و دستورالعملهای امنیتی**
- **تکنولوژی و محصولات امنیت**
- **عوامل اجرایی**

حفاظت سه بعدی از اطلاعات سازمان

- حفظ محرمانه بودن اطلاعات از طریق اطمینان از دسترسی اطلاعات تنها توسط افراد مجاز
- حفظ یکپارچگی اطلاعات از لحاظ دقت و کامل بودن و روشهای پردازش
- قابلیت دسترسی اطلاعات و دارایی های مرتبط توسط افراد مجاز در زمان نیاز

علل بروز مشکلات امنیتی

ضعف فناوری

ضعف پیکربندی

ضعف سیاست ها

ضعف فناوری

- ضعف پروتکل TCP/IP
- ضعف سیستم عامل
- ضعف تجهیزات شبکه ای

ضعف پیکربندی

- استفاده غیرایمن از account کاربران
- استفاده از system account که رمز عبور آنها به سادگی قابل تشخیص است.
- عدم پیکربندی صحیح سرویس های اینترنت
- غیرایمن بودن تنظیمات پیش فرض در برخی محصولات
- عدم پیکربندی صحیح تجهیزات شبکه ای

ضعف سیاست ها

- عدم وجود یک سیاست امنیتی مکتوب
- سیاست های سازمانی
- رها کردن مدیریت امنیت شبکه به حال خود
- نصب و انجام تغییرات مغایر با سیاست های تعریف شده
- عدم وجود برنامه ای مدون جهت برخورد با حوادث غیرمترقبه

داده ها و اطلاعات حساس در معرض تهدید

تقریبا" هر نوع تهاجم ، تهدیدی است در مقابل حریم خصوصی ، پیوستگی ، اعتبار و صحت داده ها .یک سارق اتومبیل می تواند در هر لحظه صرفا" یک اتومبیل را سرقت نماید ، در صورتی که یک مهاجم با بکارگیری صرفا" یک دستگاه کامپیوتر ، می تواند آسیب های فراوانی را متوجه تعداد زیادی از شبکه های کامپیوتری نموده و باعث بروز اشکالاتی متعدد در زیرساخت اطلاعاتی یک کشورگردد. آگاهی لازم در رابطه با تهدیدات امنیــتی و نحوه حفاظت خود در مقابل آنان ، امکان حفاظت اطلاعات و داده های حساس را در یک شبکه کامپیوتری فراهم می نماید .

ویروس ها

ویروس های کامپیوتری ، متداولترین نوع تهدیدات امنیتی در سالیان اخیر بوده که تاکنون مشکلات گسترده ای را ایجاد و همواره از خبرسازترین موضوعات در زمینه کامپیوتر و شبکه های کامپیوتری ، بوده اند. ویروس ها ، برنامه هائی کامپیوتری می باشند که توسط برنامه نویسان گمراه و در عین حال ماهر نوشته شده و بگونه ای طراحی می گردند که قادر به تکثیر خود و آلودگی کامپیوترها بر اثر وقوع یک رویداد خاص ، باشند . مثلا" ویروس ها ئی که از آنان با نام "ماکرو ویروس " یاد می شود ، خود را به فایل هائی شامل دستورالعمل های ماکرو ملحق نموده و در ادامه ، همزمان با فعال شدن ماکرو ، شرایط لازم به منظور اجرای آنان نیز فراهم می گردد.برخی از ویروس ها بی آزار بوده و صرفا" باعث بروز اختلالات موقت در روند انجام عملیات در کامپیوتر می شوند (نظیر نمایش یک پیام مضحک بر روی صفحه نمایشگر همزمان با فشردن یک کلید خاص توسط کاربر) . برخی دیگر از ویروس ها دارای عملکردی مخرب تر بوده و می توانند مسائل و مشکلات بیشتری نظیر حذف فایل

ها و یا کاهش سرعت سیستم را به دنبال داشته باشند. یک کامپیوتر صرفا" زمانی آلوده به یک ویروس می گردد که شرایط و امکان ورود ویروس از یک منبع خارجی (اغلب از طریق فایل ضمیمه یک نامه الکترونیکی و یا دریافت و نصب یک فایل و یا برنامه آلوده از اینترنت) ، برای آن فراهم گردد . زمانی که یک کامپیوتر در شبکه ای آلوده گردید ، سایر کامپیوترها ی موجود در شبکه و یا سایر کامپیوترهای موجود در اینترنت، دارای استعدادی مناسب به منظور مشارکت و همکاری با ویروس،خواهند بود.

برنامه های اسب تروا (دشمنانی در لباس دوست)

برنامه های اسب تروا و یا **Trojans** ، به منزله ابزارهائی برای توزیع کد های مخرب می باشند . تروجان ها ، می توانند بی آزار بوده و یا حتی نرم افزاری مفیدی نظیر بازی های کامپیوتری باشند که با تغییر قیافه و با لباسی مبدل و ظاهری مفید خود را عرضه می نمایند. تروجان ها ، قادر به انجام عملیات متفاوتی نظیر حذف فایل ها ، ارسال یک نسخه از خود به لیست آدرس های پست الکترونیکی ، می باشند. این نوع از برنامه ها صرفا" می توانند از طریق تکثیر برنامه های اسب تروا به یک کامپیوتر،دریافت فایل از طریق اینترنت و یا باز نمودن یک فایل ضمیمه همراه یک نامه الکترونیکی ، اقدام به آلودگی یک سیستم نمایند.

ویرانگران

در وب سایت های متعددی از نرم افزارهائی نظیر اکتیوایکس ها و یا اپلت های جاوا استفاده می گردد . این نوع برنامه ها به منظور ایجاد انیمیشن و سایر افکت های خاص مورد استفاده قرار گرفته و جذابیت و میزان تعامل با کاربر را افزایش می دهند . با توجه به دریافت و نصب آسان این نوع از

برنامه ها توسط کاربران ، برنامه های فوق به ابزاری مطئمن و آسان به منظور آسیب رسانی به سایر سیستم ها تبدیل شده اند . این نوع برنامه ها که به "ویرانگران" شهرت یافته اند ، به شکل یک برنامه نرم افزاری و یا اپلت ارائه و در دسترس استفاده کنندگان قرار می گیرند . برنامه های فوق ، قادر به ایجاد مشکلات متعددی برای کاربران می باشند(از بروز اشکال دریک فایل تا ایجاد اشکال در بخش اصلی یک سیستم کامپیوتری) .

حملات

تاکنون حملات متعددی متوجه شبکه های کامپیوتری بوده که می توان تمامی آنان را به سه گروه عمده تقسیم نمود :

- **حملات شناسائی :** در این نوع حملات ، مهاجمان اقدام به جمع آوری و شناسائی اطلاعات با هدف تخریب و آسیب رساندن به آنان می نمایند . مهاجمان در این رابطه از نرم افزارهای خاصی نظیر Sniffer و یا Scanner به منظور شناسائی نقاط ضعف و آسیب پذیر کامپیوترها ، سرویس دهندگان وب و برنامه ها ، استفاده می نمایند . در این رابطه برخی تولیدکنندگان ، نرم افزارهائی را با اهداف خیرخواهانه طراحی و پیاده سازی نموده اند که متاسفانه از آنان در جهت اهداف مخرب نیز استفاده می شود.مثلا" به منظور تشخیص و شناسائی رمز های عبور، نرم افزارهای متعددی تاکنون طراحی و پیاده سازی شده است .نرم افرارهای فوق با هدف کمک به مدیران شبکه ، افراد و کاربرانی که رمز عبور خود را فراموش کرده و یا آگاهی از رمز عبور افرادی که سازمان خود را بدون اعلام رمز عبور به مدیر شبکه ،

ترک نموده اند،استفاده می گردند. به هر حال وجود این نوع نرم افزارها واقعیتی انکارناپذیر بوده که می تواند به منزله یک سلاح مخرب در اختیار مهاجمان قرار گیرد .

- **حملات دستیابی :** دراین نوع حملات، هدف اصلی مهاجمان ، نفوذ در شبکه و دستیابی به آدرس های پست الکترونیکی ، اطلاعات ذخیره شده در بانک های اطلاعاتی و سایر اطلاعات حساس، می باشد.

- **حملات از کار انداختن سرویس ها :** در این نوع حملات ، مهاجمان سعی در ایجاد مزاحمت به منظور دستیابی به تمام و یا بخشی از امکانات موجود در شبکه برای کاربران مجازمی نمایند . حملات فوق به اشکال متفاوت و با بهره گیری از فن آوری های متعددی صورت می پذیرد . ارسال حجم بالائی از داده ها ی غیرواقعی برای یک ماشین متصل به اینترنت و ایجاد ترافیک کاذب در شبکه ، نمونه هائی از این نوع حملات می باشند.

ره گیری داده (استراق سمع)

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 .

کلاهبرداری (ابتدا جلب اعتماد و سپس تهاجم)

کلاهبرداران از روش های متعددی به منظور اعمال شیادی خود استفاده می نمایند. با گسترش اینترنت این نوع افراد فضای مناسبی برای اعمال مخرب خود یافته اند (چراکه می توان به هزاران نفر در زمانی کوتاه و از طریق اینترنت دستیابی داشت) . در برخی موارد شیادان با ارسال نامه های الکترونیکی وسوسه انگیز از خوانندگان می خواهند که اطلاعاتی خاص را برای آنان ارسال نموده و یا از یک سایت به عنوان طعمه در این رابطه استفاده می نمایند. به منظور پیشگیری از اینگونه اعمال ، می بایست کاربران دقت لازم در خصوص درج نام ، رمز عبور و سایر اطلاعات شخصی در سایت هائی که نسبت به هویت آنان شک و تردید وجود دارد را داشته باشند. با توجه به سهولت جعل آدرس های پست الکترونیکی ؛ می بایست به این نکته توجه گردد که قبل از ارسال اطلاعات شخصی برای هر فرد ، هویت وی شناسائی گردد.هرگز بر روی لینک ها و یا ضمائمی که از طریق یک نامه الکترونیکی برای شما ارسال شده است ، کلیک نکرده و همواره می بایست به شرکت ها و موسساتی که به طور شفاف آدرس فیزیکی و شماره تلفن های خود را ذکر نمی نمایند ، شک و تردید داشت .

نامه های الکترونیکی ناخواسته

از واژه Spam در ارتباط با نامه های الکترونیکی ناخواسته و یا پیام های تبلیغاتی ناخواسته ، استفاده می گردد. این نوع از نامه های الکترونیکی ، عموما" بی ضرر بوده و صرفا" ممکن است مزاحمت و یا دردسر ما را بیشتر نمایند . دامنه این نوع مزاحمت ها می تواند از به هدر رفتن زمان کاربر تا هرز رفتن فضای ذخیره سازی بر روی کامپیوترهای کاربران را شامل می شود .

ابزارهای امنیتی

پس از آشنائی با تهدیدات، می توان تمهیدات امنیتی لازم در خصوص پیشگیری و مقابله با آنان را انجام داد. بدین منظور می توان از فن آوری های متعددی نظیر آنتی ویروس ها و یا فایروال ها ، استفاده بعمل آورد .

نرم افزارهای آنتی ویروس

نرم افزارهای آنتی ویروس ، قادر به شناسائی و برخورد مناسب با اکثر تهدیدات مربوط به ویروس ها می باشند.(مشروط به اینکه این نوع نرم افزارها به صورت منظم بهنگام شده و بدرستی پشتیبانی گردند). نرم افزارهای آنتی ویروس درتعامل اطلاعاتی با شبکه ای گسترده از کاربران بوده و در صورت ضرورت پیام ها و هشدارهای لازم در خصوص ویروس های جدید را اعلام می نمایند. بدین ترتیب ، پس از شناسائی یک ویروس جدید ، ابزار مقابله با آن سریعا" پیاده سازی و در اختیار عموم کاربران قرار می گیرد. با توجه به طراحی و پیاده سازی ویروس های متعدد در سراسر جهان و گسترش سریع آنان از طریق اینترنت ، می بایست بانک اطلاعاتی ویروس ها بر اساس فرآیندی مشخص و مستمر ، بهنگام گردد .

سیاست های امنیتی

سازمان های بزرگ و کوچک نیازمند ایجاد سیاست های امنیتی لازم در خصوص استفاده از کامپیوتر و ایمن سازی اطلاعات و شبکه های کامپیوتری می باشند. سیاست های امنیتی ، مجموعه قوانین لازم به منظور استفاده از کامپیوتر و شبکه های کامپیوتری بوده که در آن وظایف تمامی کاربران دقیقا" مشخص و در صورت ضرورت ، هشدارهای لازم به کاربران در خصوص استفاده از منابع موجود در شبکه داده می شود . دانش تمامی کاربرانی که به تمام و یا بخشی از شبکه دستیابی دارند ، می بایست به صورت منظم و با توجه به سیاست های تدوین یافته ، بهنگام گردد (آموزش مستمر و هدفمند با توجه به سیاست های تدوین شده) .

رمزهای عبور

هر سیستم کامپیوتری می بایست دارای ایمنی مناسبی در خصوص رمز های عبور باشد . استحکام رمزهای عبور ، ساده ترین و در عین حال متداولترین روش به منظور اطمینان از این موضوع است که صرفا" افراد تائید شده و مجاز قادر به استفاده از کامپیوتر و یا بخش های خاصی از شبکه می باشند . فراموش نکنیم که زیرساخت های امنیتی ایجاد شده ، در صورتی که کاربران دقت لازم در خصوص مراقبت از رمزهای عبور خود را نداشته باشند ، موثر نخواهد بود (خط بطلانی بر تمامی تلاش های انجام شده) . اکثر کاربران در زمان انتخاب رمز عبور، از اعداد و یا کلماتی استفاده نمایند که بخاطر آوردن آنان ساده باشد(نظیر تاریخ تولد ، شماره تلفن).برخی دیگر از کاربران علاقه ای به تغییر منظم رمزهای عبور خود در مقاطع زمانی خاصی نداشته و همین امر می تواند زمنیه تشخیص رمزهای عبور توسط مهاجمان را فراهم نماید.

در زمان تعریف رمز عبور می بایست تمهیدات لازم در خصوص استحکام و نگهداری مطلوب آنان اندیشیده گردد :

- حتی المقدور سعی گردد از رمز های عبور فاقد معنی خاصی استفاده گردد .
- به صورت منظم و در مقاطع زمانی مشخص شده ، اقدام به تغییر رمزهای عبور گردد .
- عدم افشای رمزهای عبور برای سایرین

فایروال ها

فایروال ، راه حلی سخت افزاری و یا نرم افزاری به منظور تاکید (اصرار) بر سیاست های امنیتی می باشد .یک فایروال نظیر قفل موجود بر روی یک درب منزل و یا بر روی درب یک اطاق درون منزل می باشد . بدین ترتیب صرفا" کاربران تائید شده (آنانی که دارای کلید دستیابی می باشند) ، امکان ورود به سیستم را خواهند داشت . فایروال ها دارای فیلترهای از قبل تعبیه شده ای بوده که امکان دستیابی افراد غیر مجاز به منابع سیستم را سلب می نمایند .

رمزنگاری

فن آوری رمزنگاری ، امکان مشاهده ، مطالعه و تفسیر پیام های ارسالی توسط افراد غیر مجاز را سلب می نماید . از رمزنگاری به منظور حفاظت داده ها در شبکه های عمومی نظیر اینترنت استفاده می گردد . در این رابطه از الگوریتم های پیشرفته ریاضی به منظور رمزنمودن پیام ها و ضمائم مربوطه ، استفاده می شود.

چند نکته اولیه در خصوص ایمن سازی اطلاعات و شبکه های کامپیوتری

- **پذیرش مسئولیت به عنوان یک شهروند سایبر**

در صورتی که از اینترنت استفاده می نمائید ، شما به عنوان عضوی از جامعه جهانی و یا شهروند سایبر، محسوب شده و همانند یک شهروند معمولی ، دارای مسئولیت های خاصی بوده که می بایست پذیرای آنان باشیم .

- **استفاده از نرم افزارهای آنتی ویروس**

یک ویروس کامپیوتری ، برنامه ای است که می تواند به کامپیوتر شما نفوذ کرده و صدمات فراوانی را باعث گردد . نرم افزارهای آنتی ویروس به منظور حفاظت اطلاعات و کامپیوترها در مقابل ویروس های شناخته شده ، طراحی شده اند . با توجه به این که روزانه شاهد عرضه ویروس های جدید می باشیم ، می بایست برنامه های آنتی ویروس به صورت منظم و مرتب بهنگام گردند .

- **عدم فعال نمودن نامه های الکترونیکی ارسال شده توسط منابع نامشخص و گمنام**

نامه های الکترونیکی ارسالی توسط منابع ناشناس را می بایست همواره حذف نمود. به فایل هائی که به عنوان ضمیمه همراه یک نامه الکترونیکی ارسال می گردند، توجه گردد. حتی در صورتی که این نوع از نامه های الکترونیکی را از طریق دوستان و آشنایان خود دریافت می نمائید (خصوصا" اگر دارای انشعاب exe . باشند.) . برخی فایل ها مسئولیت توزیع ویروس ها را برعهده

داشته و می توانند باعث بروز اشکالات فراوانی نظیر حذف دائم فایل ها و یا بروز اشکال در یک وب سایت گردند. هرگز نمی بایست اقدام به فوروارد نمودن نامه های الکترونیکی برای سایر کاربران قبل از حصول اطمینان از ایمن بودن آنان نمود .

- **از رمزهای عبوری که تشخیص آنان مشکل می باشد ، استفاده نموده و آنان را محرمانه نزد خود نگه دارید**

هرگز رمزهای عبور خود را بر روی کاغذ ننوشته و آنان را به کامپیوتر نچسبانید! . تعداد زیادی از کاربران کامپیوتر دقت لازم در خصوص نگهداری رمز عبور خود را نمی نمایند و همین امر می تواند مشکلات متعددی را متوجه آنان ، نماید . رمزهای عبوری که تشخیص و یا حدس آنان آسان است ، گزینه های مناسبی در این رابطه نمی باشند . مثلا" در صورتی که نام شما Ali می باشد ، هرگز رمز عبور خود را با همین نام در نظر نگیرید . در فواصل زمانی مشخص و به صورت مستمر ، اقدام به تغییر رمز عبور خود نمائید . هرگز رمز عبور خود را در اختیار اشخاص دیگری قرار ندهید.برای انتخاب یک رمز عبور از ترکیب اعداد ، حروف و علائم استفاده گردد تا حدس و ردیابی آنان توسط افراد غیرمجاز ، مشکل شود .

- **استفاده از فایروال ها به منظور حفاظت کامپیوترها**

نصب و پیکربندی یک فایروال کار مشکلی نخواهد بود. یک فایروال ، امکان دستیابی و کنترل سیستم توسط مهاجمان را سلب نموده و پیشگیری لازم در خصوص سرقت اطلاعات موجود بر روی کامپیوتر را انجام می دهد .

- **Back-up گرفتن منظم از اطلاعات ارزشمند موجود بر روی کامپیوتر**

در فواصل زمانی مشخص و بر اساس یک برنامه خاص از اطلاعات ارزشمند موجود بر روی کامپیوتر backup گرفته شده و آنان را بر روی رسانه های ذخیره سازی نظیر لوح های فشرده ذخیره نمود .

- **دریافت و نصب منظم Patch های بهنگام شده مربوط به نقایص امنیتی**

نقایص امنیتی به صورت مرتب در سیستم های عامل و برنامه های کاربردی کشف می گردند . شرکت های تولید کننده نرم افزار ، به سرعت اقدام به ارائه نسخه های بهنگام شده ای با نام Patch نموده که کاربران می بایست آنان را دریافت و بر روی سیستم خود نصب نمایند.در این رابطه لازم است به صورت منظم از سایت های مربوط به تولید کنندگان نرم افزار بازدید بعمل آمده تا در صورت ارائه Patch ، آن را دریافت و بر روی سیستم نصب نمود .

- **بررسی و ارزیابی امنیتی کامپیوتر**

وضعیت امنیتی کامپیوتر خود را در مقاطع زمانی مشخصی ، بررسی نموده و در صورتی که خود نمی توانید این کار را انجام دهید از کارشناسان ذیربط استفاده نمائید .

- **غیر فعال نمودن ارتباط با اینترنت در زمان عدم استفاده**

اینترنت نظیر یک جاده دو طرفه است . شما اطلاعاتی را دریافت و یا ارسال می نمائید. غیرفعال نمودن ارتباط با اینترنت در مواردی که به آن نیاز نمی باشد، امکان دستیابی سایرین به کامپیوتر شما را سلب می نماید.

- **عدم اشتراک منابع موجود بر روی کامپیوتر با کاربرانی که هویت آنان نامشخص است**

سیستم عامل نصب شده بر روی یک کامپیوتر، ممکن است امکان به اشتراک گذاشتن برخی منابع موجود نظیر فایل ها را با سایر کاربران شبکه ، فراهم نماید. ویژگی فوق ، می تواند زمینه بروز تهدیدات امنیتی خاصی را فراهم نماید . بنابراین می بایست نسبت به غیرفعال نمودن ویژگی فوق ، اقدام لازم صورت پذیرد.

نقش عوامل انسانی در امنیت شبکه های کامپیوتری

یک سیستم کامپیوتری از چهار عنصر : سخت افزار ، سیستم عامل ، برنامه های کاربردی و کاربران ، تشکیل می گردد. سخت افزار شامل حافظه ، دستگاههای ورودی ، خروجی و پردازشگر بوده که بعنوان منابع اصلی پردازش اطلاعات ، استفاده می گردند. برنامه های کاربردی شامل کمپایلرها ، سیستم های بانک اطلاعاتی ، برنامه های تجاری و بازرگانی ، بازی های کامپیوتری و موارد متنوع دیگری بوده که روش بخدمت گرفتن سخت افزار جهت نیل به اهداف از قبل تعریف شده را مشخص می نمایند. کاربران ، شا مل انسان ، ماشین و دیگر کامپیوترها می باشد . هر یک از کاربران سعی در حل مشکلات تعریف شده خود از طریق بکارگیری نرم افزارهای کاربردی در محیط سخت افزار می

نمایند. سیستم عامل ، نحوه استفاده از سخت افزار را در ارتباط با برنامه های کاربردی متفاوتی که توسط کاربران گوناگون نوشته و اجراء می گردند ، کنترل و هدایت می نماید. بمنظور بررسی امنیت در یک سیستم کامپیوتری ، می بایست به تشریح و تبین جایگاه هر یک از عناصر موجود در یک سیستم کامپیوتری پرداخته گردد. در این راستا ، قصد داریم به بررسی نقش عوامل انسانی دررابطه با امنیت اطلاعات پرداخته و جایگاه هر یک از مولفه های موجود را تبین و تشریح نما ئیم . اگر ما بهترین سیستم سخت افزاری و یا سیستم عامل را بخدمت بگیریم ولی کاربران و یا عوامل انسانی درگیر در یک سیستم کامپوتری، پارامترهای امنیتی را رعایت ننمایند ، کاری را از پیش نخواهیم برد. وضعیت فوق مشابه این است که شما بهترین اتومبیل با درجه بالای امنیت را طراحی و یا تهیه نمائید ولی آن را در اختیار افرادی قرار دهید که نسبت به اصول اولیه رانندگی توجیه نباشند (عدم رعایت اصول ایمنی) . ما می بایست به مقوله امنیت اطلاعات در عصر اطلاعات نه بصورت یک کالا و یا محصول بلکه بصورت یک فرآیند نگاه کرده و امنیت را در حد یک محصول خواه نرم افزاری و یا سخت افزاری تنزل ندهیم .هر یک از موارد فوق ، جایگاه خاص خود را با وزن مشخص شده ای دارند و نباید به بهانه پرداختن به امنیت اطلاعات وزن یک پارامتر را بیش از آن چیزی که هست در نظر گرفت و پارامتر دیگری را نادیده گرفته و یا وزن غیر قابل قبولی برای آن مشخص نمائیم . بهرحال ظهور و عرضه شگفت انگیز تکنولوژی های نو در عصر حاضر ، تهدیدات خاص خود را نیز بدنبال خواهد داشت . ما چه کار می بایست بکنیم که از تکنولوژی ها استفاده مفیدی را داشته و در عین حال از تهدیدات مستقیم و یا غیر مستقیم آنان نیز مصون بمانیم ؟ قطعا" نقش عوامل انسانی که استقاده کنندگان مستقیم این نوع تکنولوژی ها می باشند ، بسیار محسوس و مهم است . با گسترش اینترنت و استفاده از آن در ابعاد متفاوت ، سازمانها و موسسات با مسائل جدیدی در

رابطه با امنیت اطلاعات و تهاجم به شبکه های کامپیوتری مواجه می باشند. صرفنظر از موفقیت و یا عدم موفقیت مهاجمان و علیرغم آخرین اصلاحات انجام شده در رابطه با تکنولوژی های امنیتی ، عدم وجود دانش و اطلاعات لازم (سواد عمومی ایمنی) کاربران شبکه های کامپیوتری و استفاده کنندگان اطلاعات حساس در یک سازمان ، همواره بعنوان مهمترین تهدید امنیتی مطرح و عدم پایبندی و رعایت اصول امنیتی تدوین شده ، می تواند زمینه ایجاد پتانسیل هائی شود که توسط مهاجمین استفاده و باعث بروز مشکل در سازمان گردد. مهاجمان همواره بدنبال چنین فرصت هائی بوده تا با اتکاء به آنان به اهداف خود نائل گردند. در برخی حالات اشتباه ما زمینه موفقیت دیگران! را فراهم می نماید . اگر سعی نمائیم بر اساس یک روش مناسب درصد بروز اشتباهات خود را کاهش دهیم به همان نسبت نیز شانس موفقیت مهاجمان کاهش پیدا خواهد کرد. مدیران شبکه (سیستم) ، مدیران سازمان و کاربران معمولی جملگی عوامل انسانی در یک سازمان می باشند که حرکت و یا حرکات اشتباه هر یک می تواند پیامدهای منفی در ارتباط با امنیت اطلاعات را بدنبال داشته باشد . در ادامه به بررسی اشتباهات متداولی خواهیم پرداخت که می تواند توسط سه گروه یاد شده انجام و زمینه بروز یک مشکل امنیتی در رابطه با اطلاعات حساس در یک سازمان را باعث گردد.

اشتباهات متداول مدیران سیستم

مدیران سیستم ، به افرادی اطلاق می گردد که مسئولیت نگهداری و نظارت بر عملکرد صحیح و عملیاتی سیستم ها و شبکه موجود در یک سازمان را برعهده دارند.در اغلب سازمانها افراد فوق ، مسئولیت امنیت دستگاهها ، ایمن سازی شبکه و تشخیص ضعف های امنیــتی موجود در رابطه با اطلاعات حساس را نیز برعهده دارند. بدیهی است واگذاری مسئولیت های متعدد به یک فرد، افزایش تعداد خطاء و اشتباه را بدنبال خواهد داشت . فشار عصبی در زمان انجام کار مستمر بر روی چندین موضوع متفاوت و بصورت همزمان ، قطعا" احتمال بروز اشتباهات فردی را افزایش خواهد داد.

در ادامه با برخی از خطاهای متداولی که ممکن است توسط مدیران سیستم انجام و سازمان مربوطه را با تهدید امنیتی مواجه سازد ، آشنا خواهیم شد.

۱ : عدم وجود یک سیاست امنیتی شخصی

اکثر قریب به اتفاق مدیران سیستم دارای یک سیاست امنیتی شخصی بمنظور انجام فعالیت های مهمی نظیر امنیت فیزیکی سیستم ها ، روش های بهنگام سازی یک نرم افزار و روشی بمنظور بکارگیری patch های جدید در زمان مربوطه نمی باشند .حتی شرکت های بزرگ و شناخته شده به این موضوع اذعان دارند که برخی از سیستم های آنان با همان سرعت که یک باگ و یا اشکال تشخیص و شناسائی می گردد ، توسط patch مربوطه اصلاح نشده است .در برخی حالات ، مدیران

سیستم حتی نسبت به آخرین نقاط آسیب پذیرتشخییص داده شده نیز آگاهی بهنگام شده ای را نداشته و قطعا" در چنین مواردی انتظار نصب **patch** مربوطه نیز توقعی بی مورد است . وجود نقاط آسیب پذیر در شبکه می تواند یک سازمان را در معرض تهدیدات جدی قرار دهد . امنیت فرآیندی است که می بایست بصورت مستمر به آن پرداخته شود و هرگز به اتمام نمی رسد.در این راستا لازم است، بصورت مستمرنسبت به آخرین حملات بهمراه تکنولوژی ها ی مربوطه ، آگاهی لازم کسب و دانش خود را بهنگام نمائیم .اکثر مدیران سیستم ، کارشناسان حرفه ای و خبره امنیتی نمی باشند ، در این رابطه لازم است ، بمنظور افزایش حفاظت و ایمن سازی شبکه ، اطلاعات و دانش مربوطه بصورت مستمر ارتقاء یابد .افرادیکه دارای گواهینامه های خاصی امنیتی و یا دانش و اطلاعات اضافه در رابطه با امنیت اطلاعات می باشند ، همواره یک قدم از کسانی مهارت آنان صرفا" محدود به شبکه است ، جلوتر می باشند .

در ادامه ، پیشنهاداتی بمنظور بهبود وضعیت امنیتی سازمان و افزایش و ارتقاء سطح معلومات مدیران سیستم ، ارائه می گردد :

- بصورت فیزیکی محل کار و سیستم خود را ایمن سازید .زمینه استفاده از سیستم توسط افرادیکه در محدوده کاری شما فعالیت دارند ، می بایست کاملا" کنترل شده و تحت نظارت باشد .
- هر مرتبه که سیستم خود را ترک می کنید ، عملیات **logout** را فراموش نکنید .در این رابطه می توان یک زمان **time out** را تنظیم تا در صورت فراموش نمودن عملیات **logout** ، سیستم قادر به حفاظت خود گردد.

- خود را عضو خبرنامه ها ی متفاوت امنیتی کرده تا شما را با آخرین نقاط آسیب پذیر آشنا نمایند. درحقیقت آنان چشم شما در این معرکه خواهند بود(استفاده مفید از تجارب دیگران) .
- سعی گردد بصورت مستمر از سایت های مرتبط با مسائل امنیتی دیدن تا درزمان مناسب با پیام های هشداردهنده امنیتی در رابطه با نرم افزارهای خارج از رده و یا نرم افزارهای غیر اصلاح شده (**unpatched**) آشنا گردید.
- مطالعه آخرین مقالات مرتبط با مسائل امنیتی یکی از مراحل ضروری و مهم در فرآیند خود آموزشی (فراگیری) مدیران شبکه است . بدین ترتیب این اطمینان بوجود خواهد آمد که مدیر مربوطه نسبت به آخرین اطلاعات و مسائل مربوطه امنیتی در کمیته های موجود ، توجیه است .
- استفاده از یاداشت ها و مقالات در ارتباط با هر نوع اطلاعات حساس نظیر رمزهای عبور و I هر چیزی که ممکن است زمینه ساز ایجاد یک پتانسیل آسیب پذیر و دستیابی به سیستم مطرح گردد را محدود نمائید. در صورتیکه از این نوع اطلاعات استفاده می شود، قبل ازترک محل کار ، آنها را از بین ببرید. افرادیکه دارای سوء نیت بوده در محدوده کاری شما می باشند ، می توانند ازمزایای ضعف های شناخته شده استفاده نمایند، بنابراین ضروری است استفاده از چنین یاداشت هائی محدود و یا بصورت کامل حذف گردد .

۲ : اتصال سیستم های فاقد پیکربندی مناسب به اینترنت

همزمان با گسترش نیازهای سازمان، سیستم ها و سرویس دهندگان جدیدی بر اساس یک روال معمول به اینترنت متصل می گردند. قطعا" توسعه سیستم با هدف افزایش بهره وری در یک سازمان دنبال خواهد شد.اکثر اینچنین سیستمهائی بدون تنظیمات امنیتی خاص به اینترنت متصل شده و می تواند زمینه بروز آسیب و حملات اطلاعاتی توسط مهاجمان را باعث گردد (در بازه زمانی که سیستم از لحاظ امنیتی بدرستی ممیزی نشده باشد ، این امر امکان پذیر خواهد بود). مدیران سیستم ممکن است به این موضوع استناد نمایند که سیستم جدید بوده و هنوز کسی آن را نمی شناسد و آدرس IP آن شناخته شده نیست ، بنابراین امکان شناسائی و حمله به آن وجود نخواهد داشت .طرز فکر فوق ، یک تهدید برای هر سازمان بشمار می رود . افراد و یا اسکریپت های پویش اتوماتیک در اینترنت ، بسرعت عملیات یافتن و تخریب این نوع سیستم های آسیب پذیر را دنبال می نمایند. در این راستا ، شرکت هائی خاصی وجود دارد که موضوع فعالیت آنان شبکه بوده و برای تست سیستم های تولیدی خود بدنبال سیستم های ضعیف و آسیب پذیر می گردند.(سیستم آسیب پذیر ما ابزار تست دیگران خواهد شد). بهرحال همواره ممکن است افرادی بصورت مخفیانه شبکه سازمان شما را پویش تا در صورت وجود یک نقطه آسیب پذیر، از آن برای اهداف خود استفاده نمایند.

لازم است در این راستا تهدیدات و خطرات را جدی گرفته و پیگری لازم در این خصوص انجام شود. در این رابطه موارد زیر پیشنهاد می گردد :

- **قبل از اتصال فیزیکی یک کامپیوتر به شبکه ، مجوز امنیتی لازم با توجه به سیاست های تدوین شده امنیتی برای آن صادر گردد (بررسی سیستم و صدور مجوز اتصال)**
- **کامپیوتر مورد نظر می بایست شامل آخرین نرم افزارهای امنیتی لازم بوده و از پیکربندی صحیح آنان می بایست مطمئن گردید.**
- **در صورتیکه لازم است بر روی سیستم مورد نظر تست های شبکه ای خاصی صورت پذیرد ، سعی گردد امکان دستیابی به سیستم فوق از طریق اینترنت در زمان تست ، بلاک گردد.**
- **سیستمی را که قصد اتصال آن به اینترنت وجود دارد ، نمی بایست شامل اطلاعات حساس سازمان باشد.**
- **سیستم مورد نظر را تحت برنامه های موسوم به Intrusion Detection System قرار داده تا نرم افزارهای فوق بسرعت نقاط آسیب پذیر و ضعف های امنیتی را شناسائی نمایند.**

۳ : اعتماد بیش از اندازه به ابزارها

برنامه های پویش و بررسی نقاط آسیب پذیر،اغلب بمنظور اخذ اطلاعات در رابطه وضعیت جاری امنیتی شبکه استفاده می گردد . پویشگرهای تشخیص نقاط آسیب پذیر ، اطلاعات مفیدی را در ارتباط با امنیت سیستم نظیر : مجوزهای فایل ، سیاستهای رمز عبور و سایر مسائل موجود، ارائه می نمایند . بعبارت دیگر پویشگران نقاط آسیب پذیر شبکه ، امکان نگرش از دید یک مهاجم را به مدیریت شبکه خواهند داد. پویشگرها ی فوق ، عموما" نیمی از مسائل امنیتی مرتبط را به سیستم

واگذار نموده و نمی توان به تمامی نتایج بدست آمده توسط آنان بسنده و محور عملیات خود را بر اساس یافته های آنان قرار دهیم . در این رابطه لازم است متناسب با نوع سیستم عامل نصب شده بر روی سیستم ها از پویشگران متعدد و مختص سیستم عامل مربوطه استفاده گردد(اخذ نتایج مطلوبتر) . بهرحال استفاده از این نوع نرم افزارها قطعا" باعث شناسائی سریع نقاط آسیب پذیر و صرفه جوئی زمان می گردد ولی نمی بایست این تصور وجود داشته باشد که استفاده از آنان بمنزله یک راه حل جامع امنیتی است . تاکید صرف بر نتایج بدست آمده توسط آنان ، می تواند نتایج نامطلوب امنیتی را بدنبال داشته باشد . در برخی موارد ممکن است لازم باشد ، بمنظور تشخیص نقاط آسیب پذیر یک سیستم ،عملیات دستی انجام و یا حتی تاسکریپت های خاصی در این رابطه نوشته گردد .

۴ : عدم مشاهده لاگ ها (Logs)

مشاهده لاگ های سیستم، یکی از مراحل ضروری در تشخیص مستمر و یا قریب الوقوع تهدیدات است . لاگ ها، امکان شناسائی نقاط آسیب پذیر متداول و حملات مربوطه را فراهم می نمایند. بنابراین می توان تمامی سیستم را بررسی و آن را در مقابل حملات مشخص شده ، مجهز و ایمن نمود. در صورت بروز یک تهاجم ، با استفاده از لاگ های سیستم ، تسهیلات لازم بمنظور ردیابی مهاجمان فراهم می گردد.(البته بشرطی که آنان اصلاح نشده باشند) . لاگ ها را بصورت ادواری بررسی و آنها را در یک مکان ایمن ذخیره نمائید.

۵ : اجرای سرویس ها و یا اسکریپت های اضافه و غیر ضروری

استفاده از منابع و شبکه سازمان ، بعنوان یک زمین بازی شخصی برای تست اسکریپت ها و سرویس های متفاوت ، یکی دیگر از اشتباهات متداولی است که توسط اکثریت قریب به اتفاق مدیران سیستم انجام می شود . داشتن اینچنین اسکریپت ها و سرویس های اضافه ای که بر روی سیستم اجراء می گردند ، باعث ایجاد مجموعه ای از پتانسیل ها و نقاط ورود جدید برای یک مهاجم می گردد (در صورتیکه سرویس های اضافه و یا اسکریپت ها بر روی سرویس دهنده اصلی نصب و تست گردند ، مشکلات می تواند مضاعف گردد). در صورت نیاز به تست اسکریپت ها و یا اجرای سرویس های اضافه ، می بایست عملیات مورد نظر خود را از طریق یک کامپیوتر ایزوله شده انجام داد (هرگز از کامپیوتری که به شبکه متصل است در این راستا استفاده نگردد) .

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 :

۱ : استخدام کارشناسان آموزش ندیده و غیرخبره

بدون تردید ، کارشناسان آموزش دیده و خبره ، یکی از منابع ارزشمند درهر سازمان محسوب می گردند. همواره می بایست از کارشناسان ورزیده در ارتباط با امنیت در یک سازمان استفاده گردد. فرصت سعی و خطاء نیست و ممکن است در این محدوده زمانی چیزی را که یک سازمان از دست می دهد بمراتب بیشتر از چیزی است که می خواهد بدست آورد. امنیت اطلاعات از جمله مقولاتی است که برای یک سازمان دارای جایگاهی است و همواره می بایست بهترین تصمیم دررابطه با استفاده از منابع انسانی ماهر ، اتخاذ گردد. استفاده از یک کارشناس غیر ماهر در امور امنیت اطلاعات و شبکه در یک سازمان ، خود تهدیدی امنیتی است که بر سایر تهدیدات موجود اضافه خواهد شد . (ما نمی توانیم مسئولیت پیاده سازی استراتژی امنیتی در سازمان را به افرادی واگذار نمائیم که در این رابطه اطلاعات و دانش لازم را ندارند) .

۲ : فقدان آگاهی لازم در رابطه با تاثیر یک ضعف امنیتی بر عملکرد 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 و دانش 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 با ادامه فعالیت سازمان را بدنبال داشته باشد. در عصر اطلاعات و دنیای شدید رقابت ، کافی است سازمانی لحظاتی آنچیزی 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 .

برخی از این تاثیرات عبارتند از :

- 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

۳ : 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، چراکه 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 و هر آنچیزی که می تواند خللی در فرآیند فوق ایجاد نماید ، باعث توقف و گاها" برگشت به عقب یک سازمان ، می گردد.

۴ : 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 .

۵ : یک مرتبه سرمایه گذاری در ارتباط با امنیت

امنیت مفهمومی فراگیر و گسترده بوده که نیازمند هماهنگی و سرمایه گذاری در دو بعد تکنولوژی و آموزش است. هر روز ما شاهد ظهور تکنولوژی های جدیدی می باشیم . ما نمی توانیم در مواجهه 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 و ارزانتر 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 در ارتباط 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 و از 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 .

اشتباهات متداول کاربران معمولی

کاربران ، به افرادی اطلاق می گردد که طی روز با داده ها ی حساس در یک سازمان سروکار داشته و تصمیمات و فعالیت های آنان، داده ها ی حساس و مقوله امنیت و حفاظت از اطلاعات را تحت تاثیر مستقیم قرار خواهد داد. در ادامه با برخی از اشتباهات متداولی که این نوع استفاده کنندگان از سیستم و شبکه مرتکب می شوند ، اشاره می گردد.

۱ : تخطی از سیاست امنینی سازمان

سیاست امنیتی سازمان ، اعلامیه ای است که بصورت جامع ، مسئولیت هر یک از پرسنل سازمان (افرادیکه به اطلاعات و سیستم های حساس در سازمان دستیابی دارند) در ارتباط با امنیت اطلاعات و شبکه را تعریف و مشخص می نماید. سند و یا اعلامیه مورد نظر ، بعنوان بخش لاینفک در هر مدل امنیتی بکارگرفته شده در سازمان محسوب می گردد.هدف عمده اعلامیه فوق ، ارائه روشی آسان بمنظور شناخت و درک ساده نحوه حفاظت سیستم های سازمان در زمان استفاده است . کاربران معمولی ، عموما" تمایل به تخطی از سیاست های تدوین شده امنیتی در یک سازمان را داشته و این موضوع می تواند عاملی مهم برای تحت تاثیر قراردادن سیستم های حساس و اطلاعات مهم سازمان در مواجهه با یک تهدید باشد. پیامد این نوع عملیات ، بروز اشکال و خرابی در رابطه با

اطلاعات ارزشمند در یک سازمان خواهد بود.بهمین دلیل است که اکیدا" توصیه می گردد که اطلاعات لازم در رابطه با نقش کاربران در تبعیت از سیاست های امنیتی در سازمان به آنان یادآوری و بر آن تاکید گردد .

۲ : ارسال داده حساس بر روی کامپیوترهای منزل

یکی از خطرناکترین روش ها در رابطه با داده های حساس موجود در یک سازمان ، فعالیتی است که باعث غیر فعال شدن تمامی پیشگیری های امنیتی ایجادشده و در گیر شدن آنان در یک فرآیند غیر امنیتی می گردد . پرسنل سازمان عادت دارند،اطلاعات حساس سازمان را بر روی کامپیوتر منزل خود فوروارد (ارسال) نمایند . در حقیقت کاربران تمایل به فوروارد نمودن یک پروژه ناتمام و یا برنامه ریزی تجاری به کامپیوتر منازل خود را داشته تا از این طریق امکان اتمام کار خود در منزل را پیدا نمایند. کاربران به این موضوع توجه نکرده اند که تغییر محیط ایمن سازمان با کامپیوتر منزل خود که دارای ایمنی بمراتب کمتری است ، بطور جدی اطلاعات را در معرض آسیب و تهاجم قرار خواهد داد . در صورتیکه ضروری است که اطلاعات را به کامپیوترهای منزل فوروارد نمود ، یک سطح مناسب ایمنی می بایست وجود داشته باشد تا این اطمینان بوجود آید که نوت بوک ها و یا کامپیوترهای منازل در مقابل مهاجمین اطلاعاتی حفاظت شده و ایمن می باشند.

۳ : یاداشت داده های حساس و ذخیره غیرایمن آنان

ایجاد و نگهداری رمزهای عبور قدرتمند ، فرآیندی مستمر است که همواره می بایست مورد توجه قرار گیرد. کاربران همواره از این موضوع نفرت دارند که رمزعبورهائی را ایجاد نمایند که قادر به بخاطرآوردن آن نمی باشند. سیاست امنیتی تدوین شده سازمان می بایست تعیین نماید که یک رمز عبور چگونه می بایست ایجاد و نگهداری گردد. بخاطر سپردن چنین رمزعبوری همواره مسائل خاص خود را خواهد داشت . بمنظور حل اینچنین مشکلی ، کاربران تمایل دارند که یاداشت های مخفی را نوشته و آنها را زیر صفحه کلید ، کیف جیبی و یا هر مکان دیگر در محل کار خود نگهداری نمایند. یاداشت ها ی فوق ، شامل اطلاعات حساس در ارتباط با داده های مربوط به رمزعبور و سایر موارد مرتبط است .استفاده از روشهای فوق برای نگهداری اطلاعات ، یک تخطی امنیتی است .دراین راستا لازم است ،کاربران توجیه و به آنان آگاهی لازم داده شود که با عدم رعایت موارد مشخص شده امنیتی ،پتانسیل های لازم بمنظور بروز مشکل در سیستم افزایش خواهد یافت . لازم است به کاربران ، روش ها و تکنیک های متفاوت بخاطر سپردن رمز عبور آموزش داده شود تا زمینه استفاده کاربران از یاداشت برای ثبت اینگونه اطلاعات حساس کاهش یابد . سناریوی های متفاوت برای آنان تشریح و گفته شود که یک مهاجم با استفاده از چه روش هائی ممکن است به اطلاعات ثبت شده در یاداشت ها ، دست پیدا نموده و زمینه بروز مشکل را فراهم نماید.

۴ : دریافت فایل از سایت های غیر مطمئن

یکی از سرویس های اینترنت امکان دریافت فایل توسط کاربران است . کاربران بمنظور دریافت فایل از اینترنت ، اغلب از امتیازات خود تعدی و حتی سیاست ها ی موجود در سازمان را در معرض مخاطره و آسیب قرار می دهند . دریافت فایل از وب سایت های گمنام و یا غیر مطمئن باعث کمک در توزیع برنامه های مهاجم در اینترنت می گردد. بدین ترتیب ما بعنوان ابزاری برای توزیع یک برنامه مخرب در اینترنت تبدیل خواهیم شد. فایل ها و برنامه های دریافتی پس از آلودگی به نوع خاصی از برنامه مخرب (ویروس ، کرم ، اسب تراوا) ، می تواند تاثیرات منفی فراوانی را در ارتباط با عملکرد یک سازمان بدنبال داشته باشد .کاربران می بایست بندرت فایل هائی را از اینترنت دریافت در مواردیکه ضرورت این کار حس و به برنامه ای خاص نیاز باشد ، اکیدا" توصیه می گردد که موضوع با دپارتمان IT (یا سایر بخش های مسئول در سازمان) درمیان گذاشته شود تا آنان بر اساس تجربه و دانش خود ، اقدام به تهیه برنامه مورد نظر از منابع مطمئن نمایند .

۵ : عدم رعایت امنیت فیزیکی

میزان آگاهی و دانش کاربران در رابطه با رعایت مسائل ایمنی خصوصا" امنیت فیزیکی ، بطرز کاملا" محسوسی افزایش امنیت و حفاظت داده ها ی حساس در یک سازمان را بدنبال خواهد داشت . عموما" ، رفتار کاربران در زمان استفاده از ایستگاه های کاری سازمان سهل انگارانه و فاقد سوادعمومی ایمنی است . کاربران ، اغلب ایستگاههای کاری خود را بدون در نظر گرفتن امنیت فیزیکی رها و screensaver آنان ، بندرت دارای رمز عبور بوده و می تواند باعث بروزمسائل متعددی گردد. به کاربران می بایست آموزش های لازم در رابطه با استراتژی های متفاوت بمنظور

استفاده از سیستم های سازمان داده شود : مطمئن شوید آنها قادرند بدرستی با اطلاعات حساس در سازمان برخورد نمایند و همواره پیامدهای عدم رعایت امنیت فیزیکی به آنان یادآوری گردد.

راه حل اولیه ایجاد امنیت در شبکه

شبکه های کامپیوتری زیر ساخت لازم برای عرضه اطلاعات در یک سازمان را فراهم می نمایند . بموازات رشد و گسترش تکنولوژی اطلاعات، مقوله امنیت در شبکه های کامپیوتری ، بطور چشمگیری مورد توجه قرار گرفته و همه روزه بر تعداد افرادی که علاقه مند به آشنائی با اصول سیستم های امنیتی در این زمینه می باشند ، افزوده می گردد .

سیاست امنیتی

یک سیاست امنیتی، اعلامیه ای رسمی مشتمل بر مجموعه ای از قوانین است که می بایست توسط افرادیکه به یک تکنولوژی سازمان و یا سرمایه های اطلاعاتی دستیابی دارند، رعایت و به آن پایبند باشند . بمنظور تحقق اهداف امنیتی ، می بایست سیاست های تدوین شده در رابطه با تمام کاربران ، مدیران شبکه و مدیران عملیاتی سازمان، اعمال گردد . اهداف مورد نظر عموما" با تاکیدبر گزینه های اساسی زیر مشخص می گردند .

" سرویس های عرضه شده در مقابل امنیت ارائه شده ، استفاده ساده در مقابل امنیت و هزینه ایمن سازی در مقابل ریسک از دست دادن اطلاعات "

مهمترین هدف یک سیاست امنیتی ، دادن آگاهی لازم به کاربران، مدیران شبکه و مدیران عملیاتی یک سازمان در رابطه با امکانات و تجهیزات لازم ، بمنظور حفظ و صیانت از تکنولوژی و سرمایه های اطلاعاتی است . سیاست امنیتی ، می بایست مکانیزم و راهکارهای مربوطه را با تاکید بر امکانات موجود تبین نماید . از دیگر اهداف یک سیاست امنیتی ، ارائه یک خط اصولی برای پیکربندی و ممیزی سیستم های کامپیوتری و شبکه ها ، بمنظور تبعیت از سیاست ها است . یک سیاست امنیتی مناسب و موثر ، می بایست رضایت و حمایت تمام پرسنل موجود در یک سازمان را بدنبال داشته باشد .

یک سیاست امنیتی خوب دارای ویژگی های زیر است :

- امکان پیاده سازی عملی آن بکمک روش های متعددی نظیر رویه های مدیریتی، وجود داشته باشد .
- امکان تقویت آن توسط ابزارهای امنیتی ویا دستورات مدیریتی در مواردیکه پیشگیری واقعی از لحاظ فنی امکان پذیر نیست ، وجود داشته باشد .
- محدوده مسئولیت کاربران، مدیران شبکه و مدیران عملیاتی بصورت شفاف مشخص گردد.
- پس از استقرار، قابلیت برقرای ارتباط با منابع متفاوت انسانی را دارا باشد . (یک بار گفتن و همواره در گوش داشتن)
- دارای انعطاف لازم بمنظور برخورد با تغییرات درشبکه باشد .(سیاست های تدوین شده ، نمونه ای بارز از مستندات زنده تلقی می گردنند .)

سیستم های عامل و برنامه های کاربردی : نسخه ها و بهنگام سازی

در صورت امکان، می بایست از آخرین نسخه سیستم های عامل و برنامه های کاربردی بر روی تمامی کامپیوترهای موجود در شبکه (سرویس گیرنده ، سرویس دهنده ، سوئیچ، روتر، فایروال و سیستم های تشخیص مزاحمین) استفاده شود . سیستم های عامل و برنامه های کاربردی می بایست بهنگام بوده و همواره از آخرین امکانات موجود بهنگام سازی (**patches , service pack , hotfixes**) استفاده گردد . در این راستا می بایست حساسیت بیشتری نسبت به برنامه های آسیب پذیر که زمینه لازم برای متجاوزان اطلاعاتی را فراهم می نمایند ، وجود داشته باشد . برنامه های : **BIND , Internet Explorer , OutLook, IIS** و **sendmail** بدلیل وجود نقاط آسیب پذیر می بایست مورد توجه جدی قرار گیرند . متجاوزان اطلاعاتی ، بدفعات از نقاط آسیب پذیر برنامه های فوق برای خواسته های خود استفاده کرده اند .

شناخت شبکه موجود

بمنظور پیاده سازی و پشتیبانی سیستم امنیتی ، لازم است لیستی از تمام دستگاههای سخت افزاری و برنامه های نصب شده ، تهیه گردد . آگاهی از برنامه هائی که بصورت پیش فرض نصب شده اند، نیز دارای اهمیت خاص خود است (مثلا" برنامه **IIS** بصورت پیش فرض توسط **SMS** و یا سرویس دهنده **SQL** در شبکه های مبتنی بر ویندوز نصب می گردد) . فهرست برداری از سرویس هائی که بر روی شبکه در حا ل اجراء می باشند، زمینه را برای پیمایش و تشخیص مسائل مربوطه ، هموار خواهد کرد .

سرویس دهندگان TCP/UDP و سرویس های موجود در شبکه

تمامی سرویس دهندگان TCP/UDP در شبکه بهمراه سرویس های موجود بر روی هر کامپیوتر در شبکه ، می بایست شناسائی و مستند گردند . در صورت امکان، سرویس دهندگان و سرویس های غیر ضروری، غیر فعال گردند . برای سرویس دهندگانی که وجود آنان ضروری تشخیص داده می شود، دستیابی به آنان محدود به کامپیوترهائی گردد که به خدمات آنان نیازمند می باشند . امکانات عملیاتی را که بندرت از آنان استفاده و دارای آسیب پذیری بیشتری می باشند ، غیر فعال تا زمینه بهره برداری آنان توسط متجاوزان اطلاعاتی سلب گردد. توصیه می گردد ، برنامه های نمونه (Sample) تحت هیچ شرایطی بر روی سیستم های تولیدی (سیستم هائی که محیط لازم برای تولید نرم افزار بر روی آنها ایجاد و با استفاده از آنان محصولات نرم افزاری تولید می گردند) نصب نگردند .

رمزعبور

انتخاب رمزعبور ضعیف ، همواره یکی از مسائل اصلی در رابطه با هر نوع سیستم امنیتی است . کاربران، می بایست متعهد و مجبور به تغییر رمز عبور خود بصورت ادواری گردند . تنظیم مشخصه های رمز عبور در سیستم های مبتنی بر ویندوز، بکمک Account Policy صورت می پذیرد . مدیران شبکه، می بایست برنامه های مربوط به تشخیص رمز عبور را تهیه و آنها را اجراء تا آسیب پذیری سیستم در بوته نقد و آزمایش قرار گیرد .

برنامه های john the Ripper ، LOphtcrack و Crack ، نمونه هائی در این زمینه می باشند . به کاربرانی که رمز عبور آنان ضعیف تعریف شده است ، مراتب اعلام و در صورت تکرار اخطار داده

شود (عملیات فوق، می بایست بصورت متناوب انجام گیرد) . با توجه به اینکه برنامه های تشخیص رمزعبور،زمان زیادی از پردازنده را بخود اختصاص خواهند داد، توصیه می گردد، رمز عبورهای کد شده (لیست SAM بانک اطلاعاتی در ویندوز) را بر روی سیستمی دیگر که در شبکه نمی باشد، منتقل تا زمینه بررسی رمزهای عبور ضعیف ، فراهم گردد . با انجام عملیات فوق برروی یک کامپیوتر غیر شبکه ای ، نتایج بدست آمده برای هیچکس قابل استفاده نخواهد بود(مگراینکه افراد بصورت فیزیکی به سیستم دستیابی پیدا نمایند) .

برای تعریف رمز عبور، موارد زیر پیشنهاد می گردد :

- حداقل طول رمز عبور، دوازده و یا بیشتر باشد .
- دررمز عبور از حروف کوچک، اعداد، کاراکترهای خاص و Underline استفاده شود .
- از کلمات موجود در دیکشنری استفاده نگردد .
- رمز های عبور ، در فواصل زمانی مشخصی (سی و یا نود روز) بصورت ادواری تغییر داده شوند .
- کاربرانی که رمزهای عبور ساده و قابل حدسی را برای خود تعریف نموده اند، تشخیص و به آنها تذکر داده شود .(عملیات فوق بصورت متناوب و در فواصل زمانی یک ماه انجام گردد).

عدم اجرای برنامه ها ئی که منابع آنها تایید نشده است .

در اغلب حالات ، برنامه های کامپیوتری در یک چارچوب امنیتی خاص مربوط به کاربری که آنها را فعال می نماید ، اجراء می گردند.دراین زمینه ممکن است، هیچگونه توجه ای به ماهیت منبع ارائه دهنده برنامه توسط کاربران انجام نگردد . وجود یک زیر ساخت PKI (Public key infrastructure) ، در این زمینه می تواند مفید باشد . در صورت عدم وجود زیرساخت امنیتی فوق ،می بایست مراقبت های لازم در رابطه با طرفندهای استفاده شده توسط برخی از متجاوران اطلاعاتی را انجام داد. مثلا" ممکن است برخی آسیب ها در ظاهری کاملا" موجه از طریق یک پیام الکترونیکی جلوه نمایند . هرگز یک ضمیمه پیام الکترونیکی و یا برنامه ای را که از منبع ارسال کننده آن مطمئن نشده اید ، فعال و یا اجراء ننمائید . همواره از برنامه ای نظیر Outlook بمنظور دریافت پیام های الکترونیکی استفاده گردد . برنامه فوق در یک ناحیه محدوده شده اجراء و می بایست امکان اجرای تمام اسکریپت ها و محتویات فعال برای ناحیه فوق ، غیر فعال گردد .

ایجاد محدودیت در برخی از ضمائم پست الکترونیکی

ضرورت توزیع و عرضه تعداد زیادی از انواع فایل های ضمیمه ، بصورت روزمره در یک سازمان وجود ندارد .بمنظور پیشگیری از اجرای کدهای مخرب ، پیشنهاد می گردد این نوع فایل ها ،غیر فعال گردند . سازمان هائی که از Outlook استفاده می نمایند، می توانند با استفاده از نسخه ۲۰۰۲ اقدام به بلاک نمودن آنها نمایند . (برای سایر نسخه های Outlook می توان از Patch امنیتی مربوطه استفاده کرد) .

فایل های زیر را می توان بلاک کرد :

نوع فایل هائی که می توان آنها را بلاک نمود .
.bas .hta .msp .url .bat .inf .mst .vb .chm .ins .pif .vbe .cmd .isp .pl .vbs .com .js .reg .ws .cpl .jse .scr .wsc .crt .lnk .sct .wsf .exe .msi .shs .wsh

در صورت ضرورت می توان ، به لیست فوق برخی از فایل ها را اضافه و یا حذف کرد. مثلا" با توجه به وجود عناصر اجرائی در برنامه های آفیس ، میتوان امکان اجرای برنامه ها را در آنان بلاک نمود . مهمترین نکته در این راستا به برنامه Access بر می گردد که برخلاف سایر اعضاء خانواده آفیس ، دارای امکانات حفاظتی ذاتی در مقابل ماکروهای آسیب رسان نمی باشد .

پایبندی به مفهوم کمترین امتیاز

اختصاص حداقل امتیاز به کاربران، محور اساسی درپیاده سازی یک سیتم امنیتی است. رویکرد فوق بر این اصل مهم استوار است که کاربران می بایست صرفا" دارای حقوق و امتیازات لازم بمنظور انجام کارهای مربوطه باشند (بذل و بخشش امتیازات در این زمینه شایسته نمی باشد!) . رخنه در سیستم امنیتی از طریق کدهای مخربی که توسط کاربران اجراء می گردند، تحقق می یابد . در صورتیکه کاربر، دارای حقوق و امتیازات بیشتری باشد ، آسیب پذیری اطلاعات در اثر اجرای کدها ی مخرب ، بیشتر خواهد شد .

موارد زیر برای اختصاص حقوق کاربران ، پیشنهاد می گردد :

- **تعداد account مربوط به مدیران شبکه، می بایست حداقل باشد .**
- **مدیران شبکه ، می بایست بمنظور انجام فعالیت های روزمره نظیر خواندن پیام های پست الکترونیکی ، از یک account روزمره در مقابل ورود به شبکه بعنوان administrator ،استفاده نمایند .**
- **مجوزهای لازم برای منابع بدرستی تنظیم و پیکربندی گردد . در این راستا می بایست حساسیت بیشتری نسبت به برخی از برنامه ها که همواره مورد استفاده متجاوزان اطلاعاتی است ، وجود داشته باشد . این نوع برنامه ها ، شرایط مناسبی برای متجاوزان اطلاعاتی را فراهم می نمایند. جدول زیر برخی از این نوع برنامه ها را نشان می دهد .**
- **رویکرد حداقل امتیاز ، می تواند به برنامه های سرویس دهنده نیز تعمیم یابد . در این راستا می بایست حتی المقدور، سرویس ها و برنامه ها توسط یک account که حداقل امتیاز را دارد ،اجراء گردند .**

برنامه های مورد توجه متجاوزان اطلاعاتی
explorer.exe, regedit.exe, poledit.exe, taskman.exe, at.exe, cacls.exe,cmd.exe, finger.exe, ftp.exe, nbstat.exe, net.exe, net1.exe,netsh.exe, rcp.exe, regedt32.exe, regini.exe, regsvr32.exe,rexec.exe, rsh.exe, runas.exe, runonce.exe, svrmgr.exe,sysedit.exe, telnet.exe, tftp.exe, tracert.exe, usrmgr.exe,wscript.exe,xcopy.exe

ممیزی برنامه ها

اغلب برنامه های سرویس دهنده ، دارای قابلیت های ممیزی گسترده ای می باشند . ممیزی می تواند شامل دنبال نمودن حرکات مشکوک و یا برخورد با آسیب های واقعی باشد . با فعال نمودن ممیزی برای برنامه های سرویس دهنده و کنترل دستیابی به برنامه های کلیدی نظیر برنامه هائی که لیست آنها در جدول قبل ارائه گردید، شرایط مناسبی بمنظور حفاظت از اطلاعات فراهم می گردد .

چاپگر شبکه

امروزه اغلب چاپگرهای شبکه دارای قابلیت های از قبل ساخته شده برای سرویس های FTP,WEB و Telnet بعنوان بخشی از سیستم عامل مربوطه ، می باشند . منابع فوق پس از فعال شدن ، مورد استفاده قرار خواهند گرفت . امکان استفاده از چاپگرهای شبکه بصورت FTP Bound servers ، Telnet و یا سرویس های مدیریتی وب ، وجود خواهد داشت . رمز عبور پیش فرض را به یک رمز عبور پیچیده تغییر و با صراحت پورت های چاپگر را در محدوده روتر / فایروال بلاک نموده و در صورت عدم نیاز به سرویس های فوق ، آنها را غیر فعال نمائید .

پروتکل SNMP (Simple Network Management Protocol)

پروتکل SNMP ، در مقیاس گسترده ای توسط مدیران شبکه بمنظور مشاهده و مدیریت تمام کامپیوترهای موجود در شبکه (سرویس گیرنده ، سرویس دهنده، سوئیچ ، روتر، فایروال) استفاده می گردد .SNMP ، بمنظور تایید اعتبار کاربران ، از روشی غیر رمز شده استفاده می نماید . متجاوزان اطلاعاتی ، می توانند از نفطه ضعف فوق در جهت اهداف سوء خود استفاده نمایند . در چنین حالتی، آنان قادر به اخذ اطلاعات متنوعی در رابطه با عناصر موجود در شبکه بوده و حتی امکان غیر فعال نمودن یک سیستم از راه دور و یا تغییر پیکربندی سیستم ها وجود خواهد داشت . در صورتیکه یک متجاوز اطلاعاتی قادر به جمع آوری ترافیک SNMP دریک شبکه گردد، از اطلاعات مربوط به ساختار شبکه موجود بهمراه سیستم ها و دستگاههای متصل شده به آن ، نیز آگاهی خواهد یافت . سرویس دهندگان SNMP موجود بر روی هر کامپیوتری را که ضرورتی به وجود آنان نمی باشد ، غیر فعال نمائید . در صورتیکه بهر دلیلی استفاده از SNMP ضروری باشد ،

می بایست امکان دستیابی بصورت فقط خواندنی در نظر گرفته شود . در صورت امکان، صرفا" به تعداد اندکی از کامپیوترها امتیاز استفاده از سرویس دهنده SNMP اعطاء گردد .

تست امنیت شبکه

مدیران شبکه های کامپیوترهای می بایست، بصورت ادواری اقدام به تست امنیتی تمام کامپیوترهای موجود در شبکه (سرویس گیرندگان، سرویس دهندگان، سوئیچ ها ، روترها ، فایروال ها و سیتستم های تشخیص مزاحمین) نمایند. تست امنیت شبکه ، پس از اعمال هر گونه تغییر اساسی در پیکربندی شبکه ، نیز می بایست انجام شود .

علل بروز مشکلات امنیتی

امنیت شبکه های کامپیوتری و ایمن سازی زیرساخت فناوری اطلاعات به یکی از چالش های مهم برای بسیاری از سازمان ها و موسسات مدرن اطلاعاتی تبدیل شده است.کارشناسان فناوری اطلاعات همواره با این پرسش مواجه هستند که علل بروز مشکلات امنیتی در یک شبکه کامپیوتری چیست و چگونه می توان بطور سیستماتیک در جهت ایجاد و نگهداری ایمن زیرساخت فناوری اطلاعات و منابع موجود بر روی آن قدم برداشت .

ریشه بسیاری از مشکلات و مسائل امنیتی را می توان در سه ضعف عمده زیر جستجو کرد :

- ضعف فناوری
- ضعف پیکربندی
- ضعف سیاست ها

در ادامه به بررسی هر یک از موارد فوق خواهیم پرداخت .

ضعف فناوری

ضعف فناوری به مواردی همچون پروتکل ها ، سیستم های عامل و سخت افزار مرتبط می گردد . اغلب به صورت پیش فرض ، پروتکل ها ، سیستم های عامل و سخت افزار ایمن نمی باشند . آگاهی از این ضعف ها به ما کمک خواهد کرد تا بتوانیم قبل از بروز تهاجم ، شبکه های خود را ایمن سازیم . در واقع ، ضعف در فناوری به عدم وجود شرایط مطلوب امنیتی در حوزه های سخت افزاری و نرم افزاری مربوط می گردد .

امروزه وجود ضعف در فناوری ها به یک چالش جدی برای متخصصان و کارشناسان فناوری اطلاعات تبدیل شده است چراکه اکثر سخت افزارها و نرم افزارهای استفاده شده در یک سازمان قبل از حضور کارشناسان در سیستم نصب و به بهره برداری رسیده است و آنان با مسائلی روبرو خواهند بود که شاید خود سهمی در ایجاد آنها نداشته اند .

ضعف در فناوری ها را می توان به سه گروه عمده تقسیم نمود :

ضعف پروتکل TCP/IP

پروتکل TCP/IP دارای ضعف های امنیتی ذاتی مختص به خود است چراکه طراحی آن به عنوان یک استاندارد باز مد نظر بوده است تا بتواند به سادگی و سهولت بیشتر امکان مبادله اطلاعات در شبکه را فراهم نماید . مهمترین دلیل گسترش پروتکل TCP/IP ، تبعیت آن از یک استاندارد باز است . علی رغم این که می توان ویژگی فوق را از نگاه مثبت ارزیابی کرد ، ولی ماهیت استاندارد باز بودن پروتکل TCP/IP می تواند دلیلی قانع کننده بر این واقعیت باشد که چرا حملات در شبکه های کامپیوتری تا به این اندازه ساده انجام می گیرد و درصد بسیار زیادی از آنها نیز توام با موفقیت است. بپذیریم که امروزه تعداد بسیار زیادی از افراد فعال در عرصه شبکه های کامپیوتری با نحوه کار این پروتکل به خوبی آشنا می باشند . همین آشنائی می تواند دانش اولیه به منظور برنامه ریزی و تدارک حملات در شبکه های کامپیوتری را در اختیار مهاجمان نیز قرار دهد . با این که برخی از مشکلات و ضعف های امنیتی پروتکل TCP/IP ماحصل ضعف در پیاده سازی این پروتکل در یک سیستم عامل خاص است که می بایست شناسائی و با آنها برخورد شود ، ولی این موضوع در جای خود نیز نگران کننده است که پروتکل فوق می تواند خود به عنوان عاملی موثر در بروز مشکلات و ضعف های امنیتی مطرح و تاثیرگذار باشد. ایجاد ضعف در مواردی نظیر حفاظت رمزعبور ، فقدان تائیدیه مورد نیاز ، پروتکل های روتینگ (که بر روی تمامی شبکه منتشر خواهند شد) و حفره های فایروال ها ، نمونه هائی در این رابطه می باشند . SMTP (برگرفته از Simple Mail Transfer Protocol) و SNMP (برگرفته از Simple

Network Management Protocol) ، دو نمونه از پروتکل های ذاتا" غیرایمن مجموعه پروتکل های TCP/IP می باشند . وجود ضعف در پروتکل TCP/IP ، تاکنون عامل بروز حملات متعددی در شبکه های کامپیوتری بوده است . IP spoofing و man-in-the-middle دو نمونه متداول در این زمینه می باشند .

ضعف سیستم عامل

با این که هر سیستم عاملی دارای ضعف های امنیتی مختص به خود است ، ولی عمومیت و رواج یک سیستم عامل می تواند زمینه شناسائی و سوء استفاده از ضعف های امنیتی آن را تسریع نماید . شاید به همین دلیل باشد که ضعف های ویندوز شرکت مایکروسافت سریع تر از سایر سیستم های عامل بر همگان آشکار می شود چراکه اکثر کاربران بر روی کامپیوتر خود از یکی از نسخه های ویندوز این شرکت استفاده می نمایند . شاید بتوان گفت که لینوکس و یا یونیکس نسبت به ویندوز دارای ضعف های امنیتی کمتری می باشند ولی سیستم های عامل فوق نیز دارای ضعف امنیتی مختص به خود می باشند که به دلیل عدم استفاده عام از آنها تاکنون کمتر شناسائی شده اند .

ضعف تجهیزات شبکه ای

تمامی تجهیزات شبکه ای نظیر سرویس دهندگان ، روترها ، سوئیچ ها و نظایر آن دارای برخی ضعف های امنیتی ذاتی می باشند . با تبعیت از یک سیاست تعریف شده مناسب برای پیکربندی و نصب تجهیزات شبکه ای می توان بطرز کاملا" محسوسی آثار و تبعات این نوع ضعف های امنیتی را کاهش

داد . نصب و پیکربندی هر گونه تجهیزات شبکه ای می بایست مبتنی بر اصول و سیاست های امنیتی تعریف شده باشد .

ضعف پیکربندی

ضعف در پیکربندی ، نقش عوامل انسانی در بروز مشکلات امنیتی را به خوبی نشان می دهد . مدیران شبکه و سایر کارشناسانی که مسئولیت نصب و پیکربندی تجهیزات شبکه ای و غیر شبکه ای در یک سازمان را برعهده دارند ، می توانند باعث بروز ضعف در پیکربندی شوند . متاسفانه ، در اغلب موارد مدیران شبکه تجهیزات شبکه ای را با پیکربندی پیش فرض استفاده می نمایند و اقدامات لازم در جهت ایمن سازی پارامترهای تاثیرگذار در این رابطه نظیر ایمن سازی **account** مدیر شبکه را انجام نمی دهند .

عوامل متعددی باعث بروز ضعف در پیکربندی می شوند :

- **استفاده غیرایمن از account کاربران**

استفاده از **account** پیش فرض **administrator** بدون رمزعبور ، عدم کنترل و نظارت صحیح و مستمر بر روی شبکه بستر و شرایط لازم برای بروز مشکلات امنیتی و انجام حملات در یک شبکه کامپیوتری را فراهم می نماید. در صورتی که از یکی از نسخه های ویندوز سرویس دهنده استفاده می نمائید ، می بایست **account** مربوط به **administrator** تغییر نام یابد . با انجام این کار ، این اطمینان اولیه ایجاد خواهد شد که مهاجمان برای نفوذ به شبکه به زمان بیشتری جهت تشخیص **account** مدیر شبکه نیاز خواهند داشت . همچنین می بایست بر اساس سیاست های تعریف شده

به هر یک از کاربران متناسب با نیاز آنان ، مجوزهائی واگذار گردد و هرگز به آنان مجوزهائی بیش از آن چیزی که برای انجام کار به آن نیاز دارند ، واگذار نگردد . بد نیست به این نکته مهم نیز اشاره نمائیم که اسامی و رمز عبور کاربران عموما" بطور غیرایمن در طول شبکه حرکت می نماید . مدیران شبکه می بایست سیاست های لازم در خصوص نحوه تعریف و حفاظت از رمز عبور را تدوین و آن را به کاربران شبکه آموزش دهند .

- **استفاده از system account که رمز عبور آنها به سادگی قابل تشخیص است**

یکی دیگر از روش هائی که می تواند مشکلات امنیتی در یک شبکه را به دنبال داشته باشد ، نسبت دادن رمزهای عبور به **system account** است که امکان تشخیص آنها به سادگی وجود دارد . برای پیشگیری از بروز این چنین مسائل امنیتی ، مدیران شبکه می بایست سیاست هائی را بر روی سرویس دهندگان در شبکه تعریف نمایند که صرفا" اجازه تعریف انواع خاصی از رمزهای عبور را فراهم نماید و هر رمز عبور دارای یک تاریخ اعتبار معتبر باشد تا پس از اتمام تاریخ مصرف ، امکان استفاده از آن وجود نداشته باشد . در این رابطه لازم است که کاربران بطور شفاف نسبت به این موضوع توجیه گردند که نمی بایست از نام خود ، نام فرزند ، تاریخ تولد ، شماره شناسنامه و مواردی از این قبیل به عنوان رمز عبور استفاده نمایند . به کاربران آموزش داده شود که برای تعریف یک رمز عبور مناسب می بایست از ترکیب حروف بزرگ ، کوچک و حروف ویژه استفاده نمایند. رعایت موارد فوق ، شبکه شما را در مقابل حملاتی نظیر **brute-force** که از فایل های دیکشنری برای حدس رمزهای عبور استفاده می نمایند ، مقاوم می نماید .

- **عدم پیکربندی صحیح سرویس های اینترنت**

برخی سازمان ها همچنان از آدرس های IP واقعی برای آدرس دهی هاست ها و سرویس دهندگان موجود بر روی شبکه استفاده می نمایند . با استفاده از امکانات ارائه شده توسط NAT (برگرفته از Network Address Translation) و PAT (برگرفته از Port Address Translation) ، دلیلی وجود ندارد که از آدرس های IP واقعی استفاده گردد . در مقابل ، شما می توانید از آدرس های IP خصوصی استفاده نمائید . بدین ترتیب ، سازمان ها می توانند از مجموعه ای از آدرس های IP که بر روی اینترنت بلاک شده اند استفاده نمایند . رویکرد فوق ، باعث بهبود وضعیت امنیت در سازمان مورد نظر خواهد شد چراکه فقط آدرس IP واقعی بر روی روتر مرزی امکان روتینگ بر روی اینترنت را خواهد داشت .

- **غیرایمن بودن تنظیمات پیش فرض در برخی محصولات**

این یک واقعیت انکار ناپذیر است که تعداد بسیار زیادی از محصولات بدون رمز عبور و یا رمزهای عبور ساده به بازار عرضه می گردند تا مدیران شبکه بتوانند پیکربندی دستگاه را به سادگی انجام دهند . برخی دستگاه ها به صورت plug and play می باشند . مثلا" سوئیچ های سیسکو به صورت plug-and-play می باشند تا بتوان به سرعت آنها را جایگزین هاب در شبکه نمود. به منظور افزایش امنیت ، می بایست بر روی سوئیچ یک رمز عبور مناسب را تعریف تا مهاجمان نتوانند به سادگی به آن دستیابی داشته باشند . شرکت سیسکو به منظور افزایش امنیت در خصوص بکارگیری این نوع تجهیزات شبکه ای تمهیدات خاصی را اندیشیده است . به عنوان نمونه ، روترها و سوئیچ های سیسکو اجازه ایجاد یک telnet session را بدون انجام یک پیکربندی خاص login بر

روی دستگاه نخواهند داد . فرآیند نصب و پیکربندی هر دستگاه در شبکه می بایست تابع یک سیاست امنیتی مدون باشد .

- **عدم پیکربندی صحیح تجهیزات شبکه ای**

عدم پیکربندی مناسب تجهیزات شبکه ای یکی دیگر از دلایل بروز مشکلات امنیتی است . رمزهای عبور ضعیف ، عدم وجود سیاست های امنیتی و غیر ایمن بودن **account** کاربران جملگی می توانند به عنوان بخشی از سیاست های عدم پیکربندی مناسب تجهیزات شبکه ای در نظر گرفته شوند . سخت افزار و پروتکل هائی که بر روی تجهیزات شبکه ای اجراء می شوند ، می توانند حفره های امنیتی را در شبکه شما ایجاد نمایند . در صورت عدم وجود یک سیاست مدون به منظور تشریح سخت افزار و پروتکل هائی که می بایست بر روی هر یک از تجهیزات شبکه ای اجراء شوند ، مهاجمان قادر خواهند بود به شبکه شما نفوذ نمایند .

به عنوان مثال ، در صورتی که شما از پروتکل **SNMP** (برگرفته شده از **Simple Network Management Protocol**) به همراه تنظیمات پیش فرض استفاده نمائید ، حجم بالائی از اطلاعات مربوط به شبکه شما می تواند به سادگی و به سرعت رمزگشائی گردد . بنابراین ، می بایست در صورتی که به پروتکل فوق نیاز نمی باشد آن را غیرفعال و در صورت ضرورت استفاده از آن ، تنظیمات پیش فرض خصوصا" **community strings** را تغییر داد . رشته های فوق به منزله رمز عبوری برای جمع آوری و دریافت داده مربوط به **SNMP** می باشند .

- **ضعف سیاست ها**

سیاست های امنیتی در یک شبکه، نحوه و زمان پیاده سازی امنیت در شبکه را تشریح می نمایند . به عنوان نمونه ، در سیاست های امنیتی تعریف شده می بایست اطلاعات لازم در خصوص نحوه پیکربندی ایمن دستگاه های شبکه ای دقیقا" مشخص گردد . عدم تدوین یک سیاست امنیتی مدون می تواند زیرساخت فناوری اطلاعات و ارتباطات یک سازمان را با مشکلات امنیتی متعددی مواجه نماید .

بدین منظور می بایست بر روی محورهای مختلفی متمرکز گردید :

- **عدم وجود یک سیاست امنیتی مکتوب**

در صورتی که یک مدیر شبکه ، و یا هر شخص دیگر ، نمی داند که در ابتدای یک کار چه انتظاری از آن وجود دارد ، آنان صرفا" خود را با وضعیت موجود هماهنگ و یا بهتر بگوئیم همراه می نمایند . تفکر فوق هرج و مرج در شبکه را به دنبال داشته و آن را مستعد انواع حملات می نماید . بدین منظور لازم است که تدوین یک سیاست امنیتی در دستور کار قرار گیرد . برای شروع می توان از کاربران و تبین وظایف آنان در زمان استفاده از زیرساخت فناوری اطلاعات و ارتباطات کار را آغاز نمود و به دنبال آن سیاست امنیتی در خصوص رمزهای عبور و دستیابی به اینترنت را تدوین نمود . در ادامه می توان سیاست های امنیتی در خصوص پیکربندی سخت افزار شبکه شامل تمامی دستگاه ها (کامپیوترهای شخصی ، سرورها ،روترها و سوئیچ ها) را تدوین نمود . این موضوع صرفا" به

پیکربندی ختم نمی شود و می بایست در این رابطه سیاست های امنیتی در خصوص حفاظت از آنها نیز تدوین گردد .

- **سیاست های سازمانی**

سیاست های سازمانی دارای یک نقش کلیدی در هر یک از بخش های سازمان می باشند . ارتباط سیاست های تعریف شده در یک سازمان با سیاست های امنیتی در خصوص استفاده از زیرساخت فناوری اطلاعات و ارتباط می بایست به دقت مشخص گردد . در این رابطه لازم است که دقیقا" تعریف امنیت از منظر مدیران ارشد سازمان مشخص شود . شاید برداشت یک مدیر از امنیت و اهداف آن با برداشت یک مدیر دیگر متفاوت باشد . بدیهی است که در مرحله نخست می بایست استراتژی و سیاست های امنیتی سازمان که متاثر از اهداف سازمان و نگرش مدیران (یک برداشت مشترک) ، تدوین یابد .

- **رها کردن مدیریت امنیت شبکه به حال خود**

ایجاد یک سیاست امنیتی قابل قبول در سازمان که شامل مانیتورینگ و بررسی امنیت شبکه نیز می باشد کار مشکلی بنظر می آید . بسیاری از افراد بر این باور هستند که همه چیز در حال حاضر خوب کار می کند و ضرورتی ندارد که ما درگیر پیاده سازی سیستمی برای مانیتورینگ و ممیزی شویم . در صورت عدم مانیتورینگ و ممیزی منابع سازمان ممکن است استفاده از منابع موجود چالش های خاص خود را به دنبال داشته باشد . وجود ضعف در مدیریت امنیت ممکن است یک

سازمان را با مسائل مختلفی نظیر برخوردهای قانونی مواجه نماید (افشاء اطلاعات حساس مشتریان در یک سازمان که به دلیل ضعف در مدیریت امنیت ایجاد شده است) .

مدیران شبکه می بایست بر اساس سیاست های امنیتی تعریف شده بطور مستمر و با دقت وضعیت شبکه را مانیتور کرده تا بتوانند قبل از بروز فاجعه در مرحله اول با آن برخورد و یا ضایعات آن را به حداقل مقدار ممکن برسانند .

- **نصب و انجام تغییرات مغایر با سیاست های تعریف شده**

نصب هرگونه نرم افزار و یا سخت افزار می بایست تابع سیاست های تعریف شده باشد . نظارت بر هر گونه نصب (سخت افزار و یا نرم افزار) و انطباق آن با رویه های تعریف شده در سیاست امنیتی از جمله عملیات مهم به منظور ایمن سازی و ایمن نگاهداشتن زیرساخت فناوری اطلاعات و ارتباطات است . نصب هر گونه تجهیزات سخت افزاری و نرم افزاری تائید نشده ، عدم پیکربندی مناسب تجهیزات نصب شده منطبق بر سیاست های امنیتی و در مجموع انجام هر گونه تغییرات غیرمجاز می تواند به سرعت حفره هائی امنیتی را در شبکه شما ایجاد نماید .

- **عدم وجود برنامه ای مدون جهت برخورد با حوادث غیرمترقبه**

شاید شما نیز از جمله افرادی باشید که فکر می کنید همواره حادثه برای دیگران اتفاق می افتد. بپذیریم که حوادث چه بخواهیم و چه نخواهیم اتفاق خواهند افتاد و ما نیز می توانیم هدف این حوادث باشیم . زمین لرزه ، آتش سوزی ، خرابکاری ، خرابی سخت افزار نمونه هائی در این زمینه می باشند . بدین منظور لازم است که هر سازمان دارای یک سیاست امنیتی مشخص به منظور پیشگیری

و مقابله با حوادث باشد . در صورتی که با این موضوع در زمان خاص خود برخورد نگردد ، پس از بروز حادثه مدیریت آن غیرممکن و یا بسیار مشکل خواهد بود .

استانداردهای 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.

- **استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس**
- **استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد**
- **استانداردهای مدیریتی سری ۲۷۰۰۰ موسسه بین المللی استاندارد**
- **گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد**
- **استاندارد ITBPM**
- **استانداردامنیتی ACSI33**
- **استاندارد AS/NZS**

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

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

استاندارد BS7799 موسسه استاندارد انگلیس

نسخه اول:	BS7799:1	1995
نسخه دوم:	BS7799:2	1999
نسخه آخر:	BS7799:2002	2002

استاندارد BS7799 موسسه استاندارد انگلیس–بخش اول

تدوین سیاست امنیتی سازمان

ایجاد تشکیلات تامین امنیت سازمان

دسته‌بندی سرمایه‌ها و تعیین کنترل‌های لازم

امنیت پرسنلی

امنیت فیزیکی و پیرامونی

مدیریت ارتباطات

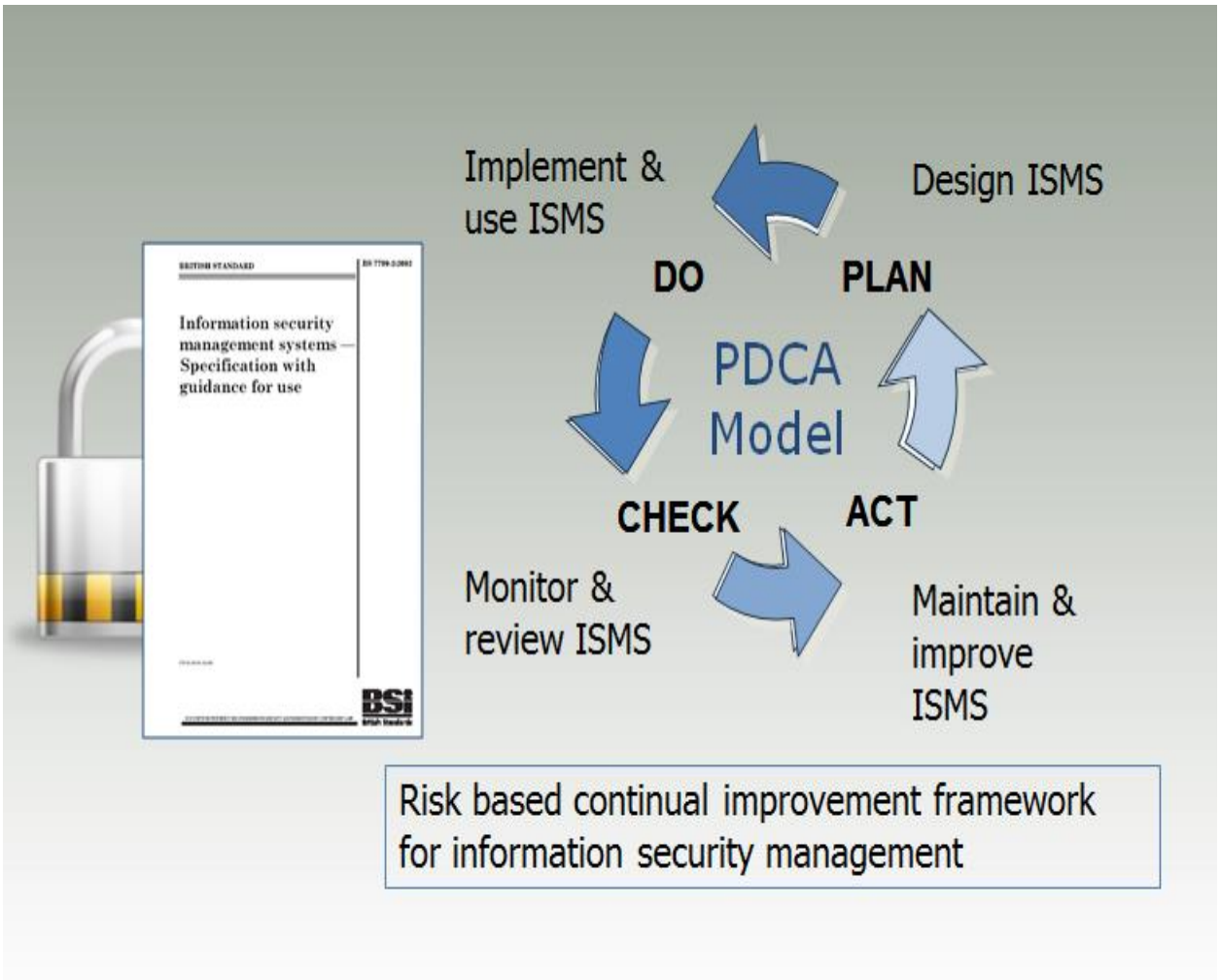
کنترل دسترسی

نگهداری و توسعه سیستم‌ها

مدیریت تداوم فعالیت سازمان

پاسخگوئی به نیازهای امنیتی

استاندارد BS7799 موسسه استاندارد انگلیس–بخش دوم



: Plan

"ISMS را برنامه ریزی کن"

این فاز در واقع مرحله مشخص شدن تعاریف اولیه پیاده سازی ISMS میباشد.تهیه سیاست هـای امنیتی ،مقاصد،تعریف پردازش های مختلف درون سازمانی و روتین های عملیاتی و..در ایـن مرحلـه تعریف و پیاده سازی میشوند.

DO :

"انجام بده (ISMS را پیاده نموده و از آن بهره برداری کن)"

پیاده سازی و اجرای سیاست های امنیتی،کنترل ها پردازش ها در این مرحله انجام میشود. در واقع این مرحله اجرای کلیه مراحل فاز اول را طلب میکند.

Check :

"کنترل کن (ISMS را پایش کرده و مورد بازنگری قرار بده) "

در این مرحله ارزیابی موفقیت پیاده سازی سیاست های مختلف امنیتی،همچنین تجربه های عملی و گزارش های مدیریتی گرد آوری خواهند شد.

Act :

"رفتار کن (ISMS رانگهداری نموده و آنرا بهبود ببخش) "

اجرای موارد ترمیمی و باز نگری در نحوه مدیریت طلاعات،همچنین تصحیح موارد مختلف در این فاز انجام میشود.

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.

- طرح تداوم خدمات تجاری
- کنترل بر نحوه دستیابی به سیستم
- توسعه و پشتیبانی سیستم
- ایجاد امنیت فیزیکی و محیطی
- انطباق امنیت
- امنیت کارکنان
- ایجاد امنیت سازمانی
- مدیریت رایانه و عملیات
- کنترل و طبقه بندی دارایی ها
- امنیت اطلاعاتی

راهنمای فنی ISO/IEC TR13335 موسسه بین‌المللی استاندارد

این گزارش فنی در قالب ۵ بخش مستقل در فواصل سالهای 1996 تا 2001 توسط موسسهٔ بین المللی استاندارد منتشر شده است. 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 طلاعات 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 سال1997 منتشر شد ، مراحل ایمن سازی و ساختارتشکیلات تامین امنیت اطلاعات سازمان ارائه شده است .

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 مولفه های 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.

مهندسی امنیت

تعریف مهندسی امنیت

مهندسی امنیت مجموعه فعالیت‌هایی است که برای حصول و نگهداری سطوح مناسبی از :

- **محرمانگی (Confidentiality)**
- **صحت (Integrity)**
- **قابلیت دسترسی (Availability)**
- **حساب پذیری (Accountability)**
- **اصالت (Authenticity)**
- **قابلیت اطمینان (Reliability)**

محرمانگی: اطلاعات برای افراد، موجودیت‌ها یا فرآیندهای غیرمجاز در دسترس قرار نگیرد یا افشا نشود.

صحت : صحت سیستم و صحت داده

صحت داده : داده ها به صورت غیر مجاز تغییر پیدا نکنند یا از بین نروند.

صحت سیستم : فعالیت‌های مورد انتظار از سیستم بدون عیب و خالی از دستکاری های غیر مجاز (تعمدی یا تصادفی) در سیستم انجام شود.

اصالت: هویت واقعی یک موجودیت با هویت مورد ادعا یکسان باشد.

قابلیت دسترسی: منابع برای یک موجودیت مجاز در هنگام نیاز در دسترس و قابل استفاده باشد.

حساب پذیری: فعالیت‌های موجودیت‌ها در سیستم اطلاعاتی به صورت جداگانه قابل ردیابی و بررسی باشد.

قابلیت اعتماد: سازگار بودن رفتارها و نتایج مورد انتظار

اصول مهندسی امنیت

- امنیت فضای تبادل اطلاعات مفهومی کلان و مبتنی بر حوزه های مختلف دانش است.
- امنیت هر سیستم تعریف مخصوص به خود دارد .
- امنیت ابزاری برای رسیدن به هدف سیستم است.
- امنیت نسبی است.
- امنیت سیستم یک طرح یکپارچه و جامع می‌طلبد.
- حیطهٔ مسئولیتها و مقررات امنیتی باید کاملاً شفاف و غیرمبهم باشد.
- طرح امنیتی باید مقرون به صرفه باشد.
- امنیت هر سیستم توسط عوامل اجتماعی محدود می‌شود.
- امنیت هر سیستم باید بطور متناوب مورد ارزیابی مجدد قرار گیرد.

چرخه ی حیات مهندسی امنیت

برای ایجاد امنیت در یک سازمان، اولین قدم تدوین اهداف، استراتژی و خط مشی امنیتی سازمان است.

- اهداف (Objectives)
- استراتژی (Strategy)
- خط مشی (Policy)

مدیریت امنیت IT :

مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع سر راه رسیدن به این اهداف و ارائه راهکارهای لازم را بر عهده دارد. همچنین مدیریت امنیت وظیفه پیاده سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهده داشته و در نهایت باید تلاش کند تا سیستم را همیشه روزآمد نگه دارد.

مدیریت امنیت IT شامل موارد زیر است:

- مدیریت پیکربندی
- مدیریت تغییرات
- مدیریت مخاطرات

مدیریت پیکربندی

فرآیندی است برای حصول اطمینان از اینکه تغییرات در سیستم تأثیر کنترل‌های امنیتی و به تبع امنیت کل سیستم را کاهش ندهد.

مدیریت تغییرات

فرآیندی است که برای شناسایی نیازمندی‌های جدید امنیتی در هنگام بروز تغییر در سیستم IT انجام می‌شود.

انواع تغییرات در سیستم IT :

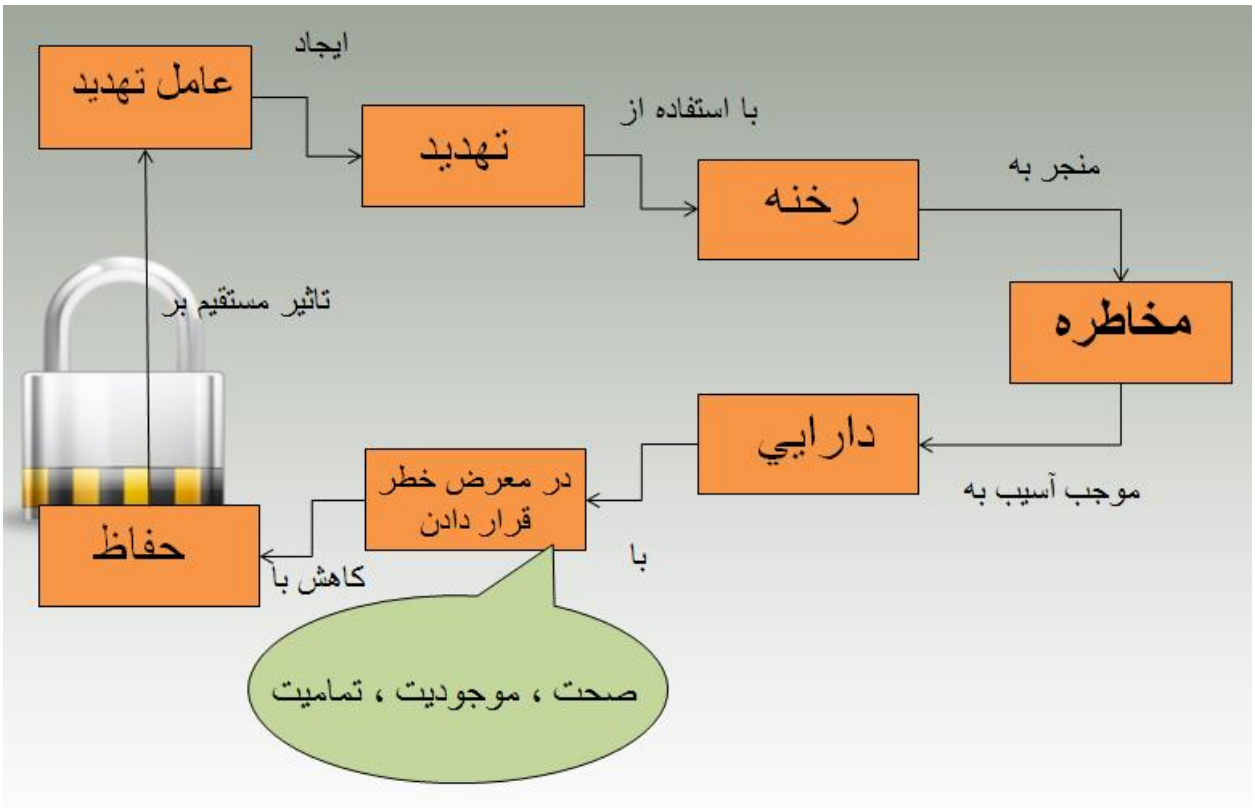
- روال‌های جدید
- بروز رسانی نرم‌افزارها
- تجدید سخت‌افزارها
- کاربران جدید
- اتصالات جدید شبکه

مدیریت مخاطرات

یکی از مهمترین قابلیتهای ISMS که در هر سازمانی به فراخور نیاز باید انجام می‌شود، مدیریت مخاطرات یا Risk Management است. ریسک یا مخاطره عبارت است از احتمال ضرر و زیانی که متوجه یک دارایی سازمان (در اینجا اطلاعات) می‌باشد. عدم قطعیت (در نتیجه مقیاس ناپذیری) یکی از مهمترین ویژگیهای مفهوم ریسک است. طبعا این عدم قطعیت به معنای غیر قابل محاسبه و مقایسه بودن ریسکها نیست.

مدیریت مخاطرات فرآیندی است برای شناسایی و ارزیابی:

- دارایی‌های که بایستی حفاظت شوند (**Assets**)
- تهدیدات (**Threats**)
- رخنه‌ها (**Vulnerabilities**)
- آسیبها (**Impacts**)
- مخاطرات (**Risks**)
- روش‌های مقابله (**Safeguards**)
- ریسک باقی مانده (**Residual Risks**)



پیاده‌سازی

- آگاهی‌رسانی امنیتی
- روش‌های دفاعی

کنترل‌های امنیت

تجربیات, روال‌ها یا مکانیزم‌های محافظت در مقابل تهدیدات

کنترل‌های امنیتی در حوزه‌های زیر قابل اعمال هستند :

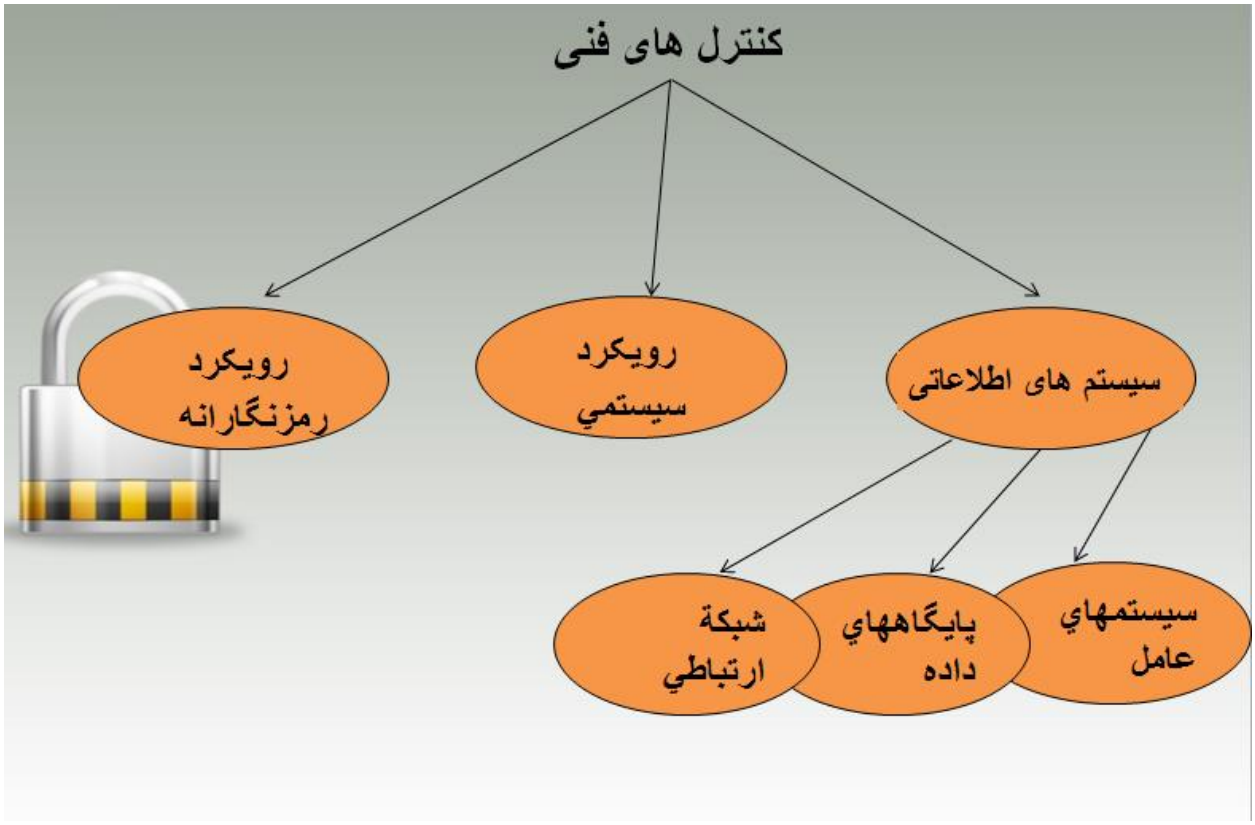
- سخت‌افزار (پشتیبانی, کلیدها و ...)
- نرم‌افزار (امضاء رقمی, ثبت وقایع (Log) , ابزارهای ضد ویروس) ارتباطات (فایروال, رمزنگاری)
- محیط فیزیکی (نرده و حفاظ و ...)
- پرسنل (آگاهی رسانی و آموزش, روال‌های استخدام, عزل و استعفا و ...)
- کنترل استفاده از سیستم‌ها (احراز اصالت, کنترل دسترسی و ...)

کنترل‌های امنیتی از یکدیگر مستقل نیستند و بایستی آنها را به صورت ترکیبی استفاده نمود.

انواع کنترل های امنیتی

- کنترلهای مدیریتی
- کنترلهای عملیاتی
- کنترلهای فنی

کنترل های فنی



سیستم های اطلاعاتی

- **سیستم عامل**

با این که هر سیستم عاملی دارای ضعف های امنیتی مختص به خود است ، ولی عمومیت و رواج یک سیستم عامل می تواند زمینه شناسائی و سوء استفاده از ضعف های امنیتی آن را تسریع نماید . شاید به همین دلیل باشد که ضعف های ویندوز شرکت مایکروسافت سریع تر از سایر سیستم های عامل بر همگان آشکار می شود چراکه اکثر کاربران بر روی کامپیوتر خود از یکی از نسخه های ویندوز این شرکت استفاده می نمایند . شاید بتوان گفت که لینوکس و یا یونیکس نسبت به ویندوز دارای ضعف های امنیتی کمتری می باشند ولی سیستم های عامل فوق نیز دارای ضعف امنیتی مختص به خود می باشند که به دلیل عدم استفاده عام از آنها تاکنون کمتر شناسائی شده اند .

- **پایگاه داده**

امنیت پایگاه داده فرآیند حفاظت از داده های سازمان در برابر دسترسی و استفاده غیر مجاز، افشاگری، تخریب و یا تغییر می باشد.

- **شبکهٔ ارتباطی**

تمامی تجهیزات شبکه ای نظیر سرویس دهندگان ، روترها ، سوئیچ ها و نظایر آن دارای برخی ضعف های امنیتی ذاتی می باشند . با تبعیت از یک سیاست تعریف شده مناسب برای پیکربندی و نصب تجهیزات شبکه ای می توان بطرز کاملا" محسوسی آثار و تبعات این نوع ضعف های امنیتی را کاهش داد . نصب و پیکربندی هر گونه تجهیزات شبکه ای می بایست مبتنی بر اصول و سیاست های امنیتی تعریف شده باشد .

سرویسهای اساسی

- حفاظت از شبکهٔ خودی
- دیواره آتش(Firewall)
- سیستم های تشخیص و مقابله با نفوذ (IDS/IPS)
- ضد ویروس
- مانیتورهای Log
- سیستمهای فریب

ارتباط امن بین‌شبکه‌ای

- روش های رمزنگاری
- شبکه اختصاصی مجازی (VPN)
- زیر ساخت کلید عمومی (PKI)
- امضاء دیجیتالی

- **روش های رمزنگاری**

رمزنگاری عبارتست از تبدیل داده ها به ظاهری که نهایتا بدون داشتن یک کلید مخصوص قرائت آن غیر ممکن باشد.هدف آن حفظ حریم خصوصی است با پنهان نگاه داشتن اطلاعات از افرادی که نباید به آنها دسترسی داشته باشند.

- **شبکه اختصاصی مجازی (VPN)**

یک VPN ، شبکه ای اختصاصی بوده که از اینترنت برای ارتباط با سایت های از راه دور و ارتباط کاربران با یکدیگر استفاده می نماید. این نوع شبکه ها بجای استفاده از خطوط واقعی نظیر خطوط Leased، از یک ارتباط مجازی به کمک اینترنت برای ایجاد شبکه اختصاصی استفاده می کنند .

- **زیر ساخت کلید عمومی (PKI)**

PKI (Public Key Infrastructure) به عنوان استانداردی که عملا برای یکی کردن امنیت محتوای دیجیتالی و فرایند های تجارت الکترونیک و همچنین پرونده ها و اسناد الکترونیکی مورد استفاده قرار می گرفت ظهور کرد.این سیستم به بازرگانان اجازه می دهد از سرعت اینترنت استفاده کرده تا اطلاعات مهم تجاری آنان از رهگیری ، دخالت و دسترسی غیر مجاز در امان بماند.یک PKI کاربران را قادر می سازد از یک شبکه عمومی ناامن مانند اینترنت به صورتی امن و خصوصی برای تبادلات اطلاعات استفاده کنند.این کار از طریق یک جفت کلید رمز عمومی و اختصاصی که از یک منبع مسؤل و مورد اعتماد صادر شده و به اشتراک گذارده می شود انجام گیرد .

- **امضاء دیجیتالی**

امضاء های دیجیتالی ، فن آوری دیگری است که توسط رمزنگاری کلید عمومی فعال گردید و این امکان را به مردم می دهد که اسناد و معاملات را طوری امضا کنند که گیرنده بتواند هویت فرستنده را تأیید کند.امضاء دیجیتالی شامل یک اثر انگشت ریاضی منحصر به فرد از پیام فعلی است که به آن One-Way-Hash نیز گفته می شود.

- **بیومتریک**

فناوری بیومتریک اگرچه از تخصصهایی سود می جوید که هر یک از آنها سابقه ی دیرینه در علم و صنعت دارند ولی دارای تعاریف، مفاهیم و کاربست های نو و جدیدی است. این فناوری که در واقع روشهای تعیین یا تایید هویت افراد به صورت خودکار، طبق شناسه های فیزیولوژیکی یا رفتاری است در سالهای گذشته، بیشتر در فیلم های سینمایی به عنوان یک فناوری پیشرفته علمی- تخیلی نمود داشته است و در عین حال در تعدادی از مراکز حساس که نیازمند به ضریب امنیتی بالایی بوده

اند نیز بکار گرفته شده است. پیچیدگی سخت افزاری و نرم افزاری سامانه ها و قلت کاربرد آنها، هزینه¬های ساخت و راه¬اندازی گزافی را به مجریان چنین طرحهایی تحمیل می کرده است .

انواع بیومتریکها

- بیومتریکهای فیزیولوژیکی
- بیومتریکهای رفتاری

اهمیت امنیت اطلاعات و ایمن سازی کامپیوترها

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 .

بیومتریک فیزیولوژیکی

بیومتریکهای فیزیولوژیکی عبارتند از:

- عنبیه نگاری
- شبکیه نگاری
- ا نگشت نگاری
- چهره نگاری
- دست نگاری
- صوت نگاری

بیومتریک رفتاری

بیومتریکهای رفتاری عبارتند از:

- امضا نگاری
- نحوه ی تایپ کردن

سایر بیومتریک

پارامترهای دیگری هم اخیراً مورد استفاده قرار گرفته است که به علل مختلف هنوز کاربرد وسیعی ندارند. از جمله می توان به بیومتریکهای زیر اشاره کرد:

- DNA
- نحوه راه رفتن
- الگوی رگهای پشت دست
- خطوط کف دست
- شکل گوش
- بوی بدن
- و الگوی بافتهای زیر پوستی دست

آموزش

- آموزش های عمومی
- آموزش های اختصاصی

ISMS درایران

برخی دلایل عدم توجه به ISMS در ایران :

الف: عدم تخصیص جایگاه مناسب به مسائل امنیتی

ب: کمبود های تئوریک و عملی کارشناسان

ج: عدم آموزش و اطلاع رسانی

کلام آخر

در این جزوه به بررسی اهم اشتباهات متداول که ممکن است از جانب عوامل انسانی در یک سیستم کامپیوتری بروز نماید ، اشاره و گفته شد که عدم رعایت مسائل مربوطه می تواند زمینه بروز مشکلات متعدد ایمنی در سازمان را بدنبال داشته باشد . مواردداعلام شده را جدی گرفته و در صورت ضرورت مدل امنیتی جاری را بازسازی نمائید . به کاربران ، مدیران شبکه و حتی مدیران سازمان آموزش های لازم داده شود تا سطح آگاهی و اطلاعات آنان دررابطه با امنیت افزایش یابد(جملگی می بایست دارای یک سطح مناسب از سوادعمومی در ارتباط با امنیت اطلاعات باشیم). تداوم عملیات یک سازمان در عصر حاضر ارتباط مستقیم به رعایت مسائل ایمنی توسط عوامل انسانی آن سازمان دارد. لذا آشنایی با مفاهیم امنیت اطلاعات و مدیریت امنیت اطلاعات در سازمان و شناخت روشهای شناسایی مخاطرات و مدیریت ریسک امنیتی و مفاهیم الزامات و کنترل های استاندارد و همچنین آشنایی با آخرین روشهای مدیریت امنیت اطلاعات در سازمان به منظور تلاش برای امنیت سایبری و خنثی کردن حمله و تأکید بر نیاز به آموزش افراد و سیستم ها برای تشخیص به موقع نفوذ از ضرورتهای هر محیط سازمانی می باشد تا در آخر ریسک سازمانی به حداقل و اجرای استراتژی مدیریت، به بهینه ترین شکل ممکن صورت پذیرد.