
بسم الله الرحمن الرحیم

تقدیم به بزرگ بانوی دو عالم حضرت فاطمه الزهرا(سلام الله علیه)

آموزش امنیت سایبری

مدیران

مولف

مهندس ناصر نامخواه

سرشناسه: نامخواه، ناصر، ۱۳٤۰

عنوان و نام پدیدآور: آموزش امنیت سایبری – مدیران

مشخصات نشر:

مشخصات ظاهری: ۲۰۵ص. ، مصور، جدول، نمودار

شابک:

وضعیت فهرست نویسی: فیپا

یادداشت: واژه‌نامه

یادداشت:

کتابنامه: ص. ۲۰۵

موضوع:

نام کتاب: آموزش امنیت سایبری – مدیران

تألیف: مهندس ناصر نامخواه

نوبت چاپ: اول، بهار ۱۳۹۰

ناشر:

صفحه آرایی : مجید بهمنی

طراح جلد : مجید بهمنی

شابک:

تیراژ:

قیمت: ریال

مقدمه

در طول تاریخ توسعه و امنیت همیشه مانند دو بال پرندگان در کنار یک‌دیگر نبوده‌اند. قبل از اختراع برق که شاید بتوان از آن به عنوان شروع عصر جدید انسان‌ها نام‌برده عصری که امروزه از آن با عنوان دوره نوین و در برخی موارد عصر دیجیتال نام بردند، امنیت همپای توسعه دارای رشد مناسبی بوده است. هر میزان دسترسی انسان‌ها به علم و فن‌آوری تا این زمان منجر به افزایش امنیت می‌گردید. ابزار تولیدی در مسیر توسعه همراه با خود امنیت فکری و اجتماعی انسان‌ها را افزایش می‌داد. با ورود بشریت به دوره جدید که برخی شروع آن را هم زمان با اختراع برق نامیده و اختراع ابزاری مانندترانزیستور و مدار مجتمع و تجهیزات الکترونیکی تهدیدات جدیدی فراروی انسان‌ها گشوده شد.

سرعت رشد تکنولوژی در اعصار جدید از سرعت بسیار بالاتری برخوردار بوده است، لکن به نظر می‌رسد که هر توسعه جدیدی همراه با خود ناامنی‌های جدید را به ارمغان می‌آورد. این مطلب باعث شده است پژوهش‌های مختلف ارتباط بین امنیت و توسعه را رابطه‌ای معکوس بنامند لذا به نظر می‌رسد یکی از راه‌های وصول به امنیت در دنیای دیجیتال شناخت واقعی عرصه ابزار مرتبط با آن می‌باشد.

با گسترش فعالیت مباحث پدافندی غیر عامل در کشور و حرکت تخصصی این فعالیت‌ها به مرور شاهد نشر دانش تخصصی در عرصه پدافند غیر عامل فاوا با رویکردهای علمی‌و عملی در زمینه تهدیدات موجود و راه‌های شناخت آسیب‌پذیری‌ها و مقابله با آن‌ها توسط سازمان‌ها، نهادها و کاربران و مدیران در این عرصه می‌باشیم.

کتابی که در پیش روی دارید که یکی از چهار جلد کتابی است که با هدف آشنایی افراد مرتبط با این گونه ابزار و به منظور حفاظت از منابع و سرمایه‌های ملی نظام جمهوری اسلامی، ایجاد ثبات در کاربرد سیستم‌ها و اطمینان از استمرار و سلامت اجرای فرآیند فعالیت‌های کاربران مختلف جمع‌آوری و تألیف گردیده است.

با توجه به این که مدیران، یکی از حساس‌ترین لایه‌های درگیر با استفاده از ابزار رایانه‌ای و دیجیتال و ارتباطی می‌باشند و منابع هر سازمان با گرایش مدیر مربوطه در این زمینه‌ها مصروف می‌گردد. در این کتاب که ویژه مدیران محترم در سطوح عملیاتی و استراتژیک تنظیم گردیده است، مطالب سمت و سوی کاربردی مدیریتی پیدا نموده و مطالب مرتبط و مورد نیاز این قشر از جامعه جمع‌بندی و تقدیم می‌گردد.

در کتاب کاربران تلاش گردیده است کاربرانی که به نوعی از رایانه‌ها و ابزار دیجیتال به صورت کاربردی در زندگی شخصی و اجتماعی و کاری بهره می‌برند، از زاویه دفاع سایبری با این ابزار آشنا شده و ضمن آشنایی با عرصه‌های امنیتی این ابزار بتوانند به‌ترین روش امنیت، پایداری و ایمنی این گونه وسائل را انتخاب و به کار بگیرند.

در کتاب متخصصان که با هدف آشنایی متخصصین و اهل فن با امنیت ابزار دیجیتال به رشته تحریر درآمده است تلاش گردیده است با عمق بخشی به مطالب زمینه استنباط علمی‌این گروه از عزیزان در حد بضاعت فراهم گردیده و نیازمندی‌های علمی‌و امنیتی آنان در کتاب مربوط به ایشان جمع آوری و ارائه گردد.

تمام دستورالعمل‌ها و اسناد عملیاتی تنظیمی‌در لایه‌های مختلف سازمان و هر جامعه‌ای می‌بایست به روش‌های علمی‌و عملیاتی و در برهه‌های مختلف از زمان ممیزی گردد و میزان کارآیی آن‌ها و قابلیت اعتماد به روش‌های اجرایی آن سنجیده شود. در کتاب ممیزان کوشش گردیده است روش‌های ممیزی و امنیت در دنیای دیجیتال و راه‌های عملیاتی نمودن این گونه ارزیابی از اجرای عملیاتی دستورالعمل‌ها سنجیده شده و بیشتر روش ممیزی ارائه شود تا دستورالعمل‌های بی‌روح ممیزی.

امید است این تحفه‌های ناقابل که قطعاً با نقادی صاحب‌نظران در اقصی نقاط کشور و مجامع علمی‌و دانشگاهی سیر رشد و تعالی خود را طی خواهد نمود زمینه‌های گسترش حرکت علمی‌در زمینه‌های پدافند غیر عامل فاوا را در کشور (ولو هر چندانک) بتواند ایجاد نموده و از نظرات و پیشنهادات صاحب نظران علمی‌استقبال نموده و با تکمیل آن‌ها در کتب آتی بتوانیم در هرچه پربارتر نمودن این گونه کتاب‌ها کوشا باشیم.

کتاب حاضر در ۶ فصل تقدیم می‌گردد. در انتهای هر فصل اهداف هر فصل برشمرده شده و پس از بررسی مطالب فصل، در انتهای فصل سئوالاتی با انگیزه کمک به هر چه به‌تر یادگیری مطالب کتاب به صورت خود آموز طراحی گردیده تا خوانندگان محترم بتوانند با مرور بر پاسخ آن‌ها یک بار دیگر فصل را بررسی و به ماندگاری مطالب در ذهن کمک بیش‌تری داشته باشد.

در فصل اول مباحث مربوط به مقدمات و مبانی مورد نیاز برای ورود به بحث اصلی پرداخته شده و ضمن آشنایی با اطلاعات و اسناد و انواع تهدیدات و فرصت‌های کلی در امنیت دیجیتال با قاعده اصلی پدافند غیر عامل در حوزه فاوا که همان قابلیت اتکا به سازندگان این گونه ابزار است آشنا شده و با انواع آسیب‌های دیجیتال آشنا می‌شویم.

فصل دوم به آشنایی با پدافند غیر عامل در حوزه فاوا پرداخته و ضمن ارائه مفاهیم امنیت، ایمنی و پایداری در این حوزه با انواع سرمایه‌ها و تهدیدات از این منظر آشنا می‌گردیم.

در فصل سوم ضمن پرداختن به پروتکل های امنیتی با اقداماتی که مدیران و سازمان می‌تواند در ایمن نگهداشتن اطلاعات داشته باشد آشنا می‌شویم.

در فصل چهارم ضمن بررسی شیوه تحلیل مخاطرات , با حفاظ های ایمنی که می‌توان برای امن نگهداشتن اطلاعات پس از شناسایی مخاطرات استفاده نمود آشنا می‌شویم.

در فصل پنجم به سیاست های امنیتی که یکی از ارکان امن سازی و ایمنی و پایداری اطلاعات و تجهیزات هر سازمان است خواهیم پرداخت.

در فصل ششم که فصل آخر می‌باشد به شیوه های نظارت و ارزیابی امنیتی پرداخته و روش های نگهداری و پشتیبانی امنیتی اطلاعات سازمان را بررسی خواهیم نمود.

امیدواریم بهره‌گیری این کتب بتواند نقشی ولو اندک در حفظ امانات شهدای گران‌قدر انقلاب اسلامی‌که همانا اطلاعات و اسناد نظام جمهوری اسلامی‌می‌باشد داشته باشد و با توصیف واقعیت‌های موجود در امنیت و ایمنی و پایداری این ابزار توانسته باشیم دریچه‌ی نگاه جدیدی را به روی کاربران گرامی‌باز کرده باشیم.

مؤلف

فهرست مطالب

فهرست تصاویر

فصل اول – تعاریف

آن چه در این فصل خواهید آموخت:

تعریف اطلاعات

تعریف اسناد

تعریف امنیت

تقسیم بندی سرمایه‌ها و مناطق قابل حفاظت

تعریف پدافند عامل

تعریف پدافند غیر عامل

تعریف تهدید نرم

تعریف مدیریت تهدید

امنیت در دنیای سنتی و نوین

۱- تعاریف

با توجه به این که امروزه اصطلاحات، عبارات و کلمات تخصصی معانی مختلفی پیدا کرده‌اند و برد استفاده از آن‌ها گستردگی فراوانی پیدا نموده است در این فصل ابتدا با تعاریف مورد نیاز برای ادامه کار آشنا شده و تعاریف عملیاتی و اختصاصی خاصی را که در ادامه کتاب به آن نیاز داریم بررسی می‌نماییم.

۱-۱- تعریف اطلاعات

با توجه به این که اطلاعات جمع اطلاع بوده و اطلاع به معنی آگاهی یافتن و واقف شدن بر کاری می‌باشد می‌توان اطلاعات را به هرگونه اقدام یا روشی که منجر به آگاه شدن از هر مطلب و مسئله‌ای می‌باشد تلقی نمود. هرگونه ابزار و یا حرکت یا نوشته و ایما و اشاره‌ای که منجر به آگاهی رسانی شود را می‌توان در حیطه اطلاعات تعریف نمود. با توجه به این که امروزه برای اطلاعات تقسیم بندی‌های مختلف انجام می‌دهند رایج‌ترین نوع اطلاعات را اطلاعات خام[۱] نامیده و شامل کلیه آگاهی رسانی‌های بدون ارزیابی شده و تمام انواع اطلاعات را در بر می‌گیرد.

با توجه به این که رایج‌ترین نوع اطلاعات را امروزه از اسناد استنتاج می‌نمایند ذیلاً به صورت تفصیلی به این مطلب می‌پردازیم.

۱-۲- تعریف اسناد

---

۱ data

به موجب ماده ۱۲۸۴ قانون مدنی ایران سند عبارت است از «هر نوشته که در مقام اثبات دعوا یا دفاع قابل استناد باشد».

۱-۳- تعریف امنیت

در تعریفی عام امنیت عبارت است از مکانیزم‌های پیش‌گیری یا کاهش احتمال وقوع رخدادهای خطرناک و جلوگیری از تمرکز قدرت در هر نقطه از شبکه و احیای شبکه در حین وقوع رخدادهای ناخوشایند (وقتی که رخدادهای خطرناک حادث می‌شوند) هر عاملی که به‌طور بالقوه بتواند منجر به وقوع رخدادی خطرناک شود یک تهدید امنیتی به شمار می‌آید.

امروز برای امنیت تعاریف مختلفی ارایه شده است و برخی امنیت را در بعد فیزیکی آن مورد بررسی قرار داده و برخی در ابعاد روانی آن را مورد بررسی قرار داده‌اند. امروزه برخی امنیت را مترادف با کلمه حفاظت دانسته و از این زاویه به آن نگاه می‌کنند. واژه security در فرهنگ فارسی معادل واژه‌هایی همچون امن، محفوظ، مطمئن، محفوظ داشتن، تامین کردن آمده است. امنیت عمدتاً به نوعی احساس روانی اطلاق می‌گردد که به‌خاطر نداشتن ترس، وضعیت آرامش و اطمینان خاطر حاصل می‌گردد.
امنیت به حداقل رساندن خطر یا تهدید است که این خطرها نه فقط از نوع سنتی و نظامی‌هستند بلکه تهدیدات جدید غیر نظامی‌را نیز در بر می‌گیرند. فقدان تهدید، عنصر اساسی تعریف امنیت است گرچه عده‌ای فقدان تهدید را امری ناممکن و دست نیافتنی دانسته و از این‌رو به حداقل رساندن تهدید را مفهوم اصلی امنیت می‌دانند.

۱-۴- تقسیم بندی سرمایه‌ها و مناطق قابل حفاظت:

امروزه با توجه به اهمیت سرمایه‌ها و مناطق قابل حفاظت آن‌ها را به دسته بندی‌های مختلفی تقسیم می‌نمایند.

۱-۴-۱- عادی

تقریبا کلیه سرمایه‌ها و مراکز عام را که انسان‌ها با آن مراوده دارند در این گروه قرار می‌گیرد. گروه عادی گروهی است که انسان‌ها به صورت عادی تلاش خاصی برای حفظ و نگهداری آن انجام نمی‌دهند و صرفاً با مالکیت قانونی یا عرفی و شرعی آن را به تصرف درآورده و در تمام دنیا برای حفظ آن قوانین مدون و غیر مدونی وجود دارد و با احترام به این قوانین و رعایت آن عملاً حفاظت از این گروه از سرمایه‌ها، مناطق انجام می‌پذیرد.

۱-۴-۲- مهم

مراکز مهم مراکزی هستند که در صورت انهدام یا بروز آسیب در کل یا قسمتی از آن‌ها، آسیب و صدمات محدودی در نظام سیاسی، اجتماعی و دفاعی با سطح تاثیر گذاری محلی و موضعی وارد می‌گردد.

۱-۴-۳- حساس

مراکز حساس مراکزی هستند که انهدام یا ایجاد اختلال در کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات جدی و مخاطره آمیز در نظام‌های سیاسی، هدایت، کنترل و مدیریت، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری منطقه‌ای یا بخشی در کشور می‌گردد.

۱-۴-۴- حیاتی

مراکز حیاتی عبارتند از مراکزی که انهدام یا ایجاد اختلال در کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و مدیریت، اقتصادی و تولیدی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و دفاعی با سطح تاثیرگذاری فرابخشی یا در سراسر کشور می‌گردد.

۱-۵- تعریف پدافند عامل

پدافند عامل عبارت از رویارویی و مقابله مستقیم و به کارگیری جنگ افزارهای مناسب و موجود توسط نیروه‌های نظامی‌به منظور دفع حمله و خنثی کردن اقدامات آفندی و در واقع شامل عملیاتی در برگیرنده حمله، مقابله و دفاع نظامی‌با ابزارها و سلاح‌های جنگی، می‌باشد.

۱-۶- تعریف پدافند غیر عامل

پدافند غیرعامل مجموعه‌ای از اقدامات، طرح‌ها و تمهیداتی است که توان دفاعی سیستم را افزایش داده، پیامدهای حوادث و بحران‌ها را کاهش دهد و هم‌چنین امکان بازیابی سیستم‌های آسیب‌دیده را با حداقل هزینه‌ی ممکن فراهم سازد.

۱-۶-۱- امنیت

امنیت اطلاعات از سه جنبه مختلف مدنظر قرار می‌گیرد: محرمانگی۱، یکپارچگی۲ و دسترس‌پذیری۳.

محرمانگی به معنای اطمینان از این موضوع است که تنها افراد مجاز به اطلاعات دست‌رسی دارند.

یک‌پارچگی به معنای اطمینان از دقیق و کامل بودن اطلاعات و روش‌های پردازش آن است.

دسترس‌پذیری به معنای اطمینان از دست‌رسی افراد مجاز به اطلاعات در صورت لزوم است.

۱-۶-۲- ایمنی

ایمنی به مفهوم امن بودن در مقابل تهدیدها و حملات سخت و نیمه سخت می‌باشد. هر سیستمی به منظور تداوم بقا و توان ارائه تولیدات و خدمات باید ایمن باشد.

۱-۶-۳- پایداری

هرچند امنیت و ایمنی سیستم‌ها از منظر پدافند غیر عامل بسیار مهم و ضروری است اما به مفهوم تامین سیستم دفاعی کامل نمی‌باشد. یکی از نکات مهم، وجود پایداری در تولید و ارائه خدمات در مراکز حیاتی، حساس و مهم است. پایداری به این معنی است که یک مرکز در شرایط عادی و یا در صورت بروز حمله و خدشه‌دار شدن هر دو یا یکی از دو جزء ذکر شده، یعنی امنیت و ایمنی، باید امکان تداوم ارائه تولیدات و خدمات خود را داشته باشد.

۱- ۷- تعریف تهدید نرم

---

۱ Confidentiality

۲ Integrity

۳ Availability

برای تعریف تهدید نرم تعاریف مختلفی ذکر شده است. تهدید نرم عبارت از «نوعی تلاش برنامه‌ریزی شده برای بهره‌گیری از ابزارها و روش‌های تبلیغی رسانه‌ای، سیاسی و روان شناختی برای تاثیر نهادن بر حکومت‌ها و مردم کشورهای خارجی به منظور تغییر نگرش‌ها، ارزش‌ها و رفتارهای آنان است. » (الیاسی ۴۶:۱۳۸۸) همچنین تهدیدهای نرم آن دسته از تهدیداتی است که اهداف متفاوتی را موضوع خود قرار داده و به جای تمامیت ارضی، هویت، هنجار، فرهنگ و. . . را هدف قرار می‌دهند. (گفتگوی علمی، فصلنامه میثاق۱۳۸۶ : ۱۴۵)

۱- ۸- تعریف مدیریت تهدید

مدیریت تهدید یا جنگ نرم از چه منظری یا با چه نگاه تئوریکی به مقوله تهدید و جنگ نرم نگریسته شود، متفاوت خواهد بود؛ از این لحاظ اگر با منظر گفتمان سلبی، در حوزه نظریات به مقوله تهدید نگریسته شود، مدیریت خاص خودش را می‌طلبد. زیرا از بعد سلبی، امنیت عبارت است از عدم وجود تهدید، در این گفتمان امنیت ماهیت برون‌گرایی و سخت‌افزاری دارد. مکاتب رئالیسم و نئورئالیسم چنین تعریفی را ارائه می‌دهند. اساسا واقع‌گرایان از منظر قدرت به امنیت می‌نگرند و امنیت را از مشتقات قدرت تلقی می‌کنند. آن‌ها ضمن آن که امنیت را واقعیتی «عینی» می‌دانند. تنها بر بعد «عینی» امنیت نیز تأکید دارند و آسیب‌های داخلی در این نگاه اساساً مورد عنایت نیست.

اگر گفتمان ایجابی مبنای نگرش به تهدید باشد، مدیریت تهدید بیش از این که نگاه برون‌گرایی داشته باشد، به داخل و سرمایه اجتماعی تکیه دارد. زیرا از این منظر، از بُعد ایجابی امنیت به معنای رضایت و تناسب بین داشته‌ها و خواسته‌ها است. (افتخاری ۱۳۸۳) در این دیدگاه امنیت دارای بستر و مجموعه متکثری است که اگر شاخص‌های آن آماده باشد، برای انسان نوعی آرامش و اطمینان به‌وجود می‌آورد در غیر این صورت ناامنی محل ظهور پیدا خواهد کرد. به عبارت دیگر، این رویکرد برای امنیت و تهدید، ماهیت تأسیسی قائل است و بر این باور است که تهدید، تنها در وضعیتی وجود دارد که آن جامعه در سطح قابل قبولی از اطمینان برای تحصیل و پاسداری از منافع ملی و ارزش‌های حیاتی‌اش نباشد. (افتخاری، ۱۳۸۴، ص ۱۶) اگر این گفتمان را ملاک قرار دهیم قبل از ظهور "تهدید عینی" یا جنگ نرم، دوره تکوین و شکل‌گیری راه را برای طراحی و اجرای مدیریت‌های پیش‌گیرانه هموار می‌سازد. این تلقی که تحت "نظریه فضایی" در کتاب کالبد شکافی تهدید مطرح شده است، بدان معنی است که سیکل

حیات تهدید در سه فضای اجتماعی، سیاسی و امنیتی معنا پیدا می‌کند و در هر فضایی الزامات و شرایط خاص خودش را دارد. در این میان حیات تهدید در فضای اجتماعی بسیار قابل توجه است و مدیریت پیش‌گیری بیش‌تر در این مرحله معنا و مفهوم پیدا می‌کند. در این فضا تلقی این است که تهدیدات در یک شبکه روابط اجتماعی شکل می‌گیرند؛ در فضای سیاسی پدیده مورد نظر با قدرت رسمی‌به‌صورت ایجابی و سلبی ارتباط پیدا می‌کند. فضای امنیتی عبارت است از قلمروی از بحث که در آن پدیده مورد نظر به‌صورت ایجابی و سلبی با ثبات نظام ملی ارتباط برقرار می‌کند.

بر این مبنا، مدیریت پیش‌گیری مبتنی بر این نظریه است که تهدیدات قبل از ورود به مقطع ظهور عینی شان، حضور دارند. از این رو، پدیده‌ها قبل از آن که در فضای خارجی، هویتی عینی بیابند، دارای هویتی اجتماعی درون ساختار جامعه می‌باشند. (افتخاری،فصلنامه میثاق ۱۳۸۵: ۷)

۱-۹- امنیت در دنیای سنتی و نوین

تحولات جوامع بشری را می‌توان به اعتبار شیوه و متد مدیریتی حاکم بر آن، به چهار عصر تقسیم نمود که هر یک از آن‌ها برای ادامه حیات خود نیازمند به ابزار و لوازم خاص خود بودند و از این جهت هر یک از این تحولات شرایط و ویژگی‌های خود را دارا می‌باشند، این چهار عصر عبارتند از :

۱) عصر شکار

در این عصر که اولین مدل مدیریتی بشر می‌باشد، هدف همه ابنا بشر جمع آوری شکار بود. گروه‌های کوچک مردم که همواره در حال حرکت و مهاجرت و تحرک بودند همه مشغول تهیه مایحتاج زندگی و غذای خود بودند. در این عصر هر کس که کار می‌کرد سهم غذا داشت در غیر این صورت امکان ادامه حیات نداشت. سبک مدیریت در این عصر قدرت زور و چماق بود.

۲) عصر کشاورزی

در این عصر توانائی بشر به حدی رسیده بود که بتواند برای خود غذا تولید نماید تا افرادی که توانائی انجام کار را ندارند نیز از غذا بهره‌مند شوند. در عصر کشاورزی انسان یاد گرفت که می‌تواند در یک منطقه سکنی گزیند و نیازی به مهاجرت دائم از یک منطقه به منطقه دیگر ندارد.

۳) عصر صنعتی

در این عصر انسان و بشر با استفاده از ماشین آلات و ابزار تولید توانست افزایش فوق‌العاده‌ای را در تولیدات مصرفی و محصولات کشاورزی ایجاد نماید.

۴) عصر فراصنعتی (اطلاعات)

در این عصر اکثر افراد در خدمت تولید فرآورده‌ای به نام اطلاعات هستند و پیش‌بینی می‌شود که این روند روزبه‌روز نیز افزایش یابد و عده‌ی قلیلی در امر تولید محصولات کشاورزی و مواد غذایی باقی بمانند و در عوض عده‌ی بیش‌تری در امر تولید و پردازش اطلاعات قرار گیرند.

عنصر با ارزش این عصر اطلاعات است و فن‌آوری‌های اطلاعات و ارتباطات کشورها را به سوی جامعه اطلاعاتی سوق می‌دهد. ظهور شبکه‌ای رایانه‌ای جهانی به مدد فن‌آوری‌های پیش‌رفته مخابراتی دنیای جدیدی به وجود آورد که عده‌ای آن‌را دنیای مجازی یا دیجیتال نامیدند. انقلاب دیجیتال و مجازی شدن همه چیز از کار و آموزش و مدیریت گرفته تا مناسبات اجتماعی و حتی جنگ از نشانه‌های شروع عصر جدیدی در جهان است.

توسعه شگفت انگیز تکنولوژی اطلاع رسانی در عصر انفجار اطلاعات نوید زمان بی‌نظیری را می‌دهد که همه ابعاد تمدن بشری از آن تاثیر پذیرفته است. در عصر اطلاعات و جامعه اطلاعات محور اقتصاد، سیاست، فرهنگ، هنر و اصولاً تمامیت دانش بشری با ابزارها و شیوه‌های تبادل الکترونیکی اطلاعات پیوند دارد.

فشرده شدن کار در واحد زمان از مشخصه‌های بارز دنیای جدید است. رشد و توسعه تکنولوژی هر روز بر این فشردگی می‌افزاید. از طرفی فشردگی کار در واحد زمان موجب می‌شود که رشد تکنولوژی با نسبتی چند برابر ادامه یابد. حافظه‌های الکترونیکی و اَبَر رایانه‌های موجود بر فشردگی مزبور می‌افزایند و هر لحظه شرایط جدیدی را برای دست‌یابی سریع‌تر به نیازمندی‌های بشر فراهم می‌آورند.

۱-۹-۱- تهدیدات و فرصت‌ها در دنیای سنتی

در دنیای حقیقی انسان‌ها باید در گروه‌ها جمع شوند تا بتوانند تاثیر گذاری در گروه‌ها داشته باشند ولی در دنیای مجازی انسان‌ها به‌صورت انفرادی می‌توانند تاثیر گذار باشند.

در دنیای حقیقی سیاست جغرافیایی مفهوم دارد ولی در دنیای مجازی سیاست مبتنی بر جغرافیا نداریم و به‌جای آن سیاست مبتنی بر زمان و تندی داریم.

در دنیای حقیقی مرزهای فیزیکی وجود دارد ولی در دنیای مجازی مرزی وجود ندارد.

۱-۹-۲- تهدیدات و فرصت‌ها در دنیای نوین

در دنیای حقیقی ما حوزه‌های هم‌پوشان منافغ نداریم (یا بسیار کم داریم) ولی در دنیای مجازی مرزهای هم‌پوشان و حوزه‌های هم‌پوشان داریم.

در دنیای حقیقی با تضاد تضادها سروکار داریم – مانند امنیت و عدم امنیت – ولی در دنیای مجازی می‌توان تضادها را با هم جمع کرد.

در دنیای مجازی امنیت و ناامنی مطلق نداریم بلکه مخلوطی از آن را داریم.

در دنیای حقیقی حذف تهدیدها داریم ولی در دنیای مجازی حذف تهدیدها نداریم بلکه قابلیت هم‌زیستی با تهدیدها داریم. یعنی قابلیت تهدید پذیری و تهدید زدایی افزایش پیدا می‌کند.

۱-۹-۲-۱- انواع تهدیدات:

تهدیدات انواع و اقسام مختلفی داشته و از زوایای مختلفی می‌توان آن‌ها را تقسیم بندی نمود. در این کتاب تلاش بر این شده است تا از زاویه منشا این تهدیدا تقسیم بندی صورت پذیرد.

۱-۹-۲-۱-۱- تهدیدات فنی

در عصر فن‌آوری اطلاعات یکی از مهم‌ترین و رایج‌ترین تهدیدات این نوع از تهدید می‌باشد. در بسیاری از مواقع خطراتی که جوامع را تهدید می‌کند به علت گستردگی ضریب نفوذ ابزار فنی، این نوع از تهدید می‌باشد. در قرن اخیر به علت دست‌یابی انسان به ابزار پیش‌رفته فنی و نقش این ابزار در زندگی بشر استفاده از این ابزار جزئی از زندگی آدمی‌شده است و بدون آن‌ها در بسیاری از مواقع ادامه حیات بسیار سخت خواهد شد و به این خاطر گرایش به سمت استفاده هر چه بیش‌تر از این ابزار می‌باشد.

۱-۹-۲-۱-۱-۱- تهدیدات سخت‌افزاری

این گونه تهدیدات از جانب سخت‌افزارهایی است که استفاده می‌شود. به طور مثال استفاده از انواع ابزار نوین مانند رایانه‌ها و خودروها و هواپیماها و لوازم اداری و صنعتی که استفاده می‌شود در این تقسیم

بندی قرار می‌گیرد. قبل از استفاده از ابزار صنعتی، تهدیدات مربوطه نمی‌توانست یک کشور را از راه دور تهدید نماید لیکن در عصر حاضر کشورهایی که استراتژی خود را بر مبنای صنعت قرار داده‌اند به مجرد این که صنعت آنان به هر علتی با رکود مواجه شود باعث خواهد شد تا امنیت ملی آن کشور نیز به خطر افتد و به همین خاطر تلاش دارند تا به هر شکل ممکن این ابزار را از خطرها دور نگه دارند و دشمنان آنان نیز تلاش دارند از این ناحیه خطر را متوجه آن کشور نمایند.

۱-۹-۲-۱-۱-۲- تهدیدات نرم‌افزاری

تهدیدات نرم‌افزاری تهدیداتی را تشکیل می‌دهند که بیش‌تر مغز افزار می‌باشند تا سخت‌افزار. این گونه تهدیدها در مواقعی خط مشی‌ها و روش‌های زندگی و نوع نگرش و نوع رفتار و الگوی رفتاری و این گونه موارد را در بر می‌گیرد و در برخی موارد نرم‌افزارهای رایانه‌ای که وظیفه مدیریت بر سخت‌افزارهای به کار گرفته را بر عهده دارد در بر می‌گیرد. در صورت ایجاد تهدیدات بالقوه در نرم‌افزارهای رایانه‌ای و به مجرد بالفعل تبدیل شدن این تهدیدات، متخاصمین خواهند توانست از راه دور و در زمان مورد نیاز اشرافیت اطلاعاتی خود را بر کشور دیگری مسلط نموده و به نوعی فکر و فرهنگ و فیزیک آن کشور را به دست بگیرند.

۱-۹-۲-۱-۱-۳- تهدیدات سیستم‌های ارتباطی

با توجه به این که امروزه کلیه کشورهای دنیا از طریق سیستم‌های ارتباطی ملی و بین‌المللی به یک‌دیگر پیوند خورده و بدون این ارتباطات عملاً هیچ کشوری قادر به ادامه حیات نخواهد بود و کلیه تحرکات خود را در ابعاد مختلف سیاسی، اقتصادی، اجتماعی، فنی، ارتباطی و دیگر مسائل از این طریق با داخل و خارج خود پیوند می‌دهد، در صورت دسترسی هر ساختاری به این ابزار ارتباطی عملاً اشرافیت بر اطلاعات تبادلی نیز صورت خواهد پذیرفت. اشرافیت بر ارتباطات به علت سهل‌الوصول بودن و استفاده از تکنولوژی‌های کنترل از راه دور معمولاً کم هزینه پرفایده می‌باشد و بسیاری از سلطه گران به علت این که این ابزار تولید آن‌ها می‌باشد به راحتی امکان تسلط بر این ابزار را از راه دور داشته و بدون حضور فیزیکی امکان اشرافیت بر اطلاعات را برای خود مهیا می‌کنند.

۱-۹-۲-۱-۱-۴- تهدیدات الکترومغناطیسی

با پیش‌رفت علم و فن‌آوری در حوزه نیمه‌هادی‌های الکترونیکی، استفاده از تجهیزات رایانه‌ای، مخابراتی و الکترونیکی کاربردهای فراوانی پیدا کرده است. امروزه تمام ابزار اداری، صنعتی و نظامی‌از تجهیزات الکترونیکی استفاده می‌کنند و این مسئله آن‌ها را در مقابل لطمات الکترو مغناطیسی آسیب‌پذیر نموده است.

مدارات بردهای الکترونیکی که از ابتدا لامپی بوده‌اند و با ولتاژهای بالایی کار می‌کردند با پیدایش ترانزیستور تبدیل به قطعات بسیار کوچک‌تری شدند که با ولتاژهای پایین‌تری کار می‌کنند. با کاهش حجم و مصرف انرژی، استفاده از نیمه هادی‌های الکترونیکی رواج بیش‌تری پیدا کردند.

با توجه به این که ادامه حیات سرمایه‌های زندگی انسان‌ها که همان ابزار کاربردی می‌باشند به قطعات و سیستم‌های الکترونیکی، رایانه‌ای و مخابراتی وابسته است به همین دلیل یکی از جدّی‌ترین مخاطرات موجود تهدیدات الکترومغناطیسی می‌باشد. که هم به صورت طبیعی و هم ساخت دست بشر وجود دارد. از این تهدیدها می‌توان به رعد و برق، سویچینگ خطوط انتقال برق، دستگاه جوش ژنراتور الکتریکی، تسلیحات الکترومغناطیسی و انفجارات اتمی‌اشاره نمود.

۱-۹-۲-۱-۲- تهدیدات مصنوعی (انسان ساخت):

تهدیدات عمدی (که بیش‌ترین خسارت و دشوارترین راه مقابله را دارند) عبارت است از «هر گونه اقدام برنامه‌ریزی شده جهت افشا، نابودی یا تغییر در داده‌های حیاتی شبکه یا ایجاد اختلال در خدمات معمول سرویس دهنده‌ها». به‌طور عامّ هرگونه اقدام برنامه‌ریزی شده برای تحقق یک « رخداد خطرناک »، یک « تهدید امنیتی عمدی » تلقّی می‌شود.

۱-۹-۲-۱-۲-۱- تهدیدات برنامه ریزی شده

سازندگان سخت‌افزار و نرم‌افزار بنا بر سیاست‌های استراتژیک خود در زمان تولید این ابزار با اهداف مختلفی امکاناتی را بر روی آن‌ها تعبیه می‌نمایند تا در زمان مورد نیاز بتوانند به صورت آشکار و پنهان از راه دور و نزدیک به این ابزار دسترسی داشته و مدیریت آن‌ها را به دست بگیرند. ساده انگارانه‌ترین این اقدام برای تعمیر این ابزار از راه دور می‌باشد و بدبینانه‌ترین آن اشرافیت پنهانی بر اطلاعاتی که

توسط این ابزار در مبدا به کارگیری تولید می‌شود و هم‌چنین مدیریت استراتژیک این ابزار در زمان جنگ می‌باشد.

در کشورهای مختلف همچون امریکا برای این کار تدابیر قانونی نیز اندیشیده شده است تا تولید کنندگان بدون رعایت این مطلب این ابزار را به دیگر کشورها صادر ننمایند.

۱-۹-۲-۱-۲-۲- تهدیدات با منشا خطای انسانی

تهدیدات غیر عمد از اشتباهات سهوی و نا خودآگاه عوامل انسانی (همانند مدیران شبکه، کارکنان و کاربران) ناشی می‌شود و می‌تواند منجر به افشا یا نابودی اطلاعات یا اختلال در خدمات معمول شبکه و گاه تحمیل خسارت‌های کلان به جمیع کاربران شود. از این تهدیدات غیر عمد، می‌توان به موارد ذیل اشاره کرد:

طراحی نا صحیح زیر ساخت شبکه یا عدم وجود افزونگی در تجهیزات شبکه

عدم تهیه‌ی نسخه‌های پشتیبان از داده‌های حیاتی

سهل‌انگاری در وظایف روزمره (مثل بررسی مستمر سیستم‌ها از لحاظ آلودگی به ویروس)

نا آگاهی کاربران از ماهیت عملیات خطرناک

بروز اشکالات پیش بینی نشده[۱] در سطح سخت‌افزار، نرم‌افزار یا سیستم عامل

عدم اعمال صحیح سیاست‌های انتخاب و تعویض مداوم کلمات عبور توسط عوامل درگیر در شبکه

۱-۹-۲-۱-۳- تهدیدات طبیعی

این تهدیدات از عواملی مانند زلزله، سیل، گردباد، رعد و برق، آتش سوزی، آتشفشان و نظایر آن از قوّه به فعل می‌رسند و نسل بشر چنین تهدیداتی را به عنوان حقایق زندگی پذیرفته است. این تهدیدها همان گونه که زندگی را هدف گرفته‌اند می‌توانند در درجات خفیف‌تر منجر به نابود شدن یا افشای اطلاعات محرمانه و اختلال در سرویس‌های مؤلفه‌های اساسی شبکه شوند. از آن‌جا که خدمات شبکه‌های رایانه‌ای مرزهای جغرافیایی را در نوردیده است لذا تهدیدات طبیعی می‌توانند در خارج از محدوده‌ی بَلا دیده نیز منجر به اختلال در عملیات روزمره‌ی افراد و انتشار بحران در سطح وسیع شوند. لذا اگرچه تهدیدات طبیعی خارج از قدرت بشرند ولی برای بازگرداندن خدمات شبکه از وضعیت بحران

---

۱ BUG

به وضعیت عادی، از همان ابتدای طراحی شبکه، تمهیداتی برای جلوگیری از گسترش دامنه‌ی بحران به مناطق دیگر پیش‌بینی و اجرا می‌شود. به عنوان مثال ایجاد تراز پشتیبان در دیگر مناطق جغرافیایی و بهره‌گیری از خطوط ماهواره‌ای در کنار خطوط فیبر نوری در این رده از تمهیدها قرار می‌گیرد.

۱-۹-۳- شناخت اطلاعات دیجیتال

اسناد دیجیتال(رایانه‌ای) : شامل داده‌های رایانه‌ای، دیسکت‌های رایانه‌ای، سی دی‌های رایانه‌ای، امواج مخابراتی. یعنی تمام اطلاعات رایانه‌ای از هر نوع که باشد به‌عنوان "اسناد دیجیتال" تلقی می‌شود. آن چه که در این جا مهم می‌باشد آن است که بدانیم اطلاعات دیجیتال به مجرد تولید شدن، قابل از بین بردن نمی‌باشند و در صورت امحا می‌توان آن‌ها را به روش‌های مختلفی بازیابی کرد یا نمی‌توان با استفاده از رمزگذاری این اطمینان را حاصل نمود که کسی به اطلاعات ما دستبرد نزند. رابطه رشد علم و فن‌آوری تولید سند با امنیت سند رابطه‌ای معکوس است. یعنی هر چه علم و فن‌آوری پیش‌رفته‌تر می‌شود امنیت آن به همان میزان پائین‌تر می‌آید. پس امروز باید نگاهمان را به امنیت اسناد تغییر دهیم و ضمن شناخت ابزار تولید سند(سخت‌افزار، نرم‌افزار، شبکه‌های مربوطه،) دیدگاهِمان را نسبت به مقوله امنیت اسناد عوض کنیم.

۱-۹-۳-۱- انواع اطلاعات دیجیتال

اطلاعات دیجیتال در ابزار ذخیره ساز انواع و اقسام مختلفی دارند و بر مبنای آن مورد استفاده‌های خاصی قرار می‌گیرند.

۱-۹-۳-۱-۱- اطلاعات ذخیره شده

این گونه اطلاعات کلیه اطلاعاتی است که در ابزار ذخیره ساز به شکل‌های مختلف ذخیره شده و حفظ و نگهداری می‌شود و در صورتی که فردی به صورت مجاز و یا در غیر مجاز به این ابزار دسترسی پیدا نماید می‌تواند به این اطلاعات دسترسی پیدا کرده و آن‌ها را در اختیار بگیرد. به‌طور مثال در صورت مفقود شدن و یا به سرقت رفتن ابزار ذخیره‌سازی کلیه اطلاعاتی که در آن زمان بر روی این ابزار وجود

دارد از نوع اطلاعات ذخیره شده می‌باشد و افراد بدون این که تلاش خاصی داشته باشند می‌توانند به این اطلاعات دسترسی و آن‌ها را مورد استفاده قرار بدهند.

۱-۹-۳-۱-۲- اطلاعات پشتیبان

به منظور اطمینان از این که همیشه اطلاعات تولید شده قابل استفاده می‌باشد در زمان‌های مختلف از اطلاعات پشتیبان تهیه شده و در صورتی خرابی اطلاعات موجود می‌توان از این اطلاعات بهره‌برداری نمود اطلاعات پشتیبان در ابزار ذخیره‌سازی جانبی کپی برداری شده و در محله‌های امر نگهداری می‌گردد درصورتی‌که است فردی به صورت مجاز و یا غیر مجاز به این ابزار دسترسی پیدا نماید می‌تواند اطلاعات آن را مورد بهره‌برداری قرار بدهد.

۱-۹-۳-۱-۳- اطلاعات در حال عبور

اطلاعات در حال عبور همان اطلاعات تعاملی می‌باشند. در شبکه موجودیت‌ها در فاصله‌های دور از هم قرار دارند برای این که کلیه کاربران بتوانند از اطلاعات شبکه استفاده نمایند می‌بایست از طریق امکانات مخابراتی به یکدیگر وصل گردند اطلاعاتی که در بستر شبکه‌های مخابراتی در حال حرکت می‌باشند از موجودیتی به موجودیت دیگر منتقل می‌شوند و اطلاعات در درون سیستم‌های ارتباطی در حال حرکت می‌باشد چنان چه فرد غیر مجازی در مسیر عبور داده‌های اطلاعاتی که از طریق یک سیستم مخابراتی و در یک بستر شبکه‌ایی در حال تبادل و عبور هستند قرار گیرد؛ خواهد توانست از اطلاعات در حال عبور بهره‌برداری نماید.

۱-۹-۳-۲- سابقه امنیت دیجیتال

سابقه امنیت دیجیتال به قدمت دسترسی انسان‌ها به ابزار دیجیتال می‌باشد. از همان روزی که انسان‌ها توان این را پیدا کردند تا در عصر حاضر از ابزار دیجیتال در زندگی خود استفاده نمایند اولین مطلبی که ذهن آن‌ها را مشغول نمود مسئله امنیت اطلاعات دیجیتال می‌باشد. بدون امنیت دیجیتال عملاً اطلاعات تولید شده توسط دشمنان به راحتی قابل دسترسی می‌باشد.

۱-۹-۳-۲-۱- اصول امنیت دیجیتال:

در امنیت دیجیتال اصول مختلفی حاکم می‌باشد و با توجه به رعایت این اصول افراد تلاش می‌کنند تا امنیت اطلاعات خود را تأمین نمایند. بدون رعایت این اصول عملاً تأمین امنیت قابل اتکا نخواهد بود. امنیت دیجیتال مانند زنجیره‌ای به هم پیوسته می‌باشد و در صورت عدم رعایت امنیت در یکی از زنجیره‌ها عملاً امنیت در کل آن مخدوش خواهد شد.

۱-۹-۳-۲-۱-۱- اصل کلی- قابلیت اعتماد و اتکاپذیری

این اصل به مفهوم آن می‌باشد که قبل از این که هر ابزار دیجیتالی را مورد استفاده قرار داد ابتدا باید بررسی نمود تولیدکنندگان این ابزار با چه هدف و با چه نیتی این ابزار را تولید و در اختیار دیگران قرار داده‌اند. آیا در چرخه دسترسی به اطلاعات دیگران از مبدا تولید و با هدف دسترسی به این اطلاعات این ابزار تولید شده است. آیا این ابزار توسط دوست و یا دشمن تهیه شده است. آیا تولیدکننده این ابزار برای صدور آن به دیگر کشورها دارای دستورالعمل یا آیین‌نامه خاصی می‌باشد یا خیر. به‌طور مثال یکی از قوانین آمریکا برای صدور سخت‌افزار و نرم‌افزار به دیگر کشورها وجود نقاط آسیب‌پذیر در آن که به تایید اف بی آی رسیده باشد می‌باشد و فقط در صورت تأیید این ابزار قابلیت صدور به دیگر کشورها را پیدا می‌کند. در این گواهی اف بی آی تأیید می‌نماید که ابزار لازم برای دسترسی از راه دور و به دست گرفتن مدیریت ابزار از راه دور در این سخت‌افزار و نرم‌افزار تأمین شده و به راحتی از راه دور می‌توان آن را به دست گرفت و بر مبنای نیاز تغییراتی در آن در زمان جنگ ایجاد نمود.

۱-۹-۳-۲-۱-۲- اصول فرعی (مبانی نقد پذیر ISMS):

علاوه بر اصل ذکر شده که با عنوان پایه اصلی امنیت اطلاعات می‌باشد و در تامین امنیت اطلاعات دارای نقش اساسی می‌باشد و بدون در نظر گرفتن اصل کلی و صرفاً رعایت اصول فرعی امنیت اطلاعات در درون سیستم تأمین شده و از خارج از سیستم به راحتی امکان اشرافیت بر اطلاعات به شکل آشکار و پنهان قابل تامین می‌باشد این مسئله باعث خواهد شد در زمان جنگ و صلح به راحتی تولیدکنندگان ابزار سخت‌افزاری و نویسندگان نرم‌افزاری به صورت آشکار و پنهان عملاً قادر به دست گرفتن مدیریت از راه دور اطلاعات باشند.

۱-۹-۳-۲-۱-۲-۱- محرمانگی

به مجموعه مکانیزم‌هایی که تضمین می‌کند داده‌ها و اطلاعات مهم کاربران از دسترس افراد بیگانه و غیر مجاز دور نگاه داشته شود، «سرویس محرمانگی» اطلاق می‌شود. این سرویس‌ها عموماً با روش‌های رمزنگاری تحقق می‌یابند. روش‌های مختلف رمزنگاری اطلاعات، زیربنای مابقی سرویس‌های امنیتی است.

۱-۹-۳-۲-۱-۲-۲- در دسترس بودن

مکانیزم‌هایی که دست‌رسی به کوچک‌ترین منابع اشتراکی شبکه را تحت کنترل درآورده و هر منبع را بر اساس سطح مجوز کاربران و پروسه‌ها در اختیار آن‌ها قرار می‌دهد، «کنترل دست‌رسی» خوانده می‌شود.

۱-۹-۳-۲-۱-۲-۳- صحت و یک‌پارچگی اطلاعات

مجموعه‌ی مکانیزم‌هایی که از هرگونه تحریف، دست‌کاری، تکرار[۱]، حذف یا آلوده سازی داده‌ها پیش‌گیری می‌کنند یا حداقل باعث کشف چنین اقداماتی می‌شوند، «سرویس تضمین صحت اطلاعات» نامیده می‌شود.

۱-۱۰- رابطه بین رشد علم و فن‌آوری و امنیت

در دنیای فیزیکی رابطه بین رشد علم و فن‌آوری و تأمین امنیت رابطه‌ای مستقیم می‌باشد یعنی هرچه علم و فن‌آوری پیش‌رفته‌تر می‌شود امنیت به‌تر قابل تمدید خواهد بود. اما این مسئله در دنیای نوین کاملاً بالعکس می‌باشد یعنی هر چه حد علم و فن‌آوری پیش‌رفته می‌کند امنیت به همان میزان کاهش پیدا می‌کند دلیل آن ابداع روش‌های دسترسی پنهان در بازار دیجیتال می‌باشد. هر وسیله‌ای دیجیتال که ساخته می‌شود همراه با خود ناامنی‌های جدیدی به همراه دارد. با قرار گرفتن این ابزار در کنار ابزار دیگر ناتوانی‌های جدید به شکل تصاعدی بیش‌تر شده و زمینه را برای دسترسی غیرمجاز عناصر بیگانه فراهم می‌آورند.

---

۱ Reply

۱-۱۱- تحقیقات اجمالی انجام شده در رابطه با کلیات امنیت در دنیای دیجیتال

در جهان سنتی و فیزیکی اندیشمندان امنیتی همیشه بر این باور بودند که با افزایش علم و فن‌آوری ، امنیت نیز حداقل به همان میزان افزایش پیدا می‌کند. اگر به دنبال حفظ و حراست از کالای گران قیمت بودند، در تلاش برای استفاده از فن‌آوری‌های نوین برای حفظ آن نیز بوده‌اند. دیوارها را بلندتر می‌ساختند تا هر چه می‌توانند فاصله بین نا امن گرایان را با متاع گران قیمت خود بیش‌تر سازند. اگر طلای خود را می‌خواستند هر چه بیش‌تر از دست سارقان دورتر نگهدارند از ابزار نوین آنالوگ مانند انواع دزدگیر و. . . استفاده می‌نمودند. و همیشه این‌اندیشه در ذهن آنان غالب بود که با افزایش علم و فن‌آوری و ابداعات در دنیای فیزیکی امنیت را می‌توان بالاتر برد.

اما در سال ۲۰۰۰ میلادی نتیجه پژوهشی که توسط دانشگاه برکلی (berkley.com)امریکا منتشر شد این نظریه را کاملا منسوخ ساخت.

این تحقیق که به مدت بیست و پنج سال از سال ۱۹۷۵ الی ۲۰۰۰ میلادی انجام شد نشان می‌داد که هر چقدر که از سال ۱۹۷۵ به سمت جلوتر حرکت می‌کنیم علم و فن‌آوری و نوآوری و میزان دسترسی انسان‌ها به ابداعات و ابتکارات جدید و کشفیات بیش‌تر می‌شود. اما اگر در سال ۱۹۷۵ برای دسترسی غیر مجاز به اطلاعات دیجیتال می‌بایست چندین مهندس کار کشته و باتجربه باید در کنار هم و با کار گروهی تلاش می‌کردند تا بتوانند با یک دسترسی کوچک به این اطلاعات دسترسی پیدا نمایند، این کار در سال ۲۰۰۰ بسیار راحت‌تر شده بود و یک نوجوان ۱۷ ساله، بدون تحصیلات دانشگاهی و به تنهایی می‌توانست یک دسترسی نسبتاً بزرگی به صورت غیر مجاز به اطلاعات مهم داشته باشد.

نتیجه بیست سال از تحقیقات بیست و پنج ساله منتشر شده است ابتدا دسترسی غیر مجاز مشکل‌تر بوده است اما هر چه جلوتر می‌رویم این کار راحت‌تر می‌شود.

دانشگاه برکلی آمریکا به دو علت عمده به این نتیجه رسیده است:

دسترسی ارزان‌تر و آسان‌تر به ابزار دسترسی غیر مجاز به اطلاعات دیجیتال

همان گونه که ملاحظه می‌نمایید هر چه به سمت سال ۲۰۰۰ حرکت می‌کنیم در طی سالیان مختلف ابزار نفوذ غیر مجاز بیش‌تری نوشته شده و به صورت ارزان و همه گیر از طریق اینترنت در اختیار همگان قرار گرفته است و هر کس می‌تواند با دسترسی به اینترنت و سی دی‌های ارزان قیمت که در همه جای دنیا قابل تهیه است به این ابزار دسترسی پیدا نموده و با استفاده از آن‌ها شانس خود را برای دسترسی غیر مجاز به اطلاعات به آزمون بگذارد.

افزایش فراوانی آسیب‌پذیری با افزایش تولید ابزار نوین جدید

هرچقدر ابزار جدید تولید می‌شود همراه با خود آسیب‌پذیری‌های جدید را به ارمغان می‌آورد. اگر زمانی که فقط پول کاغذی وجود داشت یک دغدغه خاطر وجود داشت و آن حفظ پول از دست سارقان بوده است، اما به مجرد دسترسی به پول الکترونیکی باید این پول در مکان‌های مختلف که سارقان به شکل‌های مختلف به آن دسترس داشتند مورد حفاظت قرار گیرد تا با هک[۱] شدن رمز ورود و کارت بانکی و شبکه بانکی و شبکه مخابراتی و. . . . به دست دیگران نیفتد.

۱-۱۲- آسیب‌های امنیتی (سلطه اطلاعاتی):

در دنیا تمام سلطه‌گران به دنبال اهدافی هستند. آن‌ها با توجه به این اهداف به دنبال گسترش ابزار خود در تمام دنیا بود و با استراتژی از قبل تعیین شده نسبت به تولید و توسعه این ابزار اقدام می‌نمایند.

۱-۱۲-۱- اشرافیت بر ارتباطات

یکی از اهداف توسط جهان اشرافیت در ابزار ارتباطی به کل ارتباطات در دنیا می‌باشد. امروز سیستم‌های مخابراتی ملی به بین‌المللی وظیفه ارتباط بین کلیه آحاد مختلف در دنیا را به عهده دارند. اگر چنان‌چه ساختاری بتواند به این ابزار دسترسی پیدا کند عملاً قادر خواهد بود در مسیر چرخش اطلاعات بین کلیه ابزار دیجیتالی که توسط کاربران مورد استفاده قرار می‌گیرد قرار بگیرد و بر آن اشرافیت داشته باشد.

---

۱ Hack

۱-۱۲-۲- اشرافیت بر اطلاعات

هدف اصلی سلطه‌گران اشرافیت بر اطلاعات می‌باشد کلیه اقداماتی که به منظور اشرافیت بر ارتباطات انجام می‌دهند با هدف اشرافیت بر اطلاعات بوده و تمام سرمایه‌گذاری‌ها برای تولید ابزار اطلاعاتی و ارتباطی از ابتدا با استراتژی اشرافیت بر اطلاعات تولید شده در مبدا توسط کاربران بوده و این یک نوع سرمایه‌گذاری اقتصادی محسوب می‌شود.

۱-۱۳- آسیب‌های دنیای دیجیتال:

از بین رفتن کیان و کارکرد خانواده

در جوامع سنتی، نهادی اجتماعی با مرکزیت و محوریت مشخص است و هویت افراد، با توجه به خانواده‌هایشان شناخته می‌شود. اعضای خانواده سنتی را پدر و مادر، فرزندان، پدر بزرگ‌ها و مادر بزرگ‌ها تشکیل می‌دهند و جایگاه و احترام هر کدام مشخص و حفظ می‌شود.

سرپرست خانواده، رفتار و منش اعضای خود را کنترل می‌کند و اگر زمانی فرزندان با ازدواج یا ادامه تحصیل، از خانواده جدا بشوند، باز هم از کنترل و نظارت خارج نیستند و در مواقع لزوم نیز خانواده به یاری آنان همت می‌گمارد.

دین، باورها و آداب و رسوم مذهبی، در خانواده‌های سنتی جایگاه ویژه‌ای دارد و ارتباط مستقیمی میان دین و سلامت اخلاقی و رفتاری افراد خانواده وجود دارد. از این رو، در خانواده‌های سنتی ناهنجاری‌های کنتری دیده می‌شود. معمولاً سرلوحه همه رفتارهای خانواده سنتی، محبت و فداکاری و از ویژگی‌های آشکار این خانواده‌ها، رسیدن اعضای آن به احساس آرامش و سلامت روانی است. در مقابل، تاثیری که تمدن، تکنولوژی، ماهواره و اینترنت بر خانواده‌های به اصطلاح مدرن امروزی گذاشته، آن‌ها را به نوعی کاستی و سردی در روابط و مناسبات روبه رو کرده است. در نتیجه، دوام و پایداری آن‌ها دست خوش تهدیدهای جدی قرار گرفته است.

آسیب‌های خانواده، به دو دسته بیرونی و درونی تقسیم می‌شوند. نادیده گرفتن مسائل اخلاقی و حقوقی و رعایت نکردن امور مربوط به روابط انسان‌ها، از آسیب‌های درونی هستند که متوجه اعضای خانواده می‌شود.

عوامل آسیب‌زای بیرونی را نیز باید در خارج از محیط خانواده یافت. در عصر حاضر با ورود وسایل ارتباط جمعی مانند روزنامه، کتاب، رادیو، تلویزیون، ماهواره و شبکه‌های اینترنتی، نوع زندگی خانوادگی تغییر کرده و پی‌آمدهای گوناگون و دشواری را به همراه داشته است. مدرن و به روز بودن، اصل هویت خانواده را با درگیری‌های جدی روبه‌رو ساخته است و تکنولوژی‌ها و اختراعات مختلف که برای رفاه بخشیدن به زندگی جوامع امروزی پدید آمده‌اند، خانواده را دچار سردرگمی کرده و مصرف گرایی را ترویج کرده‌اند. فعالیت‌های بیش از حد والدین نیز آسیب‌های عاطفی بسیاری را متوجه فرزندان کرده و خانواده را در به انجام رساندن مسئولیت‌هایش با مشکل روبه رو ساخته است.

ناهماهنگی و نبود تعادل در خانواده، شادابی و پویایی را نیز از جامعه می‌گیرد و بی‌توجهی به بهداشت روانی خانواده، از مشکلات مهم زندگی‌های امروزی است. پژوهشگران، بالا رفتن آمار افسردگی در مردم را از پی‌آمدهای نوع زندگی قرن بیستم می‌دانند؛ که در آن، خانواده‌ها از هم گسسته‌اند و بیش‌تر مردم در کنار خانواده و با ترتیب درست و اصولی آنان رشد نمی‌کنند. در این شرایط، والدین وقت کافی برای همراهی موثر فرزندان خود ندارند و در نتیجه، استرس‌های گوناگون، افراد را در معرض افسردگی و بیماری‌های روانی قرار می‌دهد.

افزایش زمینه‌های تحریک جنسی نیز در پی گسترش و تنوع وسایل جدید تکنولوژی، خانواده‌ها را با گرفتاری‌های نگران کننده‌ای روبه‌رو کرده است. دنیای مدرن، عصر تنوع و هیجان و نوآوری است. تعدد مشاغل مردان و فشار بیش از حد ناشی از فعالیت زنان خانه و مشاغل رسمی آنان در جامعه، همراه با افزایش استرس‌ها و ضعف مهارت زوجین در برقراری ارتباط سالم جنسی نیز کارکرد تربیت جنسی خانواده را ضعیف می‌کند.

امروزه مسئولیت خانواده‌ها در تربیت فرزندان بیش از گذشته است و پرورش فرزندانی که ثبات شخصیت و هویت اجتماعی داشته باشند، دشوارتر شده است. فرزندان نیز با وظایف سنگین حاضر و

بحران‌های پیش آمده، بسیار ضعیف و شکننده عمل می‌کنند و فرزند سالاری، در بسیاری از خانواده‌ها، اقتدار و نظارت والدین را بر هم زده است. بر این اساس، هر کدام از کارکردهای خانواده، نقش مهمی در استحکام و تقویت بنیان خانواده ایفا می‌کند. با این حال، مسئله ناخوشایند این است که در بسیاری از خانواده‌های مدرن، وظایف خانواده، به درستی انجام نمی‌شود.

از آفت‌هایی که خانواده امروزی را تهدید می‌کند، بی اعتباری تدریجی هنجارها، اخلاق، باورهای دینی و ارزش‌های مذهبی و سنتی و در کنار آن، گسترش انواع انحراف‌ها و رفتارهای ناپسند در جامعه است.

کم توجهی به ارزش‌ها در جوامع مدرن که با کنار گذاشتن خدا، دین و اخلاق همراه است، به انسان امروزی، جرات دست زدن به هر کاری را می‌دهد. اخلاق مدرن، ریشه خود را در عقل گرایی جست‌وجو می‌کند و به همین سبب، با اخلاق سنتی و دینی فاصله گرفته است. آسیب‌پذیری خانواده امروزی، ناشی از نادیده گرفتن بایدها و نبایدهای دینی و اخلاقی است. بشر امروزی، هنوز به این نتیجه نرسیده است که زندگی بدون ایمان و معنویت، رنج و عذاب روانی و همیشگی را همراه او خواهد کرد.

از بین رفتن حریم‌های خصوصی

در دنیای سنتی، ارتباطات هم سنتی بود، که شامل ارتباطات انسانی، شفاهی، چهره به چهره و بی واسطه فردی و گروهی بود که به رغم ظاهر ساده و ابتدایی می‌تواند کارکردی پیچیده و متنوعی داشته باشد. این نوع ارتباطات گرچه به دلیل گسترده و پیچیده شدن جوامع انسانی کارکرد گذشته خود را از دست داد. اما هنوز هم از نفوذ و اعتبار خاصی برخوردارند زیرا بر طبیعت انسانی و نیازهای عاطفی او نزدیک‌ترند. در فرهنگ اسلامی ایرانی ما در دنیای سنتی مراسماتی چون نقالی، شاهنامه خوانی، حضور در میادین روستا و شهرها و ... حاکم بوده است که کارکردهای مثبت فراوانی داشته که در گستره زمان جای خود را به رادیو، تلویزیون و امروز به اینترنت و ماهواره داده است و دیگر از آن کارهای مثبت و سازنده خبری نیست و بر عکس آثار زیان بار و مخربی همچون نفوذ به حریم خصوصی افراد سوغات فن‌آوری جدید بشر یعنی اینترنت می‌باشد.

اینترنت به عرصه تبدیل و انتقال آزاد و افکار گردیده و حد کنار سرعت دادن به ارتباطات بشری خود معضلی جدی گردید.

اینترنت به عرصه فعالیت متصدیان جمع آوری اطلاعات در سراسر جهان تبدیل شده است. عملیات نفوذ به سیستم با نرخی هشدار دهنده افزایش یافته است، زیرا اینترنت به محلی کاملاً راحت و جالب برای هکرها تبدیل شده است. اینترنت را با رعایت مسایل حفاظتی طراحی نکرده‌اند. اینترنت شبکه‌ای عظیم و ظریف بوده و حاوی بسیاری کاستی‌های نرم‌افزاری است. به راحتی می‌توان در شبکه بدون ذکر نام خویش فعالیت کرد. چون همه چیز به هم مرتبط است، هر چیزی قابل نفوذ بوده و متجاوزی حرفه‌ای می‌تواند با ایجاد ردپایی در میان ده‌ها سیستم در چندین کشور مختلف ردپای خود را گم کند. بسیاری از ابزار مورد استفاده هکرها که در سال‌های قبل نیاز به دانشی عمیق داشت، اکنون خودکار شده و به راحتی قابل استفاده می‌باشد.

شکسته شدن حریم خصوصی افراد از هر قشر و رده‌ای، باعث ناامنی روانی و اجتماعی می‌شود و می‌تواند پیامدهای جبران ناپذیری به همراه داشته باشد.

هم‌زمان افراد تلاش وافری در حفظ اطلاعات شخصی خود به هر شکل ممکن می‌کنند و این تلاش همیشگی دو طرفه برای کشف و حفظ اسرار شخصی افراد موجب ایجاد چالشی جدی در جوامع بشری است.

در این میان میثاق‌ها، بیانیه‌ها و قطعنامه‌های متعددی که منتشر می‌شود دست و پا زدن‌های انسان عصر مدرن را می‌ماند که سعی می‌کند خفگی‌اش را اندکی به تاخیر بیندازد.

فضای دیجیتال

بر اساس تحقیقات انجام شده ۵۱٪ از نفوذ و تخریب سیستم‌های دیجیتال توسط ویروس‌ها و۲۷ ٪ توسط کارکنان ناراضی،۵٪ خراب‌کاری از بیرون،۷٪توسط جاسوسان صنعتی انجام می‌شود.

الف : ویروس‌ها و سایر امراض نرم‌افزاری

ویروس قطعه‌ای کوچک از کد رایانه‌ای است که درون برنامه رایانه‌ای دیگری پنهان می‌شود. مثل ویروس واقعی،ویروس رایانه‌ای می‌تواند خود را تکثیر کرده و سایر رایانه‌ها را بیمار کند و سپس بدون

حرکت طی ماه‌ها یا سال‌ها باقی مانده و دوباره حمله کند. ویرس تنها یکی از چندین نوع رشته منطقی است که می‌تواند رایانه‌یا کل شبکه را صدمه بزند.

کرم‌ها، بمب‌های منطقی،و اسب‌های تروا امراضی مشابه هستند که معمولاً با ویروس‌های رایانه‌ای گروه بندی می‌شوند. کرم رایانه‌ای مثل ویروس پراکنده می‌شود اما به جای آن که درون برنامه دیگری پنهان شود،خود برنامه‌ای مستقل است. بمب منطقی برنامه‌ای است که معمولاً در اعماق رایانه اصلی پنهان شده و منتظر می‌ماند تا در مرحله‌ای خاص در آینده فعال شده و داده‌ها را خراب کند. اسب‌تروا را در قالب برنامه‌ای نرم‌افزاری و مشروع پنهان می‌سازد و منتظر می‌ماند تا آن که نوعی رویداد از قبل تعیین شده یا تاریخی مقرر سر برسد و آن گه بار خود را تحویل می‌دهد و بدین‌ترتیب فایل‌ها یا دیسک‌ها را منهدم می‌کند.

ب : هکرها

نکته: وقتی به اینترنت وصل می‌شوید، به رایانه‌های سراسر جهان متصل می‌شوید و مهم‌تر این که آنان نیز به رایانه شما وصل می‌شوند. کاربر رایانه از ارتباط دیگران خبری ندارد،اما هر ارتباطی با سایت روی اینترنت،در واقع مثل خیابانی دو طرفه می‌ماند !

هکرهای متخصص، ابزار نرم‌افزاری پیچیده‌ای را ایجاد کرده و برای دیگران می‌فرستند،تا آنان بتوانند از نقاط ضعف انسانی و فنی موجود در حفاظت از سیستم‌های رایانه‌ای دیگران استفاده کنند. این ابزار مشتمل است بر استفاده از ابزار کشف کلمات عبور،شماره گیرهای جنگی،اسکنرهای نقاط آسیب پذیر، بویشگرها، ربایندگان ای . پی. از این قبیل،چون بسیاری از این ابزار روی اینترنت موجود است،تازه واردها چه بسا از آن‌ها استفاده کرده و اقدام به دانلود آن‌ها نمایند، و سطح پیچیدگی همه انواع هکرها را افزایش دهند.

اکنون با توسعه شبکه‌های بی‌سیم،هکرها فرصت‌های تازه‌ای برای کسب دست‌رسی به رایانه شما یافته و از طریق شما به کل کشور اداره دست‌رسی می‌یابند.

نکته: هدف نخست هکر عبارت است از نیل دست‌رسی به تمامی شبکه شما به منظور خواندن فایل‌ها. در اغلب موارد،کلمات عبور بی اثر،مودم‌های نا امن، و به گفته هکرها، مهندسی اجتماعی، نخستین روزنه را به سوی سیستم می‌گشایند.

ج- مهندسی اجتماعی

مهندسی اجتماعی در اصطلاح هکرها عبارت است: از فریب کاربران مشروع رایانه برای تامین اطلاعات مفید برای هکرها به منظور دست‌رسی غیر مجاز به سیستم‌های رایانه‌ای.

هکری که از مهندسی اجتماعی استفاده می‌کند،اغلب خود را شخصی مشروع در یک سازمان معرفی کرده و از داستان ساختگی قابل باوری استفاده می‌کند تا کاربر رایانه را با نیرنگ مجبور به ارایه اطلاعات مفید کند. این امر معمولاً با تلفن انجام می‌شود،اما شاید با پیام‌های جعلی ایمیل یا ملاقات رو در رو نیز صورت پذیرد.

نکته: اکثر افراد تصورات نادرستی از سرقت‌های رایانه‌ای دارند و فکر می‌کنند این سرقت‌ها کاملا فنی بوده و در نتیجه نقص‌های فنی سیستم‌های رایانه‌ای متجاوزان امکان توفیق در کار خود را می‌یابند. حقیقت این است که به هر حال،مهندسی اجتماعی معمولاً نقش بزرگی را در کمک به هکرها برای رد شدن از موانع امنیتی بر عهده دارد. چنان چه هکر هیچ گونه مجوز دست‌رسی به سیستمی را نداشته باشد،فقدان آگاهی امنیتی و زودباروی کاربران رایانه معمولاً موجب رخنه آسان وی به درون سیستم حفاظت شده می‌شود.

د : تهدید نیروهای داخلی (کارمندان ناراضی)

عموما معتقد هستند حفاظت از رایانه‌یعنی مقابه با تهدید گروه کثیری از هکرهای بداندیش که در حال حاضر وجود دارند و بر همین اساس تمرکز بسیاری از اقدامات حفاظت رایانه به روی دور نگه داشتن افراد بیرونی از دسترسی به رایانه‌ها می‌باشد و این کار را از طریق اقدامات فیزیکی و فنی مثل دروازه‌های ورود، نگهبانان، قفل‌ها، دیوارهای آتش، کلمات عبور، و غیره انجام می‌دهند. با همه این‌ها اگر چه تهدید از ناحیه افراد بیرونی در واقع در همان حد تصور موجود، گسترده است، اما نیروهای داخلی

بد طینت نیز با دست‌رسی مجاز به سیستم نیز تهدید حتی بزرگ‌تر از تهدید نیروهای بیرونی محسوب می‌شوند!

تحقیقات پیاپی حکایت از آن دارد که اغلب خسارات را نیروهای داخلی یعنی افراد دارای دست‌رسی به شبکه رایانه‌ای وارد کرده‌اند. بسیاری از نیروهای داخلی از دست‌رسی و دانش لازم برای نفوذ و ایجاد اختلال در سیستم‌ها و شبکه‌های رایانه‌ای برخورد هستند.

افزون بر رخنه نیروهای اطلاعات خارجی حریف به سیستم، شبکه رایانه‌ای که در اختیار دارید در معرض خطراتی از جانب انواع نیروهای بیرونی نیز قرار دارد.

ه : نیروهای بیرونی

از نمونه نیروهای بیرونی به موارد زیر می‌توان اشاره کرد :

دلالان آزاد اطلاعات.

رقبای خارجی یا داخلی.

سرویس‌های نظامی کشورهای متخاصم که سرگرم توسعه قابلیت خود برای استفاده از اینترنت به عنوان سلاح نظامی هستند.

سازمان‌های تروریستی که برای آن‌ها هک کردن سازمان یافته، عاملی بالقوه و کم هزینه، کم خطر و در عین حال همراه با منافع بالا به حساب می‌آید.

سندیکاهای جرم و جنایت و کارتل‌های مواد مخدر.

هکرهای ماجراجو که برای سرگرمی یا انجام خراب کاری‌های تفریحی وارد سیستم شما می‌شوند.

سارقان عادی که متخصص در سرقت و فروش مجدد رایانه‌ها و لپ‌تاپ هستند.

۱-۱۳-۱- ایجاد شکست در فرآیند مدیریت

با توجه به این که مدیریت در هر سیستمی‌اصلی‌ترین عامل به کارگیری منابع و سازمانی بوده و راهبرد اصلی سازمان توسط مدیران طراحی و اجرا می‌گردد. بسیاری از صاحب نظران مدیریت را علم همراه با هنر مدیر تعریف کرده‌اند. مدیریت اقدامی‌نیست که در یک مرحله شروع و در همان مرحله نیز به اتمام برسد، بلکه مدیریت فرآیندی است که ازیک مدیر در سازمان شروع شده و به آخرین لایه‌های ساختاری رسوخ پیدا می‌نماید. به همین دلیل هرگونه تاثیری در مدیریت می‌تواند در کلیه امور یک سازمان و یا یک کشور اثر گذار باشد و به همین دلیل سلطه‌گران به این نتیجه رسیده‌اند که با اثر گذاری در فرآیند مدیریت می‌توانند در دیگر لایه‌های سازمانی نیز اثر گذار باشند. هر گونه شکستی در این لایه برابر است با شکست در اهداف سازمان.

۱-۱۳-۲- هدایت مدیریت به سمت مسیر خود خواسته

سلطه‌گران در رابطه با اعمال نقطه نظرات خود به‌صورت پنهان و آشکار سرمایه گذاری‌های فراوانی انجام می‌دهند. اینان به دنبال آن هستند تا با کم‌ترین سرمایه گذاری مادی و معنوی به بیش‌ترین اثرات نائل شوند. هم‌چنین با اجرای عملیات خود ، کم‌ترین آثار و تبعات ملی و بین‌المللی را به همراه داشته باشند. سلطه جویان می‌خواهند در مقابل واژه‌های خودساخته‌ای مانند حقوق بشر که امروزه تبدیل به ابزار سلطه‌گری شده است کم‌تر پاسخ‌گو بوده و به همین دلیل تلاش دارند تا فرآیند مدیریت را به سمت استفاده از ابزار مدیریت قابل هدایت از راه دور به صورت پنهان و آشکار سوق دهند تا در زمان مورد نیاز ابتکار عمل را خود به دست گرفته و در شرائط خاص بهره‌برداری خاص خود را ببرند.

۱-۱۳-۳- سرقت اطلاعات

سرقت اطلاعات در دنیای آنالوگ کاملاً آشکار بود و پس از سرقت می‌توان سریعاً متوجه این مطلب شد که کالایی به سرقت رفته است اما سرقت اطلاعات در دنیای دیجیتال به‌صورت کاملاً پنهان انجام می‌گیرد سرقت کننده به دنبال این می‌باشد که به صورت پنهانی این سرقت را انجام دهد تا مسیر برای سرقت‌های بعدی بسته نشود چنان‌چه سرقت اطلاعات در ابزار دیجیتالی صورت بگیرد ممکن است تا زمان زیادی مالکت اطلاعات متوجه این کار نشود.

۱-۱۳-۴- حملات ویروس

ویروس‌ها برنامه‌های اجرایی کوچکی می‌باشند که به مجرد اجرا شدن بر روی رایانه قربانی می‌تواند تغییرات مورد نظر را به صورت پنهان و یا آشکار بر روی رایانه ایجاد نماید.

۱-۱۳-۵- آسیب‌های اتفاقی

منظور از آسیب‌های اتفاقی آسیب‌هایی است که بدون داشتن هیچ هدفی و با استفاده کردن از ابزار به وقوع می‌پیوندد این گونه آسیب‌ها دارای هدف اولیه نبوده و با در کنار هم قرار گرفتن سخت‌افزارها و نرم‌افزارها به وجود می‌آید.

۱-۱۳-۶- خراب‌کاری و دست‌کاری

هرگاه داده‌های در حال جریان بین مبدأ و مقصد توسط شخص غیر مجاز به هر نحو دست‌کاری یا تحریف شود، حمله‌ی «دست‌کاری داده‌هاً رخ داده است.

۱-۱۳-۷- شکستگی اطلاعات

در بانک‌های اطلاعاتی از کنار هم قرار گرفتن فیلدهای اطلاعاتی رکوردها تشکیل می‌شود این فیلدها با نظم خاصی در کنار هم قرار دارند به طور مثال در کنار هر نام یک فیلد نام خانوادگی وجود دارد و هر حال نام به نام خانوادگی مربوطه متصل می‌شود. در صورت ایجاد شکستگی در اطلاعات عملاً کل اطلاعات به هم ریخته و مخدوش خواهند شد این کار ممکن است با ارتقا یا تنزل یک فیلد ایجاد شود.

۱-۱۳-۸- خطای در سیستم‌های ارتباطی

با توجه به این که سیستم‌های یک شبکه از طریق سیستم‌های ارتباطی با هم متصل می‌باشند هر گونه خطایی در سیستم‌های ارتباطی قادر خواهد بود در شبکه اثرگذار باشد. این اثرگذاری ممکن است عمدی و یا غیرعمدی صورت بگیرد.

۱-۱۳-۹- استراق سمع

هرگاه یک شخص غیر مجاز به هر نحو بتواند نسخه‌ای از داده‌های در حال جریان بین مبدأ و مقصد را به نفع خود شنود کند، حمله‌ی «استراق سمع» به وقوع پیوسته است.

۱-۱۳-۱۰- افزایش اطلاعات ناخواسته

هرگونه افزایش و کاهش اطلاعات به صورت ناخواسته می‌تواند اطلاعات هستی را مخدوش نماید. به‌طور مثال افزایش ۱۰ و یا کاهش آن در ۱ حساب بانکی می‌تواند آن را به ۱۰٪ کاهش و یا ۱۰ برابر افزایش دهد.

۱-۱۳-۱۱- اقدامات مداخله گرایانه

هرگونه اقدامی‌که نتیجه آن به هم ریختن منطق موجود سیستم باشد اقدامات مداخله گرایانه نام دارد. اقدامات با هدف اولیه مخدوش سازی سیستم و در نتیجه به دست گرفتن مدیریت سیستم و یا به هم ریختن اطلاعات صورت می‌پذیرد

۱-۱۳-۱۲- آسیب‌های سیستم عامل

نرم‌افزارها انواع و اقسام مختلفی دارند یکی از بارزترین نرم‌افزارها سیستم عامل می‌باشد. وظیفه سیستم عامل مدیریت بر سخت‌افزار و نرم‌افزار رایانه می‌باشد. با توجه به نقش مهم این نرم‌افزار در مدیریت رایانه آسیب‌های آن نیز شکل ویژه‌ای به خود می‌گیرد به همین دلیل نفوذگران تلاش می‌کنند تا از آسیب‌پذیری‌های سیستم عامل برای مدیریت بر سیستم استفاده نمایند.

۱-۱۳-۱۳- آسیب‌های سخت‌افزاری

تمام سخت‌افزارها می‌توانند دارای نقاط آسیب‌پذیر از قبل تعریف شده و یا پس از استفاده باشند این گونه نقاط آسیب‌پذیر در صورت شناسایی می‌تواند باعث دسترسی اطلاعات از راه دور باشد. هرگونه آسیب سخت‌افزاری عملاً باعث آسیب رسانی به اطلاعات خواهد شد.

۱-۱۳-۱۴- آسیب‌های نرم‌افزاری

با توجه به این که نرم‌افزارها از کدهای به هم پیوسته تشکیل شده است عملاً می‌توان با نوشتن کدهای خاص، نرم‌افزار را به سمت خاصی هدایت نمود. چنان‌چه نویسنده نرم‌افزار در نرم‌افزار خود از کدهای پنهان استفاده نماید می‌تواند باعث آسیب‌های نرم‌افزاری گردد و آسیب‌های نرم‌افزاری به صورت عمدی و یا غیرعمدی در نرم‌افزارها قرار داده شود.

۱-۱۳-۱۵- آسیب به اطلاعات خصوصی

هر کاربر زمانی که با رایانه کار می‌کند هم‌زمان تولید اطلاعات خصوصی می‌نماید. به‌طور مثال درصورتی که در نظر داشته باشد بر روی اینترنت از آدرس ایمیل استفاده نماید باید از قبل با ارائه اطلاعات خصوصی آن را ایجاد نماید و یا چنان‌چه در نظر داشته باشد برای استعلام قبولی و یا عدم قبولی در کنکور استعلامی‌انجام دهد باید اطلاعات خصوصی را در رایانه وارد نماید و یا اگر در نظر داشته باشد اطلاعات بانکی خود را کنترل نمایند باید اطلاعات خصوصی را در رایانه وارد نماید تجمیع این اطلاعات در رایانه می‌تواند باعث آسیب رسانی به اطلاعات خصوصی گردد.

۱-۱۳-۱۶- کلاهبرداری در اطلاعات

سوءاستفاده کنندگان از اطلاعات به دنبال دسترسی به اطلاعات می‌باشند تا بتوانند بر اساس آن از افراد کلاهبرداری نمایند یکی از خطراتی که رایانه و اطلاعات آن را تهدید می‌کند دسترسی افراد کلاهبردار به اطلاعات و سواستفاده از آن می‌باشد.

۱-۱۴- امنیت چالش اصلی جهان نوین

با توجه به این که در کلیه کشورهای جهان مسائل زیر به عنوان یکی از اولین اولویت‌های استفاده از ابزار نوین می‌باشد، مسئله امنیت آن نیز اولویت اول را در بر می‌گیرد. تمام کشورهای دنیا به خاطر حفظ امنیت ملی خود تلاش بر این دارند تا امنیت ابزار نوین دیجیتال خود را حفظ نمایند و این مسئله به چالشی جانی تبدیل شده است.

در تمام دنیا:

افزایش اطلاعات

تبدیل اطلاعات آنالوگ به دیجیتال

استفاده از اطلاعات در مبدأ تولید

افزایش توان بهره‌برداری از اطلاعات

سرعت بخشی به تبدیل اطلاعات به تصمیم

جزو دغدغه‌های اصلی تمام کشورها می‌باشد.

۱-۱۵- سئوالات خودآزمایی

ضمن تعریف اطلاعات، نقش اسناد در امنیت اطلاعات را بیان نمایید.

پدافند غیر عامل را تعریف کرده و اختلاف آن را با پدافند عامل بیان نمایید.

اختلاف بین تهدیدات و فرصت‌ها در دنیای سنتی و نوین را بیان نمایید.

انواع تهدیدات را نوشته و تهدیدات انسان ساخت را توضیح دهید.

انواع اطلاعات دیجیتال را نام برده و توضیح دهید.

پنج نوع از آسیب‌های دنیای دیجیتال را نام برده و توضیح دهید.

اصل کلی و اصول فرعی امنیت دیجیتال را نام برده و توضیح دهید.

فصل دوم - آشنایی با پدافند غیر عامل فاوا

آن چه در این فصل خواهید آموخت:

تعریف فاوا

تعریف پدافند غیر عامل

تعریف پدافند غیر عامل فاوا

سابقه پدافند غیر عامل فاوا

مفاهیم امنیت در فاوا

۲- آشنایی با پدافند غیر عامل فاوا

پدافند غیر عامل از ابتدا تاکنون در حوزه‌های تخصصی مختلفی نمود داشته و عرصه اقدامات پیش‌گیرانه را به روی کاربران گشوده است. یکی از عرصه‌های آسیب‌پذیر دنیای ارتباطات و فن‌آوری اطلاعات می‌باشد که در این فصل اختصاصاً به آشنایی با پدافند غیر عامل در حوزه فاوا۱ خواهیم پرداخت.

۲-۱- تعریف فاوا

هر چند به نظر می‌رسد مفهوم فن‌آوری اطلاعات، و فن‌آوری اطلاعات و ارتباطات (فاوا) روشن باشد اما در واقع چنین نیست. تعاریف مختلفی از فن‌آوری اطلاعات توسط افراد مختلف ارائه شده است. از جمله می‌توان به تعاریف زیر اشاره نمود:

مطالعه،طراحی، توسعه و مدیریت کلیه نرم‌افزارها و سخت‌افزارهایی که در یک شبکه و یک محیط ارتباطی با هم کار می‌کنند.

منظور از فن‌آوری اطلاعات همه شکل‌های فن‌آوری است که به وسیله آن‌ها عملیات دست‌یابی، ذخیره سازی و مبادله اطلاعات به شکل‌های گوناگون مثل متن، تصویر، صدا و نمایش چند رسانه‌ای انجام می‌شود.

فن‌آوری اطلاعات دانشی است که به بررسی ویژگی‌ها و چگونگی اطلاعات نیروهای حاکم بر جریان اطلاعات و ابزار آماده سازی آن‌ها برای به حداکثر رساندن دست‌یابی به اطلاعات و قابل استفاده کردن

۱فن‌آوری اطلاعات و ارتباطات

آن می‌پردازد. آماده سازی اطلاعات شامل تفکیک اطلاعات دقیق، علمی و مستند، جمع آوری، سازمان دهی، ذخیره، بازیابی، تفسیر، اشاعه و استفاده از آن می‌شود. (مؤسسه فن‌آوری جورجیا، ۱۹۶۲ – نقل از اترتون،۱۹۹۷).

اصطلاح فن‌آوری اطلاعات برای توصیف فن‌آوری‌هایی به کار می‌رود که ما را در ضبط، ذخیره سازی، پردازش، بازیابی، انتقال و دریافت اطلاعات یاری می‌کند. این اصطلاح، فن‌آوری‌هایی مانند رایانه، انتقال از طریق دورنگار، ارتباط از راه دور، تلفن، ماشین حساب، چاپ و حکاکی را نیز در بر می‌گیرد (کیت بهان و دیانا هولمز، ۱۹۹۸).

فن‌آوری اطلاعات به مجموعه به هم پیوسته‌ای از روش‌ها، سخت‌افزارها، نرم‌افزارها، و تجهیزات ارتباطی که اطلاعاتی را در اشکال گوناگون (صدا، تصویر و متن) جمع آوری، ذخیره سازی، بازیابی، پردازش، انتقال و یا عرضه می‌کند، اتلاق می‌شود (دبیرخانه شورای عالی انفورماتیک، ۱۳۷۸).

فن‌آوری اطلاعات متشکل از سخت‌افزار، نرم‌افزار، نیروی انسانی، اطلاعات، مدیریت، تولید و نگهداری است که در ارتباط متقابل با یک‌دیگرند و فضایی مملو از اطلاعات ذخیره شده به صورت نظام‌دار و با قابلیت دست‌رسی آسان پدید می‌آورند. این فضا در خدمت نیازهای اقتصادی، اجتماعی و فرهنگی جامعه قرار می‌گیرد و سبب بهره‌وری و افزایش کیفیت و محصولات سازمان‌های متبوع می‌شود (اسکاپ ESCAP).

فن‌آوری اطلاعات همانند محور و مرکز مجموعه‌ای از فعالیت‌های هدایت شده است که کنترل مدیریت، بهره‌وری، تولید، آموزش و ارتقای یک سیستم (اعم از سازمان یا پایگاه اطلاعاتی و. . .) را با یک مرکزیت بر عهده دارد. همه سازمان‌ها، ارگان‌ها، نهادها و وزارتخانه‌ها ناگزیر از برقراری ارتباط با یک‌دیگر و انتقال اطلاعات هستند. سازمان فن‌آوری اطلاعات مسؤول برقراری این ارتباطات در اشکال پیش‌رفته الکترونیکی است و به طور کلی مسؤلیت کلی تولید، حفظ، ذخیره، بازیابی و انتقال اطلاعات را در یک شبکه پیچیده را بر عهده دارد (محمدی، ۸۲).

فن‌آوری اطلاعات، نقطه هم‌گرایی الکترونیک، پردازش داده‌ها و ارتباطات دور که شامل تعدادی رایانه قوی، فن‌آوری‌های ارتباطی و هم‌چنین نرم‌افزار است، که نیاز به آن بر اثر سه عامل ایجاد می‌شود. اول آن که فن‌آوری اطلاعات خود صنعتی راهبردی (استراتژیک) و بسیار سودآور در جهان است. دوم آن که

فن‌آوری کلیدی است و در همه صنایع و خدمات کاربرد دارد. سوم آن که زیر بنای اساسی است که به همه مؤسسات و واحدهای اقتصادی امکان می‌دهد تا در استفاده از دانش بشری و انتقال آن سهیم شوند ؛ سبب کاهش هزینه‌ها می‌شود و در نتیجه به افزایش بهره‌وری و کیفیت محصول می‌انجامد (سازمان راهبردهای فن‌آوری اطلاعات آمریکاNSIT).

فن‌آوری اطلاعات تنها در ارتباط با رایانه‌ها، نرم‌افزار و یا خدمات وابسته به آن‌ها نیست. فن‌آوری اطلاعات ترکیبی از همه این موارد است با این نگرش که چگونه این فن‌آوری می‌تواند کمکی به سازمان و رسیدن به اهداف آن کند. . . . فن‌آوری اطلاعات باعث می‌شود انجام کارهای زیاد و طولانی با عملیات کمی انجام گیرد (Sutter ۲۰۰۳).

فن‌آوری اطلاعات نوعی از فن‌آوری است که در آن انتقال داده، اطلاعات و دانش انجام می‌گیرد. این مفهوم ضرورتاً وابسته به رایانه‌ها نیست، هر چند که امروزه رایانه‌ها به عنوان ابزاری در گسترش و ایجاد راه‌هایی بسیار قدرتمند در انجام امور هستند. نقشه‌کشی، هندسه تحلیلی، دستگاه‌های کپی، تلگراف، تلفن، فاکس و غیره به خوبی نمونه‌هایی از فن‌آوری اطلاعات هستند (Fischiner ۲۰۰۰).

برای بسیاری از مردم این واژه مترادف است با « فن‌آوری جدید» که از ماشین‌هایی که بر مبنای ریز پردازنده‌ها کار می‌کنند، استفاده می‌کند. به عبارت دیگر گفته می‌شود که « فن‌آوری اطلاعات » به طور ساده، بیانگر کوششی است برای ممکن نمودن توسعه و پیشرفت محرک‌های تجارتی به طور الکترونیکی و هم‌چنین ایجاد حرکتی سیاست گونه برای کنترل دسترسی به اطلاعات (Zorkoczy and Nicholas ۱۹۹۵).

در سال‌های اخیر، کتاب‌ها، مجلات، مقالات و کنفرانس‌ها، راه‌هایی را برای ارتباط پژوهشی و علمی ایجاد نموده‌اند. امروزه فن‌آوری به ویژه فن‌آوری اطلاعات، در حال تاثیر گذاری بر روی هر یک از این سیستم‌های ارتباطی است. نشر الکترونیکی، متن الکترونیکی، پیام مبتنی بر صدا و کنفرانس‌های تصویری، چند نمونه از اثر فن‌آوری اطلاعات هستند. فن‌آوری اطلاعات به ما راه‌های جدیدی برای ارتباط می‌دهد و اساساً این امکان را به وجود می‌آورد تا سیستم‌های ارتباطی موجود نیز مورد تصحیح و بهبود قرار گیرند. این کار آسان به نظر می‌رسد که تغییر و تحول از سیستم‌هایی که از تنظیمات دستی استفاده می‌کنند به سیستم‌های الکترونیکی انجام گیرد (Karamouzis ۱۹۹۹).

فن‌آوری اطلاعات ترکیبی از دو مفهوم فن‌آوری و اطلاعات است. اطلاعات مفهوم گسترده‌ای را در بر دارد و به یک سری محتویات اشاره می‌شود، در حالی که فن‌آوری به ابزارهایی که برای دست‌کاری این محتویات به کار می‌رود، گفته می‌شود. فن‌آوری یک عنصر ضروری درتراکنش‌های پردازش اطلاعات است که مشاهده، آگاهی و تجربه از یک رابطه سلسله مراتبی در آن برخوردار هستند. اطلاعات منجر به پیدایش آگاهی شده، و از به وجود آمدن آگاهی زیاد، تجربه حاصل می‌گردد. اطلاعات از داده‌هایی که ضرورتاً قابل احساس و ادراک هستند نشأت می‌گیرد. هنگامی که داده‌ها برای استفاده در برخی امور سودمند به دسته‌ها و طبقه‌هایی دسته بندی و سازمان دهی می‌شوند، تبدیل به اطلاعات می‌گردند (Chaurasia ۲۰۰۳).

فن‌آوری اطلاعات هر مجموعه‌ای از ابزارها، روش‌ها و رسانه‌ها است که برای ثبت، ذخیره، و انتقال اطلاعات به کار گرفته می‌شود. معمولاً امروزه هنگامی که این اصطلاح را به کار می‌بریم، در حقیقت در مورد زیر مجموعه خاصی از فن‌آوری اطلاعات صحبت می‌کنیم: فن‌آوری اطلاعات دیجیتالی شبکه‌ای (Willis ۲۰۰۲).

فن‌آوری اطلاعات عبارت است از سخت‌افزار، نرم‌افزار، ارتباط مخابراتی و سرویس‌ها و خدماتی از کارمندان فن‌آوری اطلاعات (Effy Oz ۲۰۰۲).

فن‌آوری اطلاعات، حوزه‌ای نسبتاً جوان در مقابله با اکثر نظام‌های علمی دیگر است. با این وجود، در حدود ۵۰ سال، این فن‌آوری به عنوان بخشی از علم و دانش در آمده که به خوبی قابل استدلال بوده و تقریباً پیچیده‌تر از نظام‌های علمی سنتی از قبیل ادبیات یا روانشناسی، و یا پیچیده‌تر از حوزه‌های حرفه‌ای از قبیل کسب و کار یا قانون است. در هر صورت، فن‌آوری اطلاعات، اساساً متفاوت از این نظام‌ها در برخی از نسبت‌های مهم بوده، و بنابراین سواد فن‌آوری اطلاعات، ضرورتا متفاوت از سواد در حوزه‌های دیگر است(Ralph ۱۹۹۷).

اما به نظر می‌رسد هیچ‌یک از تعاریف، نتواند ابعاد حقیقی مفهوم فاوا را به درستی تبیین نماید. این‌ها واژه یکسانی را برای مفاهیم مختلف به کار می‌برند. لازم به تذکر است که مفهومی که مستقل از یک واژه، با توجه به معنای لغات و صرف نظر از موارد کاربردی و استدلالات به کار برندگان آن، استنباط می‌شود، ممکن است با مفهومی که این واژه در تبیین آن مفهوم رواج دارد، متفاوت باشد. هدف ما در

این جا، شناسایی آن مفهوم است. به نظر می‌رسد سه دیدگاه مختلف، و سه دسته مختلف از تعاریف – مفاهیم برای فاوا وجود داشته باشد :

دسته اول: این دسته، مفهوم فن‌آوری اطلاعات (و ارتباطات) را به نوعی همان فن‌آوری رایانه و سیستم‌های رایانه‌ای اطلاعاتی و ارتباطی، در وجود نرم‌افزار و سخت‌افزار و شبکه و نظایر آن و مسائل مدیریتی مربوط به آن می‌دانند. اغلب تعاریف از این دسته‌اند

دسته دوم: این دسته فن‌آوری اطلاعات را از بُعد اطلاعات محض آن که حتی شامل مواردی نظیر مستند سازی و کتاب‌داری نیز می‌شود، مورد توجه قرار می‌دهند. در این دسته تمرکز بر خود اطلاعات است و فن‌آوری اطلاعات، هرگونه استفاده از ابزارها و روش‌ها و تکنیک‌هایی است که مدیریت و سازماندهی این اطلاعات را فراهم می‌کند. تعریف‌های اولیه و با سابقه بیش‌تر از این دسته‌اند. البته این مفهوم شاید نزدیک‌ترین مفهوم به معنای مستقیم واژه فاوا باشد. از جمله تعریف مؤسسه فن‌آوری جورجیا از این دسته است.

دسته سوم: این دسته، برای فاوا نقشی کلیدی و محوری نسبت به سایر فن‌آوری‌ها و کاربردها قائل می‌شود. این دسته با زاویه‌ای فراتر از زاویه‌های دو دسته قبلی به فاوا نگاه می‌کند. اما مشکل این دسته آن است که به درستی نمی‌تواند ابعادی را که برای فاوا از این زاویه مشاهده می‌کند، توضیح دهد و در یک عبارت و تعریف مشخص، بیان کند. از جمله تعریف سازمان راهبردهای فن‌آوری آمریکا (NSIT) و تعریف آخر از این دسته‌اند.erfan۲۰۰۰persiangig.ir

۲-۲- تعریف پدافند غیر عامل

علاقه به حیات و حفظ بقاء به صورت غریزی در هر انسانی وجود دارد. لذا در طول تاریخ، بشر برای دست‌یابی به ملزومات حیاتی خود از جمله غذا و انرژی به گسترش و توسعه مراتع و زمین‌های کشاورزی و معادن پرداخته یا به جهت دفع تجاوز دشمنان خود جنگ‌ها و منازعات بسیاری را پشت سر نهاده است. سلاح‌هایی که جوامع بشری قبل از دوران صنعتی در جنگ‌ها به کار می‌بردند دست ساز و بسیار ساده بود. بین روند رشد دانش و فن‌آوری با نوع سلاح‌هایی که جوامع بشری برای بهره گیری از آن‌ها در جنگ ابداع و اختراع می‌کرده‌اند، ارتباط نزدیکی وجود داشته است.

در دوران معاصر، این پیوستگی در اثر تحولات و پیشرفت‌های عظیم در فن‌آوری رو به فزونی نهاده است. پس از وقوع انقلاب صنعتی که توسعه‌ی همه‌جانبه‌ای را در همه‌ی سطوح فن‌آوری پدید آورد، تحولات گسترده‌ای در نوع و کیفیت استفاده از تجهیزات تسلیحاتی نیز ایجاد شد.

اساساً جنگ‌ها و منازعات در طول تاریخ به دلیل تعارض منافع و تمایل ذاتی انسان‌ها به برتری جویی روی داده است. در درگیری‌ها، طرفین درگیری تمایل دارند خواسته‌های خود را در حوزه‌های مختلف بر گروه مقابل تحمیل کنند و این کار در صورت عدم موفقیت در عرصه‌ی دیپلماسی منجر به جنگ می گردد.

ماهیت جنگ‌ها و تخاصمات بشری در دوره‌های مختلف تاریخ دستخوش تغییرهای زیادی گردیده است. در عصر حاضر پس از پشت سر گذاشتن سه نسل از جنگ‌ها، در چهارمین دوره از منازعاتی قرار داریم که از ابتدای تاریخ بین افراد و جوامع مختلف در گرفته است. در ادامه به بررسی نسل‌های مختلف جنگ می‌پردازیم.

نسل اول جنگ

از زمان پیدایش پدیده جنگ بین گروه‌های جمعیتی (قبایل و. . .) و با تشکیل حکومت‌ها توسط انسان بین ملت‌ها یا کشورها تا ورود سلاح‌های آتشین به میدان جنگ در این نسل از جنگ‌ها قرار می‌گیرند که عموماً متکی به تعداد نفرات و زور و بازو یا توان برخی افراد و مهارت آن‌ها در بکارگیری سلاح‌های سرد بوده است. گرچه نبوغ فرماندهان و طراحان جنگ همیشه نقش اساسی داشته است.

نسل دوم جنگ

با ورود سلاح‌های آتشین به عرصه جنگ‌ها، بسیاری از اصول و مبانی طرح ریزی و فرماندهی جنگ تغییر کرد. اهمیت زور و نیروی بدنی و تعداد نفرات تا حدودی کاسته شد. میدان درگیری و مانورها و حرکات تغییر کرد، برج و باروها و. . . آسیب پذیر شدند و بدین‌ترتیب انسان نسل دوم جنگ‌ها را تجربه کرد.

نسل سوم جنگ

انقلاب صنعتی موجب تحول و شکوفایی بشر در عرصه اختراعات و تولید فن‌آوری‌ها و ماشین‌های مختلف گردید. ورود فن‌آوری‌ها و ماشین‌ها (خودروها، تانک، نفربر، هواپیما، زیردریایی و تجهیزات پیش‌رفته) به عرصه جنگ‌ها، یک‌بار دیگر حوزه‌های طرح ریزی و فرماندهی جنگ را بشدت تحت تأثیر قرار داده و متحول ساخت. تعاریف و مفاهیم (قوی و ضعیف و. . .) تغییر کرد. عرصه‌های درگیری و نبرد به طرز حیرت آوری توسعه یافت و بشر یک دوره نسبتاً طولانی و بسیار خسارت‌بار با تلفات انسانی غیرقابل تصور از جمله دو جنگ جهانی و صدها جنگ منطقه‌ای و محدود را از این نسل جنگ‌ها تجربه کرده و در حال تجربه کردن می‌باشد.

نسل چهارم جنگ

تدوام رشد علوم و فن‌آوری‌ها موجب شد که قدرت‌های سلطه‌گر تحمیل منافع و نظرات خود بر رقبا و کشورهای ضعیف را بدون جنگ فیزیکی و نظامی و با بکارگیری ابزارهای قدرت اقتصادی، سیاسی، تبلیغاتی، فرهنگی و. . . طرح ریزی و تعقیب نمایند و ضربه و جنگ نظامی را به عنوان آخرین حربه در اولویت آخر قرار دهند تا ضمن ارائه ریاکارانه چهره‌ی مسالمت‌جو، خود را از عوارض (هزینه‌ها، تلفات و. . .) جنگ نظامی دور نگه دارند و بدین‌ترتیب بشر سال‌های نخست نسل جدید جنگ یعنی جنگ‌های نسل چهارم را آغاز کرده است.

این تغییرات که از آن به نسل چهارم جنگ‌ها تعبیر می‌شود، منجر به بروز جنگ‌های اقتصادی و اجتماعی گردیده است. در این نسل نوپا از درگیری‌ها، دشمنان با استفاده از حربه‌های اقتصادی، فرهنگی و اجتماعی و با به کارگیری همه‌ی مؤلفه‌های قدرت به زورآزمایی می‌پردازند. منازعات نسل چهارم در قدیمی‌ترین شیوه‌ی خود در تحریم‌های اقتصادی نمود یافت. اما استفاده از ابزارهای نوین اطلاع‌رسانی، گسترش شبکه‌ی جهانی اینترنت و به وجود آمدن شبکه‌های اجتماعی در بستر آن و نیز خدمات پردازش سیار به گسترش این دسته از منازعات در عرصه‌ی اجتماعی کمک شایانی نموده است. در واقع مهاجمان در این نوع درگیری‌ها با اجرای انواع توطئه‌های اقتصادی و سیاسی و نیز با گسترش فضای نارضایتی اجتماعی از طریق شبکه‌های ارتباطی و اطلاع‌رسانی، حریف خود را درگیر مشکلات داخلی و بین‌المللی نموده و از این طریق وی را به پذیرش اغراض سیاسی خود در میدان زورآزمایی‌های داخلی یا فرامنطقه‌ای مجبور می‌سازند.

در قبال این نوع منازعه تجهیز به ابزارهای دفاعی یا پدافندی تنها منحصر به نظامیان و لشکریان نیست. بلکه لازم است کلیه‌ی افراد، سازمان‌ها و مجموعه‌ها را با فرآیندها و روش‌هایی غیرنظامی برای مقابله آماده ساخت.

پدافند غیرعامل به مجموعه اقداماتی اطلاق می‌گردد که مستلزم به کارگیری جنگ افزار نبوده و با اجرای آن می‌توان از وارد شدن خسارت به تجهیزات و تاسیسات حیاتی و حساس نظامی و غیرنظامی و تلفات انسانی جلوگیری نموده و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد.

در ادبیات موضوع، علاوه بر پدافند غیرعامل، به مفهومی به نام دفاع غیرنظامی برمی‌خوریم که عبارت است از تقلیل خسارات مالی و صدمات جانی وارده بر غیرنظامیان در جنگ یا در اثر حوادث طبیعی نظیر سیل، زلزله، طوفان، آتش‌فشان، آتش‌سوزی و خشک‌سالی.

در منابع تخصصی سایر کشورها، وظایف دفاع غیرمسلحانه شامل چهار عنوان می‌باشد:

اقدامات پیش‌گیرانه و کاهش دهنده۱

آماده سازی و امداد رسانی۲

هشدار و اخطار۳

باز سازی مجدد۴

اقدامات دفاع غیرعامل شامل اصول اساسی و ملاحظاتی است که در اغلب کشورهای جهان، با کمی اختلاف پذیرفته شده‌اند ولی شیوه به کارگیری آن‌ها ابتکاری، هنرمندانه و خردمندانه است. به همین دلیل وسعت این اقدامات به خلاقیت‌های فکری بشر و شرایط زمان و مکان بستگی دارد و بعضاً نمی‌توان حد و مرزی برای آن تعیین کرد.

در تعریف دیگری پدافند غیرعامل به کلیه‌ی اقدامات و تدابیری گفته می‌شود که بدون استفاده از سلاح موجب کاهش آسیب‌پذیری، تلفات و خسارات و افزایش پایداری شود.

---

۱ Mitigation

۲ Preparation

۳ Response

٤ Recovery

به طور خلاصه می‌توان گفت پدافند غیرعامل یعنی دفاع در مقابل تهدید، بدون استفاده از سلاح. به عبارتی دفاع غیرعامل، مکمل دفاع عامل است و در حوزه‌ی امنیت ملی مفهوم دفاع، تلفیقی از دفاع عامل و دفاع غیرعامل است.

اقدامات پدافند غیرعامل در سطوح مختلفی طراحی و اجرا می‌گردند. این سطوح شامل موارد زیر است:

سطح استراتژیک: اقداماتی است که در سیاست‌های کلی کشور و تأمین مبانی و پشتوانه‌های قانونی، حقوقی و سیاست‌های برنامه بلندمدت توسعه کشور تأثیرگذار است.

سطح عملیاتی: اقداماتی است که در برنامه‌های ۵ ساله‌ی توسعه‌ی سازمان‌ها تأثیرگذار است.

سطح تاکتیکی: اقداماتی است که در برنامه‌های سالانه‌ی سازمان مؤثر است.

سطح اقدامات ویژه: که شامل اقداماتی است که تأثیر آن در اولویت‌های خاص و نقاط مهم می‌باشد.

اگر بخواهیم به صورت فهرست‌وار به برخی از اقدامات پدافند غیرعامل در حوزه‌های غیر از فن‌آوری اطلاعات اشاره کنیم، موارد زیر قابل ذکر است :

مکان یابی مناسب

انتخاب مقیاس بهینه

پراکندگی در سایت

استفاده از عمق زمین

توزیع عمل‌کرد

فریب در نمای عمل‌کردها

داشتن طرح پوشش و فریب

مدیریت بحران ناشی از جنگ

موازی سازی اقدامات

کاهش وابستگی

پوشش اطلاعاتی

چند منظوره کردن عمل‌کردها

کاهش امکان تهدید

استفاده از فن‌آوری بومی

توسعه شبکه پایش و هشدار امنیتی

ایجاد اهداف مجازی وکاذب

ایمن سازی سیستم فرماندهی وکنترل

نامرئی سازی در برابر دشمن

تولید موانع دومنظوره و چند منظوره

از منظر امنیت ملی، پدافند غیرعامل بستر مناسبی برای توسعه‌ی پایدار اقتدار ملی کشور در حوزه‌ی دفاعی است. هم‌چنین پدافند غیرعامل با سیاست‌های تنش‌زدایی هم‌راستا است. چراکه کشورهایی که توسعه پدافند غیر عامل را به عنوان یک سیاست دفاعی مستمر در دستور کار خود قرار می‌دهند هیچگاه در مظان اتهام تهدید بر علیه کشورهای دیگر قرار نمی‌گیرند.

اقدامات پدافند غیرعامل به دلیل غیرنظامی بودن، پایدارترین و ارزان‌ترین روش دفاع و هم‌چنین مناسب ترین راهکار افزایش آستانه‌ی مقاومت می‌باشد. این دسته از اقدامات مناسب‌ترین شیوه‌ی کاهش مخاطرات و آسیب‌پذیری‌ها و از طرفی مهم‌ترین ابزار بازدارندگی هستند. به عبارت دیگر کشورهایی که پدافند غیر عامل را به عنوان یک راه کار اصلی بر می‌گزینند به شرایطی از نظر کاهش آسیب‌پذیری دست می‌یابند که مطامع کشورهای تهدید کننده بر علیه آن‌ها کاهش می‌یابد.

در جهان امروز کشورهایی که نقاط آسیب‌پذیری آن‌ها فراوان است و دشمن می‌تواند با ضربات سریع، حیاتی‌ترین منابع آنان را منهدم نماید، عوامل تهدید بیرونی را تحریک و دشمنان را تحریص می‌نمایند. از این رو برای دست‌یابی به یک توسعه‌ی پایدار با سطح قابل قبولی از امنیت، پدافند غیرعامل در سطح کشور باید به یک فرهنگ عمومی تبدیل شود. (پدافند غیرعامل کشور – پورابراهیمیو بنابی -۱۳۸۹)

اقدامات پدافند غیرعامل باید در سه حوزه امنیت، ایمنی و پایداری طرح‌ریزی و اجرا شود. مجموعه این اقدامات در کنار یک‌دیگر و به عنوان سه جزء اساسی و غیر قابل تفکیک می‌باشند. ترکیب این سه جزء در کنار یک‌دیگر می‌تواند در تأمین دفاع غیرعامل و کاهش آسیب‌پذیری زیرساخت‌های ملی و مراکز حیاتی، حساس و مهم کشور در مقابل تهدیدها از طریق فرهنگ‌سازی، سیاست‌گذاری، طرح‌ریزی و برنامه‌ریزی راهبردی و تدوین ضوابط و دستورالعمل‌های تخصصی با قابلیت هدایت بخش‌های کشوری و لشکری موفق باشد.

به بیان ساده‌تر می‌توان گفت ایجاد بازدارندگی دفاعی کشور از طریق اقدامات پدافند غیرعامل مستلزم :

حفظ اسرار و اطلاعات کشور و ممانعت از دست‌رسی دشمنان به اطلاعات ارزشمند ملی و بخشی کشور

ایمن‌سازی زیر ساخت‌های ملی و مراکز حیاتی، حساس و مهم.

پایدار سازی زیرساخت‌های ملی و مراکز حیاتی، حساس و مهم کشور

می‌باشد.

در نگرش سیستمی این عوامل سه جزء یک سیستم می‌باشند که در تعامل با یک‌دیگر مفهومی تحت عنوان توسعه‌ی دفاع غیرعامل و افزایش قدرت بازدارندگی را شکل می‌دهند.

۲-۲-۱- امنیت

امنیت اطلاعات از جنبه‌های مختلف حائز اهمیت می‌باشد که محرمانگی و در دسترس بودن و حفظ تمامیت از جمله آن‌ها می‌باشد. امروزه بدون بومی‌سازی نمی‌توان انتظار ایجاد امنیت مطلوب را داشت.

امنیت از جمله مواردی می‌باشد که معمولاً در تضاد با برون سپاری بوده و می‌بایست توسط نیازمند به امنیت و به صورت بومی‌تولید و ایجاد گردد.

۲-۲-۲- ایمنی

ایمنی به مفهوم امن بودن در مقابل تهدیدها و حملات سخت و نیمه سخت می‌باشد. هر سیستمی به منظور تداوم بقاء و توان ارائه تولیدات و خدمات باید ایمن باشد. به منظور تامین ایمنی باید در خصوص هر یک از مراکز حیاتی، حساس و مهم طرح‌های لازم تهیه گردد. برای این منظور باید نسبت به تعریف و درجه بندی میزان حفاظت برای هر طرح در برابر تهدید اقدام شود.

هر چند در هر برنامه‌ریزی، تحلیل هزینه- فایده باید مد نظر قرار گیرد، در مواردی که تأمین ایمنی مراکز حیاتی، حساس مورد نظر است این اقدامات باید با اولویت بالا تامین هزینه شود. چرا که باید در مقابل منافع ظاهری، منافع مؤثر در امنیت ملی در این حوزه نیز مورد توجه باشد.

برخی از اقداماتی که در این حوزه می‌توان انجام داد عبارتند از:

سطح بندی (تعیین میزان اهمیت تأسیسات، مرکز یا تشکیلات)

تعیین اهمیت واولویت طرح‌ها

تعیین سطح ایمنی مورد نیاز

مکان یابی

طراحی

تعیین شاخص‌ها واستانداردهای پدافند غیرعامل در استقرار عمل‌کردها

تعیین شاخص‌های عمل‌کردی هر سیستم در استقرار

تعیین مجموعه ضوابط واستانداردها برای استقرار

بررسی نقاط امن در پهنه‌ی جغرافیای مورد نظر

انتخاب گزینه‌های نقاط امن برای استقرار عمل‌کردها

تعیین شاخص‌های مناسب مکان گزینی پدافند غیرعامل

امتیاز دهی و وزن دهی به شاخص‌ها بر اساس اهمیت و وزن

انتخاب جای‌گزین بهینه در مکان‌گزینی مناسب برای استقرار طرح‌ها

۲-۲-۳- پایداری

هرچند امنیت و ایمنی سیستم‌ها از منظر پدافند غیر عامل بسیار مهم و ضروری است اما به مفهوم تامین سیستم دفاعی کامل نمی‌باشد. یکی از نکات مهم، وجود پایداری در تولید و ارائه خدمات در مراکز حیاتی، حساس و مهم است. پایداری به این معنی است که یک مرکز در شرایط عادی و یا در صورت بروز حمله و خدشه دار شدن هر دو یا یکی از دو جزء ذکر شده، یعنی امنیت و ایمنی، باید امکان تداوم ارائه تولیدات و خدمات خود را داشته باشد. برای این تداوم و پایداری سیستم‌ها راه کارها و شیوه‌های مختلفی وجود دارد. برخی از این راه کارها عبارتند از:

موازی سازی

تأمین ظرفیت‌های موازی

پیش بینی روش‌های موازی

تأمین احتیاط[۱]

کاهش وابستگی

وابستگی فن‌آورانه، علمی و. . . به خارج از کشور

---

۱ Back up

وابستگی خدمات و پشتیبانی به سایر بخش‌ها (داخلی یا خارجی)

تنوع منابع پشتیبانی

توسعه اشتراک منافع

توسعه و ارتقاء موقعیت بین المللی (به‌دست آوردن فرصت‌های منطقه‌ای و بین‌المللی)

۲-۳- تعریف پدافند غیر عامل فاوا

هر اقدام غیر مسلحانه‌ای که موجب کاهش آسیب‌پذیری نیروی انسانی، ساختمان‌ها، تاسیسات، تجهیزات، اسناد و شریان‌های کشور در مقابل عملیات خصمانه و مخرب دشمن گردد، پدافند غیرعامل خوانده می‌شود.

به بیان ساده‌تر پدافند غیرعامل، مجموعه اقداماتی است که انجام می‌شود تا در صورت بروز جنگ و حتی در زمان صلح، خسارات احتمالی به حداقل میزان خود برسد.

هدف از اجرای طرح‌های پدافند غیرعامل کاستن از آسیب‌پذیری نیروی انسانی، تجهیزات حیاتی و حساس و مهم کشور علی‌رغم حملات خصمانه و مخرب دشمن و استمرار فعالیت‌ها و خدمات زیر بنایی و تامین نیازهای حیاتی و تداوم اداره کشور در شرایط بحرانی ناشی از جنگ است.

به عنوان مثالی ساده، از پدافند غیرعامل می‌توان به استتار، اختفا و ایجاد سرپناه برای تاسیسات مهم و استراتژیک اشاره کرد.

در پدافند عامل مثل سیستم‌های ضد هوایی و هواپیماهای ره‌گیر، فقط نیروهای مسلح مسئولیت دارند. در حالی که در پدافند غیرعامل تمام نهادها، نیروها، سازمان‌ها، صنایع و حتی مردم عادی می‌توانند نقش مؤثری بر عهده گیرند.

دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت‌گیرد. چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان

بازسازی مناطق آسیب‌دیده را با کم‌ترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد، ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند. به‌کارگیری تمهیدات و ملاحظات پدافند غیرعامل علاوه برکاهش شدید هزینه‌ها، کارآیی دفاعی طرح‌ها، اهداف و پروژه‌ها را در زمان تهاجم دشمن بسیار افزایش خواهد داد.

با پیچیده‌تر شدن جنگ‌ها و به کارگیری تکنولوژی و فن‌آوری در جنگ‌های نوین، پدافند غیر عامل نیز چهره‌های متفاوتی را به خود گرفته است. امروزه مردم برای ادامه زندگی نیازمند خدمات متفاوتی هستند و احتیاج به محیط آرام و قابل سکونت درون شهرها دارند و بایستی ایمنی و آسایش کافی داشته باشند.

درحال حاضر عمده‌ترین هدف پدافند غیرعامل، ایمن سازی و کاهش آسیب‌پذیری زیرساخت‌های مورد نیاز مردم است تا به تدریج شرایطی را برای امنیت ایجاد نماید. این گونه اقدامات مهم در اکثر کشورهای دنیا انجام شده و یا در حال اقدام است. این اقدامات اگر به صورت یک برنامه ریزی و با طراحی در توسعه کشور (توسعه پایدار) نهادینه شود، خودبه‌خود بسیاری از زیر ساخت‌هایی که ایجاد می‌شود، در ذات خود ایمنی خواهند داشت. برای اصلاح‌زیرساخت‌های فعلی هم می‌توان با ارائه راهکارهایی مثل مهندسی مجدد، آن‌ها را مستحکم کرد.

اهداف پدافند غیرعامل:

- کاهش قابلیتو توانایی سامانه‌های شناسایی، هدف یابی و دقت هدف‌گیری تسلیحات آفندی دشمن.

- بالا بردن قابلیت‌بقاء، استمرار عملیات و فعالیت‌های حیاتی و خدمات رسانی مراکز حیاتی، حساس و مهم نظامیو غیر نظامی‌کشور در شرایط وقوع تهدید، بحران و جنگ.

- تقلیل آسیب‌پذیری و کاهش خسارت و صدمات تاسیسات، تجهیزات و نیروی انسانی مراکز حیاتی، حساس و مهم نظامیو غیر نظامی‌کشور در برابر تهدیدات و عملیات دشمن.

- سلب آزادی و ابتکار عمل از دشمن.

- صرفه جوئی در هزینه‌های تسلیحاتی و نیروی انسانی.

- فریب و تحمیل هزینه بیش‌تر به دشمن و تقویت بازدارندگی.

- افزایش آستانه مقاومت مردم و نیروی خودی در برابر تهاجمات دشمن.

-حفظ روحیه و انسجام وحدت ملی و حفظ سرمایه‌های ملی کشور.

- حفظ تمامیت ارضی، امنیت ملی و استقلال کشور.(Persianblog. padafand-gh-amel.ir)

۲-۳-۱- امنیت دیجیتال

امنیت دیجیتال عبارت است از قابلیت اعتماد به تولید کنندگان ابزار دیجیتال که برای حفظ محرمانگی و یک‌پارچگی و دسترس‌پذیر بودن این ابزار اقداماتی را انجام داده‌اند تا در عین این که افراد مجاز به آن بتوانند دسترسی داشته باشد افراد غیر مجاز قادر به دست‌یابی و استفاده سو از آن‌ها نباشند.

۲-۳-۲- ایمنی سرمایه‌های دیجیتال

ایمنی سرمایه‌های دیجیتال به امن نگهداشتن این سرمایه‌ها در مقابل انواع تهدیدات سخت و نیمه سخت و نرم‌افزاری می‌پردازد. با توجه به این که هر سیستمی برای ادامه بقاء خود نیازمند به ایمن بودن دارد می‌بایست با تحلیل هزینه – فایده موارد تامین ایمنی هرکدام از سرمایه‌های دیجیتال مورد تجزیه و تحلیل و بررسی قرار گرفته و به‌ترین و سودمندترین روش را که با به صرفه بودن همراه است انتخاب و به کارگیری گردد.

۲-۳-۳- پایداری سامانه‌های دیجیتال

در تامین سیستم دفاعی کامل علاوه بر مد نظر داشتن امنیت و ایمنی باید به استمرار قابلیت ادامه حیات این سرمایه‌ها نیز عنایت نمود. یکی از این نکات مهم قابلیت ارائه خدمات دیجیتال در مراکز مهم، حساس و حیاتی می‌باشد. این قابلیت زمانی می‌تواند وجود داشته باشد که در صورت حمله به این مراکز و به خطر افتادن امنیت و یا ایمنی سرمایه‌های دیجیتال هم‌چنان بتوانند به حیات خود ادامه دهند و در

این زمینه پایداری لازم را داشته باشند. بدون پایداری به مجرد به خطر افتادن امنیت و ایمنی کل سرمایه دیجیتال با خطر از بین رفتن روبرو خواهد شد.

۲-۴- سابقه پدافند غیر عامل فاوا

می‌توان ادعا نمود که قدمت پدافند غیر عامل به قدمت تمدن بشری باز می‌گردد. لیکن این موضوع برای نسل‌های بشر به صورت تلاش آن‌ها برای حراست و مراقبت در برابر دشمنان طبیعی و انسانی نمایان شده است و در طول تاریخ همواره تمهیداتی را برای در امان ماندن از این حوادث مد نظر داشته است. برجو باروهای حفاظتی شهرها، قلعه‌ها و حصارها نمونه‌های بارزی در این خصوص می‌باشند.

در عصر جدید با توجه به مقتضیات عالم جدید و ایجاد دولت‌ها، این موضوع از حیطه شهری به گستره ملی انتقال پیدا نمود. با بروز جنگ جهانی اول و دوم و کشیده شدن پای جنگ به شهرها این موضوع اهمیت بیش‌تری یافت و شکل علنی به خود گرفت. پس از آن جنگ سرد و چالش‌های جهانی مرتبط با سلاح‌های کشتار جمعی اهمیت این بحث را بیش‌تر نمود. در نهایت با وقوع حادثه ۱۱ سپتامبر و جنگ‌های دهه اخیر بین کشورها، این مبحث وارد فاز جدیدی از مطالعات و برنامه‌های اجرایی شد.

جایگاه پدافند غیر عامل در قانون برنامه چهارم توسعه:

هیات وزیران در سال ۱۳۸۴ آیین‌نامه اجرائی بند پ تبصره ۱۷ قانون بودجه سال ۸۴ کل کشور را به تصویب رسانده و در فصل ۱۰ این قانون که قوانین مرتبط با امنیت ملی مطرح شده است و در بند ۱۱ ماده ۱۲۱ به موضوع پدافند غیر عامل اشاره دارد و مطابق متن زیر مواردی را در این خصوص برای خود لازم الاجرا نموده است.

رعایت اصول پدافند غیر عامل در طراحی و اجرای طرح‌های حساس و مهم و در دست مطالعه و نیز تأسیسات زیربنایی و ساختمان‌های حساس و شریان‌های اصلی و حیاتی کشور و آموزش عمومی مردم توسط دستگاه‌های اجرایی و تخصصی موضوع ماده (۱۶۰) قانون برنامه چهارم توسعه، به منظور پیش‌گیری و کاهش مخاطرات ناشی از سوانح غیرطبیعی مد نظر بوده و این دستگاه‌ها موظف‌اند بر اساس سیاست‌ها، الویت‌ها و دستورالعمل‌های کارگروه دائمی پدافند غیر عامل کشور درصدی از اعتبارات تملک دارائی‌های سرمایه‌ای خود را جهت اجرای طرح‌های مصوب کارگروه اختصاص دهند. بر

اساس این قانون کمیته‌های دائمی پدافند غیر عامل در دستگاه‌های اجرائی و تخصصی کشور به منظور اجرائی کردن اهداف پدافند غیر عامل تشکیل و فعالیت خواهند داشت.

هم‌چنین در مهر ماه سال ۸۶ سندی را با عنوان سند راهبردی پدافند غیرعامل کشور توسط مجمع تشخیص مصلحت نظام تهیه و به تصویب رسانده‌شده، که بخش عمده‌ای از طرح جامع پدافند غیر عامل کشور در آن پیش‌بینی شده است که شامل چشم‌انداز و همسو با چشم‌انداز ۲۰ ساله، اهداف کلان و بلند مدت، اهداف کوتاه مدت، سیاست‌های اجرایی و راهبردی می‌باشد.

تلاش برای توسعه پایدار کشور و تحقق اهداف چشم‌انداز ۲۰ ساله توسعه‌ای کشور ایجاب می‌کند، که عنصر پدافند غیر عامل که به معنی ارزیابی آسیب‌پذیرها و تهدیدهای احتمالی و برنامه‌ریزی برای حذف این موارد در اجرای طرح‌های اقتصادی، اجتمائی و توسعه‌ای کشور است، مورد توجه ویژه قرار گیرد.

موارد زیر اشاره به برخی موارد در خصوص تامین بودجه در سال ۸۶ در بخش پدافند غیر عامل با توجه به اهمیت موضوع دارد که در سال (۸۷) نیز این اعتبارات به صورت تکمیلی‌تر در قانون بودجه کشور لحاظ شده است:

۱) تبصره ۲۰ بند ر، بخش ششم از قانون بودجه سال ۸۶

بند "ر" ـ در اجرا طرح‌های پدافند غیرعامل و انسداد مرزها با اولویت مرز شرقی اجازه داده می‌شود، حداکثر مبلغ دو هزار و هشتصد و هفتاد و چهار میلیارد(۰۰۰. ۰۰۰. ۰۰۰. ۲. ۸۷۴) ریال اعتبار ردیف ۵۰۳۹۱۸ قسمت چهارم و ۲۰۲۰۱۰۲۴ پیوست شماره یک این قانون براساس پیش‌نهاد دستگاه‌های اجرایی و تصویب کمیته دائمی پدافند غیرعامل کل کشور در خصوص اعتبار ردیف ۵۰۳۹۱۸ پدافند غیرعامل در اختیار دستگاه‌های اجرائی ذی‌ربط قرارگیرد تا براساس شرح عملیات موافقتنامه مبادله شده با سازمان مدیریت و برنامه‌ریزی کشور به مصرف برسد. این اعتبارات از شمول قانون محاسبات عمومی و سایر مقررات کشور مستثنی می‌باشد.

۲) تبصره ۱۷ بند د، بخش ششم از قانون بودجه ۸۶

بند"د" ـ در اجرای طرح‌های پدافند غیر عامل موضوع آئین‌نامه اجرایی بند (۱۱) ماده (۱۲۱) قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران اجازه داده می‌شود حداکثر

مبلغ چهارصد و چهل میلیارد (۰.۰۰۰.۰۰۰.۰۰۰۴۴) ریال اعتبار ردیف ۵۰۳۹۱۸ قسمت چهارم این قانون، براساس پیش‌نهاد دستگاه‌های اجرایی و تصویب کمیته دائمی پدافند غیرعامل کل کشور در اختیار دستگاه‌های اجرایی ذی‌ربط قرار گیرد تا براساس شرح عملیات موافقتنامه مبادله شده با سازمان مدیریت و برنامه‌ریزی کشور (معاونت برنامه ریزی و نظارت راهبردی ریاست جمهوری) به مصرف برسد.

جایگاه فنی پدافند غیر عامل :

ریشه بحث‌های پدافند غیر عامل به نیازهای انسان برای زندگی بر می‌گردد، با مروری بر هرم نیازهای انسانی، نقش بسیار مهم خواسته‌ایمنی و امنیت آشکار است. پدافند غیر عامل به منظور تامین ایمنی و امنیت انسان در برابر پتانسیل‌های بروز خطر، می‌باشد. از طرفی دیگر پدافند غیر عامل را می‌توان از زاویه مدیریت بحران مورد تحلیل قرار داد، در این صورت شناسایی پتانسیل‌های بحران خیزی، نحوه مدیریت و کنترل بحران به عنوان ورودی‌های سیستم‌های پدافند غیر عامل شناخته می‌شوند.

هم‌چنین پدافند غیر عامل را از زاویه دید آسیب‌پذیری نیز مورد بررسی قرار می‌دهند، که در این صورت شناخت جایگاه‌هایی که به عنوان نقطه ضعف سیستم می‌باشند، به عنوان ورودی‌های سیستم بوده. ضلع دیگر مباحث پدافند غیر عامل بحث‌های ایجاد ایمنی و امنیت عمومی می‌باشد که به صورت آموزش و همکاری همگانی تبلور می‌یابد.

اهمیت، ضرورت و اهداف پدافند غیرعامل

برابر آمار سرشماری سال ۱۳۷۸، تعداد شهرهای کشور ۶۰۰ و تعداد روستاهای آن ۶۵۰۰ روستا بوده است، پدافند هوائی مراکز حیاتی و حساس موجود کشور در شهرها صرفاً با توپ ضد هوائی ۲۳ میلیمتری، نیازمند ۲۴۰۰۰۰ قبضه توپ، یک میلیون و دویست هزار نفر نیروی انسانی (خدمه)، ۳۰۰۰۰ آتشبار و ۷۵۰ گردان ویژ پدافند هوایی خواهد بود که امکان تامین، تشکیل، سازماندهی و پشتیبانی آن دور از دسترس می‌باشد.

دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت‌گیرد. چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان

بازسازی مناطق آسیب‌دیده را با کم‌ترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد، ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند. به‌کارگیری تمهیدات و ملاحظات پدافند غیرعامل علاوه برکاهش شدید هزینه‌ها، کارآیی دفاعی طرح‌ها، اهداف و پروژه‌ها را در زمان تهاجم دشمن بسیار افزایش خواهد داد.

با پیچیده‌تر شدن جنگ‌ها و بکارگیری تکنولوژی و فن‌آوری در جنگ‌های نوین، پدافند غیر عامل نیز چهره‌های متفاوتی را به خود گرفته است. امروزه مردم برای ادامه زندگی نیازمند خدمات متفاوتی هستند و احتیاج به محیط آرام و قابل سکونت درون شهرها دارند و بایستی ایمنی و آسایش کافی داشته باشند.

امروزه با توجه به توسعه فاوا در کلیه امور زندگی انسان‌ها باید به این نکته توجه داشت که وارد عصر جدیدی از زندگی شده و می‌بایست با نگاه جدیدی به پدافند غیر عامل نگریست. باید باز تعریف جدیدی از امنیت و ایمنی و پایداری در عرصه فاوا ارائه نمود. این مطلب در برنامه چهارم توسعه به خوبی خود را نشان داده است. با توجه به این که بسیاری از ارکان زندگی در عصر حاضر با فاوا گره خورده است بدون در نظر گرفتن این مسئله عملاً بسیاری از اقدامات در زمینه پدافند غیر عامل می‌تواند به هدر رفته و هدف اصلی از دیده‌ها پنهان گردد.

۲-۵- مفاهیم امنیت در فاوا

با توجه به روند جنگ‌ها و شرایط حال حاضر دنیا (چه از لحاظ تکنولوژیکی و چه از لحاظ سیاست‌های راهبردی) رویکردهای زیر برطرح پدافند غیرعامل حاکم است:

۱- به عنوان یک فرض مسلم و قطعی، پرداختن و توجه ویژه به مقوله پدافند غیرعامل از لحاظ کمی و کیفی و بررسی سامانه‌هایی که می‌بایست مورد توجه پدافند غیرعامل قرارگیرند، نقش مهم و ارزشمندی را در تعیین سرنوشت جنگ بر عهده خواهد داشت.

۲- نظر به اهمیت در خور توجه و بایسته پدافند غیرعامل و سامانه‌های آن، وحدت فرماندهی و هماهنگی در خصوص نحوه و چگونگی اجرا، هدایت و راهبرد عملیات استتاری در سطوح عمودی و افقی نیروهای مسلح کشور و سایر منابع ملی، لازمه موفقیت در عملیات‌های پدافند غیرعامل و کارآمدی مدیریت راهبردی این نوع پدافند مبتنی برشیوه‌های نوین است.

۳- بدون شک پیشرفت‌های روز افزون در حوزه‌های ارتباطات، مخابرات و سیستم‌های شناسایی و جمع آوری اطلاعات، تغییرات قابل توجهی را در مکانیسم‌ها و ساز و کارهای حاکم بر فعالیت‌ها و چالش‌های نظامی و دفاعی به‌وجود آورده است. هم‌چنین شرایط حاضر جهانی بسیار متغییر بوده و روند رو به رشد سیستم‌های مزبور بسیار شتاب‌آلود و سریع است.

۴- از آن‌جا که روش‌های طراحی، مراقبت و نگهداری، برنامه‌ریزی و توسعه میدانی در پدافند غیرعامل نوین با توجه شرایط و نحوه رویارویی و تقابل با دشمن از نظر سیاسی و جغرافیایی متفاوت است، تنوع شرایط و راهکارها، انعطاف و پویایی مفهوم فرماندهی و کنترل عملیات پدافند غیرعامل را در پی دارد.

۲-۵-۱- تهدیدات سیستم‌های ارتباطی از منظر پدافند

همان گونه که در مغز انسان ارتباطات عصبی و انتقال اطلاعات از طریق تارهای عصبی و نرون‌ها برقرار می‌شود و به مجرد آسیب رسانی به هر کدام از این تارها، تار دیگری این وظیفه را بر عهده می‌گیرد. در دنیای فاوا نیز سیستم‌های ارتباطی مختلفی برای تعامل و انتقال اطلاعات به کار گرفته می‌شوند. در صورت آسیب‌رسانی به هر کدام از این سیستم‌های ارتباطی در صورت عدم وجود سیستم ارتباطی جای‌گزین ادامه حیات ابزار دیجیتال و انتقال اطلاعات میسر نخواهد بود. آسیب‌پذیری‌های که

سیستم‌های ارتباطی را تهدید می‌نمایند به دنبال هدف از بین بردن تعاملات اطلاعاتی بوده و اصل اشرافیت بر اطلاعات را منظور نظر خود قرار می‌دهند.

۲-۵-۲- تهدیدات سیستم‌های رایانه‌ای با نگاه پدافندی

سیستم‌های رایانه‌ای از جمله سیستم‌های می‌باشند که از راه دور و نزدیک و با استفاده از ابزار دیجیتال و آنالوگ قابلیت تهدید پذیری دارند. در صورت تبدیل هر کدام از این تهدیدات از بالقوه به بالفعل عملاً ادامه عمل‌کرد سیستم‌های رایانه‌ای امکان پذیر نبوده و با اختلال مواجه خواهد شد. با توجه به این که در عصر حاضر بسیاری از روش‌های زندگی بر مبنای به کار گیری این ابزار پایه گذاری شده است، آسیب‌پذیری ابزار دیجیتال منجر به آسیب رسانی به امنیت و ایمنی و پایداری بقاء انسان‌ها خواهد شد.

۲-۵-۳- تهدیدات سیستم‌های اطلاعاتی مبتنی بر رایانه در پدافند غیر عامل

سیستم‌های اطلاعاتی مبتنی بر رایانه[۱] از انواع مختلفی تشکیل شده است. کوچک‌ترین این سیستم‌ها بانک اطلاعات می‌باشد که در ابعاد بزرگ و کوچک توسط سازمان‌ها و شرکت‌ها و موسسات و حتی افراد به صورت خصوصی به کار گرفته می‌شوند. هر چه سیستم گسترده می‌شود سیستم‌های تصمیم‌گیری[۲] به آن اضافه شده و برخی از تصمیم‌گیری‌ها روشمند شده و توسط سیستم‌ها انجام و اعمال می‌گردد. عملاً کنترل بسیاری از ابزار دیجیتال به صورت روزمره به این گونه از سیستم‌ها واگذار می‌شود و هر کس که بتواند آگاهانه یا نا آگاهانه به این سیستم‌ها دسترسی داشته و بر آن اثر گذار باشد این قابلیت را خواه داشت تا بر خروجی سیستم نیز اثر گذار باشد. به همین دلیل امن نگه داشتن این سیستم‌ها به منزله امن نگه داشتن کل فرآیند می‌باشد.

---

۱) computer based information system (CBIS

۲ (DSS) decision support system

۲-۶- سئوالات خودآزمایی

فاوا مخفف چیست ؟ توضیح دهید.

اصول کلی پدافند غیرعامل را نام برده و توضیح دهید.

پدافند غیر عامل در حوزه فاوا را توضیح دهید.

سابقه پدافند غیرعامل فاوا در ایران را بنویسید.

تهدیدات سیستم‌های ارتباطی از منظر فاوا کدامند؟ توضیح دهید.

تهدیدات سیستم‌های رایانه‌ای از منظر فاوا کدامند؟ توضیح دهید.

تهدیدات سیستم‌های اطلاعاتی مبتنی بر رایانه از منظر فاوا کدامند؟ توضیح دهید.

۳

فصل سوم: پروتکل‌های امنیتی و اصول ایمن سازی توسط مدیران و سازمان

آن چه در این فصل می خوانید

فرآیند امن‌سازی

آشنایی با پروتکل‌های امنیتی

برنامه‌ریزی امنیتی

سیاست‌های مدیریتی

سیاست‌های اجزای سیستم

۳- پروتکل‌های امنیتی و اصول ایمن سازی توسط مدیران و سازمان

به طور کلی، برای برقراری یک محیط ایمن، چند عامل اساسی باید موجود باشد. این عوامل عبارتند از:

جامعیت۱: اطمینان از این‌که اطلاعات صحیح و کامل است.

محرمانگی۲: اطمینان از این‌که اطلاعات تنها توسط افراد یا سازمان‌های مجاز قابل استفاده است و هیچ گونه فاش‌سازی اطلاعات برای افراد تشخیص و تأیید هویت نشده صورت نخواهد گرفت.

شناسایی و اعتبار سنجی۳: گیرنده و فرستنده، هر دو باید بتوانند از هویت طرف مقابل خود مطمئن باشند.

دسترس‌پذیری: اطمینان از این‌که سیستم مسئول تحویل، ذخیره‌سازی و پردازش اطلاعات همواره در زمان نیاز و در دسترس افراد مربوطه باشد.

انکارناپذیری۴: هیچ یک از دو سوی ارتباط نتوانند مشارکت خود در ارتباط را انکار کنند.

---

۱ Data Integrity

۲ Confidentiality

۳ Identification & Authentication

٤ Non-repudiation

البته باید این نکته را مد نظر داشت که این شرایط در صورتی می‌توانند امنیت را ایجاد نمایند که در محیط بومی‌شکل گرفته باشند و بدون بومی‌سازی نمی‌توان از بیگانگان انتظار تامین امنیت داشت. مخصوصا از بیگانگانی که دشمن قسم خورده می‌باشند.

برای رسیدن به یک طرح مناسب و کارا در ارتباط با امنیت بایست برای برقراری توازن در سه مورد تصمیم‌گیری کنیم:

ارائه‌ی سرویس در برابر امن‌سازی: ارائه‌ی برخی از سرویس‌ها و وجود آن‌ها در شبکه از اهمیت بالایی برخوردار نیست. باید تصمیم گرفت که چه سرویس‌هایی را می‌خواهیم ارائه کنیم. این سرویس‌ها باید آنقدر ارزشمند و مهم باشند تا صرف زمان و انرژی برای امن‌سازی آن‌ها بیهوده نباشد. یعنی این‌که با صرفه و صلاح سازگاری داشته باشند.

سادگی استفاده۱ در برابر امنیت: امن‌سازی سیستم، استفاده از آن را مشکل‌تر می‌کند. هر چه یک سیستم امن‌تر باشد استفاده از آن نیز مشکل‌تر خواهد بود. زیرا امنیت محدودیت ایجاد می‌کند، بنابراین باید بین قابلیت استفاده۲ و میزان امنیت تعادلی را برقرار ساخت.

هزینه‌ی برقرارسازی امنیت در برابر خطر از دست دادن۳: طراحی و پیاده‌سازی امنیت نیازمند صرف هزینه‌هایی در بخش‌های نیروی انسانی، نرم‌افزار و سخت‌افزار خواهد بود. باید مجموع هزینه‌هایی که در صورت از دست دادن هر کدام از منابع یا اطلاعات داخلی به سازمان اعمال می‌شوند محاسبه شده و بین این هزینه‌ها و هزینه‌های تأمین امنیت تعادل برقرار شود. هزینه‌ی از دست دادن منابع باید با توجه به احتمال از دست دادن آن‌ها مورد محاسبه قرار گیرند. در صورتی‌که احتمال از دست دادن یا دچار مشکل شدن یک منبع بسیار پایین باشد و آن منبع از درجه‌ی اهمیت بالایی نیز برخوردار نباشد صرف هزینه زیاد برای امن‌سازی آن بهینه نخواهد بود.

---

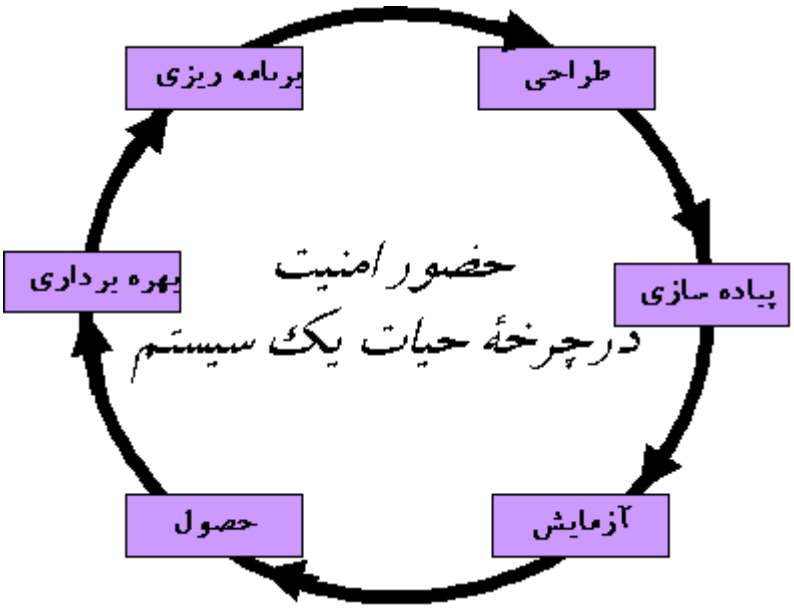
۱ Ease of use

۲ Usability

۳ Risk of loss

۳-۱- فرآیند امن‌سازی

امروزه دیگر به فن آوری امنیت به دید یک محصول نگریسته نمی‌شود، بلکه به اتفاق نظر اکثر متخصصین این فن، امنیت یک فرآیند است؛ فرآیندی که مطابق با شکل زیر باید به چرخه‌ی حیات یک سازمان تزریق شود.



حضور امنیت در چرخه‌ی حیات یک سیستم (تصویر شماره یک)

با دید فرآیند گونه بودن امنیت می‌توان به این نتیجه رسید که مقوله‌ی امنیت لازم است که در تمامی پیکره‌ی یک سازمان لحاظ شود و نه تنها بر روی اطلاعات یا تجهیزات بلکه بر تمام ارکان سازمان باید حاکم باشد. موضوعات موجود در مقوله‌ی مدیریت امنِ فن آوری اطلاعات و ارتباطات نوعاً شامل موارد زیر می‌باشد:

سیاست امنیتی (سازمانی و سیستمی)

تحلیل مخاطرات

انتخاب حفاظ

طرح دقیق امنیتی سیستمی

پیاده سازی حفاظ‌ها در هر سیستم

طرح پشتیبانی و تداوم فعالیت

ارزیابی و نظارت

تحمل‌پذیری خطا

مدیریت تغییرات

طرح مواجهه با حوادث غیرمترقبه

اطلاع رسانی و آموزش امنیتی

۳-۲- آشنایی با پروتکل‌های امنیتی

در ادامه به معرفی برخی از پروتکل‌های امنیتی مطرح در امنیت اطلاعات و ارتباطات می‌پردازیم.

۳-۲-۱- پروتکل PKI

پروتکل PKI، اطمینان لازم در محیط‌های دیجیتالی را فراهم می‌کند. PKI مبتنی بر گواهی دیجیتالی است (گواهی دیجیتالی به نوعی معادل با گذرنامه است که در دنیای فیزیکی مورد استفاده قرار می گیرد). گواهی دیجیتالی برای تائید ماهیت شخص یا مؤسسه‌ای است که در برقراری ارتباط نقش دارد و باعث تراکنش‌های دیجیتالی می‌شود. یک سیستم مبتنی بر گواهی، سرویس‌های امنیتی تصدیق اصالت، صحت داده، محرمانگی و عدم انکار را تأمین می‌کند.

اجزای اصلی PKI شامل مرجع ثبت۱ و مرجع گواهی۲ است . مرجع ثبت یا RA، وظیفه‌ی تصدیق اصالت و ثبت کاربران جدید و درخواست گواهی برای آن‌ها را دارد. مرجع گواهی یا CA، براساس تقاضاهای صورت گرفته به‌وسیله‌ی RA، صدور را انجام داده و آن‌ها را ارسال می‌کند. یک مدل PKI، هم‌چنین شامل سیاست‌ها، رویه‌ها۳ و قراردادهایی است که نحوه‌ی صدور گواهی، صدور مجدد و ابطال گواهی را تعیین می‌کنند. کاربردهایی که از PKI پشتیبانی می‌کنند، می‌توانند مدیریت گواهی‌های کاربران و تولید گواهی دیجیتالی را بر روی رایانه، تلفن‌های همراه و غیره انجام دهند.

۳-۲-۲- S-HTTP

S-HTTP۴ ضمیمه‌ای برای HTTP۵ است که سرویس‌های امنیتی را تدارک می‌بیند. HTTP پروتکلی است که اساس وب جهانی را تشکیل می‌دهد و انتقال مستندات چندرسانه‌ای را بر روی وب میسر می سازد. S-HTTP برای تدارک محرمانگی، غیرجعلی بودن، تمامیت و عدم انکار طراحی شده است. این پروتکل از چندین مکانیسم مدیریت کلید و الگوریتم رمزنگاری پشتیبانی می‌کند. استفاده از این مکانیسم‌ها و الگوریتم‌ها به‌صورت توافق بین طرفین یک تراکنش قابل انجام است. S-HTTP می‌تواند از چهار روش برای تبادل کلیدهای رمزنگاری استفاده کند. این روش‌ها عبارتند از: RSA، out-band، in-band و kerberos. چنان‌چه RSA استفاده شود، کلیدهای رمزنگاری توسط سیستم رمز با کلید عمومی RSA تبادل خواهند شد. منظور از out-band، یک قرارداد کلید خارجی است. منظور از in-band یک کلید است که در یک پیغام حفاظت شده‌ی S-HTTP در یک session دیگر انتقال یافته است. در روش kerberos، کلید از یک سرویس دهنده‌ی kerberos به دست می‌آید. الگوریتم‌های

---

۱ Registration Authority

۲ Certificate Authority

۳ Procedures

٤ Secure Hypertext Transfer Protocol

٥ Hypertext Transfer Protocol

رمزنگاری که توسط S-HTTP پشتیبانی می‌شوند، شامل DES، DES سه‌مرحله‌ای دو کلیدی و سه کلیدی، DESX، IDEA، RC۲ و CDMF هستند.

S-MIME -۳-۲-۳

S-MIME[۱] پروتکلی است که امضای دیجیتال و رمزکردن را به پیغام‌های اینترنتی MIME می‌افزاید. MIME یک قالب استاندارد پیش‌نهادی برای پست الکترونیکی اینترنتی است. پیغام‌های پست الکترونیکی شامل دو قسمت هستند: عنوان و بدنه. قسمت عنوان، مجموعه‌ای از زوج‌های فیلد/مقدار است که اطلاعات ضروری برای انتقال پیغام را تدارک می‌بیند. قسمت بدنه معمولاً بدون ساختار است مگر این که پست الکترونیکی در فرمت MIME باشد. MIME نحوه‌ی تعریف بدنه‌ی پیغام پست الکترونیکی را به‌صورت ساخت‌یافته مشخص می‌کند. فرمت MIME اجازه‌ی استفاده از متون بهبود یافته، گرافیک، صوت و ... را در پیغام‌های پست الکترونیکی می‌دهد. اما خود MIME هیچ سرویس امنیتی را تدارک نمی‌بیند. هدف S/MIME، تعریف چنین سرویس‌هایی براساس دستورات گفته شده در PKCS ۷ برای امضاهای دیجیتال و رمزکردن می‌باشد. قسمت بدنه‌ی MIME، یک پیغام PKCS ۷ را انتقال می‌دهد که این پیغام، نتیجه‌ی پردازش رمزنگاری برروی سایر قسمت‌های بدنه‌ی MIME می‌باشد. اخیرا، S/MIME مورد تایید تعدادی از شرکت‌های بزرگ مانند ConnectSoft، Frontier، FTP Software، Qualcomm، Lotus، Microsoft، Wollongong، Banyan، NCD، SecureWare، Netscape، VeriSign و Novell قرار گرفته است. این تائید را شاید بتوان به عنوان اشرافیت آن‌ها بر اطلاعات استفاده کنندگان از این روش مد نظر قرار داد.

SSL -۴-۲-۳

پروتکل SSL[۲] توسط شرکت Netscape Communications برای تدارک امنیت و محرمانگی برروی اینترنت توسعه یافته است. این پروتکل از تصدیق اصالت در سمت سرویس‌دهنده و سرویس گیرنده پشتیبانی می‌کند. پروتکل SSL وابسته به کاربرد می‌باشد و به پروتکل‌هایی نظیر HTTP، FTP و

---

۱ Secure/ Multipurpose Internet Mail Extensions

۲ Secure Socket Layer

telnet اجازه می‌دهد تا به‌صورت لایه‌ای برروی آن قرار گیرند. پروتکل SSL قادر است به توافق درباره‌ی کلیدهای رمزنگاری و نیز تصدیق سرویس دهنده قبل از تبادل اطلاعات توسط لایه‌های بالاتر اقدام نماید. پروتکل SSL، امنیت و تمامیت کانال انتقال را با استفاده از رمزکردن، تصدیق اصالت و کدهای تصدیق پیام حفظ می‌کند.

پروتکل SSL شامل دو مرحله‌ی تصدیق سرویس‌دهنده و تصدیق سرویس‌گیرنده است. از این میان، مرحله‌ی دوم اختیاری است. در مرحله‌ی نخست، سرویس‌دهنده در پاسخ به درخواست سرویس‌گیرنده، گواهی تصدیق خود را به همراه موارد دلخواهش برای رمزکردن، ارسال می‌کند. سپس، سرویس‌گیرنده یک شاه‌کلید تولید می‌کند، آن را با کلید عمومی سرویس‌دهنده رمز می‌نماید و شاه‌کلید رمز شده را به سرویس‌دهنده ارسال می‌کند. سرویس‌دهنده، شاه‌کلید را بازیابی کرده و با بازگرداندن یک پیغام (که با شاه‌کلید رمز شده است) به سرویس‌گیرنده، خودش را تصدیق می‌کند. داده‌های بعدی، به وسیله‌ی کلیدهای مشتق شده از این شاه‌کلید رمز می‌شوند. در مرحله‌ی دوم (اختیاری)، سرویس‌دهنده یک دستور شناسایی به سرویس‌گیرنده ارسال می‌کند. سرویس‌گیرنده برروی دستور شناسایی که دریافت کرده است امضای دیجیتال خودش را تولید می‌کند و آن را به همراه گواهی تصدیق کلید عمومی خود به سرویس‌دهنده باز می‌گرداند.

الگوریتم‌های رمزنگاری گوناگونی توسط SSL پشتیبانی می‌شوند. در زمان انجام فرآیند Handshaking، از سیستم رمز RSA استفاده می‌شود. بعد از تبادل کلید، تعدادی رمزنگار از قبیل RC۲، RC۴، DES، triple-DES و MD۵ استفاده می‌شوند.

PCT -۵-۲-۳

PCT[1] پروتکلی است که توسط Microsoft و Visa International برای ارتباط امن برروی اینترنت توسعه یافته است. PCT مکمل پروتکل SSL و قرینه‌ی پروتکل STT می‌باشد. این پروتکل از بسیاری جهات شبیه SSL است. در حقیقت، فرمت پیغام‌ها آن‌قدر شبیه هستند که یک سرویس‌دهنده می‌تواند هم با سرویس‌گیرنده‌های پشتیبانی‌کننده از SSL و هم با سرویس‌گیرنده های پشتیبانی‌کننده

---

۱ Private Communication Technology

از PCT تعامل داشته باشد. بر اساس مشخصات موجود، PCT برخی از نقایص و ضعف‌های SSL را تصحیح می‌کند یا بهبود می‌بخشد. موارد اختلاف عبارتند از:

PCT نسبت به SSL پیغام‌های کمتری را بین سرویس‌گیرنده و سرویس‌دهنده جابه‌جا می‌کند و البته خود پیغام‌ها در PCT کوتاه تر هستند.

PCT نسبت به SSL انتخاب‌های بیش‌تری را برای الگوریتم و فرمت‌های داده در نظر گرفته است.

تصدیق پیغام و رمزکردن آن در PCT با کلیدهای متفاوتی انجام می‌گیرد. در SSL، هر دو فرآیند مذکور با یک کلید انجام می‌شوند. بدین ترتیب، در PCT می‌توان تصدیق پیغام را با کلیدهای طولانی‌تری نسبت به رمزکردن پیغام انجام داد و به امنیت بیش‌تری دست خواهیم یافت.

در پروتکل تصدیق PCT، پاسخ سرویس‌گیرنده به الگوریتم رمز مورد مذاکره بستگی دارد؛ در حالی‌که در SSL این‌گونه نیست. این ویژگی در حکم یک دیواره آتش[1] است چون اگر دشمن موفق به بازیابی کلید رمزنگاری در یک نوبت[2] شود و یک انتخاب برای الگوریتم (مثلا یک الگوریتم ضعیف) داشته باشد، نمی‌تواند در دفعات بعدی با یک الگوریتم دیگر (مثلا یک الگوریتم قوی) را مورد مخاطره قرار دهد. SSL چنین دیوارهآتشی را تدارک نمی‌بیند.

PCT برای برقراری کلید، از الگوریتم‌های RSA، Diffie-Hellman و Fortezza استفاده می‌کند؛ الگوریتم‌های رمزنگاری مورد استفاده شامل DES، triple-DES، RC۲ و RC۴ هستند. هردو امضای دیجیتال RSA و DSA پشتیبانی می‌شوند.

با توجه به بررسی تمام این پروتکل‌ها مشاهده می‌گردد تمام این پروتکل‌ها از طرف سازندگانی که تحت نظارت نظام سلطه شکل گرفته اند به منظور تامین امنیت به استفاده کنندگان دیکته گردیده است و این مطلب غیر از تامین امنیت بوسیله ناامن گرایان نمی‌تواند مفهوم دیگری داشته باشد .

---

[1] firewall

[2] session

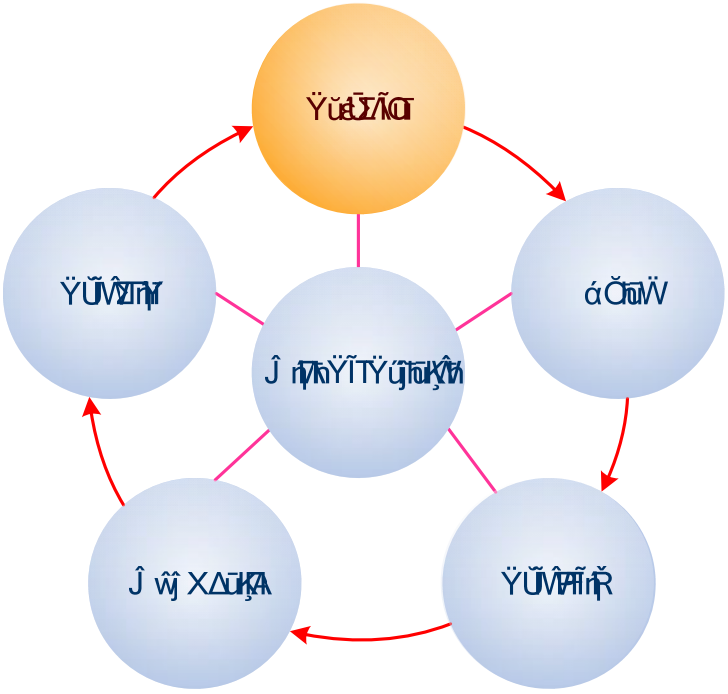
امنیتی که در اختیار آنان بوده و در هر زمان که مد نظر داشته باشند می‌توانند آن را به نفع خود تغییر دهند.

۳-۳- برنامه‌ریزی امنیتی

برای پیاده سازی امنیت در یک سازمان به دو نوع برنامه‌ریزی در آن نیاز است. برنامه‌ریزی کلان‌تر برای خط مشی‌ها و برنامه‌ریزی جزئی‌تر برای سیاست‌های امنیتی. در ادامه با این دو دسته بیش‌تر آشنا خواهیم شد.

۳-۳- ۱- برنامه‌ریزی استراتژیک امنیت

استراتژی یک جهت‌دهی یا خط مشی است که برای رسیدن به هدف یا اهدافی اتخاذ می‌شود. هدف از برنامه‌ریزی استراتژیک برای امنیت فراهم آوردن اطلاعات لازم جهت مدیریت و تصمیم‌گیری در مورد سرمایه‌گذاری‌های امنیتی است. برنامه استراتژیک عملکردهای امنیتی را به خط‌مشی‌های تجاری و حرفه پیوند می‌دهند. استراتژی‌های امنیتی رسیدن به اهداف حرفه را با شناسایی و آدرس‌دهی نیازمندی‌های امنیتی در عملکرد آن سازمان، فراهم آوردن زیرساخت‌ها، افراد و فرآیندهایی که آن نیازمندی‌ها را فراهم کند ممکن می‌سازد. همان‌طور که در شکل زیر مشخص است در حقیقت استراتژی های امنیتی هسته اصلی برای چرخه طراحی و پیاده‌سازی یک سیستم امنیتی را تشکیل می‌دهد.



چرخه‌ی طراحی استراتژی‌های امنیتی هسته اصلی(تصویر شماره دو)

استراتژی‌ها با استفاده از اهداف حرفه و اهداف امنیتی و میزان قابلیت فعلی برای تأمین این اهداف طراحی می‌شود. برای مثال ممکن است هدف یک بانک به‌دست آوردن سرمایه بیش‌تر باشد و استراتژی آن جذب بیش‌تر مشتریان باشد. یک هدف امنیتی ایجاد اتصال بیش‌تر در کنار کم کردن خطر هک[1] و ویروس تا سطح قابل قبول باشد و هدف امنیتی دیگر اطمینان از برآورده شدن انتظارات قابل دسترس بودن مشتریان باشد. بنابراین استراتژی امنیتی مربوطه با توجه به محدودیت‌های داخلی و خارجی

[1] hack

سازمان می‌تواند افزایش میزان مانیتور کردن اتصالات در جهت کاهش ریسک ویروس و هک و فراهم آوردن افزونگی۱ برای افزایش میزان دسترس‌پذیری۲ و اطمینان باشد.

۳-۳-۲- سیاست‌های برنامه‌ریزی استراتژیک

استراتژی‌ها باید به طور دوره‌ای بازبینی و اصلاح شوند تا اجازه تغییر و رشد به فرآیند حرفه مربوطه داده شود.

قسمت‌های مختلف سازمان‌باید هماهنگ با یک‌دیگر و با توجه به خط‌مشی‌های ابلاغ شده از سوی نهادهای مرکزی سازمان به طراحی استراتژی‌های خود بپردازند.

۳-۳-۳- برنامه‌ریزی سیاست‌های امنیتی

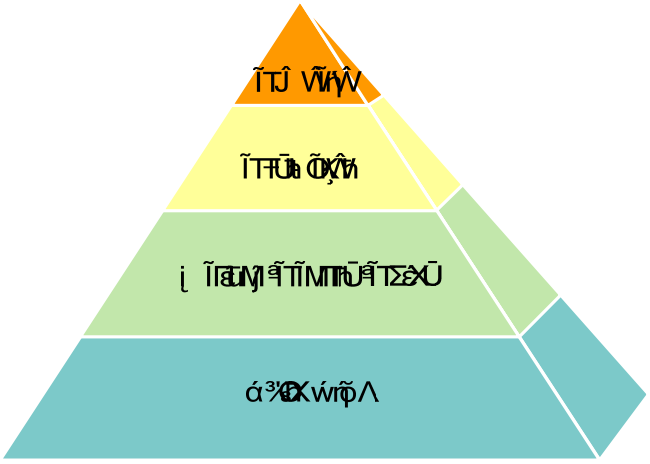
سیاست۳ در ارتباط با مدیریت امنیت معانی زیادی دارد. سیاست به معنای دستورات، قوانین و تصمیم های مدیر امنیتی برای ایجاد یک برنامه امنیتی، پایه‌ریزی کردن اهداف و تخصیص دادن مسئولیت هاست. پس از تعیین خط‌مشی‌های یک سازمان، سیاست‌های آن برنامه‌ریزی شده، استانداردها و سپس روال‌ها و راهنماهای امنیتی مربوطه برای پیاده‌سازی آن سیاست‌ها در یک محیط واقعی توسعه داده شده در اختیار کاربران و مدیران قرار داده می‌شود. این سیاست‌ها برای رسیدن به امنیت مورد نظر در سازمان باید به طور کامل پیاده‌سازی و اجرا شوند. تمام افرادی که به این منابع دست‌رسی دارند تحت تأثیر این سیاست‌ها قرار می‌گیرند و ملزم به رعایت و اجرای آن‌ها خواهند بود. این سیاست‌ها با دقت و توجه فراوان باید تدوین شوند. هر گونه اشتباه در این مرحله ممکن است امنیت سیستم را دچار مشکل کند.

---

۱ Redundancy

۲ Availability

۳ Policy



هرم برنامه‌ریزی‌های سیاست‌های امنیتی(تصویر شماره سه)

سیاست‌های امنیتی که خوب تدوین شده باشند ویژگی‌های زیر را دارا هستند:

توسط مدیران سیستم قابل پیاده‌سازی و اجرا هستند.

رویه‌های تدوین شده ساده، قابل اجرا و مورد پذیرش هستند.

توسط ابزارهای تأمین کننده‌ی امنیت موجود قابل اعمال هستند.

به طور مشخص مسئولیت‌ها و وظایف کاربران، کادر فنی و مدیران را تعیین می‌کنند.

به هنگام تدوین سیاست‌های امنیتی به سئوالات زیر باید پاسخ داد:

چه کسانی اجازه دارند از منابع استفاده کنند؟

چگونه افراد مجاز شناسایی می‌شوند؟

استفاده‌ی صحیح و مناسب از منابع چیست؟

چه کسی اجازه‌ی بخشیدن دست‌رسی و بالا بردن سطح دست‌رسی را داراست؟

چه افرادی سطح دست‌رسی مدیران[۱] را دارا هستند؟

حق و حقوق کاربران و هم‌چنین مسئولیت‌های آن‌ها چیست؟

حق و حقوق مدیران فنی و هم‌چنین مسئولیت‌های آن‌ها چیست؟

با اطلاعات حساس چه کار باید کرد؟

فعالیت‌های انجام شده در سیستم چگونه و تا چه حد نگهداری می‌شوند؟

با متخلفین و کسانی که از سیاست‌ها و قوانین پیروی نمی‌کنند چگونه برخورد می‌شوند؟

سیاست امنیتی باید در حوزه‌های بسیاری از هر سازمان باید تعیین شود که از آن جمله می‌توان به موارد زیر اشاره نمود:

سیاست دسترسی: مشخص می‌کند که چه افرادی و یا چه بسته‌هایی اجازه‌ی دست‌رسی به منابع مختلف را دارا هستند. سطح و میزان دست‌رسی آن‌ها نیز در همین بخش مشخص می‌شود. در این بخش هم‌چنین قوانینی برای ارتباطات بیرونی، انتقال داده‌ها، اتصال تجهیزات به شبکه و اضافه کردن نرم‌افزارهای جدید تدوین می‌شود.

سیاست تشخیص هویت: نحوه‌ی شناسایی افراد و بسته‌های مختلفی که متقاضی ورود به شبکه و استفاده از منابع هستند را مشخص می‌کند. یکی از مواردی که در این بخش مشخص می‌شود سیاست کلمه عبور(کلمات عبور اولیه، محدودیت در چگونگی کلمات عبور، حداکثر زمان‌ها و...) است. در این بخش هم‌چنین تعیین‌هویت‌های فرآیندهای نرم‌افزاری (مثلاً در پروتکل‌های مسیریابی به هنگام دریافت بسته‌های routing-update) نیز مورد بررسی قرار می‌گیرد.

---

۱ Administration privilege

سیاست حساب‌داری: چگونگی نگهداری اتفاقاتی که در شبکه می‌افتند را مشخص می‌کند. در این بخش مشخص می‌شود که انواع مختلف فعالیت‌های انجام شده چگونه جمع‌آوری و نگهداری می‌شوند. باید تمام اطلاعات و فعالیت‌های افراد تشخیص و تأیید هویت شوند (نام، شماره‌ی خط و یا میزبانی که از آن طریق login کرده‌اند، میزان دست‌رسی قدیم و جدید، تلاش‌های احتمالی انجام شده برای تغییر سطح دست‌رسی و. ..) با زمان دقیق نگهداری شوند.

سیاست گزارش تخلفات: مشخص می‌کند که انواع تخلفات کدامند و این تخلفات چگونه و به چه کسانی گزارش داده می‌شوند.

سیاست حریم خصوصی افراد: در این بخش مشخص می‌شود که مدیران تا چه حد و در چه شرایطی می توانند mailها را مانیتور کنند، دست‌رسی به فایل‌های کاربران و مدیران زیربخش‌ها داشته باشند، از فعالیت‌های خصوصی افراد log بگیرند، desktopها را مشاهده کنند و. ..

سیاست نگهداری شبکه: نگهداری خارجی و داخلی را مشخص می‌کند و میزان دست‌رسی افراد خارجی که برای نگهداری یا بهینه‌سازی شبکه با سازمان همکاری می‌کنند را تعیین می‌سازد. چگونگی مدیریت از راه‌دور نیز در این بخش مشخص می‌شود.

سیاست دسترس‌پذیری: میزان توقع و انتظار کاربران و مدیران از دسترس‌پذیری منابع را مشخص می کند و براین اساس افزونگی[۱] منابع و فرآیند بازیابی آن‌ها را مورد تحلیل قرار می‌دهد.

سیاست‌های آگاهی‌رسانی: چگونگی آموزش کاربران، کادر فنی و مدیران در این بخش مشخص می‌شود. در این بخش هم‌چنین مشخص می‌شود که کدام قسمت و چه افرادی باید به سئوالات کاربران و مدیران در زمینه‌ی امنیت و در هنگام بروز حوادث امنیتی پاسخ دهند و به آن‌ها کمک کنند.

پس از تعیین سیاست‌ها، رویه‌های امنیتی باید برای کاربران نهایی، مدیران شبکه و مدیران امنیتی و سایر افراد درگیر نوشته شوند. رویه‌های امنیتی هم‌چنین باید چگونگی برخورد با حوادث مختلفی که رخ می‌دهند را مشخص کنند. این رویه‌ها باید به کاربران و مدیران شبکه آموزش داده شوند.

---

۱ Redundancy

پس از آنکه قدم‌های فوق برداشته شدند دیواره‌های آتش، ضدویروس‌ها، سیستم‌های تشخیص تهاجم بومی شده و... برای امن‌سازی سازمان به خدمت گرفته می‌شوند و رویه‌های امنیتی پیاده‌سازی می‌شوند.

سیاست‌های امنیتی، تکنولوژی و متدولوژی استفاده از سیستم‌های امن و روال، گام‌های جزئی برای دنبال کردن وظایف امنیتی مربوطه را مشخص می‌کند. در این راستا پس از شناخت وضعیت معماری موجود و تهیه معماری امنیتی مطلوب باید برنامه‌ای برای حرکت از سمت معماری موجود به سمت معماری مطلوب طراحی و اجرا و کنترل نمود. سیاست‌های امنیتی باید در دسته‌های مدیریت امنیتء امنیت اطلاعات، امنیت پرسنل، امنیت شبکه و سیستم شامل سیاست‌های توسعه نرم‌افزار، سیاست‌های شبکه و مدیریت سیستم و برنامه‌ریزی تداوم عمل‌کرد سازمان ارائه شود .

۳-۳-۴- استراتژی‌های طراحی سیاست‌ها

در سازمان باید تشکیلاتی برای تأمین امنیت شبکه از نقطه‌نظر ساختار، شرح وظایف و جایگاه آن در چارت سازمانی و برنامه‌های تأمین نیروی انسانی آن طراحی شود. این تشکیلات در سه سطح سیاست گذاری، مدیریت اجرایی و سطح فنی به طراحی، نظارت و اجرای طرح‌ها و برنامه‌های امنیتی می‌پردازد.

برنامه‌ریزی‌ها باید به دو صورت کوتاه‌مدت و بلندمدت (یا میان‌مدت) با توجه به اهداف امنیت سازمان طراحی شود.

برای این‌که سیاست‌های امنیتی به خوبی پیاده‌سازی شوند تمام افرادی که وظیفه‌ی نگهداری و محافظت سیستم را به عهده دارند باید در پیاده‌سازی آن‌ها همکاری کنند.

برای برنامه‌ریزی و دادن طرح‌ها و رویه‌های امنیتی ابتدا باید سرمایه‌ها و ریسک‌ها را شناسایی و درجه بندی نمود.

پس از طراحی برنامه امنیت سازمان، طراحی برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت در سازمان باید و هم‌چنین طرح پشتیبانی حوادث امنیتی سازمان را نیز طراحی نمود.

سیاست‌های امنیتی باید برای موارد مختلفی از جمله موارد زیر طراحی شود: سیاست‌های دست‌رسی کاربران به شبکه داخلی، دست‌رسی کاربران به شبکه اینترنت، سیاست‌های امنیتی در مورد سرویس

های E-mail، وب، ویدئو کنفرانس، وب هاستینگ، بدون سیم[۱] ، دست‌رسی از راه دور، سرویس‌های اشتراک، دست‌رسی و انتقال فایل‌ها، دست‌رسی به بانک‌های اطلاعاتی، دست‌رسی کاربران به سخت افزارها، سیاست‌های انتخاب سیستم عامل، سیاست‌های انتخاب و تنظیم ایستگاه‌های کاری، سیاست های نصب نرم‌افزار، سیاست‌های پشتیبان‌گیری، سیاست‌های محافظت در مقابل ویروس، سیاست‌های بازرسی دوره‌ای امنیت ایستگاه‌های کاری، سیاست‌های امنیتی استفاده از سخت‌افزارهای مختلف، سیاست‌های دست‌رسی کاربران به نرم‌افزارها و سرویس‌های شبکه و سیاست‌های امنیت فیزیکی و. ..

در هر سازمان پس از تهیه سیاست‌ها و استانداردها و روال‌های امنیتی، معماری موجود سازمان بررسی شود، رخنه‌ها و خطرهای آن مشخص شوند. سپس با توجه به اهداف و سیاست‌ها نیازمندی‌های امنیتی شامل جزئیاتی مانند TDSها، UPNها، دست‌رسی از راه دور، حفاظت از میزبان (host protect) و حتی طراحی‌های شبکه مانند تغییر توپولوژی. .. شناسایی و اولویت‌بندی گردد.

پس از انتخاب هدف‌ها و سیاست‌های امنیتی باید به تهیه روال‌ها و دستورالعمل‌های اجرایی جهت عملیاتی کردن آن سیاست‌ها پرداخت.

۳-۴- سیاست‌های مدیریتی

سیاست‌های مدیریتی را در سه بخش بررسی می‌کنیم. در بخش اول، مسائل مربوط به مدیریت نظارت بر سیستم، بررسی می‌شوند. در بخش دوم کنترل‌های امنیتی و در بخش سوم مدیریت تهدیدهای حقوقی و حیثیت مورد بررسی قرار می‌گیرند.

۳-۴-۱-نظارت مدیریتی

مدیران سیستم مسئولیت توسعه استراتژی‌های تجاری را بر عهده دارند. یک تصمیم اولیه از دید مدیریتی آن است که آیا نیاز به ارائه سرویس‌ها و افزودن این سرویس‌ها به سرویس‌های سنتی وجود دارد یا نه؟ به طور خاص سیستم نظارت بایستی از ترکیب واضح و بدون ابهام طرح‌های ارائه شده برای سرویس‌های جدید با اهداف موجود در سیاست‌های مورد نظر اطمینان حاصل کند. هم‌چنین، تحلیل

---

۱ Wireless

ریسک بر روی فعالیت‌ها و سرویس‌های جدید پیش‌نهادی، نظارت بر پردازش‌های انجام شده بر روی ریسک‌های تعیین شده، ارزیابی نتایج فعالیت سیستم الکترونیکی و غیره از مواردی هستندکه باید اجرا شوند. به طور مشخص، توجه به اصول یک تا سه ضروری است:

۳-۴-۱-۱- اصل اول نظارت کامل بر فعالیت‌ها و سیاست ها:

مدیران سیستم باید نظارت مدیریتی لازم مرتبط با فعالیت‌ها، شامل سیاست‌ها و کنترل‌های مورد نیاز برای مدیریت این ریسک‌ها را به انجام رسانند.

برقراری مکانیزم‌های بررسی و گزارش‌دهی شامل، اقدامات لازم برای مقابله با رویدادهایی که امنیت و صحت عملکرد سیستم را دچار مخاطره می‌سازند.

توجه به عوامل ریسک متفاوتی که با بومی‌سازی , صحت، امنیت و قابلیت دست‌رسی و محصولات الکترونیکی ارتباط پیدا می‌کنند، شرکت‌های بخش سوم۱ نیز که توسعه و پیاده‌سازی محصولات را انجام داده و اطلاعات کلیدی را در اختیار دارند، بایستی به چنین مواردی توجه کافی داشته باشند.

اطمینان از این که سعی و تلاش لازم برای تحلیل تهدیدات، قبل از هر نوع فعالیت مهم صورت می گیرد.

۳-۴-۱-۲- اصل دوم عناصر کلیدی فرآیند کنترل امنیت:

مدیران بایستی مفاهیم کلیدی مربوط به فرآیند کنترل امنیتی را به کار گیرند.

عناصر کلیدی فرآیند کنترل امنیتی شامل موارد زیر است:

در نظر گرفتن فرد یا افرادی از کارمندان برای نظارت بر به‌کارگیری صحیح سیاست‌های امنیتی؛

استفاده ازکنترل‌های فیزیکی‌کافی برای جلوگیری از دسترسی‌های فیزیکی غیرمجاز به محیط‌های رایانه‌ای ؛

اعمال کنترل‌های کافی و اجرای فرآیندهای نظارتی برای جلوگیری از دسترسی‌های داخلی و خارجی غیرمجاز به کاربردها و پایگاه‌های داده .

۱- Third-Party

انجام آزمایش‌ها و بازبینی‌های منظم کنترل‌ها و اقدامات امنیتی شامل، نصب نسخه‌های جدیدتر نرم افزارها و یا بسته‌های تکمیلی آن‌ها.

۳-۴-۱-۳- اصل سوم فرآیند جامع نظارت :

مدیران بایستی یک فرآیند جامع و در حال پیشرفت برای نظارت و مدیریت ارتباطات موجود بین سازمان و عوامل خارجی و نیز شرکت‌های بخش سوم وابسته تدوین نمایند.

در رابطه با این اصل، سیستم عملیاتی، موارد زیر را در نظر می‌گیرد:

ریسک‌ها و تهدیدات حاصل از ارتباط با عوامل خارجی و شرکت‌ها به خصوص انجام فعالیت‌های شراکتی، بایستی کاملاً برای مدیران تفهیم شده باشد.

صلاحیت شرکت‌های نوع سوم‌که سرویس‌های مورد نیاز را فراهم می‌کند، قبل از انعقاد هر نوع قراردادی، باید به مناسب‌ترین شکل ممکن مورد بررسی قرارگیرد.

در انجام هر نوع ارتباطی با شرکت‌های هم‌کار، تمامی وظایف و مسئولیت‌های این شرکت‌ها، بایستی به طور واضح و بدون ابهام تعریف شود.

تمامی شرکت‌های مرتبط بایستی مطابق با سیاست‌های محرمانگی و امنیتی ، فعالیت‌های خود را انجام دهند.

پیگیری و نظارت بر عمل‌کرد شرکت‌های همکار ، بایستی به نحو مناسب و تا حد امکان انجام شود.

و دست آخر این‌که، برای فعالیت‌های سازمان و همکاری آن با شرکت‌ها و عوامل خارج از آن، باید طرح های مناسبی در نظر گرفته شده و تدوین شود.

۳-۴-۲- کنترل‌های امنیتی

مدیران مسئولیت انجام فرآیند کنترل‌های امنیتی را بر عهده دارند. این فرآیند با توجه به نیاز به افزایش امنیت در سیستم‌های الکترونیکی نیاز به توجهات خاص دارد.

۳-۴-۲-۱- اصل چهارم احراز هویت :

سازمان بایستی اقدامات مناسب برای احراز هویت، شناسایی و بررسی مجوزهای مشتریان را انجام دهد.

با پیدایش انواع روش‌های احراز هویت، ساختارها نیز در صدد تقویت روش‌های مورد استفاده خود، برای احراز هویت هستند که با در نظرگرفتن مواردی مانند موارد زیر تحقق می‌یابند:

پایگاه‌های داده احراز هویت که دست‌رسی به اطلاعات و یا سیستم‌های حساس را به وجود می‌آورند، بایستی در مقابل خرابی و نفوذ مورد حفاظت قرارگیرند.

اعتبار هرنوع تغییر در پایگاه داده مربوط به احراز هویت که در اثر حذف، تغییر و یا افزوده شدن یک عامل در سیستم حاصل می‌شود، بایستی به‌وسیله‌ی یک منبع تصدیق شده دیگر مورد تأئید قرارگیرد.

اقدام لازم در خصوص کنترل ارتباطات سیستم انجام شود به گونه‌ای که هرنوع تغییر به وجود آمده توسط عوامل خارجی امکان‌پذیر نشود.

نشست‌های احراز هویت شده درطول کل زمان نشست، امن باقی بماند و یا درصورت انقضای نشست، احراز هویت و سایرکنترل‌های امنیتی مورد نیاز مجدداً انجام گیرد.

۳-۴-۲-۲- اصل پنجم عدم امکان پذیری انکار هویت :

سازمان‌ها بایستی، روش‌های احراز هویت تراکنش که از عدم انکار پشتیبانی کرده و جواب‌گویی[۱] تراکنش‌های اطلاعاتی را تضمین می‌کند، مورد استفاده قرار دهند.

اصل عدم انکار شامل جلوگیری از تکذیب گیرنده در قبال دریافت داده‌های ارسالی فرستنده و یا تکذیب فرستنده در قبال ارسال داده‌هایی است که به گیرنده ارسال نموده است. تهدید انکار تراکنش، همواره به عنوان یک مسأله مطرح در تراکنش‌های مربوط به کارت‌های اعتباری و یا تراکنش‌های امنیتی مطرح بوده است. برای پرداختن به مسائل یاد شده، نیاز به انجام اقدامات مناسب به خصوص با درنظرگرفتن مسائل مطرح در تراکنش‌های اطلاعات است تا اطمینان از موارد زیر حاصل شود:

---

۱ Accountability

سیستم‌های بایستی احتمال انجام تراکنش‌های نامطلوب به وسیله کاربران مجاز را کاهش داده و از سوی دیگر کاربران از ریسک‌های مرتبط با هر نوع تراکنشی که آغاز می‌کنند، آگاهی کامل داشته باشند.

تمامی عوامل مرتبط با تراکنش، احراز هویت شده و کنترل لازم بر روی کانال ارتباطی وجود داشته باشد.

داده‌های تراکنش‌ها در مقابل تغییرات احتمالی محافظت شده و هر نوع تغییر توسط عوامل خارجی نیز قابل شناسایی باشد.

۳-۴-۲-۳- اصل ششم تفکیک صحیح وظایف:

ساختارها بایستی از انجام اقدامات مناسب در رابطه با تفکیک صحیح وظایف در سیستم‌های ، پایگاه های داده و کاربردها اطمینان حاصل نمایند.

یک روش کنترل داخلی سیستم که برای کاهش ریسک تقلب و کلاهبرداری در فرآیندهای پردازشی به کار گرفته می‌شود، تفکیک وظایف است. با اعمال این روش از مجاز بودن تراکنش‌های انجام شده و صحت داده‌ها حصول اطمینان شده و از انجام هر نوع تقلب جلوگیری می‌شود. نمونه‌ای از موارد به کارگرفته شده برای تفکیک وظایف در سیستم‌های الکترونیکی به شرح زیر هستند:

پردازش تراکنش‌ها و سیستم‌ها باید به گونه‌ای طراحی شوند که هیچ فرد یا کارمندی نتواند حتی درصورت داشتن مجوز در سیستم، یک تراکنش را به طور کامل و به تنهایی به انجام برساند.

تفکیک وظایف بایستی در محدوده بخش‌های شروع کننده (شامل محتویات صفحات وب) و آن‌هایی که مسئولیت بررسی صحت داده‌ها را بر عهده دارند انجام شود.

سیستم‌های الکترونیکی بایستی از لحاظ مناسب بودن سیستم تفکیک وظایف مورد آزمایش و تأئید قرار گیرند.

تفکیک وظایف بایستی در محدوده توسعه دهندگان تا مدیران سیستم اجرا شود.

۳-۴-۲-۴- اصل هفتم اطمینان از کنترل مجوزهای دسترسی:

سیستم‌ها بایستی از کنترل مجوزهای دست‌رسی و انجام دسترسی‌های مجاز به سیستم‌های الکترونیکی، پایگاه‌های داده و کاربردها اطمینان کامل حاصل نمایند.

کنترل شدید مجوزها و دسترسی‌ها به سیستم در جهت حفظ اصول مربوط به تفکیک وظایف یک امر ضروری است. هرگونه نقص در این بخش باعث می‌شود که افراد بتوانند مجوزهای خود را تغییر داده و به سیستم، پایگاه‌های داده و کاربردهای بانک اطلاعاتی به شکل غیرمجاز دست‌رسی پیدا کنند.

۳-۴-۲-۵- اصل هشتم اطمینان از صحت تراکنش ها:

سازمان‌ها بایستی از انجام اقدامات مناسب برای حفظ صحت داده‌ها، رکوردها و اطلاعات مربوط به تراکنش‌های اطلاعاتی، اطمینان کافی را حاصل نمایند.

صحت داده در واقع، عدم تغییر غیرمجاز اطلاعات در زمان انتقال آن‌ها و یا در حالتی است که بر روی یک رسانه، ذخیره شده باشند. اصول اولیه لازم برای تضمین صحت داده‌ها در سیستم بانک اطلاعاتی به شرح زیر است:

تراکنش‌های اطلاعاتی به نحوی انجام شوند که در مقابل هر نوع تقلب در طول کل فرآیند مقاوم باشند.

ذخیره‌سازی و دست‌یابی رکوردها به گونه‌ای انجام شوند که در مقابل هر نوع تخلف و عمل غیر مجاز مقاوم باشند.

تراکنش‌ها و فرآیندهای نگهداری از رکوردهای اطلاعاتی به گونه‌ای طراحی شوند که به طور مجازی، هر نوع تغییر غیرمجاز قابل تشخیص باشد.

اعمال تغییرات لازم در سیاست‌های کنترل شامل نظارت و رویه‌های تست سیستم بایستی در جهت محافظت در مقابل تغییراتی که ممکن است قابلیت اطمینان سیستم را به مخاطره بیاندازند انجام شود.

هرنوع تخلف در تراکنش‌ها یا داده‌های سیستم به وسیله پردازش تراکنش و نظارت بر انجام آن قابل تشخیص باشد.

۳-۴-۲-۶- اصل نهم ره گیری تراکنش ها:

در سیستم‌های اطلاعاتی، بایستی از انجام عملیات ردگیری تمامی تراکنش‌های انجام شده اطمینان لازم حاصل شود.

سازمان‌ها نه تنها در صدد، اعمال کنترل‌های داخلی مناسب در محیط‌های اطلاعاتی (که بسیاری از عملیات در آن‌ها به شکل خودکار انجام می‌شوند) هستند، بلکه به طور مستقل، ردگیری کنترل‌ها را به ویژه برای کاربردها و رویدادهای حساس انجام می‌دهند. مواردی که ردگیری تراکنش برای آن‌ها صورت می‌گیرد، به شرح ذیل هستند:

شروع بهره برداری و تغییر در استفاده؛

هرنوع تراکنش اطلاعاتی؛

هر نوع تقاضای صورت گرفته از جانب کاربران برای کاهش محدودیت‌ها و افزایش اختیارات او؛

هر نوع درخواست برای تغییر و یا ابطال حقوق و یا مجوزهای دسترسی به سیستم.

۳-۴-۲-۷- اصل دهم حفظ محرمانگی اطلاعات:

در جهت حفظ محرمانگی اطلاعات کلیدی و مهم سیستم بایستی اقدامات مناسب انجام شود. هم‌چنین میزان محرمانگی اطلاعات بر حسب میزان حساسیت آن‌ها تعیین می‌شود.

اطمینان از خصوصی و محرمانه ماندن اطلاعات مهم و عدم افشای آن توسط هر نوع عامل غیرمجاز، محرمانگی نامیده می‌شود. هر نوع سوء استفاده و یا افشای غیرمجاز اطلاعات، باعث می‌شود که ریسک حقوقی وریسک حیثیت به وجود آید. زمانی از حفظ محرمانگی، اطمینان حاصل می‌شود که موارد زیر تحقق یابند:

داده‌های محرمانه تنها به وسیله افراد، سیستم‌ها و یا عوامل مجاز و احراز هویت شده مورد دسترسی قرار گیرند.

نگهداری تمامی داده‌های محرمانه ، به شکل امن انجام شده و از هر نوع مشاهده و یا تغییر غیرمجاز داده‌ها در زمان انتقال در شبکه‌های عمومی و یا خصوصی محافظت شود.

کنترل‌ها و استانداردهای تعیین شده برای حفاظت و استفاده از داده‌ها در زمانی که عوامل بخش سوم (ازطریق ارتباط با سازمان) به داده‌ها دسترسی حاصل می‌کنند نیز به کار گرفته شوند.

تمامی دسترسی‌های محدوده انجام شده، ثبت شده و تلاش‌های لازم برای جلوگیری از هر نوع دسترسی غیرمجاز و انجام تغییرات در اطلاعات ثبت شده انجام گیرد.

۳-۴-۳- مدیریت ریسک‌های حقوقی و حیثیت

مقررات و قوانین مربوط به حفظ محرمانگی و حفاظت از داده‌ها و تراکنش‌های مشتریان از یک حوزه قضایی به حوزه دیگر تغییر می‌کند. با این وجود سازمان‌ها مسئولیت دارند تا به نحو مناسب از افشای اطلاعات کاربران جلوگیری کرده و اقدام لازم برای حفاظت از داده‌های آنان را انجام دهند. اصول ۱۱ الی ۱۴ به بررسی سیاست‌ها و ملزومات لازم برای ریسک‌های حقوقی و حیثیت می‌پردازد.

۳-۴-۳-۱- اصل یازدهم بومی‌سازی امنیت :

قبل از هرگونه استفاده از سیستم‌ها باید از میزان بومی‌سازی سخت افزار و نرم افزار مورد استفاده اطمینان لازم را پیدا نمود و این مسئله را مد نظر قرار داد که با عناصر وارداتی امکان تامین امنیت برای سازمان وجود نخواهد داشت.

۳-۴-۳-۲- اصل دوازدهم اقدامات امنیتی سازمان:

اقدامات امنیتی لازم باید از سوی سازمان‌ها برای به وجود آوردن محرمانگی لازم برای کاربران انجام شود.

اصولاً، حفظ محرمانگی اطلاعات کاربران یک وظیفه مهم برای سیستم می‌باشد. برای حصول این امر بایستی موارد زیر در نظر گرفته شود:

سیاست‌های اتخاذ شده برای حفظ محرمانگی مشتریان بایستی مطابق با قوانین و مقررات تعیین شده در قلمرو قضایی باشد.

کاربران بایستی از سیاست‌های محرمانگی و مسائل مرتبط با استفاده از سرویس‌ها در جهت حفظ محرمانگی داده‌های خودآگاهی کافی داشته باشند.

داده‌های کاربران به منظورهایی فراتر از آن‌چه که توافق داشته و اجازه آن را به سیستم داده‌اند، نبایستی مورد استفاده قرار گیرد.

زمانی‌که سیستم با دیگران، ارتباط ایجاد می‌کند در انجام این ارتباطات نباید داده‌های کاربران برخلاف استانداردها و مقررات تعیین شده به وسیله سازمان مورد استفاده واقع شود.

۳-۴-۳-۳- اصل سیزدهم رویدادهای غیرمنتظره:

سیستم باید طرح‌های مدیریتی لازم برای کاهش مسائل حاصل از رویدادهای غیر منتظره شامل حملات داخلی و خارجی را فراهم‌کنند.

برای اطمینان از وجود پاسخ‌های مؤثر سیستم به حوادث غیرقابل پیش‌بینی، بایستی به موارد زیرتوجه داشته باشد:

وجود طرح‌های لازم برای بازیابی سیستم در صورت رویداد هر نوع رویداد غیرمنتظره.

مکانیزم‌هایی برای شناسایی رویدادها به محض رویداد آن‌ها، برخورد با آن‌ها و کنترل ریسک حیثیت که به علت وقوع خرابی‌های احتمالی به وجود می‌آید موجود باشد.

استراتژی ارتباطی لازم برای مواقعی که حملات و یا خرابی در سیستم رخ می‌دهند ضروری است.

تشکیل تیم‌هایی که در مواقع اضطراری، بتوانند اقدامات لازم را برای شناسایی، تحلیل و ارائه‌ی سرویس های لازم انجام دهند.

انجام اقدامات لازم برای آگاه ساختن کاربران درمقابل خرابی‌ها و مشکلات به وجود آمده در سیستم.

۳-۴-۳-۴- اصل چها ردهم روحیه سلطه گری نظام سلطه

نظام سلطه همیشه به دنبال اشرافیت بر اطلاعات و ارتباطات دیگران می باشد تا به این وسیله بتواند اشرافیت همیشگی خود را بر دیگر جوامع و کشورها به صورت مستمر حفظ نماید و در این راه سرمایه گذاری های فراوانی معمول می دارد. از جمله این سرمایه گذاری ها می توان به طرح اشلون اشاره نمود که در آن کشورهای سلطه گر از جمله انگلیس و امریکا با کمک گرفتن از دیگر کشورها از شصت سال تاکنون با سرمایه گذاری های مادی و معنوی و به کارگیری حدود سیصد هزار کارمند به دنبال اشرافیت روزانه بر سه میلیارد تعامل اطلاعاتی می باشند و برای گسترش طرح خود سه مثلث شوم اشلون و سیستم های هوشمند و نظام های سلطه گر را به هم پیوند داده و با طراحی سیستم های مورد نیاز کشورهای در حال توسعه و قرار دادن سیستم های مدیریت راهبردی پنهان بر روی آن و فروش به دیگر کشورها , در زمان های حساس و مورد نیاز کنترل سیستم های اطلاعاتی و ارتباطی آن کشورها را به دست گرفته و عملا آنها را در مقابله با نظام های سلطه گر فلج می نمایند و به نوعی استعماری نو در این رابطه را قلم زده اند.

۳-۵- سیاست‌های اجزای سیستم

سیاست امنیتی، یک حکم درباره‌ی استراتژی مدیریت با توجه به امنیت می‌باشد. بیانیه‌های مربوط به سیاست، به عناوین زیر دسته‌بندی می‌شوند:

سیاست سازمان

سیاست امنیت اطلاعات

سیاست امنیت کارکنان

سیاست امنیت فیزیکی و محیطی

سیاست امنیت کامپیوترها و شبکه

مدیریت سیستم

سیاست شبکه

سیاست توسعه‌ی برنامه‌های کاربردی

پیاده‌سازی مؤفق امنیت اطلاعات به موارد زیر بستگی دارد:

اهداف و فعالیت‌های امنیتی باید برمبنای اهداف و نیازمندی‌های سازمان باشند و توسط مدیریت سیستم هدایت شوند.

باید پشیبانی و تعهد روشنی از جانب مدیریت مافوق وجود داشته باشد.

باید درک روشنی از ریسک‌های امنیتی (تهدیدات و آسیب‌پذیری‌های) مربوط به اموال سازمان و نیز سطح ایمنی درون سازمان وجود داشته باشد.

امنیت باید به‌صورت مؤثر به کلیه‌ی مدیران و کارمندان ارائه شود.

باید رهنمودهای جامع درباره‌ی سیاست و استانداردهای امنیت در میان کلیه‌ی کارمندان و پیمان‌کاران توزیع شود.

۳-۵-۱- سیاست سازمان

هر واحد مسئول ایجاد سیاست امنیتی خودش می‌باشد. این سیاست باید قواعدی را برای حفاظت داده ها و فرآیندهای تجاری مطابق با تهدیدها و ریسک‌های موجود و ارزش این اموال تعیین نماید. کلیه‌ی داده‌ها باید براساس رده‌های حساسیت موجود در سازمان، برچسب‌گذاری شوند.

۳-۵-۲- سیاست امنیت اطلاعات

برای کلیه‌ی دارایی‌های اطلاعاتی عمده باید دارنده یا مالک وجود داشته باشد.

دارنده‌ی اطلاعات باید براساس مسئولیت‌های قانونی، ارزش، سیاست سازمان و نیازهای تجاری، آن‌ها را در یکی از سطوح حساسیت قرار دهد. او مسئول حفاظت از این اطلاعات است.

دارنده‌ی اطلاعات باید افرادی را که مجاز به دسترسی به داده‌ها هستند مشخص نماید.

دارنده‌ی اطلاعات مسئول آن‌ها است و باید آن‌ها را امن نگه دارد.

۳-۵-۳- سیاست امنیت کارکنان

کاربران به‌عنوان یکی از عوامل مهم در سیستم، نقش عمده‌ای در برآورده کردن شرایط امنیتی دارند.

۳-۵-۳-۱- اصول اخلاقی

کاربران مجاز به انجام این کارها نیستند:

به اشتراک گذاشتن نام‌کاربر یا کلمات رمز با دوستان یا وابستگان،

اجرای بوکش[۱] های شبکه،

سوءاستفاده از منابع سیستم،

---

۱ sniffer

سوءاستفاده از نامه‌های الکترونیکی،

مزاحمت برای سرویس‌ها،

کاوش در فایل‌های سایر کاربران بدون اخذ اجازه از آن‌ها،

بارگذاری فایل‌های باینری و کپی کردن نرم‌افزارهای بدون مجوز.

۳-۵-۴-سیاست کلمات عبور

ترکیب نام‌کاربر و کلمه‌ی عبور، روشی برای شناسایی موجودیت کاربران در یک سیستم است. اتخاذ یک سیاست خوب برای کلمات عبور، مهم‌ترین مانع در مقابل دسترسی‌های غیرمجاز به سیستم می‌باشد. ویژگی‌های یک کلمه‌ی عبور مناسب عبارتند از:

ترکیبی از اعداد، حروف بزرگ، حروف کوچک و سمبل‌های نقطه‌گذاری باشد.

به‌خاطر سپردن آن آسان باشد.

حدس زدن آن مشکل باشد.

تایپ کردن آن با سرعت انجام شود.

تعداد کاراکترهای آن از ۷ کاراکتر کمتر نباشد.

رهنمودها

کلمه‌ی عبور را جایی ننویسید یا از طریق پست الکترونیکی ارسال نکنید.

از کلمات عبور پیش‌فرض استفاده نکنید.

کلمه‌ی عبورتان را به دیگران ندهید.

چنان‌چه کلمات عبور فاش شدند، آن‌ها را بلافاصله تغییر دهید.

از کلمه‌ی عبور مدیر سیستم به‌صورت مشترک استفاده نکنید.

در صورت امکان، سعی کنید برای یک کاربر از یک کلمه‌ی عبور یکسان برروی سکوهای مختلف استفاده کنید. چنان‌چه کاربر فقط مجبور به حفظ‌کردن یک کلمه‌ی عبور باشد، احتمالا کلمه‌ی عبور به‌تری را انتخاب خواهد نمود.

خطرات رمزشکنی های غیرمجاز۱ را به کاربران تذکر دهید.

کلیه‌ی کلمات عبور پیش‌فرض که توسط فروشنده تعیین شده‌اند، باید قبل از استفاده‌ی سیستم تغییر یابند.

کلمات عبور باید به شکل رمزشده ذخیره شوند. روش رمزنگاری باید مقاوم باشد و امکان حمله‌ی جامع۲ به آن وجود نداشته باشد.

کلمات عبور نباید در زمانی که تایپ می‌شوند، قابل دیدن باشند. حتی نمایش کاراکتر "*" به‌ازای هر کاراکتر از کلمه‌ی عبور، کار درستی نیست.

یک کاربر نباید قادر به خواندن کلمات عبور سایر کاربران از فایل کلمات عبور باشد.

از گنجاندن کلمات عبور به‌صورت آشکار در نرم‌افزار باید به‌هر قیمتی پرهیز شود. حتی کلمات عبور رمزشده هم بهتر است در نرم‌افزار گنجانده نشوند.

برای یک کلمه‌ی عبور یک کاربر باید ویژگی‌های "حداقل عمر"، "حداکثر عمر"، حداقل طول" و "لیست سوابق" مشخص شوند. منظور از "لیست سوابق"، کلمات عبور قبلی کاربر است. برای ایمنی بیش‌تر می‌توان استفاده از یک تعداد مشخص از کلمات عبور قبلی را ممنوع کرد.

---

۱ crack

۲ Brute-force

سیستم باید قبل از پذیرش کلمه‌ی عبور، محتویات آن را مورد بررسی قرار دهد و از تطبیق آن با قواعد فوق اطمینان حاصل کند.

کاربران نباید قادر به تغییر کلمات عبور سایر کاربران باشند.

در صورت امکان، تغییر کلمات عبور را در اولین ارتباط، الزامی کنید.

استفاده از روش‌های تصدیق دیگر مانند روش‌های بیومتریک را هم در نظر بگیرید.

در صورت امکان، تولید کلمه‌ی عبور اتوماتیک را که به‌منظور کمک به کاربر انجام می‌شود غیرفعال نمایید.

۳-۵-۵- شبکه‌ها

اطلاعات محرمانه

داده‌های محرمانه قبل از ارسال از طریق شبکه‌های عمومی باید رمز شوند.

اتصال به شبکه‌ها

یک کاربر نباید به ماشین‌های موجود در شبکه‌های خارج از شبکه‌ی محلی سازمان متصل شود.

دست‌رسی به شبکه‌های خارجی (عمومی و خصوصی) اگر الزامی‌باشد , باید از طریق دیواره‌ی آتش انجام پذیرند. کلیه‌ی دیواره‌های آتش باید تحت قواعد امنیتی سازمان نصب و نگهداری شوند.

مودم‌ها

کاربران نباید برروی ماشین‌هایشان از مودم استفاده کنند.

دست‌رسی dial-in به شبکه‌ی محلی سازمان فقط برای کاربران مشخصی مجاز است. کلیه‌ی دسترسی های dial-in باید از طریق سرویس‌دهنده‌های امن با مکانیزم کلمه‌ی عبور یک‌بار مصرف۱ صورت پذیرد.

۳-۵-۶- اینترنت

در محیط‌های تجاری امروزی، اتصال به اینترنت به یک فرآیند طبیعی تبدیل شده است. به‌دلیل فقدان ساختار و کنترل در اینترنت، استفاده از آن ریسک‌های بسیاری را به‌دنبال دارد:

افشای اطلاعات محرمانه

امکان نفوذ هکرها از طریق اینترنت به شبکه‌ی سازمان

امکان تغییر یا حذف اطلاعات

عدم امکان دست‌رسی به سیستم‌ها به‌دلیل بار اضافی آن.

چنان‌چه کاربران مجاز به دست‌رسی به اینترنت باشند، باید از ریسک‌های مربوط به آن و نیز سیاست سازمان در مورد استفاده از اینترنت آگاه باشند. یک سیاست اینترنت مشخص باید وجود داشته باشد و اجرا شود.

کلیه‌ی دسترسی‌ها به خارج از شبکه‌ی سازمان باید از طریق دروازه های اطلاعات۲ سازمان و مجزا از شبکه داخلی سازمان مورد تایید قرار گیرند.

چه کسانی مجاز به استفاده از اینترنت هستند؟

چه کسانی مجاز به استفاده از پست الکترونیکی هستند؟

---

۱ one-time password

۲ gateway

چه زمان‌هایی دست‌رسی به اینترنت مجاز نمی‌باشد؟

از امکانات اینترنت برای چه مواردی نمی‌توان استفاده کرد؟

چه کسانی سرویس‌های اینترنت را ارائه می‌دهند؟ تحت چه شرایطی؟

۳-۵-۷- رایانه‌های قابل‌حمل[۱]

رایانه‌های قابل‌حمل به افراد امکان می‌دهند تا بیش‌تر مولد باشند. اما از نقطه‌نظر امنیت، این رایانه‌ها عامل ریسک‌هایی مانند افشاء، دزدی و ارائه‌ی یک نقطه‌ی دست‌رسی غیرمجاز به شبکه‌ی سازمان هستند. ازطرفی، محاسبات سیار[۲] در حال رشد است و اتخاذ یک سیاست ویژه ضروری می‌باشد. سیاست‌های ممکن عبارتند از:

آیا رایانه‌های قابل‌حمل توسط کارکنان متخصص فن آوری اطلاعات آماده و راه‌اندازی شده است.

در صورت امکان، از یک برنامه‌ی رمزنگاری پیشرفته اما ساده، برای رمزکردن فایل‌ها استفاده کنید.

در صورتی که یک کاربر عادی نباید به سیستم دست‌رسی کامل داشته باشد، از یک سیستم‌عامل مانند UNIX یا NT استفاده کنید.

کاربران در خارج از ساختمان سازمان، مسئول رایانه‌های قابل‌حمل خود هستند.

مکانیزم‌های قفل‌کردن اتوماتیک صفحه‌ی نمایش و نیز کلمه‌ی عبور برای بوت‌کردن سیستم باید مورد استفاده قرار گیرند.

یک ویروس‌یاب باید برروی سیستم نصب شود.

---

۱ laptop

۲ mobile computing

حمل‌ونقل رایانه‌های کیفی در مکان‌های عمومی باید با استفاده از کیف‌های دستی معمولی صورت پذیرد.

داده‌های طبقه بندی شده نباید با استفاده از رایانه‌های قابل‌حمل انتقال یابند مگر این‌که رمز شده باشند.

در زمان عدم استفاده از رایانه آن را خاموش کنید.

۳-۵-۸-سیاست رایانه و شبکه

در این بخش به معرفی سیاست‌های مربوط به رایانه و شبکه می‌پردازیم.

۳-۵-۸-۱- سیاست مدیریت سیستم

مدیر سیستم باید مطمئن باشد که سیستم‌ها در زمان لازم قابل استفاده‌اند، اطلاعات محرمانه تنها برای افراد دارای مجوز قابل دسترسی‌اند و اطلاعات نباید بدون مجوز تغییر یابند. موارد زیر باید تعریف شوند:

چه کسی سیاست‌های مدیریتی را اصلاح می‌کند؟

چه کسی دارای مجوز برای تایید دست‌رسی و تصویب استفاده است؟ چه کسی می‌تواند امتیازات مدیر سیستم را داشته باشد؟

حقوق و مسئولیت‌های مدیر سیستم چیست؟

آیا کاربران دارای دست‌رسی در سطح مدیر سیستم به ایستگاه‌های کاری خود هستند؟

۳-۵-۸-۱-۱-امنیت فیزیکی

یک سند برای سیاست امنیت فیزیکی باید وضع شود که معیارهای مربوط به حفاظت ساختمان‌ها را با توجه به حوادث بد (مانند طوفان، آتش‌سوزی، زلزله، انفجار و قطع برق)، دزدی، کنترل دسترسی، گاوصندوق‌ها، اتاق رایانه‌ها و جعبه‌های سیم‌کشی با جزییات مشخص نماید.

تعریف نواحی الزامی است.

ناحیه‌ی ۱: نواحی باز برای عموم افراد

ناحیه‌ی ۲: نواحی بسته برای عموم افراد و باز برای کارکنان سازمان

ناحیه‌ی ۳: نواحی محافظت شده که تنها با شناسایی قابل دست‌رسی هستند و دست‌رسی به آن‌ها شدیدا کنترل می‌شود.

چه کسی مسئول تخریب دیسک‌های محرمانه‌ی معیوب است؟

چه کسی مسئول تخریب سرویس‌دهنده‌ها، دیسک‌ها و نوارهای مغناطیسی قدیمی است؟

دستوالعمل‌هایی برای اتاق سرویس‌دهنده‌ها تعریف کنید:

کلیه‌ی ابزارهای محاسباتی باید به‌صورت درست نصب و برچسب‌گذاری شوند.

سیم‌کشی باید مرتب و با برچسب‌گذاری انجام شود به‌طوری‌که تخریب یا قطع عمدی اتصالات میسر نباشد.

نقشه محل نصب همه‌ی سرویس‌دهنده‌ها باید در اختیار باشد.

دستورالعمل‌هایی برای انتقال رسانه‌های الکترونیکی (نوارهای مغناطیسی، پشتیبان‌ها، دیسک‌ها و ...) وضع کنید.

۳-۵-۸-۱-۲-کنترل دسترسی

کلیه‌ی کاربران باید دارای مجوز تعریف شده باشند.

کاربران باید قادر به تنظیم امتیازات اشیای متعلق به‌خودشان باشند.

کاربران باید از حذف فایل‌های سایر کاربران در دایرکتوری‌های مشترک منع شوند.

کنترل دست‌رسی کاربر به کلیه‌ی اشیای سیستم (فایل‌ها، چاپگرها، ابزارها، پایگاه‌های داده، فرآمین، برنامه‌های کاربردی و ...) باید براساس یک سیاست مشخص صورت گیرد.

کاربران نباید قادر به بررسی کنترل دست‌رسی واگذار شده به سایر کاربران باشند.

طبقه‌بندی داده‌ها در رده‌های مختلف طبقه بندی باید امکان‌پذیر باشد.

کنترل دست‌رسی اجباری باید تدارک دیده شود.

۳-۵-۸-۱-۳- سیاست logon

اصل اساسی: به یک کاربر، کمترین امتیازات و کوتاه‌ترین زمان لازم برای انجام کارهایش را بدهید.

Accountها فقط باید برای افراد دارای مجوز صادر شوند.

هر کاربر باید با یک نام یا شماره، شناسایی شود و به یک گروه تعلق داشته باشد.

ساختار مورد استفاده برای نام کاربر و نام گروه باید از استاندارد مشخصی پیروی کند.

کاربران و گروه‌ها باید توسط مدیر سیستم مدیریت شوند نه توسط خودشان.

شناسه‌های گروهی نباید استفاده شوند.

هر کاربر باید تنها یک شناسه در سیستم داشته باشد.

شناسه‌های میهمان[۱] نباید استفاده شوند.

در صورت انتقال یک کاربر یا خاتمه‌ی کار وی، شناسه‌ی او باید بلافاصله بلوک یا حذف شود.

حداکثر بعد از ۱۵ دقیقه بیکار بودن سیستم، باید صفحه‌ی نمایش قفل شده و برای ورود مجدد به سیستم، کلمه‌ی عبور لازم باشد.

در مورد اعمالی که امنیت را نقض می‌کنند، باید به کاربران هشدار داده شود.

چنان‌چه استفاده از یک شناسه برای ورود به سیستم در مدت زمان کوتاهی دچار مشکل شود (مثلا ۵ بار تلاش در ۱ ساعت)، باید آن را بلوک و کاربر را مطلع کنیم.

هنگامی که یک کاربر به سیستم متصل می‌شود، موارد زیر باید به وی نمایش داده شوند:

یک اخطار قانونی برای آگاه ساختن کاربر از استفاده‌ی نادرست از سیستم

---

۱ guest accounts

زمان آخرین login مؤفق و نامؤفق.

login کردن فقط باید در زمان‌های لازم امکان‌پذیر باشد (مثلا، ۶ صبح تا ۱۰ شب روزهای غیر تعطیل)

در سیستم‌های dial-up بعد از چندبار تلاش نامؤفق برای login، تلفن را قطع کنید.

اگر یک کاربر، "نام کاربر" یا "کلمه‌ی عبور" را اشتباه وارد کرد، نباید از پیغام‌های جداگانه برای اطلاع دادن به وی استفاده شود.

در صورتی که ترکیب نام‌کاربر/کلمه‌ی عبور را اشتباه وارد کرد، قبل از شروع دومین login، ۱ ثانیه تاخیر ایجاد کنید. چنان‌چه این مورد تکرار شد، هربار تاخیر را اضافه کنید تا از فعالیت برنامه‌های حمله کننده جلوگیری شود.

اعضای گروه مدیران سیستم باید از جانب مدیر انتخاب شوند.

باید روشی برای محدود کردن تعداد نشست هایی[۱] که یک کاربر می‌تواند به‌طور همزمان ایجاد نماید، وجود داشته باشد.

باید روشی برای تنظیم تاریخ انقضای شناسه‌های کاربران وجود داشته باشد.

۳-۵-۸-۱-۴- اطمینان

ممیزی‌ها باید به‌صورت منظم برروی سیستم اجرا شوند

سرویس‌دهنده‌های جدید برای مدیر سیستم نصب و آماده‌سازی می‌شوند. در این‌صورت، لازم است که کادر امنیت شبکه سازمان، آن‌ها را مطابق با یکی از رده‌های حساسیت، ممیزی و تایید کنند.

۳-۵-۸-۱-۵- پاسخ‌گویی و ممیزی

---

۱ session

فایل‌های ثبت رد ممیزی۱ و برنامه‌ها باید محافظت شوند. آن‌ها باید تنها توسط کادر امنیت شبکه قابل دسترس باشند.

فایل‌های ثبت باید شامل کلمات عبور باشند.

فعالیت‌های مدیر سیستم باید ثبت شوند.

تلاش‌های نامؤفق برای login باید ثبت شوند.

رویدادهای مهم باید به‌صورت اتوماتیک یک اعلان هشدار تولید نمایند.

باید امکان مشخص کردن نحوه‌ی ممیزی براساس موضوع یا شیء وجود داشته باشد.

هر مدخل در فایل ثبت ممیزی حداقل باید شامل این موارد باشد: نام‌کاربر، تاریخ و ساعت، شناسه‌ی ترمینال، درجه‌ی خطا (مؤفقیت یا شکست) و شرح رویداد.

در صورت امکان، فایل‌های ثبت باید برروی رسانه‌ی "فقط‌خواندنی" (کاغذ یا CDROM) نگهداری شوند. هم‌چنین، به‌تر است به‌جای نگهداری فایل‌های ثبت در ماشین‌های محلی، آن‌ها را به یک ماشین امن منتقل کنیم.

کلیه‌ی ماشین‌ها باید از ساعت همگام با بقیه استفاده کنند تا مُهرهای زمانی۲ مربوط به فایل ثبت ممیزی معتبر باشند.

۳-۵-۸-۱-۶- قابلیت اطمینان سرویس

سیاست پشتیبان‌گیری و بازیابی

پشتیبان‌ها باید به‌صورت منظم تهیه شوند.

---

۱ audit trail logs

۲ timestamps

هرچند وقت یک‌بار، باید پشتیبان‌ها را به مکانی خارج از سایت منتقل نمود.

پشتیبان‌های طبقه بندی شده باید در گاوصندوق‌های قفل‌شده نگهداری شوند. رسانه‌های قدیمی باید از بین بروند نه این‌که آن‌ها را دور بیندازیم.

برای هرسیستم یا گروهی از سیستم‌ها، باید یک سیاست پشتیبان‌گیری مستند شامل موارد زیر موجود باشد:

فاصله‌ی زمانی تهیه‌ی پشتیبان‌ها

نوع پشتیبان (افزایشی یا کامل)

مکان نگهداری رسانه‌های پشتیبان

مدت نگهداری رسانه‌های پشتیبان

چه کسی مسئول کنترل عملکرد درست پشتیبان‌ها است؟

یک سیاست بازیابی، شامل موارد زیر، باید موجود باشد:

چه کسی مسئول بررسی عملکرد درست است؟

یک شرح مفصل از برنامه‌هایی که استفاده می‌شوند و نیز نحوه‌ی بازیابی داده‌ها

یک شرح مفصل از نحوه‌ی بازیابی سیستم‌عامل بعد از خرابی دیسک یا سایر قسمت‌های سیستم

سیاست بازیابی را به‌صورت منظم مورد آزمایش قرار دهید.

مدیریت تغییرات (نصب یا به‌روزرسانی نرم‌افزار/سخت‌افزار)

تنها مدیران سیستم باید قادر به نصب نرم‌افزار برروی سرویس‌دهنده‌ها باشند. کاربران نباید بتوانند بر روی ایستگاه‌های کاری طبقه بندی شده نرم‌افزار نصب کنند.

سیستم‌ها باید براساس دستوالعمل‌های از پیش تعریف شده، به‌صورت مرتب و درست نصب شوند.

در هر سرویس‌دهنده باید یک فایل ثبت تغییرات وجود داشته باشد که کلیه‌ی تغییرات ایجاد شده در سیستم را به‌صورت مفصل نگه‌داری کند.

نصب سیستم عامل باید شامل نصب کلیه‌ی patchهای آن نیز باشد.

یک برچسب شامل اطلاعات زیر باید برروی کلیه‌ی ماشین‌ها چسبانده شود: نام ماشین، نام سازنده‌ی و مدل ماشین، آدرس IP، آدرس MAC، تاریخ پایان گارانتی و شماره‌ی تلفن بخش امداد و امنیت.

برای سرویس‌دهنده‌ها باید اطلاعات زیر هم اضافه شود: نام سرویس‌دهنده برروی کلیه‌ی ابزارهای جانبی، نوع/ تاریخ گارانتی/ پیکربندی دیسک، دستورات کنسول برای توقف یا راه‌اندازی مجدد.

تنها از patchهای فروشنده‌ی اصلی نرم‌افزار استفاده شود.

۳-۵-۸-۲- سیاست شبکه

انتقال اطلاعات میان رایانه‌ها می‌تواند یک تهدید بزرگ برای امنیت ایجاد نماید.

۳-۵-۸-۲-۱- سیاست سیستم‌های شبکه‌ای/توزیعی

اطمینان: پیکربندی شبکه باید مستند باشد.

شناسایی و تصدیق اصالت

باید راهی برای شناسایی و تصدیق هر موضوعی در شبکه‌ی سازمان وجود داشته باشد.

در صورت امکان، باید یک مکانیزم واحد برای logon کردن کاربران به سیستم‌ها و برنامه‌های کاربردی متفاوت موجود باشد.

۳-۵-۸-۲-۲- پاسخ‌گویی و ممیزی

کاربران مسئول و پاسخ‌گوی اعمال خودشان هستند. آن‌ها باید از سیاست کاربران شبکه مطلع باشند.

نودهای مهم شبکه باید فعالیت‌ها را ثبت کنند. این نودها باید به‌طور منظم برای رخنه‌های امنیتی مورد بررسی قرار گیرند.

لیست‌های کنترل دسترسی[۱] برای فیلترهای مهم باید هر ۶ ماه یک‌بار ممیزی شوند.

۳-۵-۸-۲-۳- کنترل دسترسی

پیکربندی نودهای حساس شبکه: سرویس‌های غیرضروری شبکه باید غیرفعال شوند. سرویس‌های شبکه باید به‌صورت محدود پیکربندی شوند.

---

۱ access control list

شبکه‌های موجود باید با برچسب‌های "دست‌رسی باز"، "دست‌رسی محدود" و "دست‌رسی خیلی محدود" مشخص شوند تا کاربران و صاحبان داده‌ها از نوع حفاظت ارائه شده مطلع شوند.

در صورتی‌که به شبکه‌های با دست‌رسی محدود نیاز است، کابل‌های شبکه نباید از مکان‌های عمومی عبور کنند. این کابل‌ها باید از داخل لوله گذرانده شوند. در صورت کابل‌گذاری توسط افراد خارجی، حتما آن را وارسی کنید.

۳-۵-۸-۲-۴- درستی[۱]:

نودهای مهم شبکه باید تمامیت داده‌های خود را به‌طور منظم کنترل نمایند.

۳-۵-۸-۲-۵- تبادل داده‌ها

اطلاعات محرمانه باید تنها از طریق مکانیزم‌های انتقال تاییدشده ارسال شوند.

اطلاعات مربوط به login (مثلا نام کاربر و کلمه‌ی عبور) نباید به صورت واضح از طریق شبکه ارسال شوند.

شبکه‌ها باید در مقابل شنود[۲] محافظت شوند.

هنگام تبادل اطلاعات، موجودیت فرستنده یا گیرنده باید به اطلاعات ضمیمه شود.

داده‌های طبقه بندی شده نباید برای کاربران بدون‌مجوز یا سیستم‌هایی که در رده‌های پایین قرار دارند ارسال شود.

۳-۵-۸-۲-۶- قابلیت اطمینان سرویس / قابلیت دسترسی

---

۱ accuracy

۲ eavesdropping

شبکه در ۲۴ ساعت شبانه‌روز و ۷ روز هفته موردنیاز است. نگهداری در روز چهارشنبه ساعت ۱۸ تا ۲۲؛ حداکثر زمان کارنکردن سیستم در ساعات اداری باید ۱ ساعت باشد و این رویداد هر ۲ ماه بیش از یک‌بار اتفاق نیفتد.

شبکه باید برای خطاها و مشکلات کارایی مورد نظارت قرار گیرد. عملیات پیش‌گیرانه باید قبل از قطعی های جدی در شبکه صورت گیرد.

مدیریت تغییرات: به‌روزرسانی‌ها و تغییرات پیکربندی‌ها باید ثبت شوند.

۳-۵-۹- سیاست توسعه‌ی نرم‌افزار

امنیت باید یک بخش مجتمع در سیستم‌های جدید باشد. هنگامی‌که نیازهای عملیاتی طراحی می شوند، نیازهای امنیتی نیز باید متناظر با حساسیت و قابلیت دست‌رسی داده‌هایی که قرار است توسط سیستم استفاده شوند، تنظیم گردند.

رهنمودهای کلی

محیط و داده‌های مجزا برای توسعه و تولید

در نظر گرفتن امنیت به‌عنوان یک بخش مجتمع در توسعه‌ی برنامه‌های کاربردی

داده‌های آزمایشی نباید شامل اطلاعات محرمانه باشند.

استفاده از زبان‌های برنامه نویسی دارای ویژگی‌های امنیتی به‌جای زبان‌های معمولی

۳-۶- سئوالات خودآزمایی

عوامل لازم برای برقراری یک محیط ایمن را نام برده و توضیح دهید.

چرخه برنامه ریزی استراتژیک امنیت را نام برده و توضیح دهید.

ویژگی های یک سیاست امنیتی خوب را بنویسید.

استراتژی های طراحی سیاست امنیتی را بنویسید.

چهار اصل از اصول نظارت مدیریتی بر امنیت را نوشته و توضیح دهید.

سیاست امنیتی حاکم بر استفاده از اینترنت در یک سازمان را بنویسید.

سیاست امنیتی حاکم بر استفاده از کامپیوترهای قابل حمل توسط کارمندان را بنویسید.

در رابطه با امنیت فیزیکی چه سیاست های کلی باید رعایت شوند . نام برده و توضیح دهید.

۴

فصل چهارم: تحلیل مخاطرات و حفاظ‌های امنیتی

آن چه در این فصل می خوانید

مراحل مدیریت مخاطرات

شناسایی حفاظ‌های موجود و در دست اقدام

ارزیابی مخاطرات

ارائه راهکارهای مقابله با مخاطرات

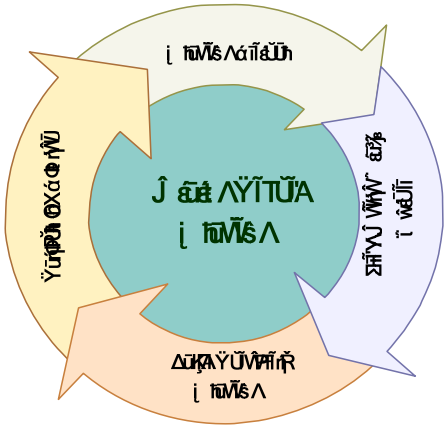
حفاظ‌های امنیتی و سیاست‌های آن‌ها

امنیت فیزیکی

تعیین هویت و تصدیق اصالت (I & A)

۴- تحلیل مخاطرات و حفاظ‌های امنیتی

تحلیل و مدیریت مخاطرات[۱] یکی از فعالیت‌های مهم در طراحی امنیت محسوب می‌شود. مدیریت مخاطرات دارای چرخه‌ای است که برای ادامه بقای یک سیستم امنیتی باید مرتباً و در طول حیات سازمان تکرار شود. به این معنا که در مرحله اول مخاطرات سازمان به گونه‌ای که در ادامه خواهیم دید ارزیابی و تحلیل می‌شوند، سپس برای هر مخاطره یا ریسک سیاست مقابله‌ای جهت برطرف کردن آن و یا کاستن میزان ضرر مربوطه تعریف و پیاده‌سازی می‌شود، در مرحله بعدی نحوه کارکرد این سیاست کنترلی و میزان تاثیر آن اندازه‌گیری می‌شود تا بر اساس آن مجدداً چرخه مدیریت مخاطرات با خطرات جدید شروع به‌کار نماید.



[۱] Risk Analysis

فرایند مخاطرات(تصویر شماره چهار)

۴-۱- مراحل مدیریت مخاطرات

برای پاسخ‌گویی به این سئوالات تحلیل مخاطرات با قدم‌های زیر مطرح می‌شود:

۴-۱-۱- تعیین منابع و موجودی‌ها

مدیریت مناسب دارایی‌ها در جهت موفقیت سیستم از موارد حیاتی به حساب می‌آید. معمولاً منابع یک سازمان شامل بخش‌های زیر می‌باشند:

سخت‌افزار: ترمینال‌ها، رایانه‌ها، چاپگرها، خطوط ارتباطی، سرورها، مسیریاب‌ها، ...

نرم‌افزار: نرم افزارهای کاربردی، سیستم‌عامل‌ها، برنامه‌های ارتباطی، برنامه‌های سرورها و. ..

داده: داده‌های برخط، داده‌های ذخیره شده، پشتیبان‌ها، ثبت کنترل و دسترسی‌ها، پایگاه داده‌ها. ..

افراد: کادر فنی، کاربران، مشتریان و. ..

مستندات: مستندات، قراردادها، طراحی‌ها، اطلاعات فنی، رویه‌های مدیریتی و. ..

محصولات و سرویس‌ها

هر یک از این منابع ممکن است نیاز به درجات متفاوت حفاظت داشته باشند. مشخصات منابع با در نظر گرفتن ارزش و حساسیت آنان تعیین می‌شود. بعد از تعیین منابع باید آن‌ها را دسته‌بندی کرد.

۴-۱-۲- تعیین خطرات امنیتی ممکن

تهدیدات ممکن است مبدأ طبیعی یا انسانی یا فنی داشته باشند و می‌توانند تصادفی یا عمدی باشند. تمام مبدأهای تهدیدات عمدی و تصادفی باید شناخته شوند و احتمال وقوع آن‌ها تخمین زده شود.

هیچ تهدیدی نباید از قلم بیافتد زیرا این مسأله می‌تواند سبب ضعف یا شکست امنیت سیستم اطلاعاتی گردد. باید به خاطر داشت ناامن‌ترین قسمت هر سیستم ضعیف‌ترین قسمت است.

در رهیافت‌های دستی و در بعضی از ابزارهای خودکار، فرد ارزیاب باید تهدیدات ممکن به سیستم را تعیین کند. از آن‌جا که استانداردی از مجموعه‌ی کامل تهدیدات و آمار آن‌ها وجود ندارد، این مسأله ممکن است نیاز به تلاش قابل ملاحظه‌ای داشته باشد. به‌ترین ابزارهای امنیتی موجود دارای مجموعه‌ی تهدیدات و آمارهای مربوطه‌ی خوبی هستند. استفاده از چنین ابزارهایی مجازاً تضمین می‌کند که حتی المقدور تهدیدی از قلم نخواهد افتاد.

در حقیقت ورودی این مرحله باید از صاحبان یا کاربران دارایی‌ها، کارمندان امور کارگزینی، متخصصان فن آوری اطلاعات و طرح‌ریزی وسایل، و هم‌چنین افرادی که مسئول حفاظت سازمان هستند، بدست آید. سازمان‌های دیگر نظیر گروه‌های حقوقی و ادارات دولتی می‌توانند به‌عنوان مثال با ارائه آمار تهدیدات در این کار کمک خوبی باشند. لیستی از تهدیدات ممکن عمومی برای انجام ارزیابی تهدیدات بسیار مفید خواهد بود. اما جمع‌آوری این اطلاعات بطور مستقل حتی برای ارزیاب‌های ماهر کار کوچکی نیست. هفته‌ها و بلکه ماه‌ها تحقیق و محاسبه لازم است و بدون تعیین اعتبار، نتایج احتمالاً معتبر نخواهند بود. این کار باید طی یک پروژه مجزا و به طور دقیق برای سازمان‌ها صورت گیرد.

بعد از شناسایی مبدأهای تهدید (چه‌کسی و چگونه سبب تهدید می‌شود) و مقصدهای آن (تهدید روی چه اجزایی از سیستم تأثیر می‌گذارد)، لازم است که احتمال وقوع تهدیدات ارزیابی شود. برای محاسبه‌ی این احتمال موارد زیر باید مد نظر قرار گیرد:

فرکانس تهدید (طبق تجربه، آمار و غیره چند وقت یک بار ممکن است تهدید اتفاق بیافتد)، اگر بتوان به آمار اطمینان کرد.

انگیزه، توانایی و فهم لازم، منابع در دسترس مهاجم احتمالی، و آگاهی مهاجم احتمالی از جذابیت و آسیب‌پذیری دارایی‌های سیستم اطلاعاتی،

فاکتورهای جغرافیایی نظیر نزدیکی به کارخانجات شیمیایی یا نفتی، احتمال شرایط آب و هوایی بد و فاکتورهایی که می‌تواند بر خطاهای انسانی یا کارکرد بد تجهیزات اثر داشته باشد، در مورد مبدأهای تهدید تصادفی.

خروجی این مرحله، لیستی از تهدیدات و دارایی‌هایی تحت تأثیر بهمراه اندازه‌های مربوط به احتمال وقوع تهدیدها بر حسب مقیاسی مانند زیاد، متوسط، و کم می‌باشد.

در مورد تهدیدات فنی می‌بایست لیست کاملی از آسیب پذیری های احتمالی که از ناحیه سخت افزار و نرم افزارهای به کار گرفته شده تهیه و دائم آن را به روزرسانی نمود.

۳-۱-۳- استخراج آسیب‌پذیری‌ها

این ارزیابی شامل شناسایی ضعف‌های موجود در محیط فیزیکی، سازمان، روال‌ها، پرسنل، مدیریت فنی و اجرایی، سخت‌افزار، نرم‌افزار یا تجهیزات ارتباطی، که ممکن است توسط یک مبدای تهدید مورد استفاده قرار گیرد و سبب ضرر و زیان به دارایی‌ها و کار سازمان گردد، می‌شود. اگر تهدیدی در مورد یک آسیب‌پذیری وجود نداشته باشد نیازی به پیاده‌سازی حفاظ برای آن وجود ندارد، اما لازم است که شناسایی شود و به منظور تغییرات مورد نظارت قرار گیرد. لازم به ذکر است که حفاظی که اشتباه پیاده شده است یا حفاظی که بد عمل می‌کند یا حفاظی که اشتباه استفاده می‌شوند، می‌توانند سبب آسیب پذیری شوند

در این ارزیابی آسیب‌پذیری‌هایی که ممکن است توسط تهدیدات مورد استفاده قرار گیرند و سادگی بهره‌برداری از آن‌ها شناسایی می‌شود. برای مثال بعضی از دارایی‌ها به راحتی مخفی یا حمل می‌شوند- تمام این خصوصیات می‌توانند به آسیب‌پذیری مربوط باشند. ورودی ارزیابی آسیب‌پذیری‌ها باید از صاحبان یا کاربران دارایی‌ها، متخصصان وسایل و کارشناسان سخت‌افزار و نرم‌افزار سیستم‌ها استفاده شود. مثال‌هایی از آسیب‌پذیری‌ها عبارتند از:

ارتباطات ناامن (برای مثال ارتباطات اینترنتی)

کاربران آموزش‌ندیده

انتخاب و استفاده‌ی غلط از کلمات عبور

کنترل‌های دست‌رسی نامناسب(فیزیکی و منطقی)

تهیه نکردن و نداشتن نسخه‌های پشتیبان از اطلاعات، نرم‌افزارها

قرارگیری در محلی که احتمال سیل در آن زیاد است

به منظور رسیدن به حداکثر سودمندی به‌تر است ارزیابی آسیب‌پذیری به‌صورت مجموعه‌ای از مصاحبه ها با تک‌تک کارمندان مسئول پیاده‌سازی سیاست سازمان می‌باشد. به منظور جامع‌تر و پایدارتر بودن و حداقل شدن میزان ذهنی بودن، تحلیل کمی باید به‌وسیله‌ی مصاحبه‌کننده‌ای انجام شود که مصاحبه شونده‌ها را از طریق مجموعه‌ی مناسبی از سئوالات که با دقت و به‌منظور کشف آسیب‌پذیری‌های مهم طراحی شده‌اند راهنمایی کند.

سادگی بهره‌برداری از هر آسیب‌پذیری باید در ارتباط با هر تهدیدی که ممکن است از آن در موقعیت خاصی بهره‌برداری کند ارزیابی شود. نتیجه‌ی این مرحله لیستی از آسیب‌پذیری‌ها و مقادیری که نشان دهنده‌ی سادگی بهره‌برداری از آن‌ها می باشند، در مقیاسی مانند زیاد، متوسط، و کم خواهد بود.

۴-۲- شناسایی حفاظ‌های موجود و در دست اقدام

در این مرحله باید تمام حفاظ‌های موجود و حفاظ‌هایی که قرار است پیاده شوند، شناسایی شوند تا از هزینه و کار غیرضروری مثلاً تکرار حفاظ‌ها جلوگیری شود. هم‌چنین به‌تر است توجیه حفاظ‌های موجود و در دست اقدام نیز ارائه شود. اگر توجیهی برای حفاظی وجود ندارد باید در مورد حذف آن، جای‌گزینی آن با حفاظ مناسب‌تر یا باقی‌ماندن آن (برای مثال بدلایل هزینه‌ای) بررسی و تصمیم‌گیری شود.

در واقع بعد از مرحله‌ی انتخاب حفاظ‌ها سازگاری حفاظ‌های موجود و در دست اقدام با حفاظ‌های انتخاب شده باید بررسی شود تا این حفاظ‌ها احیاناً اثر منفی بر یک‌دیگر نداشته باشند. درحین شناسایی حفاظ‌های موجود باید در مورد کارکرد صحیح آن‌ها اطمینان حاصل کرد. حفاظی که به کارکرد صحیح آن اطمینان شده است، اما درست کار نمی‌کند احتمالاً مبدای آسیب‌پذیری خواهد بود

نتیجه‌ی این مرحله لیستی از حفاظ‌های موجود و در دست اقدام و وضعیت پیاده‌سازی و استفاده از آن‌ها خواهد بود.

۴-۳- ارزیابی مخاطرات

هدف این مرحله، شناسایی و ارزیابی مخاطراتی که سیستم فن آوری اطلاعات و دارایی‌هایش با آن مواجه است، به منظور شناسایی و انتخاب حفاظ‌های مناسب و لازم، می‌باشد. مخاطره تابعی از دارایی هایی که با خطر مواجه هستند، احتمال وقوع تهدیداتی که موجب اثرات منفی بر کار سازمان خواهند شد، سادگی استخراج آسیب‌پذیری‌ها به‌وسیله‌ی تهدیدات شناخته شده، و حفاظ‌های موجود و در دست اقدام می‌باشد. روش‌های مختلفی برای مرتبط کردن این فاکتورها و محاسبه‌ی خطرپذیری وجود دارد. مهم این است که روش مورد استفاده قابل تکرار و پیگیری باشد. نتیجه‌ی این مرحله باید لیستی از مقادیر خطرپذیری‌برای تمام تأثیرات افشا، اصلاح، عدم‌دسترس‌پذیری، و خرابی سیستم‌های IT مورد نظر باشد. هم‌چنین، مقادیر خطرپذیری‌ها اولویت رسیدگی به آن‌ها را مشخص می‌کند.

ابزارهای مختلفی برای کمک به انجام اتوماتیک تمام یا بخش‌هایی از فرآیند تحلیل میزان خطرپذیری وجود دارد. اگر سازمانی تصمیم گرفت که از ابزاری استفاده کند باید توجه داشته باشد که رهیافت

به‌کار رفته منطبق و سازگار با سیاست و استراتژی امنیت سازمان باشد. برای نمونه CRAMM[۱] یک روش کیفی برای شناسایی اقدامات متقابل مهم فراهم می‌کند و @Risk یک رهیافت عمومی‌تری است که برای هر تصمیم‌گیری قابل استفاده است. این ابزار توزیع‌های احتمالی را به صفحات گسترده[۲] می افزاید.

مسأله‌ی بسیار مهم دیگر، فراهم کردن اطلاعات ورودی دقیق می‌باشد، زیرا هر ابزاری تا اندازه‌ای که ورودی‌هایش اجازه می‌دهند می‌تواند دقیق باشد. در حال حاضر روش غلط یا درستی وجود ندارد، بلکه آن‌چه مهم است استفاده از روشی است که سازمان با آن راحت‌تر است و به آن اطمینان دارد و نتایج تکرارپذیری فراهم می‌کند.

۴-۴- ارائه راهکارهای مقابله با مخاطرات

در ارائه راهکار باید در مورد منابعی که دارای خطر ارزیابی شده بالایی هستند، توجه و دقت بیش‌تری در طرح مد نظر قرار گرفته شود و بایست در فاز پیاده‌سازی و نگهداری نیز مد نظر قرار گیرد. در جدول زیر (صفحه بعد) لیست راهکارهای مهم و اصلی مقابله با مخاطرات و کدهای تعریف شده برای آن‌ها آورده شده است.

---

۱ CCTA Risk Analysis and Management Model

۲ Spreadsheet

راهکارهای کلی مقابله با مخاطرات
ایجاد و بالا بردن امنیت سیستمی[۱]
استفاده از تجهیزات سوییچ
تعریف لیست کنترل دسترسی (ACL) برای پالایش بسته‌ها[۲]
استفاده از دیواره آتش
تعریف Private VLAN بر روی سوییچ‌ها
سیستم‌های تشخیص نفوذ مبتنی بر میزبان
بهینه‌سازی و به‌روزسازی منابع
فرهنگ‌سازی و آموزش مدیران شبکه و کاربران
محافظت فیزیکی
ترجمان آدرس
پالایش محتوا[۳]

۱ System Security

۲ Packet Filtering

۳ Content Filtering

راهکارهای کلی مقابله با مخاطرات
احراز هویت افراد
استفاده از برنامه‌های ضد ویروس
ایجاد تونل[۱]
غیرفعال‌سازی منابع و امکانات اضافی
رمزنگاری بسته‌ها

جدول مقابله با مخاطرات(تصویر شماره پنج)

۴-۵- حفاظ‌های امنیتی و سیاست‌های آن‌ها

حفاظ: مجموعه روال‌ها یا مکانیزم‌هایی است که وظایف زیر را بر عهده دارند:

محافظت از منابع در برابر خطرات

کاهش نقاط ضعف منابع

محدود کردن تأثیر حوادث ناخواسته

تشخیص حوادث ناخواسته

ایجاد سهولت در امر بازیابی سیستم

---

۱ Tunneling

دلایل استفاده از حفاظ‌ها؛ تشخیص، ممانعت، جلوگیری، محدودیت، اصلاح، باز بینی و اطلاع رسانی می باشد. در ادامه به بررسی حفاظ‌های امنیتی مهم مطرح و مرور برخی از سیاست‌های لازم در آن‌ها می پردازیم.

۴-۶- امنیت فیزیکی

امنیت فیزیکی یکی از جنبه‌های‌بسیار مهمی است که باید در امنیت شبکه‌های‌رایانه‌ای، مد نظر قرار بگیرد.امنیت فیزیکی را باید از دو دیدگاه مد نظر قرار داد: امنیت در برابر نفوذ افراد نامعتبر، امنیت در برابر شرایط اقلیمی و آسیب های ناشی از آن.

۴-۶-۱- کنترل دست‌رسی فیزیکی

کنترل دست‌رسی فیزیکی، دست‌رسی به منابع رایانه‌ای وتجهیزات را محدود می‌کند و سیستم‌ها را در برابر خرابی‌های مختلف و صدمه‌های داخلی و خارجی، تا آن‌جایی‌که ممکن است، محافظت می‌کند. قبل از آنکه هر نوع سیستم کنترلی و امنیتی در یک مکان‌کاری پیاده‌سازی شود، در ابتدا باید سطح امنیتی که سیستم به آن نیاز دارد و برای تجهیزات مختلف مورد بررسی قرار گیرد، پس از آن بخش‌ها از دیدگاه در دسترس عموم بودن تقسیم‌بندی می‌شود: بخش‌های عمومی، بخش‌های در دسترس کارمندان، بخش‌های مراقبت شده، بخش‌هایی که تنها بامجوز قابل دست‌رسی است.

برای پیاده‌سازی کنترل دست‌رسی دو رویکرد وجود دارد: کنترل پیش‌گیرانه و کنترل امنیتی آشکارساز که سعی در تشخیص و تعیین حوادث غیرمترقبه، بعد از رویداد آن دارد. برای یک سیستم امنیتی‌کامل، هر دو نوع سیستم کنترل باید پیاده سازی شوند.

کنترل پیش‌گیرانه: در مورد کنترل پیش‌گیرانه می‌توان به موارد زیر اشاره نمود:

از گاردهای امنیتی[۱] که اغلب در محل ورودی ساختمان‌ها و تجهیزات واقع می‌شوند برای جلوگیری از ورود و خروج افراد و تجهیزات غیر مجاز یا بازرسی و گشت زنی استفاده می‌شود.

---

۱ Security Guards

با ایجاد حصار پیرامون سازمان و ساختمان‌های حساس، می‌توان حداقل از ورود افراد غریبه جلوگیری کرد. این حصارها، باید دارای سیستم‌های هشدار دهنده باشند و یا تحت نظارت مداوم گاردهای امنیتی یا تلویزیون‌های مداربسته قرار داشته باشند.

از کلیدها و قفل‌های رمزدار۲، برای کنترل دست‌رسی به بخش‌های محدود شده استفاده می‌شود.

کنترل دست‌رسی افراد از طرق روش‌های تعیین هویت مانند داشتن کارت مخصوص و یا به صورت بیومتریک و با معیارهایی همچون اثر انگشت، اثر کف دست، صدا، نمونه‌های امضا و مرور عنبیه چشم و DNA افراد استفاده می‌شود.

کنترل امنیتی آشکار ساز: کنترل به روش آشکارسازی، نیازی به انجام روزانه توسط کارمندان ندارد، به عبارتی این سیستم‌ها در حالت نامرئی هستند، تا زمانی که شخص نامعتبر وارد سیستم شده باشد یا حادثه غیر مترقبه‌ای رخ داده باشد و ما نیازمندیم بدانیم چه حادثه‌ای رخ داده است (به کمک سیستم های مراقبتی و هشدار دهنده‌ها). مواردی را که در کنترل امنیتی آشکار ساز می‌توان مد نظر قرار داد عبارتند از:

تشخیص دادن حرکات و جنب و جوش‌ها در سیستم

تشخیص دادن دود وآتش

سیستم‌های مراقبت بصری

هشدار دهنده‌های الکترونیکی.

۴-۶-۲- اعتبار سنجی فیزیکی

هدف از اعتبارسنجی فیزیکی، تعیین اعتبار افراد و دادن مجوز به آن‌ها می‌باشد تا از ورود و دست‌رسی افراد نامعتبر به سازمان و پیامدهای ناشی از آن جلوگیری شود. هر شخص برای دست‌رسی به بخش‌های

---

۲ Cipher lock

محدود شده، باید از یک تست تعیین اعتبار، بگذرد. تست تعیین اعتبار، مجوز عبور برای افراد می‌باشد که می‌تواند شامل کارت‌های ورود (کارت معمولی، کارت تعیین هویت تصویری۱، کارت کدشده نوری۲، کارت نوار مغناطیسی۱، کارت‌های هوشمند)، سیستم علامت۱ یا معیارهای بیومتریک (اثر انگشت، شبکیه یا عنبیه چشم، صدا، چهره افراد، شکل هندسی دست، سیستم DNA و نمونه امضاء) باشد.

۴-۶-۳- منبع تغذیه وقفه ناپذیر۲

منبع تغذیه وقفه ناپذیر، برای محافظت تجهیزات در برابر وقفه‌ها و آسیب‌های الکتریکی، استفاده می شود. از واحدهای UPS کوچک می‌توان برای تجهیزات شبکه استفاده‌کرد، ولی اگر یک سیستم هشداردهنده در شبکه موجود نباشد که قبل از خالی شدن منابع تغذیه اصلی پیغامی مبنی بر جایگزین۲ کردن منابع به کاربرها بدهد، باعث به‌وجود آمدن مشکلاتی در شبکه می‌شود.

با استفاده ازUPS۳ می‌توان مشکل هموار نگه داشتن ولتاژ را برطرف کرد. رایانه‌ها را به UPS وصل می کنند، اگر منبع تغذیه اصلی قطع شود، UPS ولتاژ کافی را برای رایانه‌ها فراهم می‌کند تا کاربرها بتوانند بعد از ذخیره اطلاعات، رایانه‌ها را خاموش کنند. اکثر UPSها، سیگنالی (پیغامی) مبنی بر قطع منبع تغذیه اصلی، به رایانه‌ها می‌فرستند.

۴-۶-۴- سیاست‌های امنیت فیزیکی

---

۱ Photo ID Card

۲ Optical-coded Card

۱ Magnetic Strip card

۱ Badge system

۲ UPS

۲ restore

۳ Uninterruptible Power Supply

بخش‌های مختلف سازمان‌بر حسب موقعیت و میزان امنیت مورد نیاز باید برای جلوگیری از بروز حوادث و کاستن اثرات آن‌ها تمهیداتی بیندیشد. برای این کار داشتن یک طرح مناسب برای دست‌یابی به اطلاعات حساس، حائز اهمیت می‌باشد. سیاست‌های امنیتی لازم جهت برقراری امنیت فیزیکی در سازمان را می‌توان در دسته‌بندی زیر ارائه داد.

۴-۶-۴-۱- محافظت ساختمانی و جلوگیری از دزدی

حفاظ‌های فیزیکی برای حفاظت یک ساختمان شامل کنترل دسترسی‌های فیزیکی، دیوارهای محکم، درها و پنجره‌ها می‌باشد. مناطق امن به همراه ساختمان‌ها باید از دسترسی‌های غیر مجاز، به‌وسیله‌ی کنترل دسترسی‌های فیزیکی، حفاظ‌ها و. .. حفاظت شوند.

ساختمان‌ها، به جز در ساعت‌های کاری باید قفل شده باشند. ساختمان‌ها، خصوصاً اتاق‌های رایانه‌ی و بخش‌های مهم مربوط به سیستم‌ها (اتاق ارتباطات)، باید ۲۴ ساعت تحت نظارت پرسنل امنیتی باشند. اتاق‌های رایانه باید قفل باشند، اگر امکان دارد، این کار باید با کارت‌های الکترونیکی انجام شود. تنها باید تعداد محدودی از کارکنان به این بخش‌ها دسترسی داشته باشند و دسترسی به این بخش‌ها باید بصورت تصویری ضبط و ثبت شود. اطلاعات حساس تنها باید در اختیار کارمندانی قرار بگیرد که نیاز به داشتن آن دارند. در ضبط اطلاعات مربوط به دسترسی باید مواردی از قبیل چه کسی، به چه اطلاعاتی، در چه زمانی، و برای چه مدت ضبط شود.

نگه داشتن لیستی از افرادی که اجازه دسترسی به بخش‌های خاصی مانند اتاقهای رایانه ، اتاق‌های سرور و اتاق ارتباطات دارند، از اهمیت بالایی بر خوردار است. باید مطمئن شد که حداقل جزئیات افرادی که اجازه دسترسی به بخش‌های خاصی را دارند، مانند نام شخص، تاریخ و زمان ورود و خروج ثبت شود.

دسترسی به مناطق خاص و محدود شده، باید مداوماً نظارت شود. روش‌های نظارت می‌تواند شامل: گاردهای امنیتی، سیستم‌های تشخیص الکترونیکی، یا سیستم‌های کنترل دسترسی الکترونیکی با ضبط اطلاعات مبنی بر قابلیت دسترسی به بخش باشد.

تجهیزات موجود در ماجول سرورها، دست‌رسی از راه دور، تجهیزات توزیع و دسترسی، هسته و اینترنت بایست در رک‌های در بسته و در اتاق سرورها به صورت کاملاً امن نگهداری شوند. اتاق سرورها بایست سنسورهای تشخیص دود و کپسول‌های آتش نشانی، سنسورهای تشخیص‌دهنده حرکت نصب شوند. پنجره این اتاق‌ها باید پوشانده شود و درب آهنی و محکم برای آن‌ها سفارش داده شود.

جهت اعمال کنترل بر سرمایه‌ها، همه‌ی اقلام تجهیزات باید دارای شناسه‌ی یکتا باشند و در فهرست اموال ثبت شوند. نگهبانان امنیتی باید به کنترل تجهیزات یا رسانه‌هایی که از اتاق‌ها / فضاها یا ساختمان‌ها بدون اجازه خارج می‌شوند، بپردازند. اطلاعات حساس و نرم افزارهای اختصاصی نگهداری شده روی رسانه‌های قابل حمل (مانند دیسکت و...) باید به‌صورت ویژه ای حفاظت شوند.

تمامی افرادی که اجازه دست‌رسی به بخش‌های محدود شده را دارند، باید به اصطلاح علامت‌گذاری شوند و نیاز به پوششی که شامل علامت دست‌رسی تائید شده می‌باشد، دارند. علامت دست‌رسی باید دارای حداقل اطلاعات از جمله: شماره سریال کنترل علامت که باید مُهر زده باشد، تصویر رنگی از شخص و پیوست خاص بخش محدود شده، باشد.

در سایت‌های مختلف برای نگهداری فیزیکی رایانه‌ها و سایر تجهیزات سخت‌افزاری بایست مسئول سایت وجود داشته باشد.

برای محافظت از نسخه‌های پشتیبان اطلاعات سازمان باید سیاست‌های امنیتی شدیدی جهت جلوگیری از ورود افراد غیر مجاز به محل نگهداری پشتیبان‌ها طراحی نمود.

۴-۶-۴-۲- محافظت در برابر آتش

تجهیزات و فضاهای بسته، باید در برابر گسترش آتش، از جای دیگر در ساختمان، یا نزدیک ساختمان‌ها محافظت شود. خطر آتش در نزدیکی اتاق‌ها/فضاهای قرارگیری تجهیزات باید به حداقل برسد. هم‌چنین باید اتاق‌ها/فضاهای قرارگیری تجهیزات کلیدی و مهم در برابر شروع آتش محافظت شوند. حفاظ‌ها باید شامل ردیاب‌ها، زنگ خطرها و بازدارنده‌های آتش و دود باشند. توجه به این نکته ضروری است که محافظت در برابر آتش، منجر به خسارت از طریق آب یا سایر ابزارهای خاموش کننده‌ی آتش نشود.

باید سنسورهایی برای کنترل دمای اتاق، میزان رطوبت، میزان غبار و گرد و خاک، در مکان‌های مهم نصب شده باشد که گزارش‌های مربوطه را از طریق SNMP[۱] یا SYSLOG[۲] به مسئولین اعلام نماید.

باید از عواملی که می‌تواند باعث بروز آتش شود شامل نگهداری نادرست مواد آتش‌زا، کمبود عایق و روکش روی کابل‌های اصلی و مرکزی، نبود سیستم‌های اعلان خطر به هنگام حریق و... جلوگیری نمود. روش‌هائی که می‌توان برای جلوگیری و کنترل آتش درپیش گرفت شامل نصب دستگاه‌های یابنده‌ی دود نزدیک به سیستم‌ها، نصب سنسورهائی در مجراهای ورودی و خروجی سیستم‌های تهویه، استفاده از آب‌پاش‌های اتوماتیک و کپسول‌های دی‌اکسیدکربن می‌باشد.

۴-۶-۴-۳- محافظت در برابر آب / مایعات

تمهیدات یا امکانات مورد نیاز، در هر فضایی که ممکن است خطر اتفاق افتادن سیل یا چکیدن آب یا دیگر مایعات وجود دارد نباید قرار گیرند. حفاظت مناسب باید در جایی که خطر سیل وجود دارد، اعمال شود.

عواملی که می‌تواند باعث جاری شدن آب به داخل ساختمان‌ها شود شامل باران، قطع و شکستگی در منابع آب، نقص در سیستم‌های آب پاش، خراب‌کاری عمدی در مسیر جریان آب در لوله‌ها و مسدود کردن عمدی آن‌ها و... می‌باشد که باید امکان وجود آن‌ها را به دقت بررسی نموده در صورت امکان آن را برطرف نمود. روش‌هایی که برای پیش‌گیری از نشت آب می‌توان در نظر گرفت شامل نگهداری عایق های ضد آب در کنار تجهیزات رایانه‌ای، نصب سنسورهای حساس به آب روی کف ساختمان و... هستند.

۴-۶-۴-۴- محافظت در برابر حوادث طبیعی

ساختمان‌های محل قرارگیری تجهیزات مهم، باید در برابر رعد و برق محافظت شوند. هم‌چنین خود تجهیزات باید در برابر آثار رعد و برق محافظت شوند. حفاظت در برابر دیگر حوادث طبیعی، با اجتناب

---

۱ Signaling network management protocol

۲ System log

از فضاهایی که مستعد اتفاق افتادن آن حوادث هستند، و با داشتن راهبرد و طرح استمرار تجارت سازمان در محل مناسب قابل اجرا است.

در صورتی که تجهیزات و سیستم‌ها در منطقه زلزله‌خیز واقع شده باشند، باید برای پیش‌گیری از وارد آمدن صدمات ناشی از نوسانات به سیستم‌ها و تجهیزات می‌توان راهکارهای زیر را در پیش گرفت:

تجهیزات و سیستم‌ها در جای خود محکم شده،

ترجیحاً بر روی پایه‌های لاستیکی قرار داده شوند.

از قرار دادن تجهیزات و سیستم‌ها در زیر وسایل سنگین یا در جاهای بلند پرهیز شود.

هم‌چنین از تجهیزات ضد زلزله و نوسان برای رایانه‌ها استفاده گردد.

۴-۶-۴-۵- محافظت از سیم کشی‌ها

سیم کشی‌های متداول ، داده را حمل می‌کند؛ یا سرویس‌های ICT را که باید از قطع، آسیب و بار اضافی، حفاظت شوند، پشتیبانی می‌کند. سیم‌کشی باید به صورت فیزیکی در برابر آسیب‌های عمدی یا غیر عمدی، محافظت شود. دقت در طراحی و توجه به توسعه در آینده، می‌تواند از به‌وجود آمدن مشکلات زیاد، پیش‌گیری کند. هر جایی که ممکن باشد، باید سیم‌کشی‌ها در برابر استراق سمع حفاظت شوند.

کابل‌های فیبرنوری و UTP عبوری از کانال‌ها بایست با دقت انتقال یابند و در لوله‌های PVC قرار گیرند. دست‌رسی به کابل‌های موجود در کانال‌ها توسط افراد عادی نبایست به راحتی امکان‌پذیر باشد. درب کانال‌ها بایست همیشه بسته باشد.

۴-۶-۴-۶- محافظت در مقابل برق

همه‌ی تجهیزات ICT باید در صورت نیاز، در برابر قطع برق محافظت شوند. یک منبع برق مناسب باید تولید برق برای تجهیزات را بدون هیچ‌گونه قطعی، تأمین نماید.

برای سیستم‌های خاص و مهم مثل سیستم‌های تلفنی، رایانه‌های سرور، یا تجهیزاتی که کنترل فرآیند را در صنعت و بیمارستان‌ها بر عهده دارند، از واحدهای UPS برخط که در آن‌ها رابط اصلی بین مصرف کننده‌های توان و منابع تغذیه اصلی UPS بوده، تمامی ولتاژهای مصرف‌کننده‌ها از طریق آن فراهم می شود، استفاده نمود.

سیستم‌های Line-Interactive UPS، به‌ترین نوع برای وضعیت‌هایی است که نوسان منبع، یک رویداد عادی محسوب می‌شود. در این UPS نوسانات می‌تواند به کمک مبدل‌های داخل UPS به جای باتری، کنترل شود. از آن جایی که، این نوع سیستم‌ها، دائماً در تمام مدت زمان کاری، خط منبع را نظارت می‌کنند، و همیشه در حالت آماده‌باش قرار دارند، زمان تبدیل آن، خیلی کم‌تر از سیستم‌های برون خط می‌باشد که در آن‌ها مصرف‌کننده‌های توان، مستقیماً از منابع تغذیه اصلی تغذیه شده، تنها در صورت بروز خرابی، به‌طور اتوماتیک به UPS وصل می‌شوند.

معمولاً در انتخاب UPS، آن چه که پیش‌نهاد می‌شود آن است که گنجایش سیستم UPS، حداقل ۲۵٪ بیش‌تر از کل مجموع نیازهای توان تجهیزات متصل به منبع اصلی باشد. برای نمونه رایانه رومیزی که با توان بین ۱۸۰ تا ۲۸۰ ولت‌آمپر کار می‌کند، نیاز به UPS با توان ۳۰۰ ولت‌آمپر دارد.

بخش‌هایی که در آن‌ها، رایانه‌ها، در یک اتاق قرار دارند، می‌توانند تمامی تجهیزات را به یک UPS مرکزی وصل کنند که این عمل از لحاظ هزینه نیز به صرفه می‌باشد. در هر صورت، هنگامی که تجهیزات در اتاق‌ها و مکان‌های مختلف قرار دارند، منطقی است که از UPS توزیع شده در مکان‌های مناسب، استفاده شود.

۴-۷- تعیین هویت و تصدیق اصالت (I & A)

تعیین هویت روشی است که به‌وسیله آن شخص هویت ادعا شده خویش را برای سیستم، اثبات می‌کند. در تصدیق اصالت، اعتبار این دعوی تصدیق می‌شود. در این کتاب از این دو به نام تشخیص هویت اشاره می‌شود. در عمل تشخیص هویت اولین گام از امنیت است. این فرآیند به سه صورت کلی صورت می پذیرد:

براساس آن‌چه یک فرد می‌داند (کلمه‌ی عبور، شماره شناسایی، کلید رمزنگاری)

آن‌چه یک فرد همراه دارد (کارت ATM، کارت هوشمند)

آن‌چه یک فرد هست (خصوصیات زیستی مانند اثر انگشت، صدا، دست خط)

البته روش‌های تشخیص هویت ترکیبی نیز وجود دارد که از مزایای چندین روش بهره می‌برد.

از مزایای روش اول می‌توان به سادگی، کم هزینه بودن، قابلیت تعویض ساده و امن بودن محل نگهداری آن اشاره کرد و از معایب آن می‌توان از سادگی نفوذ به سیستم، مشکل به خاطر سپردن و فراموش کردن نام برد. علی‌رغم معایب زیاد آن به علت سادگی، پراستفاده‌ترین روش است.

در روش دوم اساس کاربر استفاده از یک کلید است که می‌تواند قفل ساختار اطلاعاتی سیستم را باز کند. این کلید می‌تواند نرم‌افزاری و با کمک تکنولوژی رمزنگاری باشد و یا سخت‌افزاری و با کمک یک نشانه۱ که برای نگهداری فیزیکی اطلاعات سری به کار می‌رود.

از مزایای این روش این که معایب روش فوق را ندارد و از معایب آن این که هزینه نسبتاًبالایی دارد، به سخت‌افزارهای اضافی روی هر رایانه نیاز است و ممکن است گم یا دزدیده شود.

در روش سوم اعتبارسنجی با عنوان بیومتریک شناخته می‌شود و از ویژگی‌های منحصر به فرد هر انسان جهت شناسایی او استفاده می‌کند. از مزایای آن این که امکان به اشتراک‌گذاری، احتمال گم شدن یا فراموش شدن ندارد و از معایب آن این که بسیار پرهزینه بوده احتمال خطای تشخیص رایانه در مورد شباهت‌های زیاد مثل دوقلوها وجود دارد و در صورتی که آن ویژگی بیومتریک در مورد کسی از بین برود (مثلاًانگشت دست او قطع شود) دیگر قادر به کار با سیستم نخواهد بود.

از روش‌های ترکیبی می‌توان به روش استفاده از نشانه۲ و کلمات عبور یک بار مصرف اشاره کرد. در روش کلمات عبور یک بار مصرف۳ کاربر در هر بار ورود به سیستم از کلمه عبور جدیدی استفاده می

---

۱ Token

۲ Token

۳ One-time Password

کند. این کلمه عبور معمولاً به صورت ترکیبی از بعضی پارامترهای تصادفی تولید شده توسط سیستم به همراه کلمه رمزی کاربر ایجاد می‌شود.

۴-۸- سئوالات خودآزمایی

چرخه فازهای مدیریت مخاطرات را نوشته و توضیح دهید.

در تعیین خطرات امنیتی نظرات چه افراد حقیقی و حقوقی را باید مد نظر قرار داد؟چرا؟

راه کارهای کلی مقابله با مخاطرات را نوشته و توضیح دهید.

برای محافظت در برابر حوادث طبیعی چه اقداماتی باید انجام داد؟

انواع تعیین هویت و تصدیق اصالت را در بهره برداری امنیتی نوشته و توضیح دهید.

۵

فصل پنجم: سیاست‌های امنیتی

آن چه در این فصل می‌خوانید

سیاست‌های تشخیص هویت

کنترل دسترسی

رمزنگاری

محافظت از محرمانگی داده‌ها

سیاست‌های رمزنگاری

محافظت در برابر کدهای مخرب

دیواره آتش

سیاست‌های دیواره آتش

سیستم‌های تشخیص نفوذ

سیاست‌های تشخیص نفوذ

۵- سیاست های امنیتی

در هر سازمان به منظور تبیین نظرات حاکمیتی سازمان در رابطه با بایدها و نبایدهایی که می‌بایست توسط مجریان امنیت اطلاعات رعایت شوند سیاست هایی بیان و تصویب می‌گردند که به این سیاست‌ها , سیاست‌های امنیتی گفته می‌شود. در این فصل برخی از این سیاست‌ها مورد بررسی قرار می‌گیرند.

۵-۱- سیاست‌های تشخیص هویت

سازمان باید با توجه به میزان نیاز امنیت برای هر سرویس و منبع اطلاعاتی که ارائه می‌دهد روش مناسب تشخیص هویت کاربران را تعیین کرده، جهت اجرای طرح انتخابی برنامه‌ریزی کند. به عنوان مثال برای دست‌رسی به اطلاعات طبقه بندی شده به‌تر است از تشخیص هویت به صورت بیومتریک برد.

لیست کلیه کاربران مجاز به دست‌رسی به هر منبع تعیین شده باشد و هیچ یک از منابع سازمان نباید بدون تشخیص هویت قابل دست‌رسی باشد.

سازمان باید درخصوص مدیریت رمز عبور کاربران سیاست و دستورالعمل‌هایی تهیه کرده باشد. این سیاست‌ها باید حداقل حاوی مطالب زیر باشد:

استفاده از رمز عبور در سیستم‌عامل ایستگاه‌های کاری و سرورها و تجهیزات شبکه با ذکر حداقل طول آن

استفاده از ترکیب حروف کوچک و بزرگ و اعداد در رمز عبور

تغییر رمز عبور پیش‌فرض کلیه نرم‌افزارها و سخت‌افزارها

عدم استفاده از رمز عبور یکسان در موارد مختلف

سیاست‌هایی برای تغییر دوره‌ای رمز عبور کاربران و مدیران و تعیین حداکثر مدت مجاز آن

حذف Accountهای غیرضروری

۵-۲- کنترل دسترسی[۱]

دست‌رسی به معنای توانایی انجام کاری با یک منبع اطلاعاتی و رایانه‌ای است و کنترل دست‌رسی فرآیندی است که از طریق آن این توانایی فعال یا محدود می‌شود. کنترل دست‌رسی شامل دست‌رسی فیزیکی هم هست که در بخش امنیت فیزیکی به آن پرداختیم. هدف از این کار تأمین محافظت از منابع، با جلوگیری از دست‌رسی غیرمجاز، جامعیت و دسترس‌پذیری با محدود کردن تعداد کاربران و فرآیندها، اطمینان از اطلاعات است.

فرآیند پیاده‌سازی کنترل دست‌رسی شامل تعریف اطلاعات و مجوزهای دست‌رسی به آن اطلاعات و بعد از آن نسبت دادن این مجوزها و اختیارات برای دست‌یابی به داده‌ها به کاربران یا نقش‌های آن‌ها است. به طور کلی مجوز دست‌رسی شامل اجازه خواندن، نوشتن، به‌روزرسانی، ایجاد و حذف است. هم‌چنین مجوزهایی برای شروع یا متوقف کردن یک برنامه یا سرویس و یا دست‌یابی به سیستم‌های دیگر نیز در این دسته قرار می‌گیرد.

کنترل دست‌رسی براساس موارد زیر صورت می‌گیرد:

هویت و شناسه‌های یکتا

نقش‌ها

موقعیت‌های فیزیکی یا منطقی منابع

زمان

تراکنش

محدودیت‌های یک سرویس و حالت‌های مختلف دسترسی

---

۱ Access control

مکانیزم‌های زیادی برای کنترل دسترسی‌های داخلی و خارجی وجود دارد که برخی آن‌ها به صورت زیر است:

کنترل دست‌رسی داخلی: به معنای جداسازی آن‌چه کاربران می‌توانند با منابع سیستم انجام دهند و آن‌چه نمی‌توانند، است که ممکن است از طرق مختلف مانند استفاده از کلمات عبور، رمزنگاری، لیست های کنترل دست‌رسی یا ACLها که لیستی از کاربران و نوع دست‌رسی آن‌هاست، استفاده از اینترفیس های کاربر محدود شده از طریق منوها، منظرهای بانک اطلاعاتی که به کاربر اجازه تقاضای اطلاعات غیرمجاز را نمی‌دهد و برچسب‌های امنیتی[۱] اعمال شود.

کنترل دست‌رسی خارجی: استفاده از تجهیزات حفاظت پورت یا PPD[۲] ، دیواره‌های آتش یا دروازه‌های امن، امنیت فیزیکی، مکانیزم‌های تشخیص هویت ... که در این‌جا منظور از کنترل دسترسی همان نوع اول می‌باشد.

۵-۲-۱- سیاست‌های کنترل دسترسی

هر بخش باید نیازمندی‌های خود را برای کنترل دست‌رسی تعریف و مستندسازی کند. قوانین کنترل دست‌رسی برای هر کاربر یا گروه کاربران باید به طور واضح در سیاست‌های دست‌رسی شرح داده شود و به کاربران و فراهم‌کنندگان سرویس باید دستورالعمل‌های واضحی از نیازمندی‌های تجاری بر پایه کنترل دست‌رسی ارائه شود. این دستورالعمل‌ها به صورت پروفایل‌های استاندارد دست‌رسی کاربران برای هر دسته مشخص از شغل‌ها طراحی و موجود باشد.

برای هر کاربر یا گروهی از کاربران، سیاست کنترل دست‌رسی باید به وضوح تعریف شده باشد. این سیاست باید امتیاز دست‌رسی را بر طبق نیازمندی‌های تجاری، مانند دست‌رسی پذیری و سودمندی، اهدا نماید. ایده‌ی اصلی باید بصورت "در صورت لزوم امتیاز بیش‌تر، در صورت امکان امتیاز کمتر" باشد.

---

۱ Security Label

۲ Port Protection Device

در تعریف قوانین دست‌رسی باید همه اطلاعات و موقعیت‌ها را در نظر گرفت برای این کار توصیه می شود قوانین به صورت "همه موارد ممنوع به جز..." تعریف شود به جای "همه موارد مجاز به جز...".

برای نام‌نویسی ورود کاربران و خروج آن‌ها به منظور دست‌یابی به همه سیستم‌های اطلاعاتی چند کاربره و سرویس‌های آن‌ها باید روال‌هایی رسمی وجود داشته باشد. اختصاص و استفاده از اختیارات باید محدود و کنترل شده باشد. تخصیص کلمات عبور کاربران باید کنترل شده و از یک فرآیند مدیریت رسمی صورت گیرد.

کنترل دست‌رسی به رایانه به منظور جلوگیری از هرگونه دست‌رسی غیر مجاز به رایانه، انجام می‌شود. این امر باید امکان پذیر باشد که هرکاربر مجاز و رویدادنامهٔ۱ مربوط به تلاش موفق یا ناموفق برای ورود به سیستم را، بتوان تعیین هویت و بازبینی کرد. در این حفاظ می‌توان از کلمات رمز یا هرگونه روش‌های دیگر I&A نیز استفاده کرد.

کنترل دست‌رسی باید جهت محافظت از داده و سرویس‌ها روی یک رایانه و یا در محدوده شبکه، از دسترسی‌های غیر مجاز جلوگیری به عمل آورد. این کنترل‌ها می‌تواند با کمک مکانیزم‌های I&A مناسب، واسط مناسب بین سرویس‌های شبکه و پیکربندی شبکه به‌طوری‌که تنها دسترسی‌های مجاز روی سرویس‌های فن آوری اطلاعات امکان پذیر باشد (محدودیت تخصیص امتیازات)، انجام شود.

کلیه قوانین دست‌رسی تعیین شده برای کاربران باید به‌صورت منظم بازبینی شوند و در صورتی‌که نیاز به تغییرات امنیتی یا تجاری در دست‌رسی وجود داشته باشد، عملیات به روز آوری صورت گیرد. امتیازات دسترسی‌های تعیین شده باید به‌صورت مکرر، جهت اطمینان از عدم سوءاستفاده، بازبینی شوند. امتیازات دست‌رسی باید در صورتی‌که طولانی‌تر شدن آن لزومی نداشته باشد، پس‌گرفته شود.

کلیه وظایف انجام شده در جهت پشتیبانی فن آوری اطلاعات, باید در رویدادنامه ثبت شود. رویدادنامه ها شامل‌تلاش های موفق و ناموفق برای ورود به سیستم، ورود به سیستم جهت دست‌یابی به داده، عملکردهای مورد استفاده سیستم می‌باشد. هم‌چنین نقائص باید ثبت شود، و این رویدادنامه‌ها باید به‌طور منظم بازبینی شود. این داده‌ها باید مطابق با قوانین حفاظت داده‌ها و محرمانگی، استفاده شوند.

---

۱ Log file

برای مثال، داده‌ها ممکن است برای یک دوره‌ی زمانی محصور شده و تنها در هنگام تشخیص نقض امنیت استفاده شوند.

یک فرآیند رسمی به طور منظم و در فواصل زمانی مناسب باید حقوق دست‌یابی کاربران را مرور و در صورت لزوم بازنگری نماید.

کاربران باید فقط به طور مستقیم و به سرویس‌هایی که برای آن‌ها مجاز است، دست‌یابی داشته باشند.

دست‌یابی برای کاربران راه دور، باید بخشی از روال شناسایی و تصدیق اصالت باشد.

دست‌یابی به پورت‌هایی که برای عیب‌یابی از راه دور استفاده می‌شوند، باید کنترل شده باشد.

برای گروه‌های مجزا در شبکه، کنترل‌هایی به منظور سرویس‌های اطلاعاتی، کاربران و سیستم‌های اطلاعاتی باید معرفی شوند.

در شبکه‌های اشتراکی باید کنترل‌های مسیریابی به منظور اطمینان از اتصالات رایانه‌ها و جریان اطلاعات برطبق سیاست کنترل، دست‌یابی کاربردهای فعالیت‌های تجاری سازمان صورت گیرد.
دست‌یابی به سرویس‌های اطلاعاتی باید توسط یک فرآیند ورود امن صورت گیرد.

همه کاربران برای فعالیت‌هایشان باید دارای یک شناسه منحصر به فرد قابل ردگیری و کنترل باشند.
یک سیستم مدیریت کلمه عبور در جایی که بتواند به طور مؤثر و متعامل از کیفیت کلمه عبور اطمینان حاصل نماید، باید وجود داشته باشد. فعالیت‌های غیرمجاز باید ثبت شده، سیستم‌های نظارتی برای کنترل دست‌یابی باید وجود داشته باشد. استفاده از برنامه‌های سیستم باید به دقت کنترل و محدود شده باشد.

۵-۳- رمزنگاری[۱]

۱ Cryptography

ایمن بودن ارتباطات از جمله‌ی مهم‌ترین خصوصیات مورد نظر در بسیاری از زمینه‌های ارتباطی است. به علم و هنر دست‌کاری پیام‌ها به منظور ایمن سازی آن‌ها در مقابل انواع حملات، رمزنگاری گفته می شود. برای رمزنگاری و رمزگشایی، علاوه بر الگوریتم رمز، نیاز به عنصری بنام کلید نیز می‌باشد که معمولاً رشته‌ای از اعداد یا کاراکترهاست و نقش اصلی را ایفا می‌نماید.

به‌ترین الگوریتم‌ها آن‌هایی هستند که حتی با داشتن تعداد زیادی از پیام‌ها و پیغام‌های رمز شده متناظرشان، نتوان کلید آن را تعیین کرد. روش‌های مختلفی برای رمزنگاری وجود دارد:

۵-۳-۱- الگوریتم‌های رمزنگاری کلید عمومی:

در این روش که به رمزنگاری کلید نامتقارن نیز معروف است، نیازی به اشتراک گذاشتن کلید بین فرستنده و گیرنده نیست. این روش مبتنی بر دو کلید مختلف یعنی کلید عمومی۱ و کلید خصوصی۲ می‌باشد یعنی هر کدام از طرفین فرستنده و گیرنده یک جفت کلید دارند. روال انجام کار بدین شکل است که فرستنده با استفاده از کلید عمومی گیرنده (که از طریق صفحه‌ی وب، نامه‌ی الکترونیکی و. ... در دسترس می‌باشد) پیغام را به رمز درآورده و دریافت کننده هم با کلید خصوصی خودش آن را رمزگشایی می‌کند. پس بدون آن‌که فرستنده و گیرنده، کلیدی را به اشتراک بگذارند، می‌توانند پیغام هایشان را به‌صورت امن مبادله کنند. روش‌های رمزکردن کلید عمومی ذاتاً کندتر از الگوریتم‌های رمزکردن کلید متقارن می‌باشند. به این دلیل، در عمل معمولاً برای نقل و انتقال کلیدهایی که بعداً برای رمزکردن توده‌ی داده با الگوریتم‌های متقارن و سایر کاربردهایی که شامل جامعیت داده و اعتبارسنجی می‌باشند و برای رمزکردن آیتم‌های داده‌ی کوچک نظیر شماره‌های کارت‌های اعتباری و PINها استفاده می‌شوند.

۵-۳-۲- رمزکننده‌های بلوکی (متقارن):

---

۱ Public Key

۲ Private Key

در این روش که به آن رمزنگاری کلید متقارن۱ هم گفته می‌شود، فرستنده و گیرنده از یک کلید محرمانه مشترک استفاده می‌کنند. مساله اصلی در آن چگونگی تبادل کلید بین دو طرف به گونه‌ای محرمانه است. برای حل این مساله دو راه وجود دارد: استفاده از یک جفت کلید دیگر برای مبادله کلید محرمانه، استفاده از ۲KDC. از جمله‌ی الگوریتم‌های خیلی معروف در زمینه‌ی رمزنگاری الگوریتم DES می‌باشد. DES و به‌ویژه Triple-DES هم‌چنان در پروتکل‌های معروفی نظیر ۳SSL، ۴PCT، ۵PGP، ۶SGC، ۷SET، ۸TLS مورد استفاده قرار می‌گیرند. الگوریتم رمزنگاری AES به دلیل استحکام و انعطاف‌پذیری خوب به عنوان استانداردی در بین الگوریتم‌های متقارن بلوکی معرفی شده است.

۵-۳-۳- رمزکننده‌های جریانی:

به دلیل خصوصیات ویژه‌ی رمزکننده‌های جریانی استفاده‌ی از آن‌ها وابسته به شرایط و خصوصیات کاربرد آن می‌باشد. به عنوان مثال در صورت مواجه‌بودن با حجم کثیری از داده یا نیاز به بلادرنگی و یا کمبود بافر استفاده از آن‌ها توصیه می‌شود. منتها باید توجه داشت که سطح امنیت کاهش پیدا می‌کند. بنابراین اگر امنیت مهم‌ترین پارامتر باشد، توصیه می‌شود که از این گروه از رمزکننده‌ها استفاده نشود (البته امنیت بعضی از الگوریتم‌های جدید مطرح شده در این گروه هنوز به طور کامل مشخص نیست). الگوریتم‌های متداول در این گروه RC۴ و SEAL بوده‌اند که گهگاه مشکلاتی در آن‌ها گزارش شده است

---

۱ Symmetric Key Cryptography

۲ Key Distribution Center

۳ Secure Socket Layer

٤ Private Communication Technology

٥ Pretty Good Privacy

٦ Server Gated Cryptography

۷ Secure Electronic Transactions

۸ Transport Layer Security

(شکسته‌شدن RC۴ ۴۰ بیتی)؛ به همین دلیل الگوریتم‌های جای‌گزینی پیش‌نهاد شده‌اند (مثلاً Scream به جای SEAL).

۵-۳-۴- الگوریتم‌های امضای دیجیتالی:

پیاده‌سازی تکنیک‌های امضای دیجیتالی کلید عمومی نیازمندی‌هایی را روی شبکه به‌وجود می‌آورد. همان توابع خلاصه پیام و الگوریتم کلید عمومی که برای ایجاد امضای دیجیتالی استفاده شده‌اند باید توسط فرستنده و گیرنده استفاده شوند. جفت کلیدهای عمومی/خصوصی باید تولید و نگهداری شوند. کلیدهای عمومی باید توزیع شوند (یا در محلی که در دسترس عموم باشند، قرار گیرند) و کلیدهای خصوصی باید محافظت شوند. لذا، استفاده از این فن‌آوری نیاز به مدیریت شبکه‌ی کارکنان با دانش رمز نگاری کلید عمومی و استفاده از نرم‌افزاری که الگوریتم‌های رمزنگاری کلید عمومی و امضای دیجیتالی را پیاده‌سازی می‌کند، هم‌چنین امنیت کارکنان و نرم‌افزاری که می‌تواند کلیدهای رمزکردن/رمزگشایی را تولید، توزیع و کنترل کند و پاسخ‌گوی فقدان و مصالحه (افشای) کلید باشد، دارد.

رمزنگاری یک روش ریاضی است که به منظور ایجاد امنیت در ارسال داده استفاده می‌شود. این روش ممکن است برای اهداف مختلفی استفاده شود، به عنوان مثال، رمزنگاری می‌تواند برای ایجاد محرمانگی و یا تمامیت داده، عدم انکار و روش‌های پیشرفته تعیین هویت و تصدیق اصالت بکار رود. وقتی از رمزنگاری استفاده می‌کنیم باید از تمامی قوانین و آیین نامه‌ها در این زمینه تبعیت کنیم. سرویس‌های مهر زمانی می‌تواند در جهت پشتیبانی از کاربردهای مختلف حفاظ‌های رمزنگاری مورد استفاده قرار گیرد.

پارامترهای متفاوت استفاده از رمزنگاری در ادامه بیان شده است.

۵-۴- محافظت از محرمانگی داده‌ها

در شرح چگونگی اهمیت حفظ محرمانگی، به عنوان مثال مکان‌هایی که به‌طور خاص دارای اطلاعات حساس هستند، باید به حفاظ‌هایی جهت مخفی سازی اطلاعات برای ذخیره سازی آن‌ها یا انتقال روی شبکه توجه داشت.

۵-۴-۱- محافظت از تمامیت داده‌ها

در شرح چگونگی اهمیت تمامیت داده‌های پردازش شده یا ذخیره شده، توابع درهم‌سازی، امضای الکترونیکی و یا حفاظ‌های مربوطه باید اطلاعات ارسالی یا ذخیره شده را محافظت کنند. در واقع حفاظ‌های تمامیت (به عنوان مثال، استفاده از کدهای تصدیق اصالت پیغام (MAC)) در برابر تغییرات تصادفی یا عمدی، افزودن یا حذف اطلاعات، محافظت به‌عمل می‌آورند. حفاظ‌های امضای دیجیتالی نیز می‌تواند چنین محافظتی را از لحاظ تمامیت پیغام انجام دهند، اما علاوه بر این موارد حفاظ مربوطه دارای ویژگی‌های خاصی است که ویژگی عدم انکار را نیز پشتیبانی می‌کند.

۵-۴-۲- عدم انکار

تکنیک‌های رمزنگاری (بر پایه استفاده از امضای دیجیتال) می‌تواند به منظور اثبات پیغام یا به شکل دیگر در فرستادن، انتقال، واگذاری، تحویل و.. . پیغام‌ها، انتقالات و تراکنش‌ها مورد استفاده قرار گیرد.

۵-۴-۳- تصدیق اصالت داده

در موقعیت‌هایی که تصدیق اصالت داده از اهمیت بالایی برخوردار است، امضای دیجیتالی می‌تواند جهت تصدیق اعتبار داده مورد استفاده قرار گیرد. این امر به‌ویژه هنگامی است که مرجع داده، از منابع شخص سوم صورت می‌گیرد، یا زمانی که یک سازمان، تأکید زیادی روی صحت مرجع داده دارد. هم‌چنین امضای دیجیتال می‌تواند جهت تصدیق هویت شخص خاص فرستنده‌ی داده، مورد استفاده قرار گیرد.

۵-۴-۴- مدیریت کلید

مدیریت کلید شامل جنبه‌های تخصصی، سازمانی و رویه‌ای است که برای پشتیبانی از هرگونه مکانیزم رمزنگاری لازم و ضروری می‌باشد. هدف از مدیریت کلید، اداره و مدیریت امن کلیدهای رمزنگاری و اطلاعات مربوط به آن‌ها می باشد. مدیریت کلید شامل تولید، ثبت، تصدیق، ابطال، توزیع، نصب، ذخیره سازی، بایگانی، لغو، استخراج و تخریب محتویات کلید می‌باشد. علاوه بر این موارد، در طراحی مدیریت کلید مناسب، کاهش مخاطرات توافق کلید و هم‌چنین تعیین هویت افراد، از اهمیت بالایی برخوردار است. روال‌های مدیریت کلید وابسته به الگوریتم‌های استفاده شده، سنجش کلیدهای مورد استفاده و سیاست امنیتی می‌باشد.

برای برقراری امنیت‌در لایه‌های پایین‌تر از طریقPKI می‌توان از پروتکل‌های امنیتی معروف استفاده نمود. اما برای پیاده‌سازی در لایه‌ی کاربرد نیاز به استفاده از تکنولوژی‌هایی همانند CA، RA و گواهی‌ها داریم. برای استفاده از این تکنولوژی‌ها جدای از انواع محصولات مختلف، دو متد کلی برای پیاده‌سازی موجود است. متدهای In-House و Outsourced. روش In-House به پیاده‌سازی CA، RA و گواهی‌ها در داخل سازمان تکیه دارد و روش Outsourced به پیاده‌سازی CA، RA و گواهی‌ها در خارج از سازمان و استفاده از امکانات آن تحت وب از طریق گرفتن سرویس از شرکت ارائه کننده‌ی سرویس Outsourced، می‌پردازد.

در طراحی PKI در یک‌سازمان اولین نکته توجه به سیاست‌هایی است که برای PKI در نظرگرفته می شود. سه مدل اصلی برای سیاست‌های PKI وجود دارد:

مدل سازمان مدلی است که در آن PKI برای انتشار گواهی و مدیریت آن‌ها در سطح یک شرکت استفاده می‌شود. به عنوان مثال انتشار گواهی‌ها بین کارمندان شرکت به منظور کنترل دست‌رسی منابع شرکت در این مدل قرار دارد.

مدل تجارت که در آن PKI برای انتشار گواهی‌ها بین طرف‌های تجاری اینترنتی به‌کار می‌رود. برای مثال عمده فروشی که در اینترنت با طرف‌های تجاری خود به تبادل اطلاعات می‌پردازد.

(COI)[۱] که در آن PKI برای انتشار گواهی‌هایی به‌کار می‌رود که توسط طرف اطمینان کننده به گواهی[۲] درون یک مجمع عمومی بزرگ به‌کار می‌رود. (سرویس‌های مالی، بانکی و healthcare).

۵-۵- سیاست‌های رمزنگاری

باید برای حفاظت از اطلاعات حساس و مهم رمزنگاری صورت گیرد و در این راستا باید سیاستی در جهت استفاده از کنترل‌های توسعه یافته‌رمزنگاری تهیه شده باشد.

به منظور تصدیق اصالت، مجازسازی و یک‌پارچگی اطلاعات الکترونیکی باید از امضاهای دیجیتالی استفاده کنند.

انتخاب سیستم رمزنگاری به نوع کاربرد و اهم پارامترهای مورد نظر (مانند امنیت، کارآیی، استانداردها و قابلیت کار مشترک) بستگی دارد. در انتخاب یک الگوریتم رمز مناسب برای یک کاربرد باید با رمزشکنی و حملات علیه سیستم‌های رمزنگاری آشنا بود و الگوریتمی باید انتخاب شود که در برابر حملات شناخته‌شده مقاوم باشد.

باید مراقب حملات رمزشکن بود و در مورد آن‌ها دانش و شناخت پیدا کرد. از جمله حمله‌های مهم برای شکستن رمز می‌توان به موارد زیر اشاره نمود: حمله‌ی Ciphertext-only، حمله‌ی Known-

---

۱ Community of Interest Model

۲ Authorized Relying Party

Plaintext، حمله‌ی Chosen-Plaintext، حمله‌ی Man-in-the-middle، حمله علیه یا با استفاده از سخت‌افزار زیر لایه، حمله‌ی Known-Ciphertext، حمله‌ی Related-Key.

هر چند که قدرت الگوریتم از اهمیت بیش‌تری نسبت به طول کلید (در الگوریتم‌هایی که از کلید استفاده می‌کنند) برخوردار است، اما طول کلید نیز عامل مهمی در بالابردن امنیت الگوریتم می‌باشد.

در صورت وجود قرارداد کوتاه و موقتی outsourcing بین یک سازمان با شرکت‌های بیرونی باید تنها ترافیک رمزنگاری شده از مبدای آن‌ها (که از قبل باید مشخص شده باشد) به مقصد سرورهای تحت مدیریت سازمان اجازه عبور داشته باشد.

سازمان باید سیاست‌های خود را در مورد PKI اتخاذ کند، یک طرح خوب ممکن است به صورت ترکیبی باشد. به این معنا که دو نوع سیاست برای گواهی‌ها اتخاذ شود. سیاست اول برای گواهی‌هایی به که برای کاربردهای معمول و توسط کارمندان آن مثلاً برای امن نمودن نامه‌های الکترونیکی و یا شناسایی متقابل یک مرورگر و یک سرور به کار می‌رود. سیاست دوم شامل گواهی‌هایی می‌شود که برای تراکنش های مالی خاص بین کشورهای دیگر به کار می‌رود. در این صورت جفت کلید تولید شده برای این گواهی‌ها باید توسط مکانیزم‌های با امنیت بالاتری ساخته شود.

۵-۶- محافظت در برابر کدهای مخرب

کدهای مخرب از آغاز ایجاد رایانه تا به امروز که شبکه‌های عظیم رایانه‌ای سرتاسر دنیا را به هم مرتبط می‌سازند، یک موضوع بسیار حساس و دردسر ساز برای کاربران بوده است. آن‌ها در حقیقت هم تهدیدی برای داده‌ها و اطلاعات موجود در رایانه‌ها هستند و هم تهدیدی برای کارایی سیستم‌ها و شبکه های رایانه‌ای.

کدهای مخرب در سیستم‌ها ممکن است از طریق اتصالات خارجی و فایل‌ها و نرم افزارهای روی دیسک‌های قابل انتقال، به‌وجود آیند. کد مخرب ممکن است تا قبل از وارد آمدن اثرات مخرب آن شناسایی نشود مگر این‌که، حفاظ‌های مناسب و کافی روی سیستم‌ها پیاده‌سازی شده باشند. کدهای مخرب ممکن است در اثر مشکلات حفاظ‌های امنیتی (به عنوان مثال به‌دست آوردن و آشکارسازی

کلمه رمز)، فاش کردن غیرعمدی اطلاعات، تغییرات غیرعمدی اطلاعات، از دست دادن یک‌پارچگی سیستم، تخریب اطلاعات، یا استفاده بدون مجوز از منابع سیستم تولید شوند.

۵-۶-۱- اقسام برنامه‌های مزاحم و مخرب[۱]

برنامه‌های مخرب، اصطلاحی کلی برای کلیه برنامه‌هایی است که به نحوی اثر سوئی برای رایانه‌ها و یا شبکه‌های رایانه‌ای دارند. بر اساس نحوه عملکرد برنامه‌های مخرب و اثر تخریبی که دارند، آن‌ها را به سه دسته اصلی تقسیم می‌کنند که ذیلاً به آن‌ها اشاره شده است:

۵-۶-۱-۱- ویروس‌ها:

ویروس‌های رایانه‌ای برنامه‌ها یا قطعات اجرایی هستند که بدون اطلاع کاربر خود را به سایر برنامه‌های اجرایی مجاز می‌چسباند و یا جای‌گزین آن‌ها می‌شوند. روشی که انواع ویروس‌ها از آن استفاده می‌کنند یک وجه مشترک دارد و آن این است که برای این‌که بتوانند عمل کنند می‌بایست حتماً اجرا شوند. ویروس‌ها خود اقسام مختلفی دارند، ویروس‌های Boot Sector، ویروس‌های ترکیبی، ویروس‌های ماکرو از جمله انواع ویروس‌ها می‌باشند.

۵-۶-۱-۲- اسب‌های تروا:

اسب‌های تروا برنامه‌هایی هستند که عملی غیر از آن‌چه کاربر فکر می‌کند انجام می‌دهند و اهداف غیر تخریبی دارند. مثلاً برای دزدیدن اطلاعات حساس کاربران مثل کلمه‌های عبور و غیره به کار می‌روند. وجه تمایز ویروس‌ها با اسب‌های تروا در این است که اسب‌های تروا غالباً دارای مکانیزم‌های نمونه سازی و پخش نیستند و برای اهداف دزدی اطلاعات به‌کار می‌روند.

۵-۶-۱-۳- کرم‌ها:

کرم‌ها برنامه‌هایی هستند که غالباً از روی شبکه پخش می‌شوند. بر خلاف ویروس‌ها که اغلب به برنامه های اجرایی می‌چسبند کرم‌ها برای گسترش خود از برنامه‌های مستقل استفاده می‌کنند. از جمله

---

۱ Malicious Code

راه‌هایی که کرم‌ها برای گسترش خود استفاده می‌کنند، استفاده از آدرس‌های پست الکترونیکی کاربر است تا خود را از این طریق به رایانه های دیگر نیز منتقل کنند.

به‌ترین راه مقابله با ویروس‌ها این است که پیش از ابتلا به هر نوع ویروسی رایانه را از پیش حفاظت کرد. اولین قدم برای این کار نصب یک " نرم‌افزار ضد ویروس به‌روز شده" است.

Scannerها

شکل‌های مختلف کدهای مخرب را می‌توان از طریق نرم افزارهای scan ویژه و کنترل‌کننده‌های تمامیت، تشخیص و حذف کرد. scannerها می‌توانند در حالت‌های off-line یا on-line عمل کنند. در مود on-line، scanner به‌صورت فعال محافظت و شناسایی (و حذف در صورت امکان) را در برابر کدهای مخرب، قبل از این‌که سرایت کدها صورت بگیرد و خساراتی به سیستم IT وارد آید، انجام می دهد. scannerها روی کامپیوترها، ایستگاه‌های کاری، فایل سرورها، سرورهای پست الکترونیکی و فایروال‌ها قرار می‌گیرند. در هر حال کاربران و مدیران سیستم‌ها باید بدانند که نمی‌توان بر این امر تکیه داشت که scannerها تمامی کدهای مخرب و انواع مختلف آن را تشخیص دهند زیرا، انواع جدید این کدها به‌طور مداوم در حال افزایش است.

کنترل کننده تمامیت

نوعاً، به دیگرحفاظ‌ها جهت تکمیل محافظت تأمین شده توسط scannerها، نیاز داریم. به عنوان مثال، checksumها برای کنترل چگونگی تغییرات برنامه‌ها می‌توانند استفاده شوند. نرم افزارکنترل کننده تمامیت، باید یک بخش عمده از حفاظ‌های تخصصی محافظت‌کننده در برابر کدهای مخرب باشد. این تکنیک تنها می‌تواند برای فایل‌های داده و برنامه‌هایی که اطلاعات وضعیت آن‌ها برای استفاده در آینده نگهداری نمی‌شود، بکار رود.

کنترل جریان رسانه‌ی قابل برداشت

جریان کنترل نشده‌ی رسانه‌ها (به‌ویژه فلاپی دیسک‌ها) می‌تواند منجر به افزایش خطرپذیری سیستم های IT سازمان، در برابر کدهای مخرب شود. کنترل جریان رسانه‌ها می‌تواند از طریق موارد زیر بدست آید:

نرم افزارهای ویژه

حفاظ‌های رویه‌ای

حفاظ‌های رویه‌ای

دفترچه راهنماهای کاربران و مدیران سیستم‌ها باید شامل مطالب کلی روال‌ها بوده و آموزشی در جهت کاهش انتشار کدهای مخرب باشد. دفترچه راهنماها باید شامل بازی‌ها و دیگر نرم افزارهای قابل اجرا، استفاده از انواع مختلف سرویس‌های اینترنتی، و فایل‌های ورودی در انواع مختلف باشد. هم‌چنین در مواقع لزوم باید، بازبینی واحد کنترل داخلی از منابع یا کدهای قابل اجرا انجام شود. آموزش‌ها و اطلاع رسانی امنیتی، عملکردهای منظم و روال‌های مربوط به آن باید، در زمان مناسب ارائه شود.

۵-۶-۲- سیاست‌های ضد کدهای مخرب

تمامی رایانه‌های موجود در شبکه سازمان باید به برنامه سرویس‌گیرنده ضد کدهای مخرب مجهز باشند.

نرم‌افزارهای ضدکدهای مخرب باید دائماً و ترجیحاً به طور اتوماتیک از طریق برنامه سرور به‌روز شوند.

در سازمان باید روال‌هایی برای بازدید و کنترل سیستم‌ها جهت اطمینان از فعال‌بودن و به‌روز بودن نرم افزارهای ضدکدهای مخرب تهیه شده باشد.

نرم‌افزارهای ضد کدهای مخرب را می‌بایست به گونه‌ای تنظیم کرد تا اولاً در حافظه مقیم باشند تا هر گونه فایل ورودی به سیستم را بتوانند از نظر ابتلا به کدهای مخرب بررسی کنند. ثانیاً در صورتی که از اینترنت و یا سرویس پست الکترونیکی استفاده می‌شود، بررسی خودکار Email های ورودی به سیستم را به عهده نرم‌افزار ضد کدهای مخرب قرار داد. هم‌چنین بررسی‌های روزانه یا هفتگی سیستم را در دستور کار نرم‌افزار ضدکدهای مخرب گذاشت.

برای مقابله با ویروس‌های Boot-Sector در رایانه‌ها بهتر است در BIOS سیستم boot شدن از طریق غیر هارد را غیر فعال کرده و تنها در هنگامی که به این امکان نیاز است آن را به‌طور موقتی فعال کرد.

از آن‌جا که کدهای مخرب جدید اغلب از طریق استفاده از نقاط ضعف امنیتی سیستم عامل یا سرویس‌های گوناگون به سیستم وارد می‌شوند، لذا کاربران خصوصا در سرورها می‌بایست حتماً آخرین Patchها و اصلاحات مربوط به سیستم عامل را نصب کنند.

برنامه ضد کدهای مخرب بایست دارای ویژگی‌های زیر باشد:

قابلیت جست‌وجو در فایل‌های فشرده

امکان زمان‌بندی برای جست‌وجوی خودکار کدهای مخرب

قابلیت جست‌وجوی بلادرنگ کدهای مخرب در هر عملیات کار با دیسک سخت

امکان به روز رسانی بانک داده کدهای مخرب به‌طور مرتب

جست‌وجو در Email های ورودی به سیستم و یا خروجی از آن

جست‌وجو در حافظه اصلی برای یافتن کدهای مخرب فعال در حافظه

قابلیت قرنطینه فایل‌ها و برنامه‌های مبتلا به کدهای مخرب

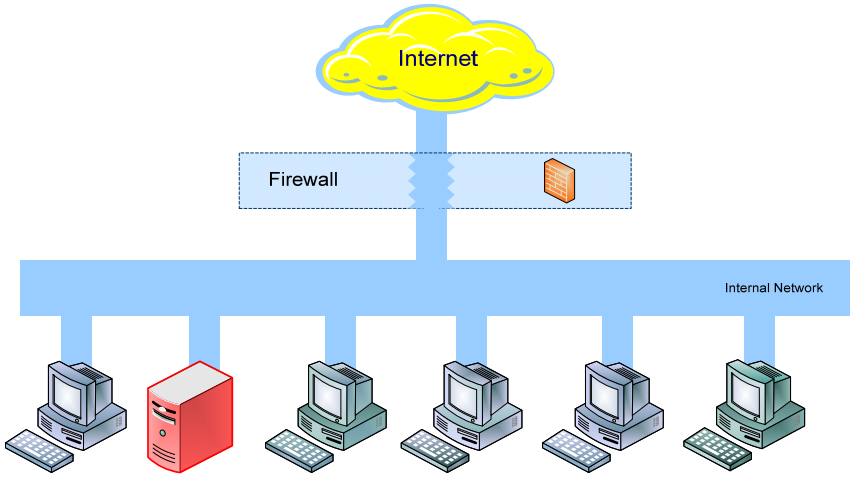
قابلیت جست‌وجو در رایانه‌های موجود در شبکه و مدیریت مرکزی آن.

۵-۷- دیواره آتش

یک دیواره‌ی آتش یک سیستم یا ترکیبی از چندین سیستم است که یک سری محدودیت را بین دو یا چند شبکه اعمال می‌کند. عموماً دیواره‌های آتش به منظور محافظت شبکه‌ی خصوصی که به یک شبکه‌ی عمومی یا مشترک[۱] متصل است به کار گرفته می‌شوند. متداول‌ترین نحوه استفاده از دیواره آتش در نقطه ورودی یا خروجی ترافیک به شبکه داخلی است(شکل زیر).

---

۱ Shared Network



دیواره‌های آتش(تصویر شماره شش)

انواع دیواره‌های آتش عبارتند از:

۵-۷-۱- دیواره‌های آتش پالایشگر بسته:

این دیواره‌های آتش ترافیک شبکه را در لایه‌ی انتقال بر اساس اطلاعات سرآیند۱ در کنار مجموعه قوانین عبور جریان داده‌ای مورد بررسی قرار می‌دهند.

۵-۷-۲- دیواره‌های آتش سطح مدار:

برای تأیید یک نشست، این دیواره‌های آتش فاز برقراری ارتباط در سطح لایه‌ی انتقال را مورد بررسی قرار می‌دهند تا مطمئن شوند دست‌دهی۲ به صورت صحیح و قانونی کامل شود و جدولی اطلاعات کامل حالات نشست۱ و اطلاعات مربوط به توالی بسته‌ها را در آن نگهداری می‌کنند.

---

۱ Header

۲ Handshaking

۵-۷-۳- دیواره آتش بسته پویا:

علاوه به نگهداری فاز برقراری، اطلاعات حالت تمام جریان‌های ارتباطی را نیز نگهداری می‌کند. آن‌ها حالت ارتباطات در لایه‌های شبکه و نشست را با ثبت اطلاعات برقراری نشست (که از دیواره آتش عبور می‌کند) به خاطر سپرده، تنها بسته‌های بازگشتی مجاز را عبور می‌دهند.

۵-۷-۴- دیواره‌های آتش لایه‌ی کاربرد:

داده‌های تمام بسته‌ها را در سطح لایه‌ی کاربرد مورد بررسی قرار می‌دهند، اطلاعات کامل حالات ارتباطات و ترتیب‌بندی بسته‌ها را نگهداری کرده، کلیه‌ی مواردی که تنها در لایه‌ی کاربرد قابل کنترل هستند، مانند کلمات عبور کاربران و درخواست‌های سرویس‌های گوناگون را پشتیبانی می‌کنند. بعضی از قابلیت‌های دیواره‌های آتش لایه کاربرد شامل فیلتر کردن URLها، فیلتر کردن بر اساس محتوای بسته‌ها، ثبت وقایع، بازرسی عبور و مرورها و فراهم آوردن امکان شناسایی حملات می‌باشد. اغلب دیواره های آتش لایه‌ی کاربرد شامل نرم‌افزارهای کاربردی خاص و سرویس‌های proxy هستند. سرویس‌های proxy برنامه‌های خاص منظوره‌ای هستند که ترافیک عبوری از دیواره‌ی آتش مربوط به سرویس‌های مختلف مانند HTTP و FTP را مدیریت می‌کنند. سرویس‌های proxy می‌توانند مکانیزم‌های کنترل دست‌رسی را پیاده‌سازی کرده، سطح دست‌رسی به منابع مختلف را محدود سازند. آن‌ها هم‌چنین با بازرسی‌بسیار دقیق داده‌های انتقالی قادرند رکوردهای حساب‌رسی گوناگونی را در ارتباط با ترافیک عبور داده شده و نیز ترافیک متوقف شده تولید کنند و در اختیار مدیر شبکه قرار دهند.

علاوه بر دسته‌بندی فوق دیواره‌های آتش دارای انواع زیر نیز هستند.

۵-۷-۵- دیواره‌های آتش مخفی۲:

دیواره‌ی آتش مخفی یک سیستم است که حضورش در شبکه به سختی قابل تشخیص است، به این علت که سرویس‌هایش به حداقل رسیده‌اند و با استفاده از پالایشگر بسته تنها به تعداد بسیار محدودی

---

۱ Session States

۲ Stealth Firewalls

از ماشین‌ها اجازه‌ی ارتباط می‌دهد. این دیواره‌های آتش از آن‌جا که به سختی در شبکه رؤیت هستند، بسیار قوی و کارا می‌باشند. این دیوارۀهای آتش که طراحی پیچیده‌ای دارند درخواست‌های ماشین‌های دیگر را با "resource denied" یا "resource restricted" پاسخ نمی‌دهد و هم‌چنین TTL بسته را کاهش نمی‌دهد، بدین ترتیب به سختی قابل تشخیص است.

۵-۷-۶- دیواره‌های آتش توزیع شده[۱]:

در ساختارهای جدید، شبکه ممکن است از نقطات متعددی به دنیای خارج متصل شود. با گسترش و Cable Modemها، خطوط Wireless کاربران قادرند با استفاده از VPN به شبکه متصل شوند. دیواره‌های آتش توزیع شده در یک مکان قرار ندارند و در سطح شبکه توزیع شده‌اند. دیواره‌های آتش توزیع شده بر روی تمام سیستم‌های نهایی و نقاط انتهایی[۲] در شبکه نصب می‌شوند. این دیواره‌های آتش بر اساس مفاهیم اصلی زیر کار می‌کنند:

Policy Language: برای تعریف و تدوین سیاست‌های هر کدام از دیواره‌های آتش.

ابزار مدیریت سیستم[۳]: برای توزیع و ارسال سیاست‌ها به دیواره‌های آتش و جمع‌آوری اطلاعات ثبت شده[۴] و گزارش‌ها.

IPSEC: برای ایجاد امنیت ترافیک شبکه و انتقال سیاست‌ها با رمزنگاری اطلاعات.

۵-۷-۷- دیواره‌های آتش شخصی[۵]:

---

۱ Distributed Firewalls

۲ Endpoints

۳ System Management Tools

٤ Logging Information

٥ desktop firewalls

نرم‌افزارهایی هستند که برای محافظت از یک رایانه تنها که به اینترنت متصل است مورد استفاده قرار می‌گیرند. این رایانه ممکن است به طور دائمی (از طریق خطوط Cable modem , DSL) و یا موقت (از طریق ارتباطات Dial-up) به اینترنت متصل باشد. در مقایسه با برنامه‌های ضدویروس دیواره‌های آتش شخصی در background و در سطحی پایین‌تر اجرا می‌شوند. دیواره‌های‌آتش شخصی با چک کردن جامعیت۱ فایل‌های سیستم، پالایش ترافیک ورودی و خروجی، اخطار به کاربر در ارتباط با حملات در حال شکل‌گیری و ... سعی می‌کنند رایانه مرتبط با اینترنت را مورد محافظت قرار دهند. در آینده‌ی نزدیک امن‌سازی سیستم‌ها با دیواره‌های آتش شخصی به یکی از استانداردهای رایانه‌های خانگی۲ تبدیل خواهد شد.

۵-۷-۸- مسیریاب‌های پالایشگر:

اغلب اوقات مسیریاب‌ها اولین خط دفاعی بر علیه دست‌رسی غیر مجاز به شبکه هستند. تنها راه ورود از خارج به درون یک اینترانت از طریق مسیریاب‌هاست. بنابراین منطقی است که باید قوانین امنیتی برای کنترل ترافیک آن وضع نمود. در واقع فیلترینگ برای پیاده‌سازی سیاست‌های امنیتی یا اجرای کنترل دسترسی‌های طرح شده بر روی ترافیک به کار می‌رود. مسیریاب‌ها می‌توانند نوع و جهت ترافیک را کنترل کنند. زمانی که مسیریاب‌ها برای حفاظت از یک اینترانت استفاده می‌شود به آن‌ها مسیریاب پالایشگر می‌گویند.

۵-۸- سیاست‌های دیواره آتش

برخی از سیاست‌های امنیتی مهمی که در تعریف قوانین بر روی دیواره آتش بایست در نظر گرفته شوند عبارتند از:

سازمان باید برای امن کردن اتصال خود به اینترنت و یا اتصال شبکه داخلی خود به دیگر شبکه‌ها باید از دیواره‌ی آتش استفاده کند. در واقع به عنوان اولین قدم دفاعی در برابر حملات خارجی باید از

---

۱ Integrity

۲ Home Computers

دیواره‌ی آتش بهره برد. سازمان ممکن است برای تأمین امنیت شبکه خود به چندین دیواره‌ی آتش مختلف نیاز داشته باشد.

بین سه دسته اول دیواره‌های آتش، یعنی سطح بسته، سطح مدار و سطح بسته پویا، نوع سوم تنها به نگهداری فاز برقراری ارتباط اکتفا نکرده، بلکه اطلاعات حالت تمام جریان‌های ارتباطی را نیز بررسی می کند و بنابراین توصیه می‌گردد. نوع چهارم یعنی دیواره‌های آتش لایه‌ی کاربرد با توجه به بررسی بسته ها در لایه‌ی کاربرد کارایی شبکه را کاهش می‌دهند، اما قادرند از بسیاری از حمله‌ها و خراب‌کاری‌ها جلوگیری کنند.

برای انتخاب یک دیواره‌ی آتش مناسب برای شبکه باید سطح امنیتی مورد انتظار برای شبکه، اندازه‌ی شبکه، اهمیت و تعداد منابع موجود در آن، بودجه‌ای که به امنیت اختصاص داده شده، نیروی انسانی و نگهداری دیواره‌ی آتش را در نظر گرفت.

سازمان‌باید در انتخاب محصولی جهت دیواره‌های آتش مناسب دقت کند، زیرا با توجه به این‌که تمام ترافیک از یک گلوگاه عبور می‌کند، هر چه سطح امنیت در یک شبکه با کمک گرفتن از دیواره‌های آتش بالاتر رود، کارایی پایین خواهد آمد. علاوه بر این "تنها نقطه‌ی شکست" بودن دیواره‌های آتش دسترس‌پذیری شبکه را نیز تحت تأثیر قرار می‌دهد. در عمل هنگام استفاده از دیواره‌های آتش با در نظر گرفتن سطح امنیت مورد نیاز و هزینه‌هایی که باید برای رسیدن به این سطح پرداخته شوند یکی از انواع دیواره‌های آتش انتخاب می‌شوند.

سیاست‌ها و قوانین گذردهی دیواره آتش باید بر اساس تحلیل‌مخاطرات و تحلیل فایده- هزینه برای منابع و کاربردهای شبکه که هر سازمان استفاده می‌کند، تهیه شود. این قوانین باید به صورت امن نگهداری و رسیدگی شود.

سیاست پیش‌فرض دیواره‌ی آتش باید بلاک کردن همه بسته باشد، مگر این‌که شرایط بسته با یکی از قوانین خاص مجاز تطبیق کند. به طور کلی تمام پروتکل‌ها و سرویس‌هایی که در شبکه سازمان‌نیازی با آن‌ها نیست، باید بلاک شوند.

یک دیواره‌ی آتش باید بسته‌های عبوری را حداقل بر اساس این پارامترها فیلتر کنند: نوع پروتکل، آدرس مبدا و مقصد، شماره پورت مبدا و مقصد، اینترفیسی که بسته از آن وارد شده.

عملیات پروکسی باید حداقل بر روی محتویات پروتکل‌های FTP, HTTP و SMTP کنترل داشته باشد.

استفاده از تکنیک ترجمان آدرس شبکه و شکافتن DNS[۱] برای مخفی سازی شبکه داخلی سازمان توصیه می‌شود.

تمام بسته‌های عبوری از دیواره آتش خصوصاً ترافیک ورودی به بخش سرورهای عمومی بایست به صورت کاملاً حالت‌دار مورد بازرسی قرار گیرند[۲] . این بسته‌ها شامل بسته‌های ICMP، UDP و TCP می‌شود. تنها ترافیکی مجاز به ورود به شبکه داخلی و هسته شبکه است که متعلق به یک نشست معتبر باز شده از شبکه داخلی باشد.

ترافیک spoof شده ورودی از هر پورت دیواره آتش بایست مورد کنترل قرار گیرد و اجازه عبور نیابد.

گروه مدیریت امنیت هر سازمان باید مرتباً گزارشات امنیتی تیم پاسخ‌گویی به حوادث و یا اطلاعات وب سایت‌های امنیتی را برای اطلاع از رخنه‌ها و حملات موجود مرور کرده، در صورت نیاز سیاست‌ها و قوانین گذردهی دیواره‌های آتش را بر اساس آن‌ها به‌روز کند.

دیواره‌ی آتش‌ها باید ترافیک‌های مجاز و غیرمجاز در فایل‌های مشخص ثبت کند و این فایل‌ها باید توسط مدیران شبکه به طور روزانه بازبینی شوند. در صورت نیاز این logفایل‌ها باید بر اساس پروتکلی مانند NTP[۳] با logفایل‌های سیستم‌های دیگر مانند سیستم‌های تشخیص تزاحم هم‌زمان[۴] شوند.

---

۱ Network address translation and split DNS

۲ stateful inspection

۳ Network Time Protocol

٤ Synchronized

برای شبکه‌هایی که نقاط اتصال به شبکه خارجی متعددی دارد و همین طور برای بالابردن کارایی و اطمینان می‌توان از دیواره‌های آتش توزیع شده استفاده کرد. اما باید دقت کرد که این دیواره‌های آتش راه‌حل مناسبی برای تمام شبکه‌ها نیست مثلاً برای ارائه سرویس‌های proxy در لایه‌کاربرد دیواره‌های آتش سنتی مناسب‌تر است و باید در انتخاب آن دقت نمود.

مدیر شبکه باید یک جدول فیلترینگ که شامل قوانینی در مورد بسته‌های مجاز و غیرمجاز تهیه کند که مسیریاب با تطبیق دادن اطلاعات هر بسته در آن در مورد عبور یا بلاک کردن بسته تصمیم می گیرد. معمولاً قوانین مختلفی برای بسته‌های ورودی و خروجی اعمال می‌شود برای مثال ممکن است به کاربران داخل یک اینترانت اجازه استفاده از سرویس Telnet داده شود ولی به کاربران خارجی خیر. هم‌چنین مسیریاب‌ها می‌توانند قوانین مجزایی برای زیرشبکه‌های متفاوت داشته باشند، زیرا ممکن است هر زیرشبکه نیازهای امنیتی متفاوتی داشته باشد.

مسیریاب‌های پالایشگر می‌توانند در مورد فعالیت‌های فیلترینگ خود log تهیه کنند و این امکان باید به منظور کشف حمله‌های ممکن فعال باشد.

هر مسیریاب بین شبکه داخلی و شبکه خارجی قرار می‌گیرد باید حداقل قوانین ابتدایی فیلترینگ را دارا باشد که در آن‌ها گفته می‌شود: اطلاعات مسیریابی از چه اینترفیس‌هایی قابل قبول است و از هر اینترفیس منطقی چه مسیرهایی مجاز است. و این که آیا همه مسیرها یا فقط یک مسیر پیش‌فرض روی یک اینترفیس انتشار داده می‌شود. بعضی از مسیریاب‌ها اینترفیس منطقی را به عنوان اطلاعات مبدا تشخیص نمی‌دهند در این مسیریاب‌ها باید لیست مسیریاب‌های مجاز دیگر را به عنوان فیلترینگ ورودی مشخص نمود.

۵-۹- سیستم‌های تشخیص نفوذ

یک سیستم تشخیص نفوذ عبارت است از یک یا چند سیستم که توانایی تشخیص تغییرات و رفتارهای خاصی در یک سیستم و یا شبکه را دارا باشند. یک سیستم تشخیص نفوذ به صورت کلی دارای بخش های زیر می‌باشد:

بخش جمع کننده اطلاعات

بخش بازبینی سیستم

بخش ذخیره اطلاعات

بخش کنترل و مدیریت

بخش آنالیز

با توجه به نحوه قرار گرفتن هر یک از بخش‌های یک سیستم تشخیص نفوذ، معماری های مختلفی برای آن به وجود می‌آید.

سیستم‌های تشخیص نفوذ بر حسب منابع اطلاعاتشان دسته‌بندی می‌شوند:

مبتنی بر میزبان: که در آن اطلاعات بر اساس منابع داخل سیستم جمع آوری می‌شوند. این سیستم‌ها خود به دو دسته تقسیم می‌شوند. مبتنی بر برنامه که در آن اطلاعات بر اساس برنامه های کاربردی که در حال اجرا جمع آوری می‌شوند. مبتنی بر مقصد که خود سیستم، اشیاء با اهمیت سیستم را مشخص و برای هر یک به صورت متناوب اطلاعاتی جمع‌آوری می‌نماید.

مبتنی بر شبکه: در این دسته، بسته‌های عبوری در سطح شبکه به عنوان منبع اطلاعات جمع آوری می شوند. این عمل با قرار دادن کارت شبکه در حالت promiscuous صورت می‌گیرد.

روش‌های آنالیز به دو دسته تقسیم می‌شوند: تشخیص سوءاستفاده که در آن آنالیزگر توسط مکانیزم های چون تشخیص الگو به دنبال نشانه‌تعریف شده‌ای از یک عمل نادرست می‌گردد و تشخیص تغییر رفتار که در آن آنالیزگر به دنبال موارد غیرمعمول می‌گردد.

در مورد زمان‌بندی آنالیز نیز دو حالت وجود دارد. در حالت دسته‌ای اطلاعات مربوط به یک دوره زمانی جمع آوری شده، سپس به آنالیزگر داده می‌شوند. در حالت بلادرنگ با هر رویدادی که رخ می‌دهد و یا در هر فاصله زمانی کوتاه، منبع اطلاعات به آنالیزگر داده می‌شود.

در رابطه با مساله کنترل سیستم‌های تشخیص نفوذ سه روش عمده مطرح است:

مرکزی: که در آن مدیریت و تولید گزارش به صورت مرکزی بوده، یک سیستم مدیریت مرکزی سیستم تشخیص نفوذ را کنترل می‌کند.

استفاده از امکانات مدیریت شبکه: که در آن اطلاعات جمع‌آوری شده توسط سیستم‌های مدیریت شبکه به عنوان یک منبع اطلاعات برای سیستم‌های تشخیص نفوذ مورد استفاده قرار می‌گیرد.

توزیع شده: در این حالت آنالیزگر با استفاده از عامل‌های متحرک در سطح شبکه حرکت کرده، نتایج جمع‌آوری شده بر روی سیستم‌های مختلف را مورد آنالیز قرار می‌دهد.

۵-۱۰- سیاست‌های تشخیص نفوذ

سازمان باید برای کنترل سیستم‌های تشخیص نفوذ خود برنامه‌ریزی کند. برای سازمان‌های بزرگ و با منابع اطلاعات توزیع شده به‌تر است از سیستم‌های کنترلی توزیع شده با عامل‌های متحرک جهت جمع آوری اطلاعات بهره گرفت. این امر به قابلیت گسترش سازمان نیز کمک می‌کند.

از دیگر خصوصیاتی که در انتخاب سیستم‌های تشخیص نفوذ باید رعایت کرد این است که فعالیت‌های خود را در برابر مسائل امنیتی و در امان بودن از دستبرد مانیتور کند.

انتخاب سیستم‌های تشخیص نفوذ باید براساس نسبت کنسول‌های کارگزار به کنسول‌های مدیر باشد و از آن‌جا که در سازمان‌ها همواره احتمال گسترش سازمان وجود دارد، باید از محصولی استفاده شود که بتواند تعداد زیادی از کارگزارها را حمایت کند.

به‌تر است با توجه به اهمیت منابع اطلاعاتی و سرورهای حیاتی شبکه از سیستم‌های تشخیص نفوذ مبتنی بر میزبان[۱] برای محافظت از سرورهای مهم موجود در ماجول اینترنت و ماجول سرورها استفاده گردد.

برای داشتن یک سیستم تشخیص نفوذ کامل باید از ترکیبی از سیستم‌های تشخیص نفوذ مبتنی بر میزبان و مبتنی بر شبکه بهره جست.

---

۱ Host-based Intrusion Detection Systems

در مورد سیستم‌های تشخیص نفوذ مبتنی بر میزبان باید منابع لازم جهت جمع‌آوری اطلاعات فراهم شود. این منابع شامل فایل‌های بازرسی که در برگیرنده اطلاعاتی از فعالیت‌های سیستم است، logهای سیستم که مشخص‌کننده رویدادهای سیستم و تنظیمات مختلف آن است و اطلاعات و رویدادهای برنامه‌های کاربردی است. در واقع این منابع باید به گونه‌ای تنظیم و پیکربندی شوند که اطلاعات مناسب برای تشخیص نفوذ را فراهم کنند.

در مورد روش آنالیز نیز به‌تر است از هر دو روش تشخیص سوءاستفاده و تشخیص تغییر رفتار هم زمان استفاده شود، هر چند در سازمان‌هایی که الگوهای رفتاری ثابت است تشخیص تغییر رفتار مناسب‌تر می‌باشد. در واقع سیستم‌های مبتنی بر تشخیص سوءاستفاده که بخش عظیمی از سیستم‌های تشخیص نفوذ را در بر می‌گیرد وظیفه حفاظت از سیستم در برابر حمله‌های از قبل تعریف شده و سیستم‌های مبتنی بر تشخیص تغییر رفتار بیش‌تر وظیفه تشخیص حملات جدید و ناشناخته را بر عهده دارد.

برای انتخاب سیستم‌های تشخیص مبتنی بر سوءاستفاده باید از پایگاه حملات و سوءاستفاده‌های کاملی استفاده کرد و عملیات به‌روزرسانی آن را متناوباً انجام داد. همین‌طور باید از IDS[1]هایی استفاده نمود که پردازش‌ها را به صورت بلادرنگ و هم‌زمان انجام دهند.

کلیه اطلاعاتی که بین کارگزارها و مدیر IDS از طریق شبکه رد و بدل می‌شود باید امن باشد.

یک IDS ایده‌آل باید بتواند به حملات تا حد مطلوبی پاسخ دهد بعضی از مکانیزم‌های پاسخ‌گویی مطرح عبارتند از: پیکربندی مجدد فایروال‌ها، مسیریاب‌ها و سوئیچ‌ها، تکنیک‌های اغفال نفوذگر، session hijacking, اصلاح نقاط آسیب‌پذیر.

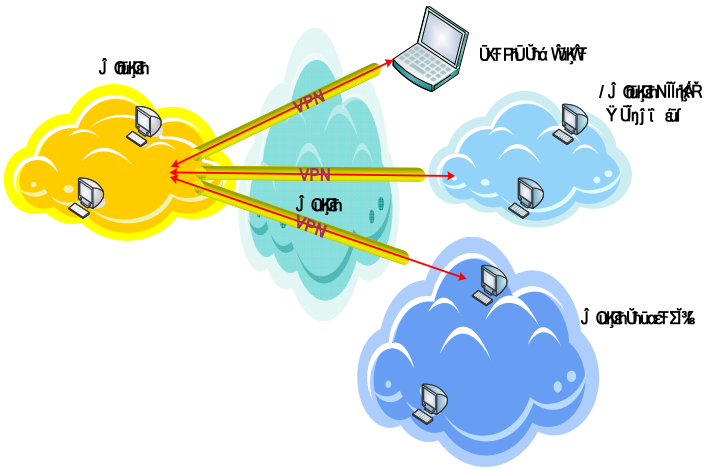
۵-۱۱- شبکه خصوصی مجازی[2] (VPN)

---

[1] Intrusion detection system

[2] Virtual Private Network

VPN شبکه داده‌ای خصوصی است که دارای زیرساخت‌های عمومی می‌باشد و محرمانگی داده‌ها را توسط پروتکل‌های تونل و روال‌های رمزنگاری تأمین می‌نماید. در شکل زیر (صفحه بعد) نمونه‌ای از به‌کارگیری شبکه‌خصوصی مجازی را مشاهده می‌کنید.



شبکه vpn(تصویر شمار هفت)

هدف از VPN ارائه قابلیت‌های خط اختصاصی leased با هزینه کمتر و از طریق شبکه معمولی است. از کاربردهای VPN می‌توان به موارد زیر اشاره کرد: ایجاد اینترانت‌های وسیع، ایجاد اکسترانت و ایجادAccess VPN.

Access VPN: امکان دست‌رسی به شبکه داخلی سازمان را از طریق شبکه عمومی و به صورت موقت فراهم می‌آورد. از این نوع VPN زمانی استفاده می‌شود که نیاز به اتصال امن و موقتی باشد بنابراین کاربران متحرک, کاربران دور و حتی دفاتر شعباتی که نیاز به اتصال دائمی به VPN ندارند می‌توانند با شماره‌گیری ISP محلی به شبکه داخلی سازمان دست‌رسی داشته باشند.

Intranet VPN: دفاتر مرکزی سازمان، دفاتر دور و شعبات را از طریق شبکه عمومی به شبکه داخلی سازمان متصل می‌کند. می‌توان گفت که شبکه‌ها اتصالی دائمی دارند (در این نوع VPN دفاتر و یا شعبات یک خط اختصاصی از ISP دارند ونیازی به شماره گیری ندارند).

Extranet VPN: علاوه بر کاربران و شعبه‌های سازمان، دست‌رسی محدودی را برای شرکا و کاربران خارج از سازمان از طریق شبکه عمومی اینترنت فراهم می‌آورد.

لازم به ذکر است که در هر یک از انواع VPN, بحث احراز هویت می‌تواند با استفاده از کلید اشتراکی و یا گواهی دیجیتالی صورت بگیرد. عموماً در حالتی که تعداد سرویس‌گیرندگان کم است از کلید اشتراکی و در حالتی که تعداد سرویس‌گیرندگان زیاد است از گواهی دیجیتالی برای احراز هویت استفاده می‌گردد. برای این که VPN بتواند سرویس‌های یک شبکه خصوصی را ارائه دهد باید دو تکنیک زیر را دارا باشد.

تونل کردن (Tunneling): پروتکل TCP/IP تنها بسته‌های IP با آدرس معتبر را مسیریابی می‌کند. بنابراین برای مسیردهی کردن یک بسته غیر IP یا یک بسته IP با آدرس غیرمعتبر باید آن را در یک بسته IP با آدرس معتبر قرار داد. این فرآیند مانند آن است که یک تونل بر روی اینترنت ایجاد شده است.

رمزنگاری: رمزنگاری برای محرمانه کردن محتوای داده‌های کپسوله شده استفاده می‌شود تا در مقابل حملات محافظت شود. همین‌طور در VPN برای تعیین هویت کاربر از کلیدهای عمومی یا خصوصی استفاده می‌شود.

استانداردهای مختلفی برای پیاده‌سازی یک VPN مطرح است که مهم‌ترین آن‌ها عبارتند از:

(Point-to-Point Tunneling Protocol) PPTP

(Layer Two Tunneling Protocol) L۲TP

(IP Security) IP Sec

که از بین آن‌ها استاندارد IP Sec که یک استاندارد لایه سوم است انتخاب به‌تر و امن‌تری است.

۵-۱۲- امنیت سیستم عامل

حتی اگر یک سیستم به سطح خوبی از اطمینان رسیده باشد، اما هنوز احتیاج به فرآیندهای پیکربندی، مانیتورینگ و سازماندهی دقیق دارد تا به آن سیستم امن گفته شود. هر سیستم‌عاملی ضعف‌ها و قوت های امنیتی خود و روش‌های امن مخصوص خود را دارد.

کاوشگر اینترنتی مایکروسافت تقریبا به‌ترین راه برای نفوذ یک هکر به رایانه‌های شخصی است. نقاط ضعف امنیتی زیادی تاکنون در این نرم افزار گزارش شده است که در صورتی که این نرم افزار به‌روز رسانی نشود می‌تواند خطرساز باشد. این ضعف‌ها حتی به یک هکر اجازه می‌دهند تا کنترل رایانه را بطور کامل در اختیار گیرد.

در این سیستم عامل اغلب مسئولیت سنگین امن کردن سیستم بر عهده مدیر سیستم است. مهم‌ترین ضعف‌های سیستم عامل ویندوز را می‌توان در موارد زیر خلاصه کرد:

کاربران آموزش داده نشده: این سیستم عامل برای توده مردم طراحی شده است و افراد زیادی بدون دانستن و مراقبت از خطرهای امنیتی با پیکربندی نادرست سیستم کار می‌کنند.

سیستم تجاری: ویندوز همیشه ابتدا یک سیستم عامل ساده و آسان ارائه می‌دهد که چندان امن نیست و بعد با افزودن قابلیت‌های جدید از مشتری‌ها می‌خواهد آن را به روز رسانی کنند. طبیعت تجاری ایجاب می‌کند نسخه‌های جدید از نسخه‌های قبلی که امن نیستند هم حمایت کند، علاوه بر آن که با ارائه هر قابلیت جدیدی مجموعه‌ای از آسیب‌پذیری‌های جدید همراه است.

رسیدگی ضعیف: قابلیت رویدادنگاری سروری در ویندوز ضعیف است، مشاهده کننده وقایع (event-viewer) آن چندان کامل و امن عمل نمی‌کند.

فرآیند نصب ناامن: در ویندوز روی گزینه‌های امنیتی پیش‌فرض کار چندانی نشده است و در صورتی که از به‌روز معمول نصب کن و فراموش کن استفاده شود بسیاری از آسیب‌پذیری‌ها باز باقی می‌مانند.

۵-۱۳- محکم‌سازی سیستم

محکم‌سازی سیستم[۱] یک اصطلاح رایج در زمینه امنیت سیستم‌هاست که نه تنها برای تشخیص مشکلات بلکه بر جلوگیری از پیدایش مشکلات تاکید دارد. محکم‌سازی یک فرآیند گام به گام برای امن کردن یک سیستم در جهت قابلیت اطمینان بالاتر و جلوگیری از دسترسی غیر مجاز است. گام‌های اصلی در محکم‌سازی سیستم شامل موارد زیر است:

اطمینان از قابل امن بودن سخت افزارها، شامل امنیت فیریکی و بالابردن دسترس‌پذیری‌ها.

انتخاب و نصب یک سیستم‌عامل مناسب و کامل. نصب service packها، تصحیح کلیه آسیب‌پذیری های شناخته شده و رعایت کلیه مواردی که در بخش امنیت سیستم‌عامل بیان شد.

نصب و پیکربندی فایل سیستم‌ها شامل پیکربندی لیست‌های کنترل، مدیریت‌مجوزها، فعال‌سازی سرویس‌های رسیدگی و رویدادنگاری

سیستم‌عامل‌های انتخابی باید از تکنولوژی‌های تحمل‌پذیری خطا حمایت کند.

پیکربندی سرویس‌ها و برنامه‌های کاربردی، نصب تنها سرویس‌های مورد نیاز، به‌روز رسانی سرویس‌ها و برنامه‌های کاربردی، تصحیح کلیه آسیب‌پذیری‌های شناخته شده، نصب تنها نرم‌افزارهای مطمئن و تست شده، حذف کلیه سرویس‌ها و برنامه‌های غیر ضروری، تنظیم کنترل دسترسی برای برنامه‌های کاربردی ممکن، حذف کلیه داده‌های مثالی.

پیکربندی کلیه اسکریپت‌ها و اپلت‌های سمت سرور.

---

۱ System Hardening

۵-۱۴- سیاست‌های امنیت سیستم‌عامل

امروزه تقریباً سیستم عامل ویندوز در زمینه سیستم عامل رایانه‌های شخصی بیش‌ترین استفاده را دارد. ذیلاً نکات اساسی که می‌بایست برای امنیت ویندوز در نظر داشت مورد بررسی قرار می‌گیرند.
میکروسافت این تدابیر امنیتی را با نام Security Checklist می‌شناسد که در حقیقت موارد و نکاتی است که یک مدیر سیستم می‌بایست برای حفظ امنیت سرور خود رعایت نماید. این تدابیر امنیتی به‌طور خلاصه ذیلا ارائه شده است:

استفاده از فایل سیستم‌های مخصوص هر ویندوز در پارتیشن‌های سرور.

استفاده از کلمه‌های عبور مطمئن‌تر برای مدیریت سیستم.

حذف و یا از کار انداختن سرویس‌های غیر ضروری.

حذف Account های غیر ضروری.

غیر فعال نمودن Guestدر صورت وجود.

غیر فعال نمودن Remote Registry در صورت وجود.

نصب آخرین Service Packها و وصله‌های(Patch) ارائه شده توسط میکروسافت.

بررسی کنترل دست‌رسی‌ها را در Registry.

محدود کردن دست‌رسی به اطلاعات امنیتی داخلی، از قبیل این‌که چه کاربرانی بر روی سیستم تعریف شده‌اند و هر کدام چه مجوزهایی دارند.

نظارت در انتخاب کلمه عبور توسط کاربران سیستم.

استفاده از سیاست قفل کردن Account برای مقابله با حملات Brute Force.

تغییر نام مدیر سیستم.

حذف Share Folderهای بلااستفاده، در صورت استفاده از سرویس File and Printer Sharing.

از کار انداختن Null Session در صورت وجود.

اعمال تنظیمات امنیتی مناسب بر روی Shareهای باقیمانده.

استفاده از قالب‌های امنیتی(Security Template) تعریف شده.

استفاده از نرم افزارهای Anti Virus.

البته باید به خاطر داشت با انجام این اقدامات , سیستم عامل برای همه امن خواهد شد به غیر از تولیدکنندگان سیستم عامل.

۵-۱۵- امنیت در سرورها

سرورها در یک شبکه رایانه‌ای مانند اینترنت و غیره می‌تواند با اهداف گوناگونی مانند وب، انتقال فایل، پست الکترونیک، بانک داده و ... مورد استفاده قرار گیرند.

نقش هر یک از سرورهای موجود در شبکه می‌بایست مشخص شود. یعنی یک مدیر سیستم می‌بایست بداند که هر کدام از سرورها چه نقشی در شبکه ایفا می‌کنند.

سیاست‌های امنیتی کلی سازمانی که شبکه در آن قرار دارد باید مشخص شود. یک مدیر سیستم باید دقیقاً بداند که چه منابعی و سرویس‌هایی در شبکه وجود دارد و هر یک از کاربران شبکه چه سطح دست‌رسی به این منابع و سرویس‌ها دارند. سیاست‌های امنیتی به‌طور کامل بر روی تمامی رایانه‌های سرور اجرا شود.

تمامی سرویس‌ها و امکانات غیر ضروری که در لیست وظایف یک سرور نیست می‌بایست بر روی سرور مورد نظر غیر فعال شود.

هر یک از سرورها از نظر خود سیستم عامل، سیستم فایل و سرویس‌هایی که روی آن‌ها نصب شده امن شوند.

۵-۱۶- امنیت در سیستم های Desktop

یک مدیر سیستم می‌بایست تمامی سیستم‌های مرتبط با سرورهای حساس خود را به‌طور کامل امن کند. هکرها در بسیاری از موارد ابتدا به سراغ رایانه‌های جانبی مثل سیستم‌های ویندوز شخصی می‌آیند چون می‌دانند مدیران سیستم به امنیت آن‌ها توجه چندانی نمی‌کنند. نفوذ یه این رایانه‌های جانبی که با سرورهای حساس شما در ارتباط هستند تقریبا معادل است با در اختیار گرفتن کامل سرورهای شما توسط عامل نفوذی. کافی است یک مدیر سیستم تنها یک بار از رایانه شخصی خود به سرورمورد نظر وارد شود تا عامل نفوذی کلمه عبوری و سایر اطلاعات حساس سرور را برباید.

۵-۱۷- سئوالات خودآزمایی

کنترل دسترسی را توضیح داده و بنویسید بر چه اساسی کنترل دسترسی صورت می پذیرد؟

سیاست های کلی کنترل دسترسی را بنویسید.

انواع رمزنگاری را نام ببرید.

اختلافات رمزنگاری متقارن و نامتقارن را بنویسید.

سیاست های کلی رمزنگاری را در امنیت اطلاعات بنویسید.

اقسام برنامه های مزاحم و مخرب را نوشته و توضیح دهید.

انواع دیواره های آتش را نام ببرید.

سیاست های کلی انتخاب دیواره های آتش را بنویسید.

۶

فصل ششم - نگهداری و پشتیبانی امنیتی

آن‌چه در این فصل می‌خوانید

نظارت و ارزیابی امنیتی

سیاست‌های نظارت امنیتی

نصب، پیکربندی و کنترل تغییرات

سیاست‌های مدیریت پیکربندی

سیستم‌هایی با دسترسی بالا

مدیریت تحمل‌پذیری خطا - پایداری سیستم

خوشه‌بندی

سیاست‌های دسترس‌پذیری بالا

مدیریت حوادث

سیاست‌های مدیریت حوادث

۶- نگهداری و پشتیبانی امنیتی

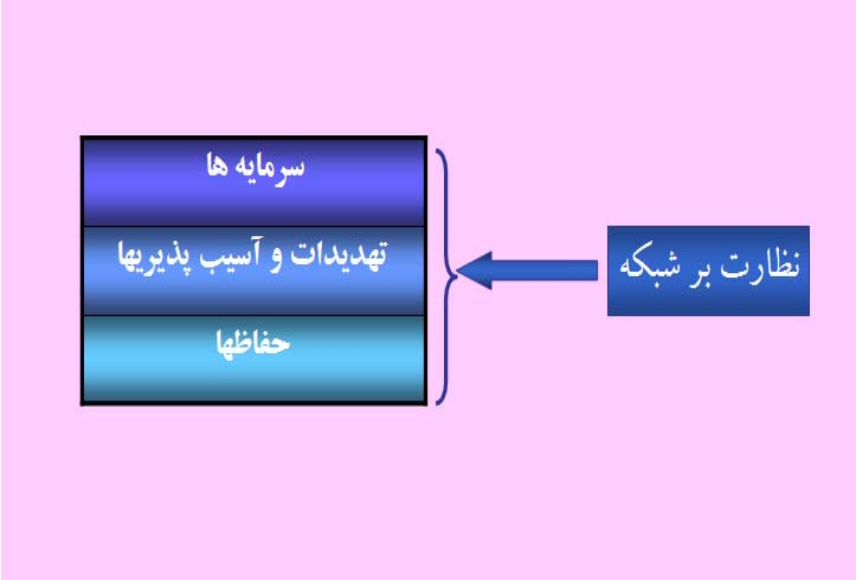
نگهداری و مدیریت حفاظ‌ها از لحاظ اطمینان از صحت عمل‌کرد آن‌ها از مباحث بسیار مهم می‌باشد. در اکثر موارد در ابتدا، سیستم و سرویس‌ها موجود هست و امنیت در مرحله دوم اضافه شده، در طول زمان فراموش می‌شود. به این معنی که توجه نسبتاً کمی روی نگهداری و ارتقای امنیت، وجود دارد. مسئله دیگری که باید مورد بررسی قرار گیرد قدیمی شدن حفاظ‌هاست. بنابراین، بازرسی برآورد امنیتی، نظارت بر محیط عملیاتی، بازبینی فایل‌های رویدادنامه و رسیدگی به حوادث امنیتی جهت اطمینان از امنیت مداوم، لازم و ضروری به نظر می‌رسد.

۶-۱- نظارت و ارزیابی امنیتی

هزینه پیش‌گیری از یک حادثه امنیتی همیشه کم‌تر از بازیابی و کنترل آن است. به همین خاطر ارزیابی استراتژی‌های امنیتی، شناسایی نقاط ضعف و قدرت وضعیت امنیتی فعلی، اندازه‌گیری خطرات امنیتی بر روی زیرساخت‌های IT و داده‌های حیاتی، کشف رخنه‌ها و آسیب‌پذیری‌های امنیتی از جمله امور ضروری برای مدیریت امنیت یک سازمان است.

اصولاً نظارت بر شبکه، یک فعالیت مداوم است که چگونگی سیستم را از لحاظ کاربران و میزان امنیت محیطی تعیین شده آن، بر طبق طرح امنیتی بررسی می‌کند. یک طرح نظارت بر شبکه به شکل روزانه باید به‌گونه‌ای تنظیم شده باشد که، راهنماها و روال‌های اضافی جهت اطمینان از عملیات امن در حال انجام را نیز ایجاد کند. کاربران، پرسنل عملیاتی و طراحان سیستم باید به صورت دوره‌ای با یک‌دیگر جلسات مشاوره داشته باشند تا این اطمینان حاصل شود که کلیه موارد امنیتی اجرا شده به صورت کامل انجام می‌شود و طرح امنیتی به‌روز می‌باشد. یکی از دلایلی که نظارت شبکه از مهم‌ترین

بخش‌های نگهداری امنیت ICT عنوان می‌شود این است که، این فرآیند، راهی جهت شناسایی تغییرات مربوط به امنیت سیستم است. مواردی که باید در نظر گرفته شود و روی آن‌ها نظارت و بررسی صورت گیرد، سرمایه‌ها و ارزش آن‌ها، تهدیدات و آسیب‌پذیری‌ها روی این سرمایه‌ها و حفاظ‌هایی که جهت محافظت از این سرمایه‌ها به‌کار می‌رود، هستند که در شکل زیر دیده می‌شود.



شکل نظارت بر شبکه (تصویر شماره هشت)

نظارت بر سرمایه‌ها به این منظور صورت می‌گیرد تا هرگونه تغییرات در مقدار و ارزش سرمایه‌ها شناسایی شود. این نتایج جهت شناسایی تغییرات در اهداف امنیتی سیستم ICT به‌کار می‌رود. دلایلی که ممکن است سبب این تغییرات شوند به‌صورت زیر می‌باشد:

اهداف تجاری سازمان.

کاربردهای در حال اجرا

اطلاعاتی پردازش شده

تجهیزات

نظارت بر تهدیدات و آسیب‌پذیری‌های شبکه به منظور تشخیص تغییرات در میزان شدت آن‌ها صورت می‌گیرد. (به عنوان مثال، دلایل تغییرات محیطی، ساختاری یا امکانات تخصصی) و در واقع هدف شناسایی نمودهایی از دیگر تهدیدات و آسیب‌پذیری‌هاست که یک مرحله جلوتر از وقوع آن‌ها صورت گیرد. تهدیدات و آسیب‌پذیری‌ها ممکن است با تغییرات روی سرمایه‌ها، تحت تأثیر قرار گیرند. کلیه تغییرات روی سرمایه‌ها، تهدیدها، آسیب‌پذیری‌ها و حفاظ‌ها می‌تواند تأثیر زیادی در خطر پذیری داشته باشد و کشف زود هنگام تغییرات سبب جلوگیری از اتفاقی که ممکن است صورت بگیرد می‌شود.

نظارت بر حفاظ‌های شبکه به این منظور صورت می‌گیرد تا کارایی و میزان تأثیرگذاری آن‌ها بر روی زمان، بررسی شود. باید این اطمینان حاصل شود که این حفاظ‌ها و محافظتی که توسط آن‌ها روی سیستم ICT صورت می‌گیرد، مناسب و کافی و در سطح مورد نیاز می‌باشد. این امر امکان پذیر است که تغییرات روی منابع، تهدیدات و آسیب پذیری‌ها روی کارایی و توانایی حفاظ‌ها تأثیر گذارد.

علاوه بر این موارد، زمانی که سیستم‌های ICT جدید، ایجاد شد یا زمانی‌که تغییرات سبب به‌وجود آوردن سیستمی دیگر شد، نیاز خواهیم داشت تا مطمئن شویم تغییراتی از این قبیل، تأثیری روی وضعیت حفاظ‌های موجود و سیستم های جدید ایجاد شده با این حفاظ‌های امنیتی، نخواهد داشت.

زمانی‌که رفتارهای ناسازگار در فرآیندهای امنیتی دیده می‌شود، در این مرحله نیاز به بررسی و رسیدگی احساس شده و هم‌چنین ضرورت دارد گزارش نتایج بدست آمده، به مدیریت ارائه شود تا بازبینی‌های امکان پذیر از حفاظ‌ها صورت پذیرد و یا در صورت خطرات جدی این فرآیندها، باید به بررسی و بازبینی سیاست امنیتی سیستم ICT و هم‌چنین تحلیل خطر پذیری پرداخته شود.

این مرحله در طراحی و پیاده‌سازی امنیت مرحله‌ای است که تا زمانی که یک سازمان به حیات خود ادامه می‌دهد در تکرار است و پایان ندارد. سطح امنیتی سازمان باید اندازه‌گیری و تست شده مورد ارزیابی قرار گیرد، وضعیت شبکه‌های آن مانیتور شود، گزارش‌های امنیتی و اخبار مربوط به حملات و

مشکلات امنیتی جدید مرور شوند و تا با بازنگری سیاست‌های امنیتی، تعریف مجدد رویه‌های امنیتی، اعمال patchها و fixهای مورد نیاز، تغییر و بهینه‌سازی ابزارهای تأمین کننده‌ی مورد نیاز، استفاده از ابزارهای جدید و ... سطح امنیتی سازمان بالاتر و بالاتر رود. به منظور اطمینان از تبعیت سیاست امنیتی سیستم ICT، بعضی از منابع مهم باید به صورت روزانه نظارت شوند. این منابع عبارتند از:

حفاظ‌های جاری

ایجاد سیستم‌ها یا سرویس‌های جدید

تغییرات طرح ریزی شده برای سیستم‌ها یا سرویس‌های جاری

اکثر حفاظ‌ها خروجی‌هایی به‌شکل رویدادنامه از وقوع حوادث، ایجاد می‌کنند. روی این وقایع ثبت شده باید به صورت دوره‌ای بازبینی صورت گیرد و در صورت امکان با استفاده از روش‌های آماری مورد تحلیل واقع شوند. با استفاده از این نتایج، در نهایت در زمان کوتاه‌تری تغییرات، شناسایی شده و از تکرار اتفاقات ناگوار جلوگیری خواهد شد. نظارت باید شامل روال‌هایی جهت گزارش دهی منظم به مسئول امنیت ICT مربوطه و هم‌چنین مدیریت باشد. لازم است مسئولیت مشخصی به منظور تحلیل این رویدادنامه تعیین شود.

در محیط‌های توزیع شده، ثبت وقایع ممکن است فقط روی اطلاعات مربوط به یک محیط صورت گیرد. برای این‌که ماهیت یک حادثه پیچیده به‌درستی فهمیده شود، لازم است که اطلاعات مربوط به وقایع ثبت شده متفاوت را در یک جا جمع کرده و آن‌ها را ترکیب کرده و به‌صورت یک حادثه واحد، ثبت کرد. این حادثه ثبت شده، باید در معرض تحلیل قرار گیرد. ترکیب حوادث ثبت شده کار پیچیده‌ای است و مهم‌ترین بخش آن شناسایی پارامتر یا پارامترهایی است که اجازه می‌دهد وقایع ثبت شده متفاوت با اطمینان در یک‌جا ترکیب شوند.

تکنیک مدیریتی در جهت کنترل نظارت روزانه‌ی شبکه، آماده سازی سندی تحت عنوان روال‌های عملیاتی امنیت[۱]، به منظور فعالیت‌های مورد نیاز، می‌باشد. این سند کلیه اقدامات لازم را جهت

---

۱ Securing Operating Procedure

اطمینان از مراحل امنیتی کلیه سیستم‌ها و سرویس‌های نگهداری شده توضیح می‌دهد ولی، شامل سیستم‌ها و سرویس‌هایی که در حال بررسی و توسعه هستند، نمی‌شود. هم‌چنین باید روال‌هایی جهت نظارت حفاظ‌های امنیتی شرح داده شود و خط مشی و بسامد بازبینی رویدادنامه‌ها باید تعیین گردد. استفاده از روش‌های تحلیل آماری و ابزار آن باید مشخص شده باشد. در دستورالعمل‌ها باید چگونگی تنظیم آستانه‌های بازرسی بر پایه شرایط عملیاتی متفاوت، تعیین شده باشد.

۶-۲- سیاست‌های نظارت امنیتی

سازمان باید روال‌هایی برای ارزیابی امنیتی سیستم‌ها و شبکه خود داشته باشد که به صورت دوره‌ای بازدید شده، نقاط ضعف برای اصلاح به بخش‌های مربوطه اطلاع داده شود.

در مرحله اول باید یک آشنایی کلی از دیدگاه عملیاتی هر سازمان نسبت به مقوله امنیت به دست آورد. مرحله دوم ارزیابی وضعیت امنیت سیستم‌ها، در نهایت برنامه‌های کاربردی، تجهیزات و شبکه است. این ارزیابی به کمک بخش مبارزه با حوادث امنیتی آمده برنامه‌ای برای تشخیص، دفاع و پاسخ‌گویی به حملات رایانه‌ای طراحی می‌شود.

از طریق پویشگرهای پورت به منظور مشخص کردن تمام میزبان‌های فعال موجود در شبکه سازمان، سیستم عامل‌های آن‌ها، سرویس‌های موجود و برنامه‌های کاربردی روی آن‌ها می‌توان بهره برد.

پویش آسیب‌پذیری به منظور تشخیص رخنه‌های مربوط به سیستم‌عامل‌ها و برنامه‌های کاربردی، تست انطباق وضعیت شبکه با سیاست‌های امنیتی و ایجاد آمادگی برای انجام تست نفوذ صورت می‌گیرد. این پویشگرها در دو نوع پویشگر شبکه و پویشگر میزبان بوده، به‌تر است حداقل ماهی دو بار در مورد سیستم‌های اساسی و حداقل هر چهار ماه یک بار در مورد سایر سیستم‌ها صورت گیرد.

باید امکان رویدادنگاری کلیه برنامه‌ها و سیستم‌های ممکن فعال بوده، به‌گونه‌ای تنظیم گردد که اطلاعات مفید از دست نرود. هم‌چنین برای استفاده درست از این logها باید سیستم‌ها هم‌زمان بوده، در صورت نیاز log فایل‌های تولید شده در سیستم‌های مختلف باهم ترکیب گردند. برای پردازش Log فایل‌های تولید شده می‌توان از ابزار تحلیلگر log فایل‌ها بهره گرفت که برحسب شرایط تنظیم شده به طور اتوماتیک به بررسی Log فایل‌ها که اغلب شامل اطلاعات حجیم، خام و آشفته‌ای است می‌پردازد. تنظیم و پیکربندی سرویس‌های تهیه logها باید با دقت صورت گیرد به گونه‌ای که هر اطلاعات مهم و مفیدی را ثبت کند.

مانیتورینگ امنیتی شبکه به معنای جمع‌آوری، آنالیز علائم و اخطارها برای تشخیص نفوذها و پاسخ‌گویی به آن‌هاست. تعریف و شاخص‌گذاری برای این علائم و اخطارها امر مهمی است که باید مورد توجه قرار گیرد. مانیتورینگ می‌تواند به صورت برخط صورت گرفته و اخطارهای اولویت‌بندی و دسته

بندی شده برای مدیران ارسال شود. به این منظور باید خصوصاً کلیه گذرگاه‌های اتصال شبکه سازمان به شبکه‌های بیرونی و اینترنت به‌دقت مانیتور شود.

هر سیستم IT می‌تواند بر اساس یک‌سری فرآیندها یا روال‌ها تعریف شده برای سازگاری با چک لیست تعریف شده‌ای مقایسه شود. به مکانیزم تأیید این‌که فرآیند یا روال با چنین چک تطبیق دارد رسیدگی می‌گویند. در بسیاری از سازمان‌ها سیاست‌های امنیتی این چک‌لیست را تعریف می‌کند. مثلاً تمام کلمات عبور باید از ۸ حرف بیش‌تر بوده، هر ماه عوض شود. روش بررسی سازگاری هم اغلب مشخص و واضح است. امکان رسیدگی در هر سیستمی اطلاعاتی در مورد عملیاتی که ممکن است بر روی امنیت سیستم اثر بگذارد را ثبت می‌کند. برای هر عملی، اطلاعات کافی در مورد آن از جمله رد انجام‌دهنده آن عمل، تاریخ و زمان دقیق آن، وضعیت موفقیت یا شکست آن، نام، نوع، وسیله، فایل، داده یا هر چیزی که عمل بر روی آن صورت گرفته و. .. ثبت می‌شود. ثبت و رسیدگی به دو شکل ممکن است: ثبت وقایع و اتفاقات شامل اتفاقات سیستم، برنامه‌های کاربردی، کاربران، شبکه و. ... و یا ثبت هر چیز برای مانیتورینگ و کنترل. این ثبت‌ها و logها باید به طور دائم و متناوب بازبینی شود که بازبینی‌ها می‌تواند بلادرنگ و اتوماتیک باشد.

۶-۳- نصب، پیکربندی و کنترل تغییرات

از آن‌جا که ایجاد تغییرات در یک سازمان اجتناب‌ناپذیر است، یکی از بخش‌های لازم امنیت، مدیریت تغییرات یا پیکربندی است. هدف از این مقوله اطمینان از اعمال این تغییرات به صورت کاملاً کنترل شده و شناخته شده و مطلوب می‌باشد. چرخه مراحل مختلف برای مدیریت تغییرات و پیکربندی در شکل زیر (صفحه بعد) نمایش داده شده است.

فرآیند نصب , پیکربندی و کنترل(تصویر شماره نه)

از یک نگاه دیگر مدیریت پیکربندی را می‌توان به سه وظیفه اصلی تقسیم نمود:

شناسایی: روال‌های مدیریت پیکربندی باید شخص را قادر به شناسایی پیکربندی یک سیستم به منظور کنترل تغییرات و نگهداری یک‌پارچه پیکربندی کند. ثبت جزئیات و به روزرسانی اطلاعاتی که سیستم ها و شبکه‌های یک سازمان را (شامل قطعات نرم‌افزاری و سخت‌افزاری) توصیف کند از وظایف این بخش است. چنین اطلاعاتی به طور عمومی شامل ویرایش‌ها و وصله‌هایی[۱] که به نرم‌افزارهای نصب شده اعمال شده‌اند و آدرس‌های محلی و شبکه‌ای تجهیزات سخت‌افزاری نیز می‌شوند. زمانی که یک سیستم به ارتقا نیاز دارد مدیر پیکربندی با مراجعه به برنامه پیکربندی و بانک اطلاعاتی آن می‌تواند

---

۱ Patch

وضعیت موجود را مشاهده کند. شناسایی پیکربندی باید در مراحل اولیه طراحی و توسعه سیستم امنیت سازمان صورت گیرد.

کنترل پیکربندی: کنترل پیکربندی شامل ارزیابی، هماهنگی، تصویب یا رد همه تغییرات پیش‌نهاد شده یا تقاضا شده می‌باشد.

حساب‌رسی وضعیت پیکربندی: هدف اصلی از این مرحله ثبت و گزارش‌گیری از کلیه اطلاعاتی است که برای فرآیند مدیریت پیکربندی حائز اهمیت می‌باشد. این که چه چیزی مهم است در برنامه مدیریت پیکربندی گفته می‌شود. این عمل به منظور ردگیری تغییرات در یک شکل ساختار یافته و به روز صورت می‌گیرد. این ثبت‌ها و گزارشات باید شامل وضعیت پیکربندی فعلی، لیست تاریخچه تغییرات، طراحی‌های اصلی و وضعیت تقاضاهای تغییرات و پیاده‌سازی آن‌ها با قابلیت ردگیری همه تغییرات باشد. وقتی یک تغییر به یک سیستم اعمال می‌شود، باید برای چگونگی تأثیر آن بر روی دیگر اعضای سیستم مرور و رسیدگی شود. این امر شامل مرور و تست همه نرم‌افزارها و سخت‌افزارهای سیستم جهت اطمینان از این که تغییر به شکل صحیح صورت گرفته می‌باشد.

۶-۴- سیاست‌های مدیریت پیکربندی

برنامه مدیریت پیکربندی و تغییرات باید در ابتدای ایجاد مدیریت پیکربندی طراحی شود. این برنامه باید با دستورالعمل‌های ساده و واضح باید آن‌چه در جریان مدیریت پیکربندی صورت می‌گیرد را شرح دهد. این که چگونه باید وظایف مدیریت پیکربندی شامل شناسایی، کنترل، حساب‌رسی و رسیدگی با جزئیات مهم آن اجرا شوند تا تغییرات با به‌ترین وجه به سیستم اعمال گردد.

تنها مدیران سیستم باید قادر به نصب نرم‌افزار بر روی سرورها باشند. هم‌چنین کلیه تغییرات از جمله تغییرات فیزیکی و شبکه‌ای باید با اطلاع مدیر تغییرات صورت گیرد. فرد یا افراد مسئول برای مدیریت و پیکربندی و تغییرات مشخص شود.

لیستی از کلیه نرم‌افزارها، سخت‌افزارها پیکربندی‌های سیستم، خصوصیات شبکه برای هر سرور مانند سطح سرویس آن وضعیت موقعیت و سرویس‌گیرنده‌های آن با کلیه توضیحات مورد نیاز به صورت در یک بانک اطلاعاتی مخصوص نگهداری شود.

لیستی از تغییرات صورت گرفته (چه کسی، چه کاری و چه موقع انجام داده است) بر روی سرورها و ایستگاه‌های کاری مهم نگهداری شود.

نصب نرم‌افزارها و سیستم عامل‌ها کامل و با کلیه وصله‌های موجود صورت گیرد.

توصیه می‌شود از نرم‌افزارهای اتوماتیک که به صورت امن و موازی تغییرات و به‌روزرسانی‌ها را بر روی چندین سرور به طور هم‌زمان اعمال می‌کنند استفاده شود. این نرم‌افزارها باید امکان بازگشت به قبل[۱] را داشته باشند تا در صورت بروز مشکل و یا هر دلیل دیگر به راحتی بتوان به یک یا چند مرحله پیکربندی قبل بازگشت.

کلیه تجهیزات، نرم‌افزارها و سخت‌افزاری هر سیستم باید برای بهره‌گیری امن و محدود کاربران پیکربندی و تنظیم شده باشند. این پیکربندی مسائل زیادی را در بر می‌گیرد از جمله تنظیمات درایورهای سیستم، پورت‌های ارتباطی، تعیین ترتیب اولویت درایوها در زمان Boot سرویس‌دهنده‌ها، تعیین نحوه تخصیص آدرس IP به سیستم‌ها، تنظیم نرم‌افزارهایی مانند فایروال‌های شخیص سیستم های تشخیص نفوذ مبتنی بر میزبان، آنتی‌ویروس‌ها و...

برای مثال در مورد پیکربندی دیواره‌های آتش مبتنی بر میزبان باید گام‌های مختلفی برداشت:

قدم اول: فعال‌سازی سیستم رویدادنگاری[۲] از تمام عملیات دیواره آتش.

قدم دوم: پیکربندی یک قانون اصلی مبنی بر ممنوع کردن دست‌رسی به تمام سرویس‌ها از هر منبعی به این معنی که هیچ بسته‌ای عبور داده نشود.

قدم سوم: ثبت قوانین زنجیره ورودی[۳] برای کاربرد مورد نیاز.

---

۱ rollback

۲ Logging

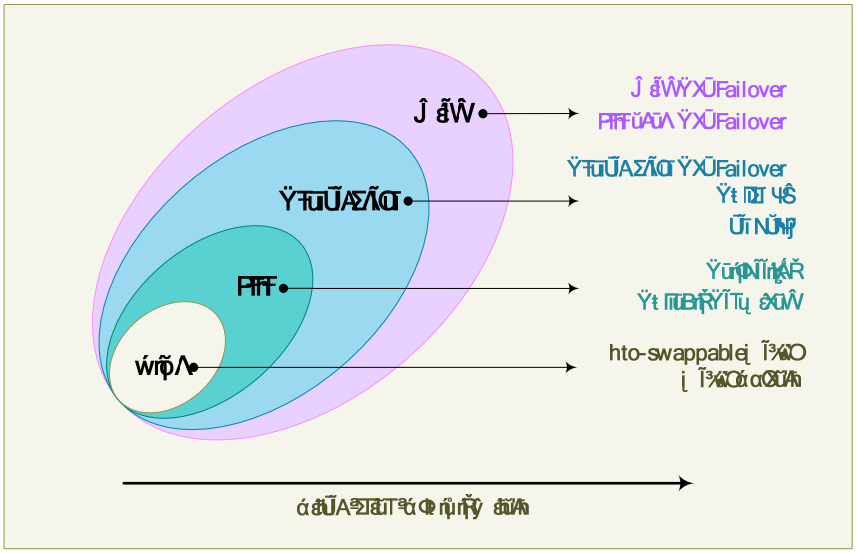
۳ Input chain

۶-۵- سیستم‌هایی با دسترسی بالا

امروزه میزان زمان وقفه قابل قبول برای سیستم‌های تجاری به سرعت در حال کاهش است و از چندین روز به چند ساعت، چند دقیقه و حتی چند ثانیه تقلیل یافته است. تمایل سیستم‌ها برای جهانی شدن باعث شده تا دسترس پذیری به صورت یک پارامتر اساسی در طراحی یک تجارت در نظر گرفته شود. برای بسیاری از سازمان‌ها، وابستگی به سیستم‌های رایانه‌ای و اطلاعات روی آن آنقدر شدید است که در دسترس نبودن آن می‌تواند باعث صدمه های سنگین به سیستم شود. در نتیجه امروزه بسیاری از سیستم‌ها نیاز دارند که ۲۴ ساعته و در هر هفت روز هفته ۲۴×۷ در دسترس باشند. یک شبکه یا یک سیستم بسیار امن بدون تدابیر دسترسی پذیری در واقع کارآمد نیست.

دسترس پذیری در سطوح مختلفی قابل طرح است. این سطوح به ترتیب در جهت افزایش پیچیدگی، کارایی و دسترس‌پذیری عبارتند از: سطح محیط، سطح داده، سطح برنامه‌کاربردی، و سطح سایت.

برای هر کدام از این سطوح راه‌حل‌های متعددی وجود دارد که در شکل زیر نمونه‌ای از آن‌ها را مشاهده می‌کنیم.



جدول دسترس پذیری سیستم(تصویر شماره ده)

۶-۶- مدیریت تحمل‌پذیری خطا ۱- پایداری سیستم

تحمل پذیری خطا یکی از ملزومات و راه‌حل‌های سیستم های با دست‌رسی بالاست. یک سیستم تحمل پذیر خطا سیستمی است که در شرایط خرابی۲ سخت‌افزار و یا نرم‌افزار بتواند هم‌چنان به عمل‌کرد صحیح خود در وظیفه‌ی مربوطه ادامه دهد. اساس کار در چنین سیستم هایی نیز بر مبنای افزونگی است که باید برای تمام قطعات سیستم در نظر گرفته شود.

انواع خطاهایی که ممکن است در یک سیستم رخ دهد شامل موارد زیر است: خطاهای نرم افزاری (مانند bugها)، خطاهای سخت‌افزاری (مانند خرابی‌های قطعات سخت افزاری یا واسط‌های آن‌ها)، خطاهای حالت۳ که نتیجه تفاوت بین درک یک ماشین هوشمند از محیط با محیط واقعی است، خطاهای زمان (وقتی رخ می‌دهد که یک کار نمی‌تواند به صورت بلادرنگ در زمان مشخص شده تمام شود).

چگونگی برخورد با خطا

در یک طراحی خوب برای سیستم بدون وقفه، خطا قبل از منتشرشدن، محبوس شده و برطرف می شود. در برابر مفهوم خطا، بسته به کاربردسیستم، عملیات مختلفی ممکن است انجام شود:

"جلوگیری از خطا۴ با مکانیزم‌هایی مانند کم کردن بار تقاضاها یا توزیع کردن آن‌ها، برطرف کردن خطا ۵ که ابتدا خطا دقیقاً تشخیص داده شده، سپس رفع می‌شود و بسیار هزینه‌بر است. تحمل کردن اشکال و گریز از اشکال۱ یا شناسایی انحرافات۲."

---

۱ Fault tolerant Management

۲ Failure

۳ State Error

٤ Fault Avoidance

٥ Fault Removal

۶-۷- پشتیبان‌گیری

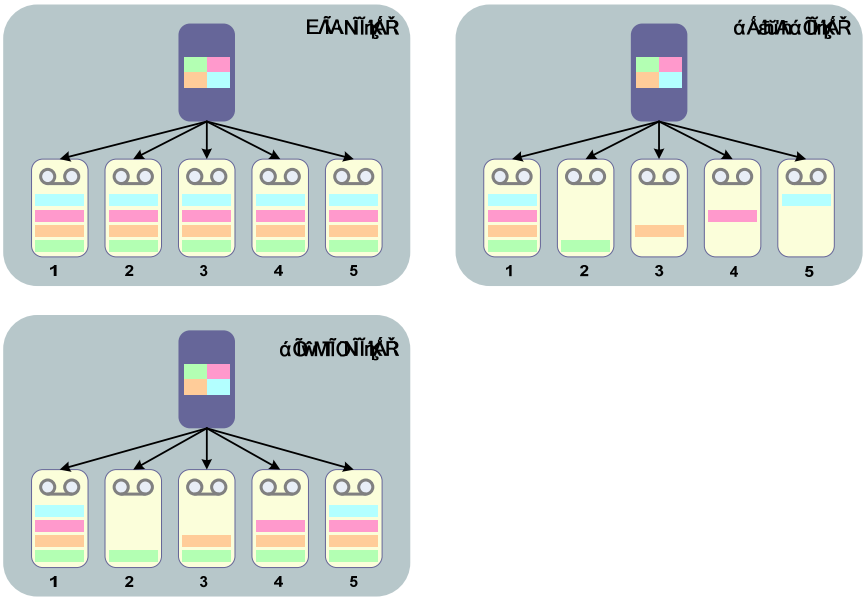
گرفتن نسخه پشتیبان از داده‌های مهم ضرورت غیر قابل انکاریست. هر چند که سیستم مطمئنی داشته باشیم باز امکان ایجاد اختلال وجود دارد. روش‌های مختلفی برای پشتیبان گیری وجود دارد. در روش پشتیبان کامل از کلیه داده‌های موجود پشتیبان تهیه می‌شود، چه داده‌ها تغییر کرده باشند چه بدون تغییر باشند. در روش پشتیبان افزایشی۳ تنها از فایل‌هایی پشتیبان تهیه می‌شود که بعد از آخرین نوبت پشتیبان‌گیری تغییر کرده باشند. روش پشتیبان ناهمسانی۴ مانند روش افزایشی است با این تفاوت که هر بار از فایل‌هایی‌که نسبت به آخرین پشتیبان‌گیری‌کامل تغییرگرفته‌اند پشتیبان گرفته می‌شود. (شکل زیر)

۱ Fault Evasion

۲ Aberration

۳ incremental backup

٤ differential backup



انواع پشتیبان گیری (تصویر شماره یازده)

۶-۸- خوشه‌بندی

یکی از تکنولوژی‌هایی که به عنوان یک راه حل کلیدی برای افزایش دسترس‌پذیری در سیستم‌های بزرگ استفاده می‌شود خوشه‌بندی است. خوشه یک گروه از رایانه‌های مستقل است که با یک‌دیگر کار می‌کنند و یک سیستم دیده می‌شوند و یک سرویس را ارائه می‌دهند. خوشه‌بندی را برای دست‌رسی بالا، تحمل خطا، توازن بار، پردازش موازی، مدیریت سیستم و توسعه‌پذیری توصیه می‌کنند. در صورتی که یک گره در یک خوشه دچار مشکل شود، خطا روی آن گره با کمک FailOver از کل سیستم مجزا شده و بار کاری به طور اتوماتیک روی گره‌های زنده پخش می‌شود. این کار یا به طور مستقیم باعث افزایش دسترس پذیری می‌شود و یا با تکنیک‌های توازن بار، به طور غیر مستقیم و با کم کردن بار هر سرور و در نتیجه کاستن احتمال خرابی آن. خوشه‌های با دست‌رسی بالا کمک می‌کنند.

۶-۹- سیاست‌های دسترس‌پذیری بالا

سازمان باید در جهت پشتیبان‌گیری از اطلاعات خود مراحل زیر را دنبال کند: طراحی زمان‌بندی پشتیبان‌گیری، تعیین فایل‌ها و اطلاعاتی که نیاز به پشتیبان دارند، انتخاب سخت‌افزارهای مورد نیاز، انتخاب مناسب نرم‌افزار پشتیبان‌گیری، تعیین محل نگهداری پشتیبان‌ها، توسعه رویه‌های ذخیره‌داده، توسعه رویه های بازیابی، توسعه رویه های کنترل و تست کردن پشتیبان‌ها.

سازمان باید با بررسی نیازها و محدودیت‌های خود باید روش پشتیبان‌گیری مناسب را انتخاب کند. برای مواقعی که نمی‌توان زمان زیادی را صرف پشتیبان‌گیری کرد و یا عملیات ذخیره و بازیابی پشتیبان‌ها خیلی به ندرت پیش می‌آید و یا هر بار فقط تعداد کمی از فایل‌ها تغییر می‌کند می‌توان از روش‌های پشتیبان‌گیری افزایشی یا پشتیبان‌گیری ناهمسانی که در آن هر چند وقت یک‌بار یک پشتیبان کامل و پس از آن به صورت دوره‌ای پشتیبان‌های افزایشی تهیه می‌شود. برای مواردی که محدودیت زمانی برای پشتیبان‌گیری وجود ندارد و یا نیاز به عملیات ذخیره و بازیابی زیاد اتفاق می‌افتد و یا هر بار اغلب فایل‌ها تغییر می‌کند به‌تر است از پشتیبان‌گیری کامل استفاده شود.

برای سرویس‌هایی که نیاز به دسترس‌پذیری بالا دارند باید از روش‌های پشتیبان‌گیری برخط استفاده شود که در طول مدت پشتیبان‌گیری سیستم قابل دست‌رسی باشد. در چنین مواردی باید راه‌حل‌هایی برای مسأله سازگاری پشتیبان با اصل (برای داده‌های در حال تغییر) در نظر گفته شود. برای موارد دیگر می‌توان به صورت برون‌خط و در ساعات غیراداری به پشتیبان‌گیری پرداخت.

در جهت افزایش اطمینان بیش‌تر و کاستن هزینه‌های مدیریتی و یک‌پارچه‌سازی به‌تر است از پشتیبان گیری‌های متمرکز استفاده نمود به این ترتیب که یک شبکه محلی جدا برای پشتیبان و بازیابی از تمام قسمت‌های سازمان استفاده نمود که در آن سرورها و کتابخانه‌های پشتیبان‌گیری به صورت پویا تمام اطلاعات پشتیبان را دریافت و مدیریت می‌کنند.

اطلاعات پشتیبان‌گیری‌ها باید در جایی غیر از محل خود سازمان و حتی شهرهای دیگر ذخیره شود تا در صورت بروز مشکلاتی مانند بلایای طبیعی پشتیبان‌ها سالم باقی مانند.

باید امنیت‌های فیزیکی لازم در جهت حفاظت پشتیبان‌ها رعایت شود.

پس از برآورد میزان اطلاعات پشتیبان‌گیری، سرعت مورد نیاز و هزینه در نظر گرفته شده باید نوع وسیله پشتیبان‌گیری را از بین انتخاب‌های متعددی مانند CD، DVD، نوار مغناطیسی، DAT۱ ، ۲ DLT، LTO۳ ، کتابخانه نوارها و ... انتخاب کرد.

سیستم‌هایی که سرویس‌های حیاتی۴ ارائه می‌دهند، برای بالا بردن میزان دسترس‌پذیری باید از تکنیک‌های خوشه‌بندی۵ استفاده کند. برای کاستن هزینه افزونگی خوشه‌بندی از نوع N+۱ که در آن چند سرور با یک سرور اضافی جهت failover گروه‌بندی می‌شوند توصیه می‌گردد. خوشه‌بندی در مورد سرویس‌های مهم‌تر می‌تواند علاوه بر روی سرور، به صورت چند سایته نیز صورت گیرد که این نوع بیش‌ترین میزان دسترس‌پذیری البته با اعمال هزینه بالا را در بر خواهد داشت.

سازمان باید برای کنترل و تحمل خطا در سیستم‌های خود برنامه‌ریزی کند، به این صورت که ابتدا رویکرد خود را در مواجهه با خط با توجه به سرویسی که ارائه می‌دهند تعیین نموده تجهیزات و نرم افزارهای لازم جهت پیاده‌سازی این رویکرد تهیه نماید.

۶-۱۰- مدیریت حوادث

برنامه‌ریزی برای کنترل حوادث و بازیابی پس از آن به مجموعه‌ای از فعالیت‌های پشتیبانی جهت کم کردن احتمال و محدود کردن صدمات حاصله از یک حادثه بر روی فرآیندهای سازمان می‌گویند. هدف سازمان از ارائه چنین طرحی تأمین تداوم امنیت شبکه است. منظور از حوادث امنیتی اغلب حوادث مشخصی شامل از کاراندازی سرویس۶ کدهای مخرب دست‌رسی غیرمجاز و استفاده نامناسب می‌باشد.

---

۱ Digital Audio Tape

۲ Digital Linear Tape

۳ Linear Tape Open

٤ critical

٥ Clustering

٦ Denial of Service

مراحل مختلف مدیریت حوادث در شکل زیر نمایش داده شده است. همان‌طور که می‌بینید این مراحل شامل موارد زیر است.

آماده‌سازی سیستم جهت جلوگیری از بروز حادثه یا کاستن میزان ضرر آن، تشخیص سریع و تحلیل حادثه و عواقب آن در هنگام بروز حادثه، مقابله با حادثه حداقل به صورت محدود سازی اثرات آن یا در صورت امکان ریشه‌کنی حادثه و اصلاح و ترمیم خرابی‌های ناشی از آن، و در انتها فعالیت‌های بعد از ترمیم مانند برطرف آسیب‌پذیری‌های سیستم و آگاهی‌رسانی به افراد جهت مقابله با این حادثه.

فرآیند مقابله با حوادث(تصویر شماره دوازده)

برای این حوادث باید برنامه پاسخ‌گویی ارائه شود. دسته‌بندی تیم‌های پاسخ‌گویی به حوادث به صورت تیم پاسخ به حوادث مرکزی، توزیع شده و تیم اطلاع‌رسانی است که هر تیم مسئولیت‌ها و شرح فعالیت مخصوص به خود دارد. همین طور این تیم می‌تواند به صورت خودگردان، جزئی سفارشی و تا تمام سفارشی عمل کند. در سازمان بزرگی مانند بانک در سطح کشور ممکن است انواع مختلفی از این تیم با یک‌دیگر به همکاری بپردازند. برای نمونه به‌تر است یک تیم مرکزی در تهران به صورت خودگردان و با قابلیت‌های زیاد به هماهنگی و ایجاد ارتباط بین تیم‌های کوچک دیگری که در شهرها و استان‌های دیگر پراکنده هستند بپردازد.

تیم مدیریت حوادث برحسب نوع خود سرویس‌های مختلفی ارائه می‌دهد که عبارتند از:

سرویس مشاوره‌ای آسیب‌پذیری‌ها

ارزیابی آسیب‌پذیری‌ها

آموزش و اطلاع‌رسانی

تشخیص تهاجم

مدیریت وصله‌ها

تحقیق و توسعه

متدولوژی پشتیبانی حوادث دارای چندین فاز است:

آماده‌سازی

تشخیص و تحلیل

محدودسازی و ترمیم

فعالیت‌های بعد از ترمیم

۶-۱۱- سیاست‌های مدیریت حوادث

یک گروه مرکزی در هر استان و زیر نظر گروه استان تهران جهت پاسخ‌گویی به حوادث امنیتی ایجاد شود. این گروه وظیفه مدیریت حوادث و هماهنگی‌های لازم تا رفع مشکل و رسیدن به پاسخ را دارد. افراد این تیم مرکزی باید تخصص‌های لازم جهت مدیریت حوادث را داشته، دوره‌های لازم را دیده باشند، در کنار این تیم مرکزی، تیم‌های درون‌شهری نیز پیش‌نهاد می‌شود که بتوانند مشکلات کم اهمیت‌تر را برطرف کرده وظیفه هماهنگی با تیم استان و اجرای دستورات آن‌ها در رابطه با حوادث بزرگ را داشته باشند.

تیم‌های مدیریت حوادث در مرحله اول باید امکانات لازم شامل سیستم‌های ارتباطی، سیستم‌های ذخیره‌سازی امن، نرم‌افزارها و سخت‌افزارهای تحلیل حوادث، ابزارهای کاهش حوادث را فراهم کنند.

تیم مدیریت حوادث باید چک لیست‌هایی برای انجام هر یک از مراحل پشتیبانی حوادث در دو سطح کلی و جزئی تهیه کند. به‌تر است این چک لیست‌ها با هماهنگی تیم مدیریت حوادث مرکزی تهیه شود تا چیزی از قلم نیفتد.

تیم‌ها باید اقدامات پیش‌گیرانه لازم جهت جلوگیری از بروز حوادث مانند مدیریت وصله‌ها، امنیت میزبان، امنیت شبکه و اطلاعات، ممانعت از سرایت کدهای مخرب را در برنامه‌خود بگنجانند.

تیم‌ها باید روال‌هایی جهت تشخیص و تحلیل حوادث داشته باشند. تشخیص سریع این که حادثه‌ای رخ داده و تعیین وسعت، شدت و میزان خرابی ناشی از آن.

تیم‌ها برحسب توانایی خود باید یا روالی برای تحلیل حوادث طراحی کنند و یا اطلاعات لازم جهت مدیریت تیم مرکزی استان را فراهم سازند.

تیم‌ها باید حوادث را اولویت‌دهی کنند و هشدارهای لازم در مورد وقوع یک حادثه را به اطلاع کاربران مربوطه برسانند.

تیم‌ها باید بتواند در جهت محدودسازی، ترمیم و ریشه‌کنی حادثه تصمیم‌گیری کنند و در صورت نیاز به جمع‌آوری اسناد و مدارک لازم برای تعیین منبع حادثه و جرم‌شناسی برای طی مراحل قانونی بپردازند.

هر تیم پشتیبانی حادثه باید به بررسی و تدوین تجارب اندوخته شده بپردازد و اقدام به یادگیری و افزایش دانش و تجربه خود نماید.

سازمان باید سیاستی برای بایگانی اطلاعات تیم پشتیبانی حوادث خود داشته باشد.

تیم مدیریت حوادث مرکزی باید به بررسی حوادث امنیتی رخ داده در سایر نقاط جهان بپردازد و اطلاعات و تجربیات آن‌ها را به همراه توصیه‌هایی برای جلوگیری از آن در یک سایت امن در اختیار

سایر تیم‌های درون سازمانی قرار دهد و تیم‌های درون سازمانی نیز موظف به پیگیری و اجرای آن توصیه‌ها هستند.

تیم مدیریت حوادث مرکزی باید در عین حالی که باید به تکمیل تخصص افراد خود برای مدیریت حوادث بپردازد و هم‌چنین باید لیستی از افراد متخصص بیرون از تیم که در صورت نیاز و در شرایط بحرانی بتوان از تخصص آن‌ها استفاده کرد تهیه کند. هم‌چنین این تیم باید قراردادهایی برای ارتباط با این افراد تهیه کند از رعایت نکات امنیتی و محرمانگی توسط متخصصین خارجی مطمئن شود.

تیم مدیریت حوادث باید روال‌هایی برای هماهنگی و تبادل اطلاعات با تیم مدیریت حوادث ملی در زمان‌هایی که حادثه عظیمی رخ می‌دهد داشته باشد.

۶-۱۲- آموزش و تربیت امنیتی

آگاهی‌رسانی و آموزش امنیتی نقش بزرگی در ایجاد امنیت و تداوم آن یک سازمان ایفا می‌کند. هدف برنامه آموزشی سازمان باید حفاظت از محرمانگی، جامعیت و دسترس‌پذیری سرمایه‌ها و داده‌های آن سازمان باشد. انستیتوی ملی استاندارد و تکنولوژی NIST[۱] چهار مرحله اصلی مطرح کرده است که هر برنامه آگاه‌سازی امنیتی باید داشته باشد.

طراحی و برنامه‌ریزی برنامه آگاهی‌رسانی و تربیت.

توسعه ملزومات و مراجع و مستندات لازم برای آن برنامه.

پیاده‌سازی برنامه‌آگاهی‌رسانی.

اندازه‌گیری تأثیر و به روزرسانی برنامه.

مخاطبین برنامه آگاهی‌رسانی و تربیت در زمینه امنیت بازه وسیعی شامل افراد زیر است: خود سازمان و سازمان‌های مطبوع، حمایت‌کنندگان برنامه، طراح، مجری و ناظر برنامه (مدیر فن‌آوری اطلاعات، مدیر

---

۱ National Institute of Standard & Technology

امنیت اطلاعات)، فن‌آموزان (پرسنل تیم پشتیبانی امنیت شبکه، مسئولین سیستم‌ها و نرم‌افزارها، عموم پرسنل سازمان).

هدف از آگاهی‌رسانی جلب توجه مخاطبین به اهمیت مقوله امنیت در سطح سازمان و ایجاد هوشیاری و آگاهی امنیتی بیش‌تر توسط ابزارهایی مانند پوستر، بروشور، بولتن، روزنامه، مجله، رسانه صوتی، تصویری و غیره است.

تربیت نیروی انسانی تلاش در جهت کسب مهارت و شایستگی برای راهبری هر چه به‌تر سیستم‌های فن آوری اطلاعات بوده در سطوح مختلف مقدماتی، متوسطه، پیش‌رفته صورت می‌پذیرد.

هدف از آموزش امنیتی، کسب دانش و تجربه در امر طراحی، پیاده‌سازی و پشتیبانی سیستم‌های امنیتی می‌باشد.

۶-۱۳- سیاست‌های آموزش و آگاهی رسانی

کمیته راهبری امنیت سازمان باید اقدام به سیاست‌گذاری و نظارت بر پیاده‌سازی برنامه آگاهی‌رسانی، تربیت و آموزش کند.

این کمیته ابتدا باید به شناسایی نیازهای مرتبط با آگاهی‌رسانی، تربیت و آموزش سازمان و اولویت‌دهی آن‌ها بپردازد.

سازمان باید برنامه آگاهی‌رسانی، تربیت و آموزش نیروهای انسانی خود را در زمینه امنیت تهیه کند. مراجع و سرفصل‌ها و نحوه اجرای هر برنامه تعیین گردد.

برنامه براساس این نیازها طراحی شده بودجه مالی برای هر یک پیش‌بینی می‌شود.

در سازمان بر اجرای برنامه‌ها نظارت شده، ارزیابی و بازخورد خود را از طریق روش‌هایی مانند فرم‌های ارزیابی، مصاحبه، محک، ممیزی و. .. اعلام کند. هم‌چنین تداوم آموزش و استمرار آگاهی‌رسانی باید مورد توجه مدیران سازمان قرار گیرد.

در صورتی که ارزیابی‌ها و بازخوردها ضرورت انجام بعضی تغییرات را نشان دهد، لازم است این تغییرات صورت گیرد. باید برنامه‌هایی جهت حمایت و تشویق از مجریان و مخاطبین در جهت ایجاد انگیزه طراحی شود.

۶-۱۴- سئوالات خودآزمایی

منظور از نظارت و ارزیابی امنیتی چیست؟ توضیح دهید.

سیاست های کلی نظارت امنیتی را بنویسید.

سیاست های کلی مدیریت پیکربندی را بنویسید.

منظور از پشتیبان گیری را نوشته و انواع پشتیبان گیری را نام برده و توضیح دهید.

تیم مدیریت حوادث چه سرویس هایی را ارائه می دهد. نام برده و توضیح دهید.

آموزش و تربیت نیرو چه تاثیری در امنیت اطلاعات دارد؟

منابع:

کتب:

اظهری علی – رازهای پنهان هیپنوتیزم – انتشارات میر – ۱۳۷۷

اللهیاری فرد، م، ارزیابی گسترش بانک‌داری الکترونیک در کشورهای اسلامی ، تازه‌های اقتصاد

باطنی محمدرضا – ساخت و کار ذهن – انتشارات واژه – ۱۳۶۹

بانک مرکزی و بانک‌داری الکترونیک ، بانک‌داری الکترونیک، ۱۳۸۷، ۳، ۲۲.

پزشکی، ی، دباغ رضایی، س، ۱۳۸۴ نقش فن‌آوری اطلاعات و ارتباطات در رشد اقتصادی ، تدبیر، ۱۳۸۴، ۱۶۳.

پورابراهیمی و بنابی - آشنایی با اصول امنیت محیطی در حوزه فن‌آوری اطلاعات و ارتباطات – پدافند غیرعامل کشور –۱۳۸۹

جمالیان سید رضا – قدرت خود هیپنوتیزم – انتشارات اسپرک – ۱۳۶۸

جنگ و دفاع سایبر

جهانگیری، ف، ۱۳۸۶ بررسی عوامل موثر در آمادگی الکترونیکی برای بانک‌داری الکترونیکی در بانک صادرات پایان نامه کارشناسی ارشد، دانشگاه‌تربیت مدرس۱۳۸۶

چالش‌های تحول الکترونیکی- پرتو ملت، ۲۰و۲۱، ۱۳۸۶، ۵۲-۴۹.

خدادادی مهدی – مصاحبه تشخیص – انتشارات مدبر – ۱۳۸۵

دهستانی مهدی – آسیب شناسی روانی – انتشارات طیف نگار – ۱۳۸۶

رشیدی، د، زادگان باوی، ه، بانک‌داری متمرکز؛پیش نیازی برای تحول در ارائه خدمات بانکی تازه‌های اقتصاد، ۳۱-۲۵

سید محمدی یحیی – آسیب شناس روانی – انتشارات نشر روان – ۱۳۸۶

سید محمدی یحیی – روانشناس عمومی – انتشارات نشر ارسباران – ۱۳۸۶

طاووس شعبان – روانشناس هیپنوتیزم – انتشارات کابوک – ۱۳۵۶

عزبدفتری بهروز – ذهن و جامعه – انتشارات فاطمی – ۱۳۷۲

عزیزی سرخنی، م. ج، اله قلی زاده آذری، م، کردلوئی، ح. ر، بررسی زیر ساخت‌های موجود بانک تجارت برای استقرار بانک‌داری الکترونیکی، (پژوهشگر)مدیریت، ۱۳۸۷، ۱۰، ۱۱.

فرس پل – روانشناسی تجربی – سازمان انتشارات آموزش انقلاب اسلامی - ۱۳۶۹

فکور ثقیه، ا. م- تاثیر فن‌آوری اطلاعات بر صنعت بانک‌داری مدیریت، ۱۸، ۱۳۸۵، ۱۰۸-۱۰۷.

کریستااسون – حافظه مجرمان از جرایم خشونت بار – انتشارات نشر آگاه – ۱۳۸۸

کلمان ژاگوپل – روش‌های علمی مانیتیسم، هیپنوتیسم، تلقین – انتشارات ققنوس – ۱۳۸۳

گنجی حمزه – مصلحی زیبنده – ایزد دوست یوسف – روان شناسی – چاپ و نشر ایران – ۱۳۷۲

مجوز عبدالله – دنیای خود هیپنوتیزم و بهبودی با تلقین – موسسه فرهنگی انتشاراتی حیان – ۱۳۷۶

محمدزاده علی اکبر – ولیزاده صمد – روانشناس هیپنوتیزم – انتشارات تلاش

مدیریت ریسک - سایت اینترنتی هیراد انجمن ایرانیان

مک فی نیل –تری راجر – هنر مخفی مصاحبه با افراد – انتشارات نشر آگاه – ۱۳۸۸

منجمی علیرضا – روش‌های تقویت حافظه – نشر آزاد مهر – ۱۳۸۸

هیپنوتیزم‌هارتلند – جمالیان سید رضا – انتشارات جمال الحق – ۱۳۷۵

ترجمه:

ترجمه بخشی از کتاب : security risk assessment - biringer rodolph .by betty E and management

کتاب مدیریت ریسک – نوشته : سی آرتور ویلیامز،دیچارد دام. هینز – ترجمه : دکتر داور ونوس و گودرزی

نگاهی به بانک‌داری خرده فروشی درآینده ترجمه جندقی، م، ماهنامه آموزشی، خبری بانک ملی ایران، ۱۳۸۶، ۲۱-۱۹. ۱۳۵.

فصلنامه و ماهنامه:

ایلداری، س، "تاثیر تجارت الکترونیک بر بانک‌داری خرد، ماهنامه بانک صادرات، ۳۰.

دو مانع پیش روی بانک‌داری الکترونیک"ماهنامه بانک‌داری الکترونیک" ۱۳۸۷، ۵، ۱۰.

فخری,مجید, "سنجش از راه دور و کاربردهای نظامی اطلاعات ماهواره ای, فصلنامه خبری آموزشیء فرماندهی ستاد,تهران ,سال دوم,شماره ۵ , ۱۳۷۸

فصلنامه میثاق بسیج متخصصین، سال سوم، شماره ۱۱، پاییز ۸۹

عابدینی , مهدی, "ماهواره‌ها و تحولات نظامی" نشریه علمی و خبری ماهواره‌ها , تهران : مرکز ماهواره‌ها , سال اول , شماره اول , ۱۳۷۹

کیمیایی، پ، ۱۳۸۱"بانکداری سنتی و بانک‌داری الکترونیکی تقابلی اجتناب ناپذیر" فصلنامه بانک، شماره۲۲.

مقالات:

مقاله مدیریت ریسک - نوشته‌ی دکتر محمد علی بابایی و حمید رضا وزیر زنجانی

مقاله مدیریت ریسک استراتژیک – نویسنده : آلن ورینگ و حسن مهدی زاد

مقاله نقش فن‌آوری اطلاعات در مدیریت ریسک، نشریه جهان اقتصاد

سایت:

سایت اینترنتی هیراد انجمن ایرانیان- مدیریت ریسک

سایت فن‌آوری اطلاعات برای مدیران

منابع لاتین:

Agence France Press، Mar، ۲۸، ۲۰۰۱

Air Force، Operation Iraqi Freedom، Information Operation Lessons Learned:

Airpower Journal، July، ۱۹۹۶

Appraisal: The Changing Role of Information in Warfare، RAND، ۱۹۹۹،

CANADIAN FORCES COLLEGE، ADVANCED MILITARY STUDIES

Carrington، M، ۱۹۹۷، " The banking Revolution : how Technology in creating winners and losers "، Great Britain، pitman publishing company.

Center، Beijin Special Lecture، Mar، ۱۹۹۷،

Charles F. Hawkins، China Defense Science & Technology Information

Col. Andrew Borden، USAF، What is Information Warfare? The Information

Col. Timothy Thomas، Russian Views on Information-Based Warfare،

Conflict in the Information Age، RAND، ۱۹۹۷،

Costas Courcoubetis and Richard Weber، Pricing Communication Networks، Publishing John Wiley and Sons، ۲۰۰۳.

COURSE ۲، NOV، ۱۹۹۹،

David Alexander، http://www. davidalexanderbooks. Com /www /informat. htm

David Fulghum، Sneak Attack، Aviation Week & Space Technology، June ۲۸،

David Ruppe، Directed-Energy Weapons: Possible U. S. Use Against Iraq،

DoD dictionary of Military and Associated Terms،

Dorothy Denning، Information Warfare and Security، Addison-Wesley، ۱۹۹۹

Durhin، M. ، Howcroft، B. ، ۲۰۰۳، " Relationship marketing in the banking sector "، marketing Intelligence and planning، vol ۲۷.

Elaine Grossman، Info Targets largely Cobbled on-the-fly for Officials: Space،

Feb ۲، ۲۰۰۳، http://www. globalsecrutiy. org/org/news

Frenchelon، The large ears made in France،

Frist Look، http://www. cadre. maxwell. af. mil/ warfarestudies /iwac /downloads،

Giampiero Giacomello، Measuring digital wars: Learning from the experience

IAnewsletter، Vol. ۳، No. ۴

InfoWarCon، ۲۰۰۰، Sep ۱۲، ۲۰۰۰، Washington D. C.

Iraq، Inside Pentagon، May ۲۹، ۲۰۰۳

ITU-toolkit page\ICT Regulation Toolkit. htm

Jack Moteff، Critical Infrastructures: Background & Early Implementation of

James Mulvenon، The PLA and Information Warfare

John Arquilla and David Ronfeldt (Ed) In Athena's Camp: Preparing for

،Joint Information Operations Planning Handbook

Jr۰۲-۲۰۰۹ tracking ghostnet

”Individual difference in privat ،۲۰۰۳ ،and Salo. j ،Kaoivumaki. t ،Kajaluoto. h
th hawii international ،banking:empirical evidence from finlandhngs of the ۳
p۱۹۶. ،Hawaii ،big island ،conference on system sciences(H۱CSS)

A Russian View of Future War: m ،Lester W. Grau and Timothy L. Thomas

" Technoloyy Acceptance Model for wireless ،۲۰۰۳ J. ،Yao ،c. ،L iu ،LU. J.
No۳. ،vol ۱۳ ،Electronic Networking Applications and policy ،internet "

،۱۹۹۹ ،Defining Information Warfare: Easier Said than Done ،Megan Burns

،۱۹۹۸ ،RAND ،Strategic Information Warfare Rising ،Mesic

۱۹۹۶ ،May ،Beijing ،Military Strategic Research Center

،Department of Defense Report to Congress ،Network Centric Warfare

،۲۰۰۰ ،Sep ۲۹ ،US Space Command ،News Release

،The Information Warfare Site ،of peace research and arms control

،۲۰۰۰ ،Feb ،CIA says ،Other countries developing cyber attack capability
PDD-۶۳

۲۰۰۱. ،United Kingdom ،BWCS ltd ،Interconnect Costing ،Peter Cartwright

Proceeding of the ۲۰۰۱ IEEE Workshop on Information Assurance and

،Principles of cyber-warefare ،Raymond C. Parks and David Duggan

Richard F. ،David A. Mussington ،Peter W. Wilson ،Roger C. Molander

،Cornerstones of Information Warfare ،Ronald Fogleman and Sheila Widnall

،Security ،Untied States Military Academy ،West Point ،NY ،June۵ ۶-، ۲۰۰۱

©ARTECH ،Edition ۲nd، Mike Hendry،Smart Card Security and Applications
۲۰۰۴.۱۹۹۶. ۱۳۵.House INC۰۲۸. Pdf

۱۹۹۹ ،Dec ،A National Security Strategy for a New Century ،The White House

Sep ،Issue ۹. ۳ ،The Journal of Slavic Military Studies ،Theory and Direction

،۲۰۰۲ ،Agust ۱۶ ،Global Security Newswire ،Threaten International Regims

،U. S Military concerned about China's cyberwarfare capabilities: General

http://www. stratcom. af. Mil /factsheet. ،US Strategic Command Fact File
shtml

،USAF Doctrine of Information Operations

http://www. iwar. org. uk /iwar /resources /airchronicles ،Warfare Site
/borden. htm

۲۰۰۵ ،Analytical Cost Model Broadband Network ،WIK-Consult

،U. S may debut secret microwave weapons versus Iraq ،Will Dunham
،Reuters

http:///wordnet. princeton. edu ،Wordnet Princeton University

”Factors affecting the adoption of Internet ،۲۰۰۷، Adgar. d ،Grant. k ،Yiu. c. s
Banking in Hong kong-implication for the banking sector”International
Journal of Informetion management، ۲۷، ۳۳۳۶-

Strategic ،Andrew W. Marchal (Ed) ،John P. White ،Zalmay Khalizad

اینترنت:

http:// www. microsoft. com

http://www. aerocenter. ir/forum/showthread. php?t=۶۸۸۰&page=۱

http://www. af. mil/lib/corner. html

http://www. ahmady aghma. blogfa. com

http://www. articles. com

http://www. bashg. net

blogfa. com.http://www. beheshtnet.

http://www. berkley. com

Com .berkley .http://www

http://www. cs. cmu. edu/~burnsm/InfoWarfare. html

http://www. daneshnameh. roshd. ir

http://www. dod. mil/nii/NCW/

http://www. dtic. mil/doctrine/jel/doddict/data/i/index. html

http://www. duzli-oghlan. blogfa. com

http://www. ege. eslsca. fr

http://www. fa. wikipedia. org

http://www. farya. com

http://www. firooz. ir

http://www. forum. silvapc. com/index. php?topic=۲۶۷۶. ۰٪ ۳bwap۲

http://www. forun. manuatoo. com

http://www. georgetown. edu/sfs/programs/stia/students/vol. ۰۳ / Johnson _IW. ht

http://www. giganews. ir

http://www. globalsecrutiy. org/org/news

http://www. hamedbanaei. com

http://www. hamshahri. Org

http://www. herolibrary. org/iwa۴web. htm

http://www. imi. ir/tadbir/tadbir-۱۳۴/article-۱۳۴/۴. asp

http://www. infoguerre. com

http://www. insidedefense. Com / secure / data _ extra / pdf۳ / dplus ۲۰۰۴ _۲۶۵. pdf

http://www. iricap. Com

http://www. it .behdasht .gov .ir

http://www. it .behdasht .gov .security_۱۱۹۱_۱۰۱/uploads/ir .doc

http://www. itirn. com

http://www. iwar. org. uk/infocon

http://www. iwar. org. uk/iwar/resources/jiopc/io-handbook. pdf

http://www. iwar. org. uk/iwar/resources/usaf/maxwell/students/۲۰۰۱/۰۱-

http://www. networkworld. com/news/۲۰۰۰/۰۲۲۴cia. html

http://www. noorportal. net

http://www. p۳۰lords. com/forum/archive/index. php/t-۹۲۶۳. html

http://www. parsiblog. Com

http://www. peace. ca/canadianinformationoperations. htm

http://www. ponemonen. com

http://www. rand. org/publications/MR/MR۹۶۴/MR۹۶۴. pdf

http://www. rand. org/pubs/monograph_reports/MR۱۰۱۶/

http://www. rand. org/pubs/monograph_reports/MR۸۸۰/index. html

http://www. sans. org/newlook/resources/IDFAQ /solar_sunrise. htm

http://www. shabakeh-mag. com/articles/Show. aspx?n=۱۰۰۳۴۱۴

http://www.shabakeh-mag. com/articles/Show. aspx?n = ۱۰۰۳۴۱۴& p = ۳

http://www. social. iran-emrooz. net

http://www. spacecom. af. mil/usspace/re۱۱۵-۰۰. htm

http://www. srco. ir/articles/docview. asp۲id=۱۸۲

http://www. tebyan. net/science _ technology / computermagazine /interview_report/۲۰۰۴/۱۳/۵۸۰۲. html

http://www. tebyan-ardebill. ir

http://www. thefreedictionary. com/IW

Error! Hyperlink reference not valid.

Error! Hyperlink reference not valid.

http://www. zdnet. fr/actu/tech/secu/a۰۰۱۴۷۶۸/html

Error! Hyperlink reference not valid.

Error! Hyperlink reference not valid.

http://www.emmaf۲. isuisse. com/emmaf۲/iw/what. htm

http://www.en. wikipedia. org/wiki/Command_and_control_warfare

http://www.farsnews. ir

Ir .persianblog .http://www.padafand-gh-amel

واژه نامه:

اجتناب	avoidance
احیا	recovery
اختفا	privacy
ارتباطات	communication
اطلاعات خام	data
اعتبار	authority
افزونگی	redundancy
ایمن	secure
آزمایشی	trail
آشکارسازی	detection
بازرسی	inspection

بوکش sniffer

بی قاعده promiscuous

بیسیم wireless

پسوند extensions

پشتیبان backup

تائیدیه certificate

تجزیه و تحلیل analysis

تخفیف mitigation

تصاعدی incremental

تصدیق authentication

تقابلی interactive

توزیع شده distributed

ثبت اطلاعات ورود به سیستم logs

جدی critical

چند منظوره multipurpose

دسترسی access

دیواره آتش firewall

رسوخ intrusion

رمز cipher

رمزشناسی cryptography

زنجیره chain

شناسایی identification

شناسایی یکدیگر handshaking

صحت accuracy

صحت integrity

عقب گرد rollback

قابلیت ارائه availability

کارت card

لیست رمز acl

لیست کنترل checklist

متن آشکار plaintext

متن رمز شده ciphertext

مجازی virtual

محرمانگی confidentiality

مدیریت management

مزاحم malicious

مستحکم سازی hardening

مسولیت پذیری accountability

مشکلات پنهان نرم افزاری bug

ممانعت denial

ممیزی audit

نرم افزار software

نشست session

نقطه نهایی endpoints

ورود به سیستم login

هماهنگ شده synchronized

اندیکس:

ا

اتوماتیک, ۸۲, ۸۴, ۸۸, ۱۰۱, ۱۰۹, ۱۱۱, ۱۳۰, ۱۵۵, ۱۵۶, ۱۵۹, ۱۶۳

اختلال, ۱۲, ۱۳

ارزیابی, ۱۷۱

استاندارد, ۶۱, ۸۶, ۱۱۹, ۱۴۲, ۱۶۸

استتار, ۴۴

استراتژی, ۶۴, ۶۵, ۷۸, ۷۹, ۱۰۱

استراق, ۲۶

اطلاعات, ۱۲, ۱۳, ۱۷۱, ۱۷۲

اعتبارسنجی, ۱۰۵, ۱۱۲, ۱۲۲

افزار, ۱۳

افشا, ۱۲

افندی, ۵, ۴۵

اقتصاد, ۱۷۱

اکسترانت, ۱۴۱

الکترومغناطیسی, ح, ۱۱, ۱۲

الکترونیک, ۳۴, ۱۴۵

الکترونیک, ۱۸, ۱۷۱, ۱۷۳

اللهیاری, ۱۷۱

امنیت, ی, ک, ل, ن, ۶, ۷, ۱۰, ۴۰, ۴۱, ۴۲, ۴۳, ۴۷, ۴۹, ۵۸, ۵۹, ۶۰, ۶۲, ۶۳, ۶۴, ۶۶, ۶۷, ۶۹, ۷۰, ۷۱, ۷۲, ۷۳, ۷۹, ۸۰, ۸۴, ۸۵, ۸۷, ۸۸, ۸۹, ۹۰, ۹۲, ۹۵, ۹۷, ۹۸, ۱۰۱, ۱۰۳, ۱۰۴, ۱۰۶, ۱۱۱, ۱۱۷, ۱۱۸, ۱۲۰, ۱۲۳, ۱۲۴, ۱۲۵, ۱۲۶, ۱۲۷, ۱۳۳, ۱۳۵, ۱۳۶, ۱۴۲, ۱۴۳, ۱۴۴, ۱۴۵, ۱۴۶, ۱۵۱,