
بسم الله الرحمن الرحيم

تقدیم به شهدای دانش پژوه

انقلاب اسلامی ایران

امنیت دنیای سایبری

کاربران عمومی

مولف

مهندس ناصر نامخواه

سرشناسه: نامخواه، ناصر، ۱۳۴۰
عنوان و نام پدیدآور: **امنیت دنیای سایبر – کاربران عمومی**
مشخصات نشر:
مشخصات ظاهری: ۳۱۷ ص. ، مصور، جدول، نمودار
شابک:
وضعیت فهرست نویسی: فیپا
یادداشت: واژه‌نامه
یادداشت:
کتابنامه: ص. ۳۱۷
موضوع:
موضوع :
شناسه افزوده:
رده بندی کنگره:
رده بندی دیویی:
شماره کتاب‌شناسی ملی:
کد پیگیری:

نام کتاب : امنیت دنیای سایبر – کاربران عمومی

تألیف : مهندس ناصر نامخواه

نوبت چاپ : اول، بهار۱۳۹۰

ناشر :

صفحه آرایی: مجید بهمنی

طراح جلد:

شابک :

تیراز :

قیمت :

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 - در فصل کتاب مفصلی بین تحقیق پرداخته شده است - لذا به نظر می‌رسد یکی از راه‌های وصول به امنیت در دنیای دیجیتال شناخت واقعی این 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 علمی و 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.

در این کتاب تلاش بر این گردیده است کاربران عمومی 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 دوم 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 علمی این گروه از عزیزان در حد بضاعت فراهم گردیده و نیازمندی‌های علمی و امنیتی آنان در کتاب مربوط به ایشان جمع آوری و ارائه گردد.

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 کتاب سوم که ویژه مدیران محترم در سطوح عملیاتی 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 گردیده است.

تمام دستورالعمل‌ها و اسناد عملیاتی تنظیمی در لایه‌های مختلف سازمان و هر جامعه‌ای می‌بایست به روش‌های علمی و عملیاتی و در برهه‌های مختلف از زمان می‌بایست ممیزی گردد و میزان کارآیی آن‌ها و قابلیت اعتماد به روش‌های اجرایی آن سنجیده شود. در کتاب چهارم که به نام ممیزان تقدیم می‌گردد کوشش گردیده است روش‌های ممیزی و امنیت در دنیای دیجیتال و راه‌های عملیاتی نمودن این گونه ارزیابی از اجرای عملیاتی دستورالعمل‌ها سنجیده شود. در کتاب ممیزان تلاش گردیده است 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 علمی و دانشگاهی سیر رشد و تعالی خود را طی خواهد نمود زمینه‌های گسترش حرکت علمی در زمینه‌های پدافند غیر عامل فاوا را در کشور (ولو هر چنداندک) بتواند ایجاد نموده و از

نظرات و پیشنهادات صاحب‌نظران علمی استقبال نموده و با تکمیل آن‌ها در کتب آتی بتوانیم در هرچه پربارتر نمودن این گونه کتاب‌ها کوشا باشیم.

کتاب حاضر در ۱۲ فصل تقدیم می‌گردد. در انتهای هر فصل اهداف هر فصل برشمرده شده و پس از بررسی مطالب فصل، در انتهای فصل سؤالاتی 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 که اختصاص به امنیت اطلاعات دارد با اسناد به عنوان یکی از اصلی‌ترین ابزار نقل و انتقال اطلاعات که نیاز به امنیت دارند آشنا شده‌اند و به اطلاعات ذخیره شده در ذهن انسان‌ها پرداخته و با انواع اطلاعات موجود در ابزار دیجیتال که نیاز به امنیت دارند آشنا می‌شویم.

با توجه به این که امروزه گلوگاه اصلی ارتباط انسان‌ها با دنیای دیجیتال رایانه‌های شخصی می‌باشد در فصل چهارم تلاش گردیده است و از نگاه امنیت سایبری به این وسیله که انواع و اقسام مختلفی دارد نگریسته شود.

رایانه‌های شخصی بر طبق مطالب گفته شده در کتب مختلف و به روش‌های مختلف ایمن می‌گردند که این گونه امنیت رایانه‌ها مورد نقادی قرار گرفته و انواع روش‌هایی که این گونه پایداری اطلاعات را در این ابزار تهدید می‌کنند و به کاربران عزیز تقدیم می‌گردد.

در فصل پنجم که اختصاص به امنیت شبکه‌های رایانه‌ای دارد انواع شبکه‌های رایج که در کشور از آن‌ها استفاده می‌شود پرداخته شده است برای تأمین امنیت در شبکه‌های مختلف انتقال اطلاعات از طریق لایه‌های مختلف انجام می‌شود که مدل مرجع osi در این کتاب مورد بحث و بررسی قرار گرفته است.

انواع حملات این گونه شبکه‌ها را تهدید می‌کند که تلاش شده است حملات را رایج در این قسمت از کتاب مورد بحث و بررسی قرار گرفته و وظایف کاربران و ساختار و مدیران در رابطه با این حملات تبیین گردند.

فصل ششم اختصاص به امنیت بانک‌های اطلاعاتی دارد. امروز تقریباً تمام اطلاعات دیجیتال مورد نیاز در بانک‌های اطلاعاتی گردآوری و توسط این نرم‌افزارها برای استفاده ارائه می‌گردد. به منظور رعایت حیطه بندی بین کاربران مختلف برای دسترسی هر لایه روش‌های ایمنی خاصی در نظر گرفته می‌شود. در این فصل تلاش شده است انواع این روش‌ها و راه‌های ایجاد آن مورد بحث و بررسی قرار گیرند.

اتوماسیون اداری هرچند که دیرتر از انواع دیگر نرم‌افزارهای کاربردی به کار گرفته شده، لیکن با توجه به سهولت سازی کاربران سازمان‌ها برای چرخش اطلاعات به سرعت و با ضریب نفوذ بالایی تقریباً در کلیه سازمان‌ها به کار گرفته شده است. تلاش گردیده است در فصل هفتم امنیت اتوماسیون اداری با نگرش سیستم‌های اطلاعات مبتنی بر رایانه مورد بحث قرار گیرد.

در اتوماسیون اداری لایه‌های مختلفی از کاربران از قبیل طراحان و برنامه نویسان و مدیران و سیاست‌گذاران نقش دارند سعی شده است نقش هر کدام از این لایه‌ها در بهبود امنیت سیستم‌های اداری مورد بررسی واقع شود .

فصل هشتم اختصاص به امنیت اینترنت داشته و از زاویه نگاه سلطه گران به اینترنت نگاه شده و با ذکر تاریخچهٔ پیدایش اینترنت، نقش آن به عنوان یکی از اصلی‌ترین روش‌های اشرافیت بر اطلاعات تولید در مبدأ و در خدمت سلطه‌گران مورد تجزیه و تحلیل قرار گرفته است.

اینترنت همراه با خود واژه‌های جدیدی از قبیل سلاح‌های سایبری و جنگ اطلاعات و جنگ رسانه‌ای را ارمغان آورده است که در ادامه فصل این گونه واژه‌ها نیز مورد واکاوی قرار می گیرند.

کلیه اطلاعات از طریق ارتباطات دیجیتال ایجاد شده مورد تعامل با دیگران قرار می‌گیرند. در فصل نهم ضمن آشنایی با سیستم‌های ارتباطی به مقوله امنیت این سیستم‌ها پرداخت می شود.

انواع شبکه‌های با سیم و بی‌سیم و ماهواره‌ای و دیجیتال در این فصل بررسی شده و امنیت و دلایل نفوذپذیری این گونه شبکه‌ها بحث می‌شود.

در فصل دهم به امنیت محیطی و فیزیکی پایگاه‌های داده‌ای و دیجیتال پرداخت می‌شود. عدم رعایت نکات حفاظتی در طراحی و اجرای طرح‌های حفاظت فیزیکی می‌تواند ساختارها را به چالش کشیده و باعث از دست دادن اطلاعات گردد.

رعایت اصول پدافند غیر عامل در جایابی شبکه‌های رایانه‌ای و ارتباطی می‌تواند از خطرات قابل پیش بینی و یا پیش‌بینی نشده جلوگیری نماید.

سیاست‌ها و استانداردها و مدیریت امنیتی که در فصل یازدهم بررسی می‌گردد می‌تواند با مدیریت ریسک باعث کاهش آسیب‌پذیری‌ها شده و به نوعی عوامل موفقیت را به ارمغان آورد.

در صورت وقوع بحران می‌بایست اقداماتی انجام داد که در ادامه این فصل آن‌ها نیز مورد بررسی قرار می‌گیرند. هرچند امروزه در بسیاری از کشورهای مختلف استانداردهایی برای این کار تأکید شده است لکن با توجه به آسیب‌پذیر بودن برخی از آن‌ها نکات مربوط که می‌بایست مدنظر قرار گیرند مورد مداقه قرار می‌گیرد.

فصل پایانی کتاب که همان فصل دوازدهم می‌باشد به بررسی ابزارهای امنیتی و تست نفوذ ابزار دیجیتال می‌پردازد.

نام بردن از ابزارهای خاص در این فصل نشان دهنده تأیید و یا تکذیب آن‌ها نمی‌باشد بلکه تلاش شده است از هر گونه از ابزار که امروز با عنوان چاقوی دولبه (امنیت و ضدامنیت) استفاده می‌شود بررسی شده و صرفاً نقش و شیوه کاربرد آن‌ها مدنظر بوده است.

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

مؤلف

فهرست مطالب:

۱

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

۱-۱- تعاریف

با توجه به این که امروزه مفاهیم معانی مختلفی پیدا کرده‌اند و برد استفاده از آن‌ها گسترگی 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.

۱-۲- 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 ذیلا به صورت تفصیلی به این مطلب می‌پردازیم.

۱-۳-تعریف اسناد

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

---

[۱] **data**

۱-۴- 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 نداشتن‌ترس ، وضعیت آرامش و اطمینان خاطر حاصل می‌گردد. امنیت به حداقل رساندن خطر یا تهدید است که این خطرها نه فقط از نوع سنتی و نظامی هستند بلکه تهدیدات جدید غیر نظامی را 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. طبق نظر "ولفرز" « امنیت در معنای عینی فقدان تهدید در برابر ارزش‌های کسب شده را مشخص می‌کند و در معنای ذهنی ، فقدان‌ترس و وحشت از حمله علیه ارزش‌ها را. . . یک ملت زمانی امنیت دارد که بتواند بدون خطر از ارزش‌های اساسی خود حفاظت کند، از جنگ اجتناب نماید و بتواند در هنگام چالش ارزش‌های خود را با موفقیت حفظ نماید».

۱-۵- 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.

۱-۵-۱- 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.

۱-۵-۲- 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.

۱-۵-۳- 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.

۱-۵-۴- 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.

۱-۶- تعریف پدافند عامل

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

۱-۷- 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.

۱-۷-۱- امنیت

امنیت اطلاعات از سه جنبه مختلف مدنظر قرار می‌گیرد: محرمانگی[۱]، یکپارچگی[۲] و دسترس‌پذیری[۳].

- 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.

۱-۷-۲-ایمنی

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

۱-۷-۳- 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.

۱-۸- تعریف تهدید نرم

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

---

۱ Confidentiality
۲ Integrity
۳ Availability

که اهداف متفاوتی را موضوع خود قرار داده و به جای تمامیت ارضی، هویت ، هنجار، فرهنگ و . . . را هدف قرار می‌دهند. (فصلنامه میثاق،گفتگوی علمی۱۳۸۶: ۱۴۵)

۱-۹- 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. (فصلنامه میثاق،افتخاری ۱۳۸۳) در این دیدگاه امنیت دارای بستر و مجموعه متکثری است که اگر شاخص‌های آن آماده باشد ،برای انسان نوعی آرامش و اطمینان بوجود 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. (همان، افتخاری، ۱۳۸۴، ص ۱۶) اگر این گفتمان را ملاک قرار دهیم قبل از ظهور "تهدید عینی" یا جنگ نرم، دوره تکوین و شکل گیری 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 رسمی به‌صورت 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. (همان ، افتخاری، ۱۳۸۵: ۷)

۱-۱۰- 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 اصولا 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 ابر رایانه‌های موجود بر فشردگی مزبور می‌افزایند و هر لحظه شرایط جدیدی را برای دستیابی سریع‌تر به نیازمندی‌های بشر فراهم می‌آورند.

۱-۱۰-۱- 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.

۱-۱۰-۲- تهدیدات و فرصتها در دنیای نوین

در دنیای حقیقی ما حوزه‌های همپوشان منافع نداریم (یا بسیار کم داریم) ولی در دنیای مجازی مرزهای همپوشان و حوزه‌های هم پوشان 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 تهدیدات داریم ولی در دنیای مجازی حذف تهدیدات نداریم بلکه قابلیت همزیستی با تهدیدات داریم. یعنی قابلیت تهدید پذیری و تهدید زدایی افزایش پیدا می‌کند.

۱-۱۰-۲-۱- 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 تهدیدات تقسیم بندی صورت پذیرد.

۱-۱۰-۲-۱-۱- 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 جزوی از زندگی آدمی شده 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.

۱-۱۰-۲-۱-۱-۱- 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 خطرات دور نگه دارند و دشمنان آنان نیز تلاش دارند از این ناحیه خطر را متوجه آن کشور نمایند.

۱-۱۰-۲-۱-۱-۲- تهدیدات نرم‌افزاری

تهدیدات نرم‌افزاری تهدیداتی را تشکیل می‌دهند که بیش‌تر مغز افزار می‌باشند تا سخت‌افزار . این گونه تهدیدات 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.

۱-۱۰-۲-۱-۱-۳- 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.

۱-۱۰-۲-۱-۱-۴- 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 نظامی از تجهیزات الکترونیکی استفاده می‌کنند و این مسئله آن‌ها را در مقابل لطمات الکترومغناطیسی آسیب‌پذیر نموده است.

مدارات بردهای الکترونیکی که از ابتدا لامپی بوده‌اند و با ولتاژهای بالایی کار می‌کردند با پیدایش‌ترانزیستور تبدیل به قطعات بسیار کوچک‌تری شدند که با ولتاژهای پایین‌تری کار

می‌کنند . با کاهش حجم و مصرف انرژی ، استفاده از نیمه‌هادی‌های 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 تهدیدات می‌توان به رعد و برق ، سویچینگ خطوط انتقال برق، دستگاه جوش ژنراتور الکتریکی ، تسلیحات الکترومغناطیسی و انفجارات اتمی اشاره نمود.

۱-۱۰-۲-۱-۲- 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.

۱-۱۰-۲-۱-۲-۱- 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.

۱-۱۰-۲-۱-۲-۲- 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:

۱. طراحی نا صحیح زیر ساخت شبکه یا عدم وجود افزونگی در تجهیزات شبکه
۲. عدم تهیه‌ی نسخه‌های پشتیبان از داده‌های حیاتی
۳. سهل‌انگاری در وظایف روزمره (مثل بررسی مستمر سیستم‌ها از لحاظ آلودگی به ویروس)
۴. نا آگاهی کاربران از ماهیت عملیات خطرناک
۵. بروز اشکالات پیش بینی نشده[۱] در سطح سخت‌افزار، نرم‌افزار یا سیستم عامل
۶. عدم اعمال صحیح سیاست‌های انتخاب و تعویض مداوم کلمات عبور توسط عوامل درگیر در شبکه

۱-۱۰-۲-۱-۳- تهدیدات طبیعی

این تهدیدها از عواملی مانند زلزله، سیل، گردباد، رعد و برق، آتش سوزی، آتشفشان و نظایر آن از قوّه به فعل می‌رسند و نسل بشر چنین تهدیدهایی 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 تهدیدهای طبیعی می‌توانند در خارج از محدودهٔ بَلا دیده نیز منجر به اختلال در عملیات روزمرهٔ افراد و انتشار بحران در سطح وسیع شوند. لذا اگرچه تهدیدهای طبیعی خارج از قدرت بشرند ولی برای بازگرداندن خدمات شبکه از وضعیت بحران به وضعیت عادی، از همان ابتدای طراحی شبکه، تمهیداتی برای جلوگیری از گسترش دامنهٔ بحران به مناطق دیگر پیش بینی و اجرا می‌شود. به عنوان مثال ایجادتراز پشتیبان در دیگر مناطق جغرافیایی و بهره‌گیری از خطوط ماهواره‌ای در کنار خطوط فیبر نوری در این رده از تمهیدات قرار می‌گیرد.

۱-۱۰-۳- 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

---

[۱] BUG

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.

۱-۱۰-۳-۱- انواع اطلاعات دیجیتال

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

۱-۱۰-۳-۱-۱- 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 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.

۱-۱۰-۳-۱-۲- 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 محل‌های امن نگهداری می‌گردد درصورتی‌که فردی به صورت مجاز و یا غیر مجاز به این ابزار دسترسی پیدا نماید می‌تواند اطلاعات آن را مورد بهره‌برداری قرار بدهد.

۱-۱۰-۳-۱-۳- 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 سیستم های 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 .

۱-۱۰-۳-۲- 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.

۱-۱۰-۳-۲-۱- 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 .

۱-۱۰-۳-۲-۱-۱- 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 اف‌بی‌آی رسیده باشد می‌باشد و فقط در صورت تأیید این ابزار قابلیت صدور به دیگر کشورها را پیدا می‌کند. در این گواهی اف‌بی‌آی تأیید می‌نماید که ابزار لازم برای دسترسی از راه دور و به دست گرفتن

مدیریت ابزار از راه دور دراین 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 .

۱-۱۰-۳-۲-۱-۲- 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.

۱-۱۰-۳-۲-۱-۲-۱- 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.

۱-۱۰-۳-۲-۱-۲-۲- 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.

۱-۱۰-۳-۲-۱-۲-۳- صحت و یکپارچگی اطلاعات

مجموعهٔ 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.

۱-۱۱- رابطه بین رشد علم و فن‌آوری و امنیت

[۱] Reply

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 ابزار 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.

۱-۱۲- تحقیقات اجمالی انجام شده در رابطه با کلیات امنیت در دنیای دیجیتال

در جهان سنتی و فیزیکی‌اندیشمندان 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 قیمیت بودند ، در تلاش برای استفاده از فن‌آوری‌های نوین برای حفظ آن بودند . 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[۱] (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 . 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 به یک دسترسی کوچک به این اطلاعات دسترسی پیدا نمایند ، این کار در سال ۲۰۰۰ بسیار راحت‌تر شده بود و

---

[۱] berkley

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[1] شدن رمز ورود و کارت بانکی و شبکه بانکی و شبکه مخابراتی و . . . . به دست دیگران نیفتد.

۱-۱۳- 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 ابزاراقدام می‌نمایند.

۱-۱۳-۱- اشرافیت بر ارتباطات

[1] Hack

یکی از اهداف سلطه گران 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.

۱-۱۳-۲- اشرافیت بر اطلاعات

هدف اصلی سلطه‌گران اشرافیت بر اطلاعات می‌باشدکلیه 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 مبدأ توسط کاربران بوده و این یک نوع سرمایه‌گذاری اقتصادی محسوب می‌شود.

۱-۱۴- آسیب‌های دنیای دیجیتال:

- از بین رفتن کیان و کارکرد خانواده

در جوامع سنتی، خانواده 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 با 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 راترویج 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 باترتیب 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 کارکردتربیت جنسی خانواده را ضعیف می‌کند.

امروزه مسئولیت خانواده‌ها درتربیت 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 می تواند 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.

۱-۳) دنیای دیجیتال

بر اساس تحقیقات انجام شده ۵۱٪ از نفوذ وتخریب سیستم‌های دیجیتال توسط ویروس‌ها و۲۷ ٪ توسط کارکنان ناراضی ، ۱۵٪ 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 . ویروس 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 مهم‌تراینکه آنان نیز به کامپیوتر شما وصل می شوند . 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 ، رباینده‌گان ای . پی و 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 بی سیم ، هکرها فرصت‌های تازه‌ای برای کسب دسترسی به رایانه شما یافته و از طریق شما به کل کشور 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 .

- 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 رایانه ی .

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 رایانه ی دارند و فکر می‌کنند این سرقت‌ها کاملا فنی بوده و در نتیجه نقص‌های فنی سیستم‌های رایانه ی 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 .

« کوین میتنیک» ، بدنام‌ترین هکر رایانه‌ای در کشور آمریکا بعد از آزاد شدن از زندان در جلسه شهادت خود در مقابل کنگره گفت ، ضعیف‌ترین عنصر در حفاظت از رایانه عنصر انسانی است . میتینک گفت: «در مهندسی اجتماعی چندان پر قدرت بودم که بندرت پیش می‌آمد نیازی به حمله فنی داشته باشم »

ج : 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 نگهداشتن افراد بیرونی از دسترس 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 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.

د : 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.

۱-۱۴-۱- ایجاد شکست در فرآیند مدیریت

با توجه به این که مدیریت در هر سیستمی اصلی‌ترین 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 اقدامی نیست 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 .

۱-۱۴-۲- هدایت مدیریت به سمت مسیر خود خواسته

سلطه‌گران در رابطه با اعمال نقطه نظرات خود به‌صورت پنهان و آشکار سرمایه گذاری‌های فراوانی انجام می‌دهند. به دنبال آن می‌باشند تا با کم‌ترین سرمایه گذاری مادی و معنوی به بیش‌ترین اثرات نائل شوند. به دنبال اجرای عملیات خود با کم‌ترین آثار و تبعات ملی و بین‌المللی می‌باشند. به دنبال این مطلب می‌باشند تا در مقابل واژه‌های خودساخته‌ای مانند حقوق بشر که امروزه تبدیل به ابزار سلطه‌گری شده است کم‌تر پاسخ‌گو باشند. 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 داشته باشند.

۱-۱۴-۳- 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 به صورت 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 .

۱-۱۴-۴- حملات ویروس

ویروس ها برنامه های اجرایی کوچکی می باشند که به مجرد اجرا شدن بر روی رایانه قربانی می تواند تغییرات مورد نظر را به صورت پنهان و یا آشکار بر روی رایانه ایجاد نماید.

۱-۱۴-۵- 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.

۱-۱۴-۶- خرابکاری و دستکاری

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

۱-۱۴-۷- 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 در 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.

۱-۱۴-۸- 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 .

۱-۱۴-۹- 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، حملهٔ «استراق سمع» به وقوع پیوسته است.

۱-۱۴-۱۰- افزایش اطلاعات ناخواسته

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

۱-۱۴-۱۱- اقدامات مداخله گرایانه

هرگونه اقدامی که 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

۱-۱۴-۱۲- 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.

۱-۱۴-۱۳- 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 به اطلاعات از راه دور باشد . هرگونه آسیب سخت‌افزاری عملاً باعث آسیب رسانی به اطلاعات خواهد شد.

۱-۱۴-۱۴- 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.

۱-۱۴-۱۵- آسیب به اطلاعات خصوصی

هر کاربر زمانی که با رایانه کار می‌کند هم‌زمان تولید اطلاعات خصوصی می‌نماید. به‌طور مثال درصورتی‌که 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 استعلامی انجام 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.

۱-۱۴-۱۶- کلاهبرداری در اطلاعات

سواستفاده 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 .

۱-۱۵- 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 جهانی تبدیل شده است .

در تمام دنیا:

- افزایش اطلاعات
- تبدیل اطلاعات آنالوگ به دیجیتال
- استفاده از اطلاعات در مبدا تولید

- افزایش توان بهره‌برداری از اطلاعات
- سرعت بخشی به تبدیل اطلاعات به تصمیم

جزو دغدغه‌های اصلی تمام کشورها می‌باشد.

۱-۱۶- سئوالات خودآزمایی

۱. ضمن تعریف اطلاعات، نقش اسناد در امنیت اطلاعات را بیان نمایید.
۲. پدافند غیر عامل را تعریف کرده و اختلاف آن را با پدافند عامل بیان نمایید.
۳. اختلاف بین تهدیدات و فرصت‌ها در دنیای سنتی و نوین را بیان نمایید.
۴. انواع تهدیدات را نوشته و تهدیدات انسان ساخت را توضیح دهید.
۵. انواع اطلاعات دیجیتال را نام برده و توضیح دهید.
۶. پنج نوع از آسیب‌های دنیای دیجیتال را نام برده و توضیح دهید .
۷. اصل کلی و اصول فرعی امنیت دیجیتال را نام برده و توضیح دهید.

•

۲

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 فاوا[۱] 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 آن می‌پردازد . آماده سازی اطلاعات شامل تفکیک اطلاعات دقیق ، علمی و مستند ، جمع آوری، سازمان

---

[۱] فن‌آوری اطلاعات و ارتباطات

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 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 آنکه 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 اطلاعات‌ترکیبی 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 اطلاعات‌ترکیبی 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 پچیده‌تر 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 ، ضرورتاً 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 رایانه ی 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 . (erfan۲۰۰۰. persiangig. 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 می‌گردد.

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 سلطه گر 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 دهنده[۱]
- آماده سازی و امداد رسانی[۲]
- هشدار و اخطار[۳]
- باز سازی مجدد[۴]

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.

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.

---

[۱] Mitigation
[۲] Preparation
[۳] Response
[۴] Recovery

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

۱. سطح استراتژیک: اقداماتی است که در سیاست‌های کلی کشور و تأمین مبانی و پشتوانه‌های قانونی، حقوقی و سیاست‌های برنامه بلندمدت توسعه کشور تأثیرگذار است.
۲. سطح عملیاتی: اقداماتی است که در برنامه‌های ۵ ساله‌ی توسعه‌ی سازمان‌ها تأثیرگذار است.
۳. سطح تاکتیکی: اقداماتی است که در برنامه‌های سالانه‌ی سازمان مؤثر است.
۴. 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 وفریب
- 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 مناسب‌ترین 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 – پورابراهیمی و 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 درتأمین دفاع غیرعامل و کاهش آسیب‌پذیری زیرساخت‌های ملی و مراکز حیاتی، حساس و مهم کشور در مقابل تهدیدات 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 جنبه های مختلف حائز اهمیت می باشد که محرمانگی و در دسترس بودن و حفظ تمامیت از جمله آنها می باشد . امروزه بدون بومی سازی نمی توان انتظار ایجاد امنیت مطلوب را داشت. امنیت از جمله مواردی می باشد که معمولا در تضاد با برون سپاری بوده و می بایست توسط نیازمند به امنیت و به صورت بومی تولید و ایجاد گردد.

۲-۲-۲- ایمنی

ایمنی به مفهوم امن بودن در مقابل تهدیدات و حملات سخت و نیمه سخت می‌باشد. هر سیستمی به منظور تداوم بقا 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 برنامه ریزی، 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 (پشتیبانی[۱])
- کاهش وابستگی

[۱] Back up

- وابستگی فن‌آورانه، علمی و . . . به خارج از کشور
- وابستگی خدمات و پشتیبانی به سایر بخش‌ها (داخلی یا خارجی)
- تنوع منابع پشتیبانی

- توسعه اشتراک منافع
- توسعه و ارتقاء موقعیت بین‌المللی (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 اصلاح زیرساخت‌های فعلی هم می‌توان با ارائه راهکارهایی مثل مهندسی مجدد، آن‌ها را مستحکم کرد.

اهداف پدافند غیرعامل:

- کاهش قابلیت و توانایی سامانه‌های شناسایی، هدف یابی و دقت هدف‌گیری تسلیحات آفندی دشمن.
- بالا بردن قابلیت بقا، استمرار عملیات و فعالیت‌های حیاتی و خدمات رسانی مراکز حیاتی، حساس و مهم نظامی و غیر نظامی کشور در شرایط وقوع تهدید، بحران و جنگ.
- تقلیل آسیب‌پذیری و کاهش خسارت و صدمات تاسیسات، تجهیزات و نیروی انسانی مراکز حیاتی، حساس و مهم نظامی و غیر نظامی کشور 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. (padafand-gh-amel. persianblog. 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 دسترس پذیر 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 بقا 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 . برج و 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 ۱۳۸۴آئین نامه 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 درطراحی 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 ،الویت‌هاو دستورالعمل‌های کارگروه دائمی پدافند غیر عامل کشور درصدی از اعتبارات تملک دارائی‌های سرمایه‌ای خود راجهت 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 کشورتوسط مجمع تشخیص مصلحت نظام تهیه و به تصویب رسانده شده، 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 برنامه ریزی 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 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 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 خواسته ایمنی 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.

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 جمع‌آوری اطلاعات، تغییرات قابل توجهی را در مکانیسم‌ها و ساز و کارهای حاکم بر فعالیت‌ها و چالش‌های نظامی و دفاعی بوجود آورده‌است. 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 وکنترل 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 آسیب رسانی 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 بقا 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 تصمیم گیری[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 خواهد 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] (CBIS) computer based information system
[۲] (DSS) decision support system

۲-۶- سئوالات خودآزمایی

۱. فاوا مخفف چیست ؟ توضیح دهید.
۲. اصول کلی پدافند غیرعامل را نام برده و توضیح دهید.
۳. پدافند غیر عامل در حوزه فاوا را توضیح دهید.
۴. سابقه پدافند غیرعامل فاوا در ایران را بنویسید.
۵. تهدیدات سیستم‌های ارتباطی از منظر فاوا کدامند؟ توضیح دهید.
۶. تهدیدات سیستم‌های رایانه‌ای از منظر فاوا کدامند؟ توضیح دهید.
۷. تهدیدات سیستم‌های اطلاعاتی مبتنی بر رایانه از منظر فاوا کدامند؟ توضیح دهید.

۳

فصل سوم – امنیت اطلاعات

آن چه در این فصل می‌خوانید:

- **امنیت**
- **علل سرمایه گذاری در رابطه با امنیت اطلاعات**
- **جهانی شدن امنیت**
- **مهندسی اجتماعی و امنیت**
- **ردیابی اطلاعاتی و بر چسب امنیتی**
- **شناسایی اسناد کاربران امنیت در اطلاعات**
- **تعیین سطوح طبقه بندی مجاز برای اطلاعات ساختار**

۳- امنیت اطلاعات

با توجه به این که اطلاعات دارای انواع و اقسام مختلفی می‌باشد ، در این فصل ضمن آشنایی با اطلاعات و انواع آن به روش‌ها و شیوه‌های امن نگهدای اطلاعات خواهیم پراخت.

۳-۱- امنیت

امنیت از جمله دیرپاترین آمال بشر بوده است. دل نگرانی‌های ناشی از تامین امنیت، همواره همزاد انسان بوده و از بدو تولد بشر واژه امنیت جزو جدّی‌ترین دغدغه‌های وی بوده است. امنیت جزو اساسی‌ترین نیازهای بشر است. تعریف امنیت در دوره‌های مختلف زندگی بشر توسعه پیدا کرده است. در جوامع اولیه مفهوم امنیت در حفظ جان و دفع ضرر حمله حیوانات وحشی و یا در پیدا کردن آب و غذا و تامین نیازهای اولیه زیستی دیده می‌شد. کم کم با گسترش جوامع و بوجود آمدن حکومت‌ها، تامین امنیت کشور (شامل سرزمین، حاکمیت، استقلال و. . .) وظیفه اصلی حکومت‌ها شد و امنیت بیش‌تر در حوزه نظامی آن تعریف می‌شد.

۳-۲- اسناد

یکی از مهم‌ترین ابزار و روشی که در تعاملات اطلاعاتی به کاربرده شده و توسط آن اطلاعات بین افراد مختلف انتقال می‌یابد اسناد است. از زمانی که انسان‌ها آموختن را یاد گرفتند اسناد نیز هم پای انسان‌ها تولید شده و رشد نمود. بستگی به دوره‌ای که انسان‌ها در آن زندگی می‌کنند اسناد انواع و اقسام مختلف داشته و به روش‌های مختلف از آن حفظ و نگهداری می‌شود.

۳-۲-۱- تعریف سند

- **تعریف سند از نظر اداری و بایگانی:**

((هر نوع سابقه‌ای که به صورت مکتوب مانند نامه‌های اداری ، منقوش مثل نقشه‌ها و نمودارها ، مضبوط مثل نوار و صفحه گرامافون در یک سازمان برای انجام وظایف اداری و توسط ماموران آن سازمان و در حدود وظایف مصوب رسما ایجاد ، دریافت و یا صادر شده باشد.))

به طور کلی هر مدرکی (نوشته یا شیء)که قابل ارزش باشد و بتوان از آن اطلاعاتی کسب کرد ، سند نام دارد. مانند نامه ، یادداشت ، طرح ، دستورالعمل ، جدول ، کروکی ، گرافیک ، فهرست ، رمز ، تلگراف ، عکس ، فیلم ، اسلاید ، کارت مشخصات ، فرمهای اداری ، تعرفه‌های پرسنلی ، فیش ، کاغذ استنسیل ، کاربن ، نوار مستعمل ، ماشین تحریر و . . . .

۳-۲-۱-۲- سند در قانون

در قانون در رابطه به اسناد ، مخصوصا اسناد دولتی در موارد مختلف نام برده شده است که ذیلا به آن‌ها اشاره می‌شود:

قانون اساسی جمهوری اسلامی

اصل ۲۵ : بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی ، افشای مخابرات تلگرافی و تلکس ، سانسور ، عدم مخابره و نرساندن آن‌ها ، استراق سمع و هر گونه تجسس ممنوع است مگر به حکم قانون .

قانون رسیدگی به تخلفات اداری

ماده ۸ _ تخلفات اداری به قرار زیر است :

بند ۱۰ : تسامح در حفظ اموال و اسناد و وجوه دولتی ، ایراد خسارت به اموال دولتی.

بند ۱۱ : افشای اسرار و اسناد محرمانه اداری .

بند ۱۶ : ارائه گواهی یا گزارش خلاف واقع در امور اداری .

بند ۲۶ : جعل یا مخدوش نمودن و دست بردن در اسناد و اوراق رسمی یا دولتی .

بند ۲۷ : دست بردن در سئوالات ، اوراق ، مدارک و دفاتر امتحانی ، افشای سئوالات یا تعویض آن‌ها .

بند ۳۱ : توقیف ، اختفاء ، بازرسی یا بازکردن پاکت‌ها و محمولات پستی یا معدوم کردن آن‌ها و استراق سمع بدون مجوز قانونی .

تخلیهٔ اطلاعاتی

ماده ۵۰۶ - چنان‌چه مأمورین دولتی که مسئول امور حفاظتی و اطلاعاتی طبقه بندی شده می‌باشند و به آن‌ها آموزش لازم داده شده است در اثر بی مبالاتی و عدم رعایت اصول حفاظتی توسط دشمنان تخلیهٔ اطلاعاتی شوند به یک تا شش ماه حبس محکوم می‌شوند .

معدوم کردن اسناد و نوشتجات و اوراق اداری

ماده ۶۰۴ _ هر یک از مستخدمین دولتی اعم از قضایی و اداری نوشته‌ها و اوراق و اسنادی را که حسب وظیفه به آنان سپرده شده یا برای انجام وظایفشان به آن‌ها داده شده است را معدوم یا مخفی نماید یا به کسی بدهد که به لحاظ قانون از دادن به آن کس ممنوع می‌باشد علاوه بر جبران خسارت وارده به حبس از سه ماه تا سه سال محکوم خواهد شد .

۳-۲-۲- انواع اسناد

با توجه به محل نگهداری اسناد و نوع اسناد می‌توان آن را به اسناد مختلف تقسیم بندی نمود.

۳-۲-۲-۱- اسناد کاغذی

امروزه بیش‌ترین اسنادی که در بین عامه مردم به عنوان سند از آن‌ها نام برده می‌شوند اسناد کاغذی نام دارند که به صورت مفصل در رابطه با آن‌ها در قانون بحث گردید.

۳-۲-۲-۲- اسناد شیمیایی

منظور از اسناد شیمیایی کلیه اسنادی است که به شکل شیمیایی نگهداری می‌شوند که مهم‌ترین آن‌ها اسناد نگهداری شده در فیلم‌ها و عکس‌ها و کاغذهای‌ترمال و . . می‌باشد.

۳-۲-۲-۳- اسناد ذهنی

ذهن در معنای لغوی به معنای فهم، دریافت، یاد، هوش، قوه باطنی که مطالب را به یاد نگه می‌دارد می‌باشد.

از آنجایی که از معانی لغوی ذهن بر می‌آید، ذهن مجموعه‌ای از فهم و درک، دریافت اطلاعات، یادآوری و بازیابی و موضوع هوش که موارد فوق به‌ترتیب مربوط به بخش‌های:

۱. ادراک

۲. تفکر

۳. نظام حسی و شناختی می‌شود.

حافظه

اعمال حافظه به طور معمول در ۴ زمینه مورد بررسی قرار می‌گیرد:

۱. حافظه آنی یا فوری (ذخیره سازی و یادآوری فوری)[۱]

۲. حافظه نزدیک [۲]

۳. حافظه گذشته نزدیک [۳]

۴. حافظه دور [۴]

حافظه آنی یا فوری:

اندازه گیری فراخنای ارقام: توانایی تکرار شش رقم پس از دیکته شدن توسط مصاحبه کننده (مثلا ارقام ۱ و ۴ و ۹ و ۲ و ۵ بلافاصله بعد از تکرار مصاحبه کننده ، شنونده به صورت درست و برعکس تکرار کند). کسانی که حافظه سالم دارند می‌تواند ۶ رقم معکوس را تکرار کنند. توانایی تکرار ۳ کلمه مثل میز، شانه، درخت بلافاصله بعد از شنیدن و پس از چند دقیقه پس از شنیدن.

حافظه نزدیک

در خصوص این که امروز ساعت چند چه کرده است؟ یا دیروز یا پری روز نهار یا شام چه خورده است؟

حافظه گذشته نزدیک:

مربوط به چند ماه گذشته است، مثلاً در چند ماه گذشته چه کرده است؟

حافظه دور:

جواب به پرسش در مورد دوران کودکی بیمار و یا اتفاقات سال‌های قبل و مربوط به دوران جوان یا کودکی.

توضیح اینکه در افراد سالخورده و کودکان عقب مانده ذهنی و سندرم‌های عضوی مغز، ابتدا حافظه کوتاه مدت یا حافظه نزدیک (حافظه فعال) آسیب می‌یبند و حافظه دور یا بلند مدت تقریباً دست نخورده باقی می‌ماند و یا بعدها مختل می‌شود.

در سطح (ذخیره) اطلاعات عمومی و هوش، اگر حدس اختلال شناختی می‌رود ، باید دقت کرد که بیمار در انجام اعمال ذهنی نظیر محاسبه باقی مانده ۱۰۰۰ تومان پس از خرج ۶۳۷

---

[۱] Immediate retention and recall
[۲] Recent memory
[۳] Recent past memory
[۴] Remote memory

تومان دچار اشکال می‌شود یا نه و یا دادن محاسبات ساده‌تر مثل چند ۵ تومانی می‌شود ۷۵ تومان. هوش بیمار با واژگان و ذخیره کلی معلومات مرتبط است.

یکی از مباحث مهم در زمینه اطلاعات ذهنی مباحث مربوط به چگونگی اطلاعات ذهنی مجرمین و ادعای آنان در جهت فرار از قانون است. بحث از دست دادن حافظه و به یاد نیاوردن، که به نوبه خود، دستگاه قضایی و پلیسی را در نحوه برخورد با این گونه مجرمین دچار سردرگمی می‌کند.

در آینده اسکن مغزی مرتباً جهت بررسی موارد مشکوک به منظور تایید حقایق استفاده خواهد شد حال حاضر شواهد بسیاری هم وجود دارد که نشان می‌دهد برخی ناهنجاری‌های ریخت شناسی و متابولیکی، در اشخاص بروز می‌کند که سابقه کیفری دارند.

مجله نیچر جلد ۴۳۷ منتشره در سال ۲۰۰۵، اعلام می‌دارد که دانشمندان آماده شناسایی‌تروریست‌ها با توجه به علم اعصاب و اسکن مغزی می‌باشند.

اخیراً حتی با استفاده و بررسی در کمیت مصرف گلوگز، توضیح دهیم که فعال سازی گلوکز در مغز انسانی با کارکرد طبیعی در نواحی معمول و یا در نواحی پردازش حافظه، کاهش می‌یابد یا نه.

۳-۲-۲-۴- اسناد دیجیتال

اسناد دیجیتال(رایانه‌ای) : شامل داده‌های رایانه‌ای ، دیسکت‌های رایانه‌ای ، سی‌دی‌های رایانه‌ای ، امواج مخابراتی . یعنی تمام اطلاعات رایانه‌ای از هر نوع که باشد به‌عنوان "اسناد دیجیتال" تلقی می‌شود.

آئین نامه طرزنگهداری اسنادسری ومحرمانه دولتی مصوب ۱۳۵۴/۱۰/۱

قسمت اول_ طبقه بندی اسناد:

ماده۱- اسناد سری و محرمانه دولتی به اعتبار مقدار مراقبتی که باید در حفظ آن‌ها بشود به چهار طبقه تقسیم می‌شود.

طبقه اول- اسنادی است که افشای غیرمجاز آن‌ها به اساس حکومت و مبانی دولت ضرر جبران ناپذیری برساند.

طبقه دوم- اسنادی است که افشای غیرمجاز آن‌ها منافع عمومی و امنیت ملی را دچار مخاطره کند.

طبقه سوم- اسنادی است که افشای غیرمجاز آن‌ها نظام امور سازمان‌ها را مختل و اجرای وظائف اساسی آن‌ها را ناممکن کند.

طبقه چهارم- اسنادی است که افشای غیرمجاز آن‌ها موجب اختلال امور داخلی یک سازمان شود یا با مصالح اداری آن سازمان مغایر باشد. اسناد سری در طبقات اول و دوم و اسناد محرمانه در طبقات سوم و چهارم قرار می‌گیرند(اسناد طبقه اول با عنوان بکلی سری و اسناد طبقه‌ی دوم با عنوان سری و اسناد طبقه سوم با عنوان خیلی محرمانه و اسناد طبقه چهارم با عنوان محرمانه مشخص می‌شود).

تبصره- کلمه سازمان در این آئین نامه به جای وزارتخانه و موسسه دولتی و وابسته به دولت و شرکت دولتی به کار رفته است.

ماده۲- طبقه هر سند با توجه به مفاد آن تعیین می‌شود. هرگاه سند مضبوط در پرونده یا ضمیمه نامه‌ای باشد پرونده یا نامه نیز در طبقه‌ی مربوط به آن سند بایگانی می‌شود. اگر اسناد متعدد و در طبقات متفاوت باشند پرونده یا نامه‌ای که اسناد مذکور منضم به آنست درطبقه‌ی مهم‌ترین آن اسناد بایگانی خواهد شد.

ماده۳- طبقه‌ی هر سند را مسئول واحدی که آن سند را تهیه کرده است تعیین می‌کند، درصورتی که نظر مسئول واحد بر سری شناختن سند باشد باید موافقت رئیس سازمان یا مقام مادون ازطرف او را جلب کند.

ماده۴- برای تغییر طبقه یک سند یا خروج آن از طبقات چهارگانه هریک ازسازمان‌ها به مقتضای وظائف و طبع کار خود دستورالعملی تهیه خواهدکرد اگر تغییر طبقه یا خروج از طبقات به سندی مربوط باشد که از سازمانی به سازمان دیگر فرستاده شده است اتخاذ تصمیم به توافق هر دو سازمان منوط خواهد بود. اعلان یا افشای مفاد اسناد سری یا محرمانه از طرف مراجع ذی‌صلاحیت سند مذکور را از عداد اسناد سری و محرمانه خارج می‌کند. تغییرات مذکور باید در روی سند منعکس شود.

قسمت دوم- نحوه مشخص کردن نوع اسنادسری و محرمانه:

ماده۵- نـوع و طبقـه هر سنـد در صدر و ذیل سند و اگر سند در چند صفحه تهیه شده باشد در صدر و ذیل همه‌ی صفحات درج می‌شود. صفحات یک سند به‌ترتیب شماره گذاری و تعدادکل صفحات نیز در روی هرصفحه منعکس می‌شود. اگر سند طبقه اول و دوم در نسخ متعدد تهیه شده باشد هریک از نسخ نیز در روی هر نسخه درج می‌شود.

سندسری یا محرمانه نباید به بیش از نسخ مورد لزوم تهیه شود.

۳-۲-۵- امنیت اطلاعات اسناد ذهنی

- در مغز انسان دست کم ۱۲ میلیارد یاخته (سلول) عصبی به نام نورون وجود دارد که واحدهای پایه‌ای دستگاه عصبی محسوب می‌شوند شناخت نورون‌ها و مکانیزم ارتباطی آن‌ها مهم است زیرا که بدون شک آن‌ها رازهای یادگیری و کارکردهای روانی بی‌شماری را در خود پنهان دارند
- علم بشر تا به امروز به چگونگی انتقال و هماهنگ سازی تکانه‌های عصبی آگاهی پیدا کرده است لیکن در پرده گشایی از کارکردهای پیچیده و رمز و راز آلود این ودیعه خدادادی هنوز در آغاز راه است
- نورون : سلول‌های ویژه عصبی را نورون می‌نامند نورون‌ها بر حسب کارکردشان دارای‌اندازه‌ها و اشکال متفاوتی هستند

نورون‌ها از اجزای مختلفی به نام‌های دندریت (برگرفته از لغت یونانی denderon به معنای درخت) ، هسته ، آکسون و تکمه‌ها و یا شاخه‌های انتهایی تشکیل شده‌اند نورون‌ها به سه دسته حسی ، حرکتی و ارتباطی تقسیم می‌شوند نورون‌های حسی وظیفه دریافت تحریکات حسی از جمله گرما ، سرما ، فشار ، درد و . . . را بر عهده دارند . نورون‌های حرکتی وظیفه انتقال این تحریکات به مغز و متقابلا دستورات مغزی به اعضا را بر عهده دارند . و نهایتا نورون‌های ارتباطی حد فاصل نورون‌های حسی با نورون‌های حرکتی هستند نورون‌های ارتباطی صرفاً در مغز و نخاع وجود دارند

- عصب: عبارت است یک دسته آکسون مطول که به صدها یا هزاران نورون تعلق دارند . طول برخی آکسون‌ها من جمله آکسون نخاعی ممکن است به ۶۰ تا ۹۰ سانتی متر یعنی تا نوک انگشت پا برسد حال آنکه برخی آکسون‌ها کم‌تر از یک هزارم سانتی متر است
- سیناپس : فاصله بین دو نورون که با مایع شیمیایی خاصی اشغال شده را سیناپس می‌نامند .
- تکانه عصبی : فرآیند خاص (برقی ، شیمیایی) بین دو نورون تکانه عصبی نام دارد .

- داروهای روانگردان : داروهایی هستند که بر روی کارکردهای روانی مغز تاثیراتی بر جای می‌گذارند تاثیراتی چون تحریک یا آرامش یابی ، خواب یا جلوگیری از خواب ، حدت بخشی به ادراک یا ایجاد توهم و . . . .
- بین غشای دو نورون عصبی یک خاصیت‌تراوایی وجود داردتراوایی غشای نازکی که پروتوپلاسم یاخته را در خود جای داده نسبت به یون‌های داخل پروتوپلاسم و مایع احاطه کننده یاخته (مایع خارج یاخته‌ای موجود در سیناپس) که بار الکتریکی دارند یکسان نیست . در حالت استراحت غشای یاخته یون‌های سدیم مثبت را در خارج از خود نگه می‌دارد و یون‌های پتاسیم مثبت و کلر منفی را به درون می‌پذیرد. لیکن هر گاه یک آکسون تحریک شود پتانسیل الکتریکی دو طرف غشای سلولی کاهش می‌یابد در نتیجه‌تراوایی اشاره شد تنت به طور ناگهانی تغییر یافته و به یون‌های سدیم اجازه ورود به داخل را می‌دهد در چنین شرایطی با الکتریکی خارج یاخته نسبت به داخل آن منفی شده و بر بخش دیگر آکسون اثر می‌گزارد این تغییر و تکرار فرآیند یک تکانه عصبی نام دارد.
- اتصال سیناپسی بین نورون‌ها اهمیت فوق‌العاده‌ای دارد چرا که یاخته‌های عصبی از این طریق پیام‌های خود را مبادله می‌کند این حالت (انتقال پیام) زمانی رخ می‌دهد که تحریکاتی که از سیناپس‌های مختلف وارد می‌شود از آستانه مشخصی عبور کند
- وقتی یک تکانه عصبی به انتهای آکسون می‌رسد کیسه‌های سیناپسی را به‌ترشح یک ماده انتقال دهنده عصبی به درون شکاف سیناپسی وا می‌دارد ملکول‌های انتقال دهنده عصبی با ملکول‌های گیرنده در غشای یاخته‌ی دریافت کننده در عملی شبیه قفل و کلید عمل می‌کنند .
- فقط یک نوع ماده انتقال دهنده در کیسه‌ها سیناپسی وجود دارد.
- نورون‌ها به‌طور مستقیم با هم ارتباط ندارند بین آن‌ها فاصله کوچکی بنام سیناپس وجود دارد که جریان عصبی را عبور می‌دهد در اکثریت قریب به اتفاق یک ماده شیمیایی نقش مهمی در این انتقال را بر عهده می‌گیرد که ماده انتقال دهنده نامیده می‌شود . این ماده به درون فضای سیناپسی‌ترشح می‌شود.

۳-۲-۵-۱- تحمیل اراده

تحمیل اراده با اهداف مختلفی صورت می‌پذیرد. با توجه به این که ذهن بشر در رابطه با اقدامات فیزیولوژیکی و روان شناسی دارای آستانه تحمل بوده و این آستانه در انسان‌ها متفاوت می‌باشد تحمیل کنندگان اراده تلاش می‌نمایند تا با روش‌های مختلف آن‌ها را به آستانه تحمل رسانیده و پس از آن شروع به درخواست و کسب اطلاعات مورد نیاز نمایند. ممکن است این کار با زمینه سازی‌های مختلفی صورت پذیرفته و پس از اقدامات روانی در موقعیت مناسب زیرپاکشی از افراد و اخذ اطلاعات مورد نیاز صورت پذیرد. معمولاً تحمیل ارادی به شکلی صورت می‌پذیرد تا متحمل شونده احساس مصلوب الاراده شدن نداشته باشد زیرا یکی از راه‌های مقاومت در مقابل تخلیه ذهن به صورت ناخودآگاه مقاومت در برابر فرد یا افرادی می‌باشد که تلاش دارند این مقاومت را بشکنند.

۳-۲-۵-۲- هیپنوتیزم

تاریخچه

حدود ۳۰۰ سال پیش فردی به نام فذانتس مسمر که یک پزشک بود راهی تازه در درمان برخی بیماران خود پیدا کرد که استفاده از میدان مغناطیسی ناشی از آهن ربا بود .

وی در جریان مداوای بیماران خود به ناگاه دریافت برخی بیماران در مواجه با این میدان مغناطیسی دچار نوعی از خود بی خود شدن و خلسه می‌گردند.

۲۰۰ سال پیش یک پزشک فرانسوی به نام شارکو هیپنوتیزم را نشانه هیستری و نوعی اختلالات دستگاه عصبی به شمار آورد.

بعدها پزشک دیگری به نام برنهایم به مبارزه با آرای شارکو برخاست و اظهار می‌داشت : هیپنوتیزم ناشی از تلقین است .

تا دهه‌های اخیر مسئله هیپنوتیزم در زمره مسایل متافیزیکی و اسرار آمیز به شمار می‌رفت اما امروزه به عنوان یک روش علمی که در درمان برخی بیماری‌ها کاربرد موثری دارد مورد استفاده برخی روانشناسان قرار می‌گیرد.

هیپنوتیزم چیست ؟

هیپنوتیزم : برگرفته از کلمه یونانی Hypnos به معنای خواب است . به دلیل این که در حالت هیپنوتیزم ، هیپنوتیزم شونده فاقد کنترل بر هشیاری کامل خود است لذا در تعاریف از آن به نوعی خواب یاد می‌شود اما در حقیقت هیپنوتیزم خواب نبوده بلکه نوعی تمرکز است که هیپنوتیزور به کمک هیپنوتیز شونده ایجاد می‌کند. به عبارتی نوعی پاسخ دهی شدید است به آنچه که هیپنوتیزور در هیپنوتیز شونده ایجاد می‌کند .

ضمیر ناخود آگاه :

ذهن انسان به مانند یک نوار مغناطیسی تمامی وقایع را از لحظه بیدار شدن تا خواب مجدد و حتی در زمان خواب ثبت و ضبط می‌کند. لیکن بازیابی این وقایع و اتفاقات که عمدتا در ضمیر آگاه فرد به خاطر آورده نمی‌شود تابع شرایط خاصی می‌باشد. دانشمندان در مقایسه ضمیر آگاه و ناخود آگاه آن را به کوه یخ تشبیه کرده‌اند که بخش اعظم آن که در زیر آب پنهان است به ضمیر ناخود آگاه اطلاق می‌شود. فهم و مطالعه ضمیر ناخود آگاه برای ریشه‌یابی رفتار آدمی مهم است . به تعبیر زیکموند فروید قسمت عمده‌ای از رفتار آدمی در فرآیندهایی ریشه دارد که ناهشیارند فرآیندهایی چون‌ترس ، خشم و تمایلاتی که از علت آن در شرایط عادی بی خبر هستیم .

تلقین:

تلقین : تلقین در هیپنوتیزم فرآیندی است که طی آن هیپنوتیزور با کاربرد کلام و یا نمادهای غیر کلامی هیپنوتیز شونده را وادار به تفکر و اداراک آنچه خود در پی آن است می‌کند.

- امواج : بدن انسان از خود امواجی ساتع می‌کند که در دستگاهای نوار مغزی و غیره قابل ثبت و شناسایی است . طول موج این امواج بستگی به تمرکز و ممارست افراد قابل تغییر است تحلیل ارتباط از راه دور بین افراد به ویژه افرادی که ارتباط و صمیمیت ذهنی باهم دارند (تله پاتی) از این طریق ممکن است .
- پاس دادن: فرآیندی است که طی آن هیپنوتیزور با کشیدن دست خود برقسمت‌هایی از بدن هیپنوتیز شونده با فاصله معین امواج ساتع شده از بدن را تحت تاثیر قرار می‌دهد.

- خود هیپنوتیزم : به فرآیند هیپنوتیز کردن یک شخص توسط خودش ، خودهیپنوتیزم یا اتوهیپنوتیزم گفته می‌شود. در این حالت شخص با کاربرد تمرینات و روش‌های رلکس ماهیچه‌ها و ایجاد تمرکز ذهنی به نوعی خلسه وارد می‌شود. یکی از روش‌های مطرح با الگو برداری از فلسفه چینی و یا هندی ، مراقبه است که دو حالت دارد : مراقبه راه‌گشا و مراقبه متمرکز . در مراقبه راه‌گشا ، شخص ذهن خود را برای دریافت تجارب تازه ذهنی از هر گونه افکار مزاحم پاک می‌کند . لیکن در روش مراقبه متمرکز ، شخص با اندیشیدن و یا تمرکز بر موضوعی خاص به نوعی تمرکز دست می‌یابد.

برخی آثار هیپنوتیزم

- ✓ در تغییرات ناشی از هیپنوتیزم تصمیم گیری متوقف می‌شود.
- ✓ دقت مجددا توزیع شده و بیش‌تر از حالت عادی انتخابی می‌گردد.
- ✓ تخیلات غنی به آسانی برانگیخته می‌شود.
- ✓ تلقین پذیری به شدت افزایش می‌یابد.
- ✓ پس از هیپنوتیزم اغلب ، چیزی به خاطر هیپنوتیز شونده نمی‌آید مگر این که توسط هیپنوتیزور با نشانه‌هایی از پیش تعیین شده مراحلی به یاد آورده شود و یا کاری صورت پذیرد.

۳-۳- علل سرمایه گذاری در رابطه با امنیت اطلاعات

هزاره سوم را عصر دانایی نامیده‌اند. اقتصاد جدید عبارت است از داد و ستد دانش. دانایی، سرمایه را فراهم آورده و پایه‌های قدرت فردی و سازمانی را تشکیل می‌دهد. اطلاعات موجود هر سه یا چهار سال دو برابر می‌شود. قدرت تفکر عنوان با ارزش‌ترین دارایی سازمانی تلقی می‌شود. این دانش تعیین کننده وضعیت رقابتی در جهان است. در حال حاضر بزرگ‌ترین چالش مدیران، علاوه بر ایجاد سرمایه دانایی، ایمن سازی و توزیع مجدد آن است. بدون شک گسترش و توسعه روز افزون فن‌آوری ارتباطات و اطلاعات و همگرا شدن آن‌ها ، ظهور اینترنت و رسانه‌ها دلیل توفیقاتی است که بشر امروزه ، شاهد آن است و موجب نام‌گذاری عصرحاضر به عصر اطلاعات گردیده است.

تفاوت این عصر با سایر اعصار را بایستی در سرعت تغییرات فن‌آوری‌ها ، رشد سریع و چشمگیر علوم می‌باشد و همه این‌ها را باید مدیون دسترسی وسیع همگانی به اطلاعات دانست. هم‌چنین برخی از اندیشمندان ، دنیای امروز را دنیای اطلاعات ، سرعت و شتاب دانسته‌اند. به قول بیل گیتس اگر ویژگی دهه **۱۹۸۰** رویکرد به کیفیت و دهه **۱۹۹۰** دوران مهندسی مجدد فرآیندها بوده است ، دهه **۲۰۰۰** را باید دوران شتاب دانست. دسترسی گسترده همگانی به اطلاعات ، موجب شکوفایی استعدادهای نهفته گردیده و در سایه شکوفایی استعدادهاست که موفقیت‌های بشری شکل می‌گیرید و هر روز محصول جدیدی معرفی می‌شود. هیچ کشوری جزء در سایه بلوغ فکری مردم خود ، به توسعه پایدار و همه جانبه دست نخواهد یافت و بلوغ فکری تنها از طریق افزایش اطلاعات حاصل می‌گردد. از طرفی تولید اطلاعات ، دانش و علم در سازمان‌ها بسیار حیاتی و حفظ و نگهداری از آن‌ها در هزاره سوم که عصر دانایی نام گرفته است و اقتصاد آن از طریق داد و ستد دانش و اطلاعات شکل می‌گیرد جهت حفظ و تعالی سازمان‌ها بسیار سرنوشت ساز می‌باشد. دانایی ، سرمایه را فراهم آورده و پایه‌های قدرت فردی و سازمانی را تشکیل می‌دهد.

اطلاعات موجود هر سه یا چهار سال دو برابر می‌شود. قدرت تفکر ، عنوان با ارزش‌ترین دارایی سازمان تلقی می‌شود. این دانش تعیین کننده وضعیت رقابتی در جهان است. اطلاعات در حال حاضر مهم‌ترین گنجینه به حساب می‌آید. در بعضی سازمان‌ها و حتی در موارد شخصی از بین رفتن اطلاعات و حتی آسیب دیدن اطلاعات منجر به صرف زمان و نیروی کار غیر قابل تصور جهت دسترسی به آن‌ها می‌شود و حتی در برخی موارد اصول کاری یک سازمان را مورد تهدید قرار می‌دهد. تکنولوژی اطلاعات(IT) یک سکه دو روست . هم فرصت است و هم تهدید ! اگر به همان نسبتی که به توسعه و همه گیری‌اش توجه و تکیه می‌کنیم به " امنیت " آن توجه نکنیم می‌تواند به سادگی در کسری از ثانیه تبدیل به یک تهدید و مصیبت بزرگ شود.

۳-۴- مهندسی اجتماعی و امنیت

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 رایانه ی.

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 رایانه ی دارند و فکر می‌کنند این سرقت‌ها کاملا فنی بوده و در نتیجه نقص‌های فنی سیستم‌های رایانه ی 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 .

« کوین میتنیک» ، بدنام‌ترین هکر رایانه‌ای در کشور آمریکا بعد از آزاد شدن از زندان در جلسه شهادت خود در مقابل کنگره گفت ، ضعیف‌ترین عنصر در حفاظت از رایانه عنصر انسانی است . میتینک گفت: «در مهندسی اجتماعی چندان پر قدرت بودم که بندرت پیش می‌آمد نیازی به حمله فنی داشته باشم »

۳-۵- ردیابی اطلاعاتی و بر چسب امنیتی

ردیابی اطلاعات بسته به نوع استفاده می‌تواند متفاوت باشد و هر نوع ردیابی اطلاعاتی و حتی نظارت و کنترل را به ارمغان بیاورد.

ساده‌ترین شکل و ملموس‌ترین حالت استفاده از راه حل ردیابی شیيء متحرک از راه دور و بی سیم می‌تواند ردیابی خودرو باشد. سیستم مدیریت ردیاب وسایل نقلیه با استفاده از فن‌آوری ماهواره‌ای GPS و نرم‌افزار طراحی شده و بکارگیری شبکه ارتباطی موبایل یا ماهواره‌های ارتباطی و یا با بهره گیری از شبکه‌های مختلف مخابراتی می‌تواند در هر لحظه و در تمام ساعات شبانه روز، با استفاده از گیرنده‌های جی پی اس و نقشه استفاده شده در سیستم موقعیت خودرو(موقعیت و زمان) را در هر نقطه به‌دست آورده، گزارش نماید و همچنین با پردازش ثانویه می‌توان سرعت و جهت جغرافیایی شیيء متحرک را در هر نقطه‌ای که گیرنده وجود دارد محاسبه و ارسال نماید.

به عبارت دیگر این نوآوری در صنعت حمل و نقل، یک سیستم جامع نظارت و مدیریت ناوگان با هزینه قابل توجیه و بسیار اندک را پیش‌نهاد می‌نماید که ضمن ارائه سیستم مدیریت، بازگشت سرمایه را به سرعت تضمین می‌نماید.

سیستم ردیابی اطلاعات

سیستم ردیاب offline

در این سیستم اطلاعات حرکتی مسیر، موقعیت و سرعت گرفته شده از ماهواره‌های GPS در یک ممووری ذخیره شده و در پایان هر ماموریت تحویل مقام مسئول جهت کنترل و رد یابی اطلاعات می‌شود و اطلاعات در مسیر حرکت و زمان حرکت قابل دسترسی نیست.

گیرنده GPS

وسیله‌ای است که با دریافت سیگنال‌های خاص از ۲۴ ماهواره، می‌تواند موقعیت خودرو را به صورت طول و عرض جغرافیایی و ارتفاع از سطح دریا محاسبه نماید. آنتن این گیرنده کوچک روی سقف خودرو نصب می‌گردد و با دریافت اطلاعات از ماهواره، موقعیت خودرو را پیدا نموده و به‌ترمینال جایاب یا ردیاب منتقل می‌نماید.

ترمینال ردیاب

اطلاعات مربوط به موقعیت، زمان، سرعت و جهت را در فواصل زمانی از متحرک دریافت نموده و در حافظه ذخیره می‌کند تا بعدا به رایانه منتقل گردد. در این دستگاه حافظه خاصی برای نگهداری و ذخیره سازی مسیرهای حرکتی درنظر گرفته شده است. در نوع ساده حافظه در داخل دستگاه به صورت ثابت، و در نوع کارتی به صورت کارت جداگانه درنظر گرفته شده است.

کارت حافظه

در مدل کارتی کارت حافظه به پورت‌ترمینال ردیاب وصل می‌شود و می‌توان به راحتی آن را از دستگاه جدا نموده و با اتصال مستقیم به رایانه اطلاعات موقعیتی روی آن را تخلیه نمود.

نرم‌افزار ردیاب

پس از بازگشت خودرو از ماموریت یا سفر، با برداشتن کارت حافظه از روی خودرو و اتصال آن به رایانه مرکز کنترل مسیر حرکت، موقعیت خودرو، سرعت، انحراف از مسیر برنامه ریزی شده، سرعت یا توقف غیرمجاز و دیگر اطلاعات مورد نیاز روی نقشه نمایش داده شده و به صورت گزارش‌های مختلف در اختیار مدیران قرار می‌گیرد.

سیستم جایاب online

در این سیستم اطلاعات حرکتی گرفته شده از ماهواره‌های GPS از یک بستر انتقال online مانند بی سیم، GSM یا GPRS به مرکز منتقل شده و مقام مسئول به‌صورت online

می‌تواند موقعیت خودروهای خود را ملاحظه کرده و با آن‌ها ارتباط برقرار نماید. در این روش در زمان‌های منتخب می‌توان موقعیت خودرو را برروی نقشه‌های دیجیتال شهر یا استان موردنظر و یا نقشه ایران مشاهده کرد.

ترمینال ردیاب

الف) بدون صفحه نمایش

اطلاعات موقعیتی دریافتی از GPS را پردازش کرده و پس از فشرده سازی و مدولاسیون به سیستم ارتباطی منتقل می‌نماید. این دستگاه قابل نصب برروی انواع بی‌سیم و فرستنده‌های رادیویی ازقبیل VHF، UHF، FM، AM و همچنین‌ترمینال‌های تلفن ماهواره‌ای و تلفن همراه (GSM) می‌باشد.

ب) با صفحه نمایش

در این مدل یک صفحه نمایش LCD و ۴ کلید نیز در خودرو تعبیه شده تا راننده بتواند پیام‌های از پیش تعیین شده از قبیل کمک یا آلارم‌های دیگر را به مرکز ارسال نماید. همچنین می‌توان اطلاعاتی از قبیل نشانی محل را از مرکز برای راننده به صورت پیام متنی ارسال نمود.

وسیله ارتباطی

اطلاعات موقعیتی خودرو در سیستم جایاب از طریق سیستم ارتباطی مناسب به دفتر مرکزی منتقل می‌گردد. انتخاب سیستم ارتباطی بر مبنای امکانات موجود، پوشش مورد نیاز (شهری، کشوری، بین‌المللی) و بودجه درنظر گرفته شده برعهده کاربر می‌باشد. استفاده بی‌سیم معمولاً برای پوشش شهری مناسب می‌باشد. در صورت نیاز به پوشش کشوری و بین‌المللی باید از موبایل و تلفن ماهواره‌ای استفاده نمود.

ردیابی نفرات

در این سیستم با استفاده از گوشی‌های موبایل خاص مجهز به سیستم GPS، موقعیت مکانی نفرات دائما از طریق شبکه موبایل به صورت SMS برای مرکز ارسال گردیده و در مرکز یا روی اینترنت موقعیت آن‌ها را روی نقشه نشان می‌دهد.

ترمینال شبکه

این‌ترمینال اطلاعات دریافتی از خودروها را از کد بندی خارج کرده و پس از پردازش به رایانه منتقل می‌کند.

نرم‌افزار جایاب

این نرم‌افزار در دفتر مرکزی نصب شده و با پردازش اطلاعات دریافتی، علاوه بر نمایش مسیر حرکت و موقعیت برروی نقشه دیجیتال، اطلاعاتی از قبیل سرعت متوسط انحراف از مسیر برنامه ریزی شده و دیگر اطلاعات مورد نیاز برروی نقشه نمایش داده و به صورت گزارش‌های مختلف در اختیار مدیران قرار می‌دهد.

ردیابی اطلاعات با امواج رادیویی RFID

استفاده ازتراشه‌های رادیویی که توانایی ساطع کردن فرکانس‌های ویژه بارکد هر انسان را خواهند داشت در آینده می‌تواند امکان دست‌یابی به انسان‌ها را در سراسر جهان تسهیل کرده و جان بسیاری از افراد را از مرگ نجات دهد.

دانشمندان در حال حاضر برای مطالعه رفتارهای جان‌داران مختلف و محافظت از آن‌ها در برابر انقراض با استفاده از برچسب‌هایی آن‌ها را نشانه گذاری می‌کنند. در این میان برخی از دانشمندان بر این باورند همه انسان‌ها نیز باید با استفاده از این برچسب‌ها نشانه گذاری شوند در این صورت زمانی که در جستجوی فردی باشید می‌توانید با جستجوی کد میکروتراشه وی در گوگل به راحتی وی را بیابید.

RFIDچیست؟

RFID مخفف عبارت Frequency Identification Radio و به مفهوم «ردیابی از طریق فرکانس رادیویی» است.

از این فن‌آوری در شناسایی خودکار کالاها، حیوانات، انسان‌ها و غیره استفاده می‌شود. شیوه به‌کارگیری آن نیز به زبان ساده نصب‌تراشه‌ای کوچک روی این اشیاست که فرکانس رادیویی اختصاصی خود را دارند و تنها با دریافت این فرکانس توسط دستگاه گیرنده و تطبیق آن در بانک اطلاعاتی شییء شناسایی شده یا شییء مورد نظر ردیابی می‌شود.

RFID را می‌توان نسل تکامل یافته بارکد دانست، زیرا از بارکد نیز برای همین نوع شناسایی استفاده می‌شود و البته این فن‌آوری هنوز نیز مورد استفاده قرار می‌گیرد.

بارکد ردیفی متشکل از ۱۲ خط عمودی به ظاهر نازک و کلفت است که معرف عددی ۱۲ رقمی بوده و در سراسر جهان به‌طور انحصاری نمایانگر کالایی خاص است.

بارکد توسط دستگاه اسکنر بارکد خوانده شده و بدین‌ترتیب نوع کالا توسط سیستم بدون نیاز به انسان شناسایی می‌شود.

این فرآیند از خطاهای ورود دستی اطلاعات توسط کاربر نیز می‌کاهد. اما بارکد کاستی‌هایی نیز دارد. به‌طور مثال، در سیستم بارکد فقط کد شناسایی وارد می‌شود و اطلاعات دیگری راجع به کالا نمی‌توان در آن جای داد. از دیگر موارد ضعف بارکد این که اسکنر فقط زمانی قادر به خواندن صحیح آن است که دقیقا در دید مستقیم اسکنر قرار گرفته باشد و اگر شما بخواهید آمار کالاهای زیادی را مثلا در یک انبار یا فروشگاهی بزرگ ثبت کنید، حتما باید تک تک کالاها را روبه‌روی اسکنر بگیرید تا کد آن‌ها اسکن شود که کاری است بس دشوار، خسته کننده و زمان‌بر.

در RFID ازتراشه‌ای به نامTAG یا همان برچسب استفاده می‌شود، این قطعه در واقع یک فرستنده رادیویی است که از یک میکروچیپ، یک آنتن و یک برد الکترونیکی تشکیل شده است. در این TAG می‌توان اطلاعاتی راجع به کالا، حیوان یا انسانی که TAG روی آن نصب می‌شود، قرار داد. این اطلاعات می‌تواند، اطلاعاتی ساده مثل اسم و آدرس صاحب یک حیوان و یا اطلاعات پیچیده‌ای نظیر چگونگی مونتاژ یک خودرو باشد.

این اطلاعات از طریق امواج رادیویی منتشر و توسط آنتن گیرنده RFID دریافت و وارد سیستم می‌شود. حال اگر در همان فروشگاه بزرگ تعداد زیادی کالا خریداری کرده باشید، با نزدیک شدن سبد کالا به صندوق که محل نصب آنتن گیرنده RFID است، تمام کالاهای خریداری شده به‌طور خودکار توسط صندوق شناسایی می‌شود و با رسیدن شما به صندوق، فاکتور کالاها نیز آماده جهت پرداخت است. با این کار ضمن صرفه‌جویی در زمان، از ازدحام در محل صندوق فروشگاه‌ها نیز جلوگیری می‌شود. همه این‌ها دست به دست هم داده و کم‌کم واژه احترام به مشتری را از حالت حرف به اجرا نزدیک می‌کند.

البته این نمونه‌ای ساده از خدمات این فن‌آوری بود که فقط برای روشن شدن قضیه گفته شد. هم‌اکنون پاسگاه‌های مرزهای زمینی آمریکا به این فن‌آوری مجهز شده‌اند و کارت شناسایی جدید شهروندان آمریکایی نیز به‌طور متقابل مجهز به RFID شده و ساده‌ترین تصوری که از این تعامل می‌توان داشت، این است که با نزدیک شدن شهروندان به مرز هنگام خروج یا ورود به کشور، کلیه کار شناسایی و انجام امور گمرکی آن‌ها نیز انجام شده و این فرد بدون هیچ توقفی به راحتی از مرز عبور می‌کند، البته اگر ورود یا خروج وی از نظر دولت مانعی نداشته باشد!

در حالتی دیگر می‌توان شرکتی بزرگ را در نظر گرفت که کلیه کارکنان آن به RFID مجهز بوده و ضمن انجام خودکار ورود و خروج اشخاص، محل دقیق این افراد نیز در طبقات و واحدهای مختلف به‌سرعت و به‌راحتی قابل شناسایی است.

شیوه کار نیز بدین‌ترتیب است که با نصب آنتن‌های گیرنده RFID در نقاط مختلف شرکت، به راحتی با یک جست‌وجوی ساده می‌توان از روی آنتن دریافت‌کننده امواج شخص، محل وی را نیز تشخیص داد. همین کار را نیز می‌توان برای شناسایی و کنترل ورود و خروج وسایط نقلیه شرکت انجام داد.

کنترل‌ترافیک شهرهای بزرگ، کنترل ورود و خروج خودروها در پارکینگ‌ها و بزرگراه‌ها، کنترل موجودی انبارهای بزرگ، استفاده در قفل ضد سرقت خودروها و . . . ، همه و همه تنها می‌تواند مواردی از هزاران مورد کاربری RFID باشد.

کیفیت کارایی و نحوه عمل‌کرد RFID به عوامل مختلفی از قبیل کیفیت ساخت، نوع پروتکل به کار گرفته شده، طراحی نوع آنتن، کیفیت واحد بسته‌بندی کالا (در صورت استفاده از RFID برای شناسایی آن کالا) وابسته است.

کاربرد تکنولوژی RFID در زنجیره تامین و چالش‌های فراروی کاربرد آن

چند سالی بیش نیست که فن‌آوری RFID به طور عام در دسترس مصرف کنندگان قرار گرفته است، اما در همین مدت کوتاه با قابلیت‌های مختلف خود توانسته خود را به عنوان فن‌آوری انقلابی قرن ۲۱ در بین کاربران فن‌آوری اطلاعات به اثبات برساند. انقلابی که در اروپا آغاز شد و در آمریکا به اوج خود رسیده است .

در عین حال این مانع را نیز در مقابل توسعه خود دید که باید مخالفانی را توجیه کند که ادعا می‌کنند که هرچه این تکنولوژی بیش‌تر رشد می‌کند از آن طرف حقوق مدنی و شهروندی بیش‌تر تحت تأثیر قرار گرفته و دامنه آن محدودتر می‌شود.

البته لازم به ذکر است که این نگرانی فقط در مورد آزادی‌های مدنی و حقوق شهروندی نیست بلکه بسیاری از این نگرانند که ضعف‌های فنی این تکنولوژی مورد سوء استفاده قرار بگیرند.

اصولا به هر سیستمی که قادر به خواندن و تشخیص اطلاعات افراد یا کالاها باشد سیستم شناسایی یا System Identification گفته می‌شود. به طور کلی شناسایی خودکار و نگهداری

داده‌ها (AIDC) روشی است که طی آن تجهیزات خواه سخت‌افزاری یا نرم‌افزاری قادر به خواندن و تشخیص داده‌ها بدون کمک گرفتن از یک فرد هستند.

بارکدها، کدهای دوبعدی، سیستم‌های انگشت نگاری با استفاده از فرکانس رادیویی، سیستم شناسایی با استفاده از قرنیه چشم و صدا و . . . . از جمله این راهکارها در مقابل آن می‌باشد. یکی از جدیدترین مباحث مورد توجه دانشمندان جهت شناسایی و ردیابی افراد یا کالاها استفاده از سیستم شناسایی با استفاده از فرکانس رادیویی یا RFID می‌باشد.

هولوگرام یا برچسب امنیتی HoloGram

این واژه از دو بخش Holo به معنای همه یا تمام یک شییء و Gram به مفهوم نگاشتن یا نمایاندن بصری یک شییء تشکیل شده که می‌توان معادل پارسی بعد نگار یا تمام نگار را برای آن در نظر گرفت .

عموما هولوگرام را به عنوان یک برچسب نقره‌ای با ظاهری رنگین کمانی می‌شناسند که در مقابل تابش نور تغییرات نوری رنگارنگی در آن ایجاد می‌گردد و تمام نگار را صرفاً نوعی عکس سه بُعدی می‌دانند . درعکاسی و تمام نگاری از فیلم‌ها و پلیت‌های عکاسی استفاده می‌کنند ولی این امر تقریباً کل وجه اشتراکی است که این دو دارند . مهم‌ترین فرق بین آن‌ها نحوه ایجاد تصویر است .

به‌طور خلاصه هولوگرام عبارت است از یک ساختار تقریبا مسطح تشکیل شده از اجزا حدود یک مایکرون یا کوچک‌تر ، که بر اثر نوردهی مناسب طی فرآیندی پیچیده و بسیار دقیق اپتیکی به‌صورت یک عکس سه بُعدی ایجاد می‌گردد و در واقع نور منعکس شده از آن همان انعکاس از یک شییء واقعی است .

۳-۶- چک لیست‌های حفاظتی

با توجه به این که ابعاد مختلف کنترل امنیت ، ایمنی و پایداری بسیار زیاد می‌باشند و از زاویه‌های مختلف به این مطلب نگاه می‌شود عملاً در بسیاری از مواقع بدون جمع آوری اطلاعات اولیه تحلیل درستی از وضعیت امنیت نمی‌توان ارائه نمود . به منظور درگیر نمودن کلیه کاربران در امنیت و برای باز آموزی نکات امنیتی چک لیست‌های حفاظتی توسط طراحان امنیتی طراحی و برای تکمیل شدن به قسمت‌های مختلف ارسال می‌شود. پس از تکمیل شدن چک لیست‌ها که معمولاً با سوالات بسته و با جواب بله یا خیر طراحی می‌گردد، فرم‌ها جمع‌آوری و پس از تجزیه و تحلیل نمای عمومی امنیت به دست می‌آید. البته ممکن است چک لیست‌ها به منظور اتقان در اعتبار و روایی تکمیل شدن به صورت رندومی توسط تحلیل گر مورد کنترل مجدد واقع گردند.

۳-۷- انواع سرمایه‌های قابل امنیت گذاری

معمولاً سرمایه‌های قابل حفاظت را به پنج نوع سرمایه تقسیم می‌نمایند:

کاربران: که مهم‌ترین سرمایه هر سازمانی می‌باشد و کاربران انواع و اقسام مختلفی داشته و کلیه افرادی که چه به صورت رسمی و سازمانی و چه به صورت غیر رسمی با سازمان ارتباط دارند را در بر می‌گیرد. از پائین‌ترین رده سازمانی تا بالاترین رده را در بر می‌گیرد.

سخت‌افزار: منظور کلیه سخت‌افزاری است که به صورت ثابت و یا موقت در اختیار یک سازمان بوده و از آن برای حفظ و نگهداری و مدیریت بر اطلاعات استفاده می‌کند.

نرم‌افزار:کلیه نرم‌افزارهایی که به صورت مستقیم و یا غیر مستقیم در یک ساختار درگیر با اطلاعات سیستم می‌باشد را در این قسمت قرار می‌دهند. ممکن است این نرم‌افزارها توسط عوامل داخلی نوشته شده باشند و یا این که توسط افراد ناشناسی برای مقاصد خاصی نوشته شده باش.

اطلاعات: منظور از اطلاعات کلیه اطلاعات به صورت آنالوگ و دیجیتال که اسناد سازمان را در بر می‌گیر می‌باشد. این اطلاعات ممکن است در اذهان انسان‌ها بوده و هنوز متولد نشده باشند و یا به صورت اسناد کاغذی بوده و یا این که در زمان تولید مستقیما به شکل دیجیتال تولید شده باشند.

ارتباطات: با توجه به این که اطلاعات کالای ارزشمندی بوده و برای بهره مندی بیش‌تر باید بین افراد مجاز دائم در حال حرکت باشند در عصر حاضر از ارتباطات به منظور به چرخش درآوردن اطلاعات استفاده می‌شود . ارتباطات انواع و اقسام مختلفی داشته و بستگی به نوع سند از روش‌های نوین و یا سنتی برای این امر استفاده می‌شود و همیشه ارتباطات به عنوان یکی از گلوگاه‌های مورد علاقه سلطه گران برای اشرافیت بوده است . به مجرد اشرافیت بر ارتباطات اشرافیت بر اطلاعات نیز ایجاد می‌شود.

۳-۸- شناسایی اعتبار کاربران در امنیت اطلاعات

با توجه به این که بین کاربران مجاز و غیر مجاز در یک سیستم می‌بایست تعریف شفافی ایجاد شود و بر آن کنترل گردد امروزه معمولاً از یک یا چند روش زیر برای این کار استفاده می‌شود. برای صدور اجازه ورود برای یک فرد نیاز داریم وی را شناسایی و هویت وی را تایید کنیم و مورد نظرما انجام بررسیهایی است که به‌صورت خودکار توسط یک سیستم صورت بگیرد.

در اصل تمام روش‌های شناسایی با سه مورد زیر ارتباط دارد:

۱- آنچه که شما می‌دانید (یک کلمه عبور یا PIN)

۲- آنچه که شما دارید (یک کارت یا نشانه‌های دیگر)

۳- آنچه که شما هستید (مشخصات فیزیکی یا رفتاری)

مورد آخر به نام زیست سنجی[۱] نیز شناخته می‌شود.

هرکدام از این موارد مزایا و معایبی دارد: کلمات عبور ممکن است حدس زده شوند یا از دست داده شوند اما به کاربر اجازه می‌دهند که قدرت خود را در اختیار کس دیگر قرار دهد. بسیاری از افراد به راحتی کلمات عبور را فراموش می‌کنند، مخصوصا اگر بندرت از آن‌ها استفاده کنند. نشانه‌ها می‌توانند گم یا دزدیده شوند اما می‌توانند در صورت لزوم به کس دیگر منتقل یا قرض داده شوند. مشخصات فیزیکی انعطاف ندارند. برای مثال، نمی‌توان آن‌ها را از طریق خطوط تلفن به کس یا جای دیگر منتقل کرد. طراحان سیستم‌های امنیتی باید این پرسش را مطرح کنند که آیا کاربران باید توانایی انتقال اختیارشان را به دیگران داشته باشند یا خیر. پاسخ این پرسش در انتخاب روش و ابزار شناسایی و تعیین هویت موثر است.

روش‌های شناسایی می‌توانند به‌صورت ترکیبی مورد استفاده قرار گیرند: یک کارت و یک کلمه عبور یا کارت و زیست سنجی معمول هستند. این‌ترکیب می‌تواند مطابق با نیازها متفاوت باشد. برای مثال، ممکن است فقط از یک کارت برای ورود به ساختمان استفاده کنیم، از یک کارت و یک PIN برای ورود به اتاق رایانه ، اما از یک کارت و اثرانگشت برای عملیات انتقال پول در سیستم‌های رایانه‌ی.

۳-۹- انواع اطلاعات

اطلاعات انواع و اقسام مختلفی داشته و به منظور امکان بررسی دقیق‌تر آن را تقسیم بندی می‌نمایند. در این قسمت اطلاعات را با توجه به منشا تولید اطلاعات و اهمیت آن‌ها می‌توان به یکی از سه نوع ذیل تقسیم بندی نمود.

۳-۹-۱- اطلاعات رسمی

اطلاعات رسمی شامل کلیه اطلاعاتی است که در سیستم قانونی و رسمی یک کشور تولید شده و برای شیوه تولید و حفظ و نگهداری آن روش‌های رسمی تعریف شده و در مجاری قانونی آن کشور به لحاظ حقوقی قابل پیگیری می‌باشد . مانند اسناد مکاتباتی اداری و اسناد رسمی تملیکی و سجلی.

---

[۱] Biometrics

۳-۹-۲- اطلاعات آشکار

این گونه اطلاعات شامل کلیه اطلاعات یک کشور می‌باشد که به صورت آشکار تولید و در اختیار عموم قرار داده می‌شود. برای تولید این اطلاعات معمولاً قوانین خاصی وجود نداشته و صرفاً با توجه به امنیت ملی هر کشور حدود و ثغور آن مشخص می‌شود. اطلاعات آشکار بر روی مجلات و روزنامه‌ها و رادیو و تلویزون و گفتگوهای محاوره‌ای هر کشور تولید و به گردش در می‌آید. ظاهرا این اطلاعات فاقد طبقه بندی می‌باشد لیکن امروزه بالای ۵۰ درصد نیازمندی‌های سازمان‌های جاسوسی از این طریق و بدون صرف هزینه بالا تامین می‌گردد و این نشاندهنده اهمیت این اطلاعات می‌باشد.

۳-۹-۳- اطلاعات پنهان

اطلاعات پنهان شامل تمام انواع اطلاعاتی می‌باشد که از نظر تولید کننده اطلاعات در یکی از طبقه بندی‌های حفاظتی و قانونی آن کشور قرار گیرد. در تمام کشورها برای دسترسی به این گونه اطلاعات شرائط خاصی را در نظر می‌گیرند و چنان‌چه فرد یا افرادی این شرایط را رعایت ننمایند به عنوان متخلف با آن‌ها برخورد نموده و معمولاً جرائم امنیتی در این رابطه تعریف شده و افرادی که به عنوان جاسوس در کشورها محاکمه می‌شوند به یکی از جرائم مرتبط با این نوع از اطلاعات محکوم می‌شوند.

۳-۱۰- تعیین سطوح طبقه بندی مجاز برای اطلاعات ساختار

در هر ساختاری مسئول اصلی سطوح طبقه بندی مجاز اطلاعات و مشخص کردن افراد غیر مجاز و مجاز برای دسترسی به اطلاعات با تولید کننده اطلاعات می‌باشد . با توجه به این که اطلاعات دولتی معمولاً توسط ساختارهای حقوقی دولتی تولید می‌شوند جایگاه حقوقی افرادی که این اطلاعات را تولید می‌کنند مدنظر بوده و با تغییر افراد در جایگاه‌های حقوقی تغییری ایجاد نمی‌شود. به منظور یکسان سازی بین افراد حقیقی که در جایگاه‌های حقوقی قرار می‌گیرند معمولاً در کشورهای مختلف تعاریف قانونی و حقوقی برای این کار انجام می‌شود. کلیه افراد آن کشور می‌بایست این قوانین را رعایت نمایند.

۳-۱۱- طرح اشلون و نقش آن در نا امنی جهانی

طرح اشلون طرحی اشرافیتی بر اطلاعات بوده که از سال ۱۹۴۸ بر اساس پیمان بین پنج کشور آمریکا، انگلیس، زلاندنو ، کانادا و بسته شده و تا سال ۲۰۰۱ به صورت پنهانی اقدامات خود را پیگیری می‌کردند. در سال ۲۰۰۱ اولین گزارش رسمی این طرح منتشر گردید و در آن به موارد ذیل اشاره شد:

استفاده از ۱۲۰ ماهوار

استفاده از ۱۱۰۰ پایگاه زمینی

استفاده از ۳۰۰۰۰۰ کارمند

دریافت و تجزیه و تحلیل و بهره‌برداری روزانه از سه میلیارد تعامل اطلاعاتی اعم از صوت و نمابر و اطلاعات رایانه‌ی

با توجه به این گزارش ملاحظه می‌شود این کشورها به عنوان سردمدار دسترسی غیر مجاز به اطلاعات دیگران و اشرافیت سلطه‌گری بر اطلاعات دیگران با استفاده از انواع ابزار ارتباطی و مخابراتی و رایانه‌ای به دنبال اطلاعات تولیدی توسط دیگر کشورها به منظور بهره‌برداری سو از آن‌ها در تمایلات دولتی می‌باشند.

۳-۱۲- سئوالات خودآزمایی

۱. امنیت را تعریف نموده و تاریخچه مختصر آن را بنویسید.
۲. انواع امنیت را نام برده و توضیح دهید.
۳. انواع کلی اسناد را نام برده و توضیح دهید.
۴. مراحل تولید سند را نام برده و توضیح دهید.
۵. نقش داروهای کنترل رفتار در حفاظت اسناد را بیان نمایید.
۶. رابطهٔ بین جهانی شدن و امنیت را بنویسید.
۷. منظور از برچسب امنیتی چیست؟ توضیح دهید .
۸. چالش‌های امنیتی را نام برده و توضیح دهید.
۹. تقسیم‌بندی کلی اطلاعات را نوشته و توضیح دهید.
۱۰. نقش طرح اشلون را در ناامنی جهانی توضیح دهید.

۴

فصل چهارم - امنیت رایانه‌های شخصی

آن چه در این فصل می‌خوانید:

- تعریف رایانه شخصی و انواع آن
- امنیت سخت‌افزاری رایانه‌های شخصی
- امنیت نرم‌افزاری رایانه‌های شخصی
- امنیت رایانه شخصی و نرم‌افزارهای مخرب
- اختلاف بین نسل جدید و قدیم نرم‌افزارهای مخرب
- انواع روش‌های آلوده سازی رایانه شخصی به نرم‌افزارهای مخرب
- انواع اطلاعات موجود بر روی رایانه‌های شخصی
- احیا اطلاعات در رایانه‌های شخصی
- رمز نگاری اطلاعات رایانه و انواع رمز نگاری
- امنیت رایانه‌های شخصی در سفر

•

۴- امنیت رایانه‌های شخصی

دسترسی فیزیکی به رایانه شخصی می‌تواند انواع مختلف داشته باشد زمانی ممکن است فردی با حضور در کنار این وسیله به آن دسترسی فیزیکی پیدا نماید و زمانی ممکن است تحت عنوان تعمیر یا گارانتی و تعویض قطعات و یا به روز رسانی نرم‌افزار و یا نصب سخت‌افزار این وسیله به نزد عناصر مجاز و یا غیر مجاز برود و نتیجه هر دو یکی است و آن در کنار یک‌دیگر قرار گرفتن رایانه با فردی است که در نظر دارد دسترسی به رایانه پیدا کند می‌باشد.

ممکن است این دسترسی در محیط خودی و داخل کشور صورت پذیرد و یا این که در محیط غیر خودی و کشورهای دیگر و در درون هواپیما و کشتی و . . . صورت پذیرد.

ممکن است این دسترسی برای دقایق اندکی صورت پذیرد و یا این که برای ساعات متمادی این دسترسی استمرار داشته باشد. ممکن است در سفرهای خارج از کشور و توسط مأمورین اعزامی رایانه به نزد عناصر غیر مجاز بود و یا این که تحت عنوان استفاده از کارشناسان خارجی آن‌ها به نزد رایانه‌های بیایند و نتیجه همه این موارد یکی است و آن در هم جواری قرار گرفتن رایانه با عناصر غیر مجاز می‌باشد.

در برخی از موارد ممکن است دسترسی به رایانه از طریق ابزار ارتباطی با رایانه صورت پذیرد و عناصر غیر مجاز به عوض این که در کنار رایانه قرار گیرند دسترسی به ابزار ارتباطی به رایانه از قبیل کابل‌های مخابراتی و ارتباطی که از طریق مودم‌ها به رایانه وصل می‌باشند به این وسیله دسترسی پیدا نمایند.

ممکن است دسترسی به رایانه و اجزا آن در زمان تولید اطلاعات صورت پذیرد و یا این که پس از گذشت زمان اندک و یا زیاد که از تولید اطلاعات گذشته باشد این دسترسی صورت پذیرد به طور مثال ممکن است فردی چندین سال قبل اطلاعاتی بر روی رایانه خود تولید کرده باشد و حتی به خاطر نیاورد که چه اطلاعاتی را در چه زمانی بر روی رایانه خود تولید کرده است.

تمام این دسترسی‌ها می‌تواند با هدف دست‌یابی به اطلاعات صورت پذیرد . با توجه به این که دانستیم انواع رایانه شخصی به شکل‌های مختلفی امروزه استفاده می‌شود. انواع رایانه‌های شخصی انواع دستگاه‌های نوت بوک انواع تلفن‌های همراه – انواع دستگاه‌های کپی و تکثیر

دیجیتال انواع دوربین‌های دیجیتال – انواع دستگاه‌های ضبط کنندهٔ صدا- انواع دستگاه‌های نمابر انواع لوازم صنعتی و خانگی که امروز مورد استفاده قرار می‌گیرد از انواع رایانه‌های شخصی می‌باشند تمام این دسترسی‌ها با این هدف صورت می‌پذیرد تا افراد غیر مجاز بتوانند به اطلاعات دسترسی پیدا نمایند.

۴-۱- تعریف رایانه شخصی و انواع آن

رایانه شخصی[۱] که با علامت اختصاری PC شناخته می‌شود، رایانه‌ی است که برای استفاده اشخاص طراحی شده است. این نوع از رایانه‌ها دارای بخش‌های متعددی نظیر : حافظه ،هارد دیسک، مودم و. . . بوده که حضور آن‌ها در کنار یک‌دیگر به منظور انجام عملیات مورد نظر است . به کمک این نوع از رایانه‌ها می‌توان عملیات متنوعی نظیر تایپ یک نامه ، ارسال یک نامه الکترونیکی، طراحی و نقشه کشی و . . . را انجام داد. LabTop و Pocket pcها را هم می‌توان در ردیف رایانه‌های شخصی به حساب آورد. این نوع از رایانه‌ها دارای قدرت محاسباتی و عملیاتی نظیر رایانه‌های شخصی می‌باشند. با توجه به ویژگی‌های متعدد این نوع از رایانه‌ها خصوصا" قابلیت حمل، می‌توان آن‌ها را در موارد متعددی استفاده کرد .

رایانه همراه، رایانه‌ی کوچک و قابل حمل می‌باشد که دارای صفحه تصویر مسطح و صفحه کلیدی است که روی هم تا می‌شوند . رایانه‌های همراه که با باتری کار می‌کنند اغلب دارای یک صفحه تصویر LCD (نمایشگر کریستال مایع) میباشند.

۴-۲- امنیت سخت‌افزاری رایانه‌های شخصی

برای این که بتوانیم امنیت را در مورد رایانه شخصی خود رعایت کنیم ابتدا باید اجزای یک این گونه رایانه‌ها را از نظر مخاطرات امنیتی شناخته سپس سیاست‌های پیش‌گیرانه امنیتی را در مورد آن‌ها به اجرا در آوریم.

۴-۲-۱- اجزا رایانه از نظر امنیتی

---

[۱] Personal Computer

اجزا سخت‌افزاری و نرم‌افزاری رایانه‌ها دارای جایگاه‌های مختلف امنیتی می‌باشند و همه آن‌ها از یک تعریف یکسان تبعیت ندارند . به منظور آشنایی با نقش هر کدام از سخت‌افزارهای رایانه در امنیت آن ذیلا به بررسی نقش هر کدام در این رابطه می‌پردازیم.

۴-۲-۱-۱- ابزار ذخیره ساز اطلاعات

ابزار ذخیره ساز اطلاعات در رایانه امروزه انواع و اقسام مختلفی دارد که برخی از آن‌ها به راحتی قابل شناسایی و برخی دیگر دارای شکل ظاهری نامشخصی می‌باشد. بر مبنای اهدافی که سازندگان سخت‌افزار در ذهن دارند شکل و اندازه و محل قرار گرفتن این ابزار می‌تواند متفاوت از یک‌دیگر باشد. در ذیل به بررسی برخی از این ابزار خواهیم پرداخت.

انواع ذخیره سازهای موجود بر روی رایانه‌های مستقل عبارتند از

- هارد
- فلاپی
- سی دی و دی وی دی
- انواع کارت‌های حافظه
- فلاش مموری
- حافظه‌های سخت‌افزاری

این قطعات از این نظر دارای اهمیت می‌باشند که کلیه اطلاعات در زمان تولید و بازتولید برروی این قطعات قرار گرفته و با جابه‌جایی آن‌ها اطلاعات نیز جابه‌جا می‌شوند و در صورتی که افراد غیرمجاز به این قطعات دسترسی داشته باشند عملاً به اطلاعات دسترسی پیدا خواهند نمود.

۴-۲-۱-۱-۱-هارد رایانه

هارد دیسک HDD، که پیش از این به عنوان دیسک گردان ثابت شناخته می‌شد) یک حافظه دایمی است که به‌طور دیجیتالی رمزنگاری شده و اطلاعات را روی سطح مغناطیسی دیسک‌های خود ذخیره می‌کند. . یک‌هارد دیسک پیش‌رفته قادر به ذخیره سازی حجم بسیار بالائی از اطلاعات در فضائی اندک و بازیابی اطلاعات با سرعت بسیار بالا است . اطلاعات ذخیره شده برروی‌هارد دیسک در قالب مجموعه‌ای از فایل‌ها ذخیره می‌گردند. فایل نامی دیگر برای مجموعه‌ای از بایت‌ها است که به‌نوعی در آن‌ها اطلاعاتی مرتبط به هم ذخیره شده است . زمانی

که برنامه‌ای اجرا و در خواست فایلی را داشته باشد،هارد دیسک اطلاعات را بازیابی و آن‌ها را برای استفاده پردازنده ارسال خواهد کرد.

۴-۲-۱-۱-۲- Cd/dvd/flopy

CD-ROM دیسک‌های فشرده رایج هستند که حجم آن‌ها از ۶۵۰ مگا بایت به بالاست و برای ذخیره و جابه‌جایی اطلاعات می‌باشد.

- DVD- ROM[۱] این نوع رسانه مانند CD می‌باشد با این تفاوت که دارای حجم بسیار بالا و کیفیت فوق‌العاده می‌باشد.

نکته: البته رسانه‌های دیگری نیز مانند Optical Drive، دیسک‌های بزرگ معروف به درایوB ، Tape Backup و سایر موارد نیز وجود داشته‌اند که درحال حاضر با آمدن CD، DVD و رسانه‌های بسیار حرفه‌ای‌تر، غیر قابل استفاده شده‌اند.

۴-۲-۱-۱-۳- فلاش مموری و کارت‌های حافظه

کارت‌های حافظه و انواع فلاش مموری از ابزاری هستند که امروزه به فراوانی برای ذخیره سازی و انتقال اطلاعات از آن‌ها استفاده می‌شود. این ابزار در بین رایانه‌های مختلف حرکت کرده و اطلاعات را در بین آن ها جابجا می نمایند .

۴-۲-۱-۱-۴- ابزار تهیه پشتیبان و نوار ذخیره ساز

برای حفاظت از اطلاعات رایانه شخصی که بر روی‌هارد سیستم ذخیره می‌شود راه‌های متفاوتی وجود دارد که یکی از آن‌ها تهیه یک نسخه پشتیبان بر روی ابزاری غیر از خودهارد است. از نمونه‌های این ابزار می‌توان به انواع TAPE اشاره کرد این ابزار همانند نوارهای کاست ظبط صوت‌های قدیمی است که قابلیت ذخیره اطلاعات با ظرفیت‌های متفاوت را دارد. از دیگر ابزار پشتیبان گیری می‌توان به NAS و SAN اشاره کرد.

•

۴-۲-۱-۱-۵- برد اصلی و اجزا آن

تخته، مدار الکتریکی است که تمام قطعات رایانه بر روی آن نصب می‌شوند. پردازش‌گر و حافظه به طور مستقیم بر روی برد اصلی نصب خواهند شد. ولی ممکن است

---

[۱] Digital Versatile Disc

بعضی از قطعات به صورت غیرمستقیم به برد وصل شوند. مانند کارت صدا که می‌تواند به صورت یک برد مجزا باشد و از طریق پایه به برد اصلی متصل گردد.

۴-۲-۱-۱-۶- پورت‌های ورودی و خروجی

پورت‌ها، درگاه‌های ارتباطی رایانه می‌باشند. که از طریق آن‌ها اطلاعات بین رایانه و محیط خارج مبادله می‌شود. پورت‌ها بر اساس نحوه و سرعت تبادل به گونه‌های مختلف تقسیم می‌شوند که از جمله می‌توان به پورت‌های Parallel[۱]، Serial[۲] ، USB و . . . اشاره کرد.

۴-۲-۱-۱-۷- پورت‌های فیزیکی

- موازی[۱] : این نوع اتصال عموماً برای چاپگرها به کار می‌رود.
- سریال[۲]: این نوع پورت‌ها جهت اتصال دستگاه‌هایی مانند مودم خارجی به کار می‌رود.
- پورتUSB[۳]: این نوع پورت برای اتصال دستگاه‌هایی مانند اسکنر و یا دوربین‌های دیجیتالی استفاده می‌شود.

۴-۲-۱-۱-۸- پورت‌های مجازی

پورت‌های مجازی راه‌های ارتباطی مجازی بین سخت‌افزارها و نرم‌افزارهای دیجیتال که قابلیت تعامل اطلاعات با یک‌دیگر را دارند ایجاد می‌شود . تعداد این پورت‌ها در حال حاضر ۶۵۵۳۵ پورت می‌باشد که هر کدام از آن‌ها وظیفه انتقال نوع خاصی از اطلاعات را به عهده دارند. در صورتی که فردی بر روی هر کدام از پورت‌ها فال‌گوش بایستد می‌تواند به اطلاعاتی که از طریق این پورت در حال عبور می‌باشد دسترسی پیدا نماید. از طرف دیگر از این ویژگی پورت‌ها می‌توان برای ممانعت از دریافت و یا ارسال اطلاعات ناخواسته استفاده نمود. و اصطلاحاً با فیلترینگ هر پورت مانع ازتردد اطلاعات مربوطه گردید.

۴-۲-۱-۱-۹- Cmos/setup/bios

بایوس[۴] در واقع یک برنامه بسیار حیاتی برای رایانه‌هاست. این نرم‌افزار در ارتباط مستقیم با سخت‌افزار رایانه می‌باشد.

۴-۲-۱-۱-۱۰- کارت‌های توسعه

---

[۱] Parallel
[۲] Seriall
[۳] Universal Serial BUS
[۴] (BIOS) basic input output system

با توجه به این که در یک رایانه می‌توان از امکانات مختلف استفاده نمود و هر کدام از امکانات نیاز به سخت‌افزار خاصی دارند بدین منظور کارت‌های توسعه با توجه به نوع نیاز و امکانات مربوطه طراحی و مورد استفاده قرار می‌گیرد و معمولاً بر روی بردهای اصلی هر رایانه محل‌های را در نظر می‌گیرند تا بتوان از این کارت‌ها استفاده نمود.

۴-۲-۱-۱-۱۱- کارت شبکه

کارت شبکه ، یکی از مهم‌ترین عناصر سخت‌افزاری در زمان پیاده سازی یک شبکه است.

هر رایانه موجود در شبکه ((سرویس گیرندگان و سرویس دهندگان)) ، نیازمند استفاده از یک کارت شبکه است. کارت شبکه، ارتباط بین رایانه و محیط انتقال ((نظیر کابل‌های مسی و یا فیبرنوری)) را فراهم می‌نماید.

۴-۲-۱-۱-۱۲- کارت صدا و تصویر

این کارت جهت پخش و ضبط مناسب صدا به کار می‌رود و پس از نصب آن بر روی برد اصلی ، میکروفن و بلند گوها به آن متصل می‌شوند . معمولاً دسته بازی joy stick را نیز به خروجی مخصوصی در کارت‌های صوتی نصب می‌کنند.

۴-۲-۱-۱-۱۳- کارت مودم

PC یک وسیله دیجیتالی است که بیش‌تر کارهایش را با روشن و یا خاموش کردن یک سری کلیدهای الکترونیکی انجام می‌دهد. هر رقم صفر در دستگاه اعداد دودویی، بیانگر یک کلید خاموش است و هر رقم ۱ در دستگاه اعداد دودویی، نمایشگر یک کلید روشن است. در این میان هیچ انتخاب دیگری وجود ندارد .

سیستم تلفن یک دستگاه آنالوگ (پیوسته) است، (زمانی که تلفن ساخته شد، الکترونیک رقمی (دیجیتال) هنوز شناخته نشده بود)، که برای انتقال صوت‌ها و طنین‌های گوناگون صدای انسان طراحی شده است. این صداها به صورت یک سیگنال آنالوگ همانند جریان الکتریسته‌ی پیوسته که فرکانس و شدتش به آرامی تغییر می‌کند به طور الکترونیکی منتقل می‌شوند. این (جریان) را می‌توان بر روی نوسان‌سنج (اسیلوسکوپ) به صورت یک خط موج‌دار نمایش داد.

مودم پلی است میان سیگنال‌های پیوسته (آنالوگ) و رقمی(دیجیتالی) که با تغییر و یا تلفیق (مدولاسیون) فرکانس یک موج الکترونیکی، داده‌های دیجیتالی را به داده‌های آنالوگ و یا بر عکس تبدیل می‌کند. این مرحله شبیه به چیزی است که باند رادیوئی FM از آن استفاده

می‌کند. در انتهای دریافت یک ارتباط تلفنی، مودم بر عکس عمل می‌کند، (یعنی) سیگنال‌های پیوسته را به کد دیجیتالی (رقمی) تفکیک می‌نماید.

نام مودم از دو کلمه مودوله[۱] و دِمدوله[۲] گرفته شده است.

در رایانه‌های شخصی، ارتباطات مودمی(ارتباطاتی که از طریق مودم انجام می‌شوند) به سه عنصر با حداقل استاندارد نیاز دارند (این سه عنصر عبارتند از: (درگاه‌های سریال، فرمان‌های مودم و نرم‌افزارهای ارتباطی. به علت وجود مودم‌های متفاوت، ارایه روش مطلقی که نحوه کار همه‌ی مودم‌ها را نشان دهد غیر ممکن است، اما عمل‌کردی که در این جا توضیح داده شد دقیقاً نرم‌افزارهایی را تشریح می‌کند که از فرمان (دستورالعمل) شرکت «هایس»[۳] (یکی از سازنده‌های مودم) استفاده می‌کنند. در این فرمان، مودم برای درگاه سری با ۲۵ پایه Pin تنظیم شده است (daneshju. ir)

امروزه علاوه بر استفاده از مودم‌های مخابراتی از جریان برق نیز برای انتقال اطلاعات استفاده می‌کنند.

پریزهای معمولی برق، به وسیله‌ی‌تراشه‌های جدید ساخته شده توسط شرکت ماتسوشیتا۴، می‌توانند به‌عنوان وسیله‌ای برای ارتباط با اینترنت پرسرعت در خانه‌ها استفاده شوند و مصرف‌کنندگان را از کابل‌های Ethernet و دردسر اتصال به شبکه‌های بی‌سیم، نجات دهند.

۴-۲-۱-۱-۱۴- کارت VGA[۵]

کارت گرافیکی رابطی است میان مانیتور و کل سیستم تا اطلاعات خروجی را پردازش کرده و به مانیتور بدهد. این کارت دارای پردازنده و حافظه مجزا مربوط به خود است. در انواع مادربُردها این کارت بر روی خود مادربُرد تعبیه شده است[۶] که از حافظه و CPU کل سیستم به صورت اشتراکی استفاده می‌کند.

۴-۲-۱-۱-۱۵- کیبرد

---

[۱] Modulate
[۲] DEModulate
[۳] Hayes
[۴] Matsushita
[۵] Video Graphic Adaptor
[۶] Onboard VGA

مهم‌ترین و رایج‌ترین وسیله ورودی رایانه ، صفحه کلید است و از آن برای ورود اطلاعات برنامه‌ها ،و دستور العمل‌ها به رایانه استفاده می‌شود صفحه کلیدها از نظر ظاهر انواع مختلفی دارند اغلب صفحه کلیدهای استاندارد دارای ۱۰۱تا ۱۰۴ کلید هستند. ارتباط صفحه کلید و رایانه توسط کابل مخصوص یا به‌صورت بی‌سیم برقرار می‌شود .

۴-۲-۱-۱-۱۶- مونیتور

صفحه نمایش یا مونیتور مهم‌ترین دستگاه خروجی است که برای نمایش اطلاعات ورودی رایانه به کار می‌رود بدون وجود این دستگاه کاربر قادر به استفاده از رایانه نخواهد بود.

۴-۲-۲- توسعه و ارتقا سخت‌افزار رایانه و امنیت

رایانه‌های شخصی بعد از مدتی که استفاده می‌شوند و با توجه به رشد تکنولوژی نیازمند به توسعه و ارتقا می‌باشند . این توسعه معمولاً سخت‌افزاری بوده و نیاز به تغییر در اجزا سخت‌افزاری دارد. با توجه به این که بسیاری از کاربران تخصص لازم برای این کار را ندارند از متخصصین و شرکت‌های مربوطه برای این کار استفاده می‌نمایند. در این مرحله سخت‌افزار و نرم‌افزار رایانه برای مدت کوتاه و یا زیادی در اختیار افرادی قرار می‌گیرند که ممکن است از آن‌ها شناخت کافی وجود نداشته باشد و در صورتی که عناصر غیر مجاز در نظر داشته باشند از اطلاعات دارنده رایانه بهره‌برداری سو نمایند در این فاصله زمانی ممکن است این اتفاق بیفتد.

۴-۲-۳- فروش و واگذاری سخت‌افزار رایانه و امنیت

با توجه به این که بسیاری از قطعات سخت‌افزاری رایانه (مخصوصاً ابزار ذخیره ساز اطلاعات آن‌ها مانندهارد) دارای حافظه‌های برای حفظ و نگهداری اطلاعات می‌باشند و اطلاعات دیجیتال به مجرد تولید شدن دیگر قابل از بین بردن نخواهند بود ، لذا در صورتی که رایانه بعد از استفاده واگذار گردیده یا به فروش برسد باید این نکته را مد نظر داشت که همراه با رایانه کلیه اطلاعات تولید شده در گذشته که شاید برخی از آن‌ها را از یاد هم برده باشیم به دیگران واگذار می‌شود. امروزه استفاده از نرم‌افزارهای احیا اطلاعات برای کسب اطلاعات حذف شده تبدیل به روشی بسیار آسان شده و بسیاری از افراد حتی با داشتن کم‌ترین تجربه در بهره‌برداری از نرم‌افزارهای کاربردی قادر به این کار خواهند بود. لذا فروش و واگذاری سخت‌افزار رایانه می‌تواند باعث از دست دادن اطلاعات خصوصی و محرمانه‌ای که در این رایانه ذخیره و پاک شده‌اند گردد.

۴-۲-۴- گارانتی و تعمیر رایانه شخصی و امنیت

در زمان خرید رایانه‌های شخصی ، معمولاً این سخت‌افزار به وسیله فروشندگان برای مدت خاصی گارانتی شده و در این مدت در صورت هرگونه خرابی سخت‌افزاری به صورت رایگان توسط آنان تعمیر و یا جای‌گزین می‌گردند. با توجه به این که در مدت گارانتی خریدار رایانه از آن استفاده نموده و اطلاعات شخصی و یا اداری خود را بر روی آن ذخیره می‌نماید ، به مجرد ارسال برای گارانتی ممکن است اطلاعات موجود در آن مورد سواستفاده دیگران قرار گیرد. لذا در مدت گارانتی رایانه باید به این نکته توجه داشت که ممکن است در زمان ارسال برای گارانتی و جای‌گزین شدن قطعات معیوب اطلاعات ذخیره شده نیز به دست افراد غیر مجاز بیفتد.

۴-۳- امنیت نرم‌افزاری رایانه‌های شخصی

امنیت نرم‌افزاری رایانه‌های شخصی در مراحل مختلفی به خطر می‌افتد که در این قسمت به آن پرداخته می‌شود.

۴-۳-۱- امنیت سیستم عامل

سیستم عامل مهم‌ترین نرم‌افزاری است که در هر رایانه می‌بایست استفاده شود. وظیفه اصلی سیستم عامل مدیریت بر منابع نرم‌افزاری و سخت‌افزاری رایانه می‌باشد و بدون سیستم عامل نمی‌توان از رایانه استفاده نمود. با توجه به نقش اصلی این نرم‌افزار در رایانه‌ها افراد سود جو به دنبال استفاده از نقاط آسیب‌پذیر آن برای به دست آوردن اطلاعات به صورت غیر مجاز می‌باشند . با توجه به این که سیستم‌های عامل انواع و اقسام مختلفی داشته و موارد امنیتی هر کدام به صورت جداگانه می‌باشد در این قسمت به بررسی انواع رایج سیستم عامل و نقش آن در امنیت اطلاعات می‌پردازیم.

۴-۳-۱-۱- امنیت سیستم عامل DOS

این سیستم عامل از قدیمی‌ترین سیستم‌های عامل می‌باشد که توسط شرکت میکروسافت تهیه و توزیع گردیده است و در نسخه‌های مختلف طی سالیان متمادی مورد استفاده کاربران بوده است . هرچند که استفاده از این سیستم عامل امروزه در بسیاری از نقاط دنیا منسوخ شده است لیکن هنوز در برخی از نقاط دنیا و همچنین در برخی از سازمان‌های دولتی و عمومی کشورمان و بعضا در سیستم خصوصی مورد استفاده قرار می‌گیرد .

با مطالعه در کتب چاپ شده توسط شرکت میکروسافت ملاحظه می‌گردد که مقوله‌ای تحت عنوان امنیت در این سیستم عامل دیده نشده است و این به مفهوم آن می‌باشد که هر ساختاری که از این سیستم عامل استفاده نماید اهمیتی به مقوله امنیت اطلاعات خود نداده و در حقیقت دسترسی دیگران به اطلاعات اهمیتی ندارد و اطلاعات را پس از تولید در محلی قرار داده است که هر شخصی که دسترسی فیزیکی به رایانه دارای این سیستم عامل پیدا نماید می‌تواند به راحتی به اطلاعات این رایانه با کم‌ترین دانش رایانه‌ای دسترسی پیدا نماید.

بعضی از کاربران برای ایمن نمودن رایانه‌های خود در گذشته اقداماتی را انجام می‌دادند به طور مثال در هنگام فرمت کردن رایانه خود از نرم‌افزارهایی (مانند ADM)[۱] استفاده نموده وهارد رایانه را به پارتیشن‌های کوچک‌تری تقسیم بندی نموده و برای هر پارتیشن نام‌گذاری عددی که با صفر (بالاترین سطح دسترسی) شروع و همین‌طور افزایش می‌یافت قرار می‌دادند. برای هر پارتیشن کاربر می‌توانست رمز دلخواهی را قرار داده و پارتیشن خود را محفوظ نگاه دارد. (از محدودیت‌های این سیستم این بود که معمولاً پارتیشن‌های کم حجم (۲۰ مگا بایتی) را تحت پوشش قرار می‌داد.)

همگام با این اقدام کاربران نفوذگران نیز نرم‌افزاری را نوشته و اسم آن را ADMPASS گذاشته و به مجرد boot شده رایانه با سیستم عامل dos و اجرای این نرم‌افزار از طریق فلاپی و یا هر مدیا دیگر دو اقدام قابل انجام بوده است:

نشان دادن رمز مربوط به کاربران (مخصوصا کاربر صفر)

از بین بردن رمز کاربران کاربران (مخصوصا کاربر صفر)

در هر دو حالت نفوذگر قادر به دسترسی به اطلاعات سیستم بوده و می‌توانست از آن کپی تهیه کرده و از سیستم خارج نماید. در حالت اول رد پایی از خود به جای نمی‌گذاشت و در حالت دوم نفوذگر رمز پاک شده را با رمز دیگری جای‌گزین می‌کرده است و کاربر برای ورود به سیستم با اشکال مواجه شده و در برخی از مواقع احساس می‌کرده است که یا رایانه خراب شده است و یا این که او رمز را فراموش کرده است!

از مهم‌ترین دلایل عدم امنیت سیستم عامل DOS امکان دسترسی فرد نفوذگر به سیستم از طریق فلاپی BOOT بوده است . و به همین دلیل میکروسافت تصمیم گرفت با توجه به رشد

---

[۱] Advanced disk manager

نیازهای کاربران به استفاده از رایانه در امور مختلف ضمن طراحی سیستم عامل‌های جدید تلاش در ارتقای امنیت سیستم عامل را نیز داشته باشد.

۴-۳-۱-۲- امنیت سیستم عامل ویندوز

سیستم عامل ویندوز انواع و اقسام مختلفی داشته و ما به بررسی رایج‌ترین انواع آن که در کشومان استفاده می‌شود می‌پردازیم.

۴-۳-۱-۲-۱- امنیت سیستم عامل ویندوز گروه ۹X

اشکالات اساسی سیستم عامل ویندوز گروه ۹X

۱- در صورتی که فردی رمز مربوط به کاربری خود را فراموش کرده باشد و یا این که اصلا رمز را نداند (فرد غیر مجاز نفوذگر) در صورت انجام هر کدام از اقدامات ذیل رمز سیستم عامل را نیاز نداشته و وارد قسمت عمومی سیستم عامل خواهد شد.

در قسمت ورود به سیستم (صفحه دستک تاپ) اگر چنان چه فرد از روی صفحه کیبرد دگمه ESC را فشار دهد.

در قسمت ورود به سیستم به جای این که رمز را زده و سپس دگمه OK را کلیک نماید دگمه Cancel را کلیک نماید.

در هر کدام از حالات فوق فرد غیر مجاز یا فرد مجازی که رمز را فراموش کرده باشد وارد قسمت عمومی رایانه خواهد شد. و اگر مدیر رایانه ، رایانه را به خوبی پیکر بندی نکرده باشد فرد می‌تواند از طریق My Computer به قسمت‌های دیگر رایانه دسترسی داشته و وارد محیط‌های اختصاصی کاربران شده و به اطلاعات آن‌ها دسترسی پیدا کند.

فرض بر این می‌گیریم که مدیر سیستم این کار را انجام داده باشد و ورود کننده به این قسمت از رایانه دیگر دسترسی به محیط‌های اختصاصی پیدا نمی‌کند! شما چه فکر می‌کنید . (قسمت بعد را مطالعه فرمایید)

در زمانی که مدیر سیستم برای هر کاربر رمز ورود جداگانه‌ای را تعریف می‌نماید به صورت اتوماتیک و توسط سیستم عامل ویندوز ۹X یک فایل به نام کاربر (نام کار بر هر چه باشد این فایل نیز به همان نام ایجاد می‌شود - به طور مثال اگر نام کار بر علی باشد نام این فایل نیز علی خواهد بود یا اگر ۱۲۳ باشد نام آن فایل نیز ۱۲۳ خواهد بود). پسوند این فایل توسط سیستم به نام PWL[1] خواهد بود . این فایل در قسمتی و فولدری که سیستم عامل در

[1] Password list

آنجا نصب شده باشد ایجاد می‌گردد پس پیدا کردن آن وقت زیادی نخواهد خواست و با یک جستجوی ساده فایل‌های با پسوند PWL می‌توان آن‌ها را پیدا کرد. اگر فرد تلاش نماید تا با باز کردن این فایل‌ها به روش عادی مانند استفاده از یک واژه پرداز به محتویات این فایل‌ها که همان تنظیمات امنیتی و رمز کاربری می‌باشد دسترسی پیدا کند عملاً نه این که به هیچ چیز دسترسی پیدا نمی‌کند بلکه باعث خراب شدن این فایل خواهد شد. اما اگر این فایل را از محل اصلی خود جابه‌جا کرده (با دستور CUT و PASTE) و رایانه را یک بار خاموش و روشن نماید همان اتفاقی که نباید بیفتد خواهد افتاد و این بار دیگر از نفوذگر رمز عبور را درخواست نخواهد کرد و نفوذگر می‌تواند اطلاعات مورد نظر را کپی کرده و از رایانه خارج نماید. (ممکن است این سوال به ذهن خواننده رسوخ کند که کاربر اصلی پس از دسترسی به رایانه متوجه خواهد شد که در رایانه‌ش اتفاقی افتاده است و دیگر از او رمز نمیخواهد)

حال اگر نفوذگر پس از اتمام کار فایلی را که جابه‌جا کرده است را به جای اولیه برگرداند و رایانه خاموش و روش شود انگار که هیچ اتفاق نیفتاده است و دلیلی بر این وجود ندارد که کاربر اصلی متوجه شود در زمانی که دور از رایانه بوده است برای رایانه اتفاقی افتاده است!!

و به همین راحتی ممکن است فرد نفوذگر بدون دانستن یک رمز خوب (ولو رمزی که تمام شرایط یک رمز خوب را داشته باشد) می‌تواند در این سیستم عامل به اطلاعات به شکل غیر مجاز دسترسی پیدا نماید بدون این که رد پایی از خودش به جای گذارد.

۴-۳-۱-۲-۲- امنیت سیستم عامل ویندوز گروه NT

شرکت میکروسافت پس از ارایه سیستم عامل جدید خود اولین اقدامی را که انجام داد این بود که به کاربران نشان داد که نه تنها سیستم عامل جدید مشکلات امنیتی سیستم عامل قبلی را ندارد بلکه علاوه بر اضافه نمودن نکات کاربردی در این سیستم عامل امنیت را نیز بالا برده است . در این سیستم عامل کاربران دیگر نمی‌توانستند با زده دگمه ESC از رمز عبور ، عبور نموده و وارد محیط عمومی سیستم عامل گردند . دیگر در صفحه ورود کاربران دگمه Cancel وجود نداشت تا کاربران بتوانند بر روی آن کلیک کرده و از رمز عبور گذر کنند. در این سیستم عامل جدید از فایل‌هایی با نام کاربر و پسوند PWL خبری نبود تا کاربران بتوانند با حذف آن‌ها وارد صفحات اختصاصی کاربران گردند و . . . . .

در سیستم عامل جدید اطلاعات امنیتی مربوط به کاربران در فایل‌هایی با پسوند SAM بوده است لیکن با بالا آمدن سیستم عامل این فایل‌ها به علت امنیتی از دسترسی کاربران خارج می‌شده و امکان دخل و تصرف و تغییرات در آن‌ها وجود نداشته است.

احتمالا در سایت میکروسافت و سایت‌های مختلف و وبلاگ‌ها و کتب مختلف آموزشی و دوره‌های آموزشی ICDL این مطلب به شما گوشزد شده است که اگر رمز خود و مدیر سیستم را فراموش نمایید دیگر قادر به دسترسی به اطلاعات خودتان نمی‌باشید و مجبورید یک نسخه جدید ویندوز را نصب نمایید و با این عمل اطلاعات قبلی قابل دسترسی نخواهد بود!

بسیاری از کاربران از این خبر خوشحال شده و امیدوار می‌شوند که اگر این اقدامات امنیتی را رعایت کنند اطلاعات آن‌ها توسط افراد غیر مجاز قابل دست‌یابی نخواهد بود.

- این قبیل کاربران در زمانی که رایانه آن‌ها با مشکل سخت‌افزاری و یا نرم‌افزاری روبرو می‌شود پس از انجام اقدامات امنیتی آن را به راحتی در اختیار افراد مجاز و غیر مجاز برای تعمیر قرار می‌دهند.
- این قبیل کاربران در مسافرت‌های خارج از کشور خود به راحتی نوت بوک خود را ایمن ساخته و همراه خود به سفر برده و با آن اطلاعات خود را مدیریت می‌نمایند.
- این قبیل کاربران رایانه‌های خود را ایمن نموده و آن را برای دقایقی همراه با افراد مجاز و غیر مجاز به تنهایی رها می‌سازند.
- و بسیاری موارد دیگر که باعث دسترسی فیزیکی افراد به رایانه می‌شود.
- در این مرحله فرض می‌نماییم ما دارای یک رایانه‌ای هستیم که تمام کاربران آن ایمن شده و با استفاده از دستورSYSKEY دارای یک رمز شده و رمز آن به داخل یک فلاپی منتقل شده و همیشه همراه ما می‌باشد . می‌خواهیم بررسی نماییم اگر یک فرد غیر مجاز در نظر داشته باشد به اطلاعات این رایانه دسترسی داشته باشد:
  - ✓ چه میزان اطلاعات فنی مورد نیاز دارد؟
  - ✓ چه میزان سرمایه گذاری مادی برای این کار نیاز دارد؟
  - ✓ چه میزان زمان برای این کار نیاز دارد؟
  - ✓ چه ابزاری برای این کار نیاز دارد؟

- ✓ چه رد پایی از خودش به جای می‌گذارد تا پس از به دست گرفتن رایانه خود مشکوک به دسترسی افراد غیر مجاز به رایانه خود شویم و در نظر داشته باشیم موضوع را پیگیری نماییم.

جواب کلی به تمام سوالات فوق " یک نفر با تحصیلات ابتدایی رایانه‌ای و با داشتن حداکثر پانصد تومان و در زمان دو دقیقه و بدون گذاشتن هیچ رد پایی موفق به این کار خواهد شد "

استفاده از LIVE CD ویندوز

در این روش با توجه به این که فرد مهاجم از یک سیستم عامل دیگری برای ورود به رایانه استفاده می‌نماید و سیستم عامل اولیه به هیچ عنوان فعال نمی‌شود تا بتواند نرم‌افزارهای امنیتی و گذر واژه‌ای را فعال نماید به همین خاطر پس از BOOT شدن رایانه با این سیستم عامل و دسترسی به کلیه اطلاعات رایانه و انجام هرگونه اقدام مد نظر از قبیل کپی‌گیری از اطلاعات و یا فعال کردن نرم‌افزار مخرب و . . . . و سپس خاموش کردن رایانه و خارج کردن سیستم عامل ثانویه هیچ‌گونه اثری بر روی رایانه باقی نخواهد ماند و در صورت مراجعه کاربر عادی به رایانه ، به حالت عادی می‌تواند با رمزهای تعریف شده و به شکل قبلی کار را ادامه دهد.

استفاده از نرم‌افزارهای حمله کننده به رمز:

این گونه نرم‌افزارها که امروزه با نازل‌ترین قیمت و در برخی از اوقات به صورت مجانی در اینترنت و مغازه‌ها یافت می‌شود می‌توانند در مدت زمان حدود ۱۵ الی ۴۵ ثانیه کلیه رمزهای تعریف شده را غیر فعال ساخته و باعث دسترسی بدون نیاز به رمز به اطلاعات رایانه گردد. در برخی مواقع دیده شده این نفوذگران برای این که ذهن کاربران عادی را از دغدغه خاطر داشتن دسترسی افراد غیر مجاز به رایانه دور کنند پس از اتمام کار یک رمز دیگری را برای رایانه تعریف نموده و سپس رایانه را خاموش می‌نمایند و کاربر عادی در مراجعه به رایانه خود نمی‌تواند با رمز قبلی وارد رایانه شود و برخی از کاربران آماتور احساس می‌کنند یا رمز را فراموش کرده‌اند و یا این که رایانه خراب شده و به هم ریخته است. (ولی کاربران حرفه‌ای می‌دانند که تنها اتفاقی که افتاده است این است که اطلاعات به دست افراد غیر مجاز رسیده است)

پس:

- اگر در مراجعه به رایانه خود متوجه شدیم که هیچ اتفاقی نیفتاده است و رایانه ما با همان رمزهای قبلی به خوبی کار می‌کند مطمئن نباشیم که کسی به اطلاعات ما دسترسی پیدا نکرده است زیرا ممکن است طرح LIVE CD اجرا شده باشد!
- اگر در مراجعه به رایانه خود متوجه شدیم رایانه ما فاقد رمز شده است مطمئن باشیم که حتما کسی به رایانه ما دسترسی غیر مجاز پیدا کرده است.
- اگر در مراجعه ما به رایانه خود مواجه با تغییر رمزها و عدم قبول رمز خودمان روبرو شدیم مطمئن باشیم که حتما کسی به رایانه ما نفوذ کرده است.

پس راه حل چیست؟ اطمینان از عدم دسترسی افراد غیر مجاز به صورت فیزیکی به رایانه ما ولو برای ۱۵ ثانیه!!

۴-۳-۱-۲-۳- امنیت سیستم عامل ویندوز ویستا و ۷

با توجه به این که یکی از دلایل تغییر سیستم عامل ویندوز ایکس پی به سیستم‌های عامل جدیدتر توسط شرکت میکروسافت مسئله امنیت آن بوده است ، توسط این شرکت اقدامات بی شماری برای این کار صورت گرفت لیکن باید در نظر داشت به مجرد دسترسی فرد غیر مجاز به رایانه‌های دارای سیستم عام ویندوز ویستا و سون ، کاربران غیر مجاز قادر خواهند بود در دقایق اندکی با استفاده از سی دی‌های خاص و نرم‌افزارهای مربوطه رمز کاربران را مورد هدف قرار داده و با تعویض و جای‌گزینی آن به اطلاعات دسترسی داشته باشند . استفاده از livecd یکی از روش‌های رایج برای این کار می‌باشد که بدون گذاشتن رد پا از نفوذگر به اطلاعات دسترسی پیدا می‌کند. لذا باید در نظر داشت که امنیت اعلام شده توسط شرکت تولید کننده صرفاً نسبی بوده و به راحتی خدشه پذیر می‌باشد.

۴-۳-۱-۳- امنیت سیستم‌های عامل open source

امروزه نرم‌افزارها و روش‌های مختلفی توسط نفوذگران برای دسترسی به اطلاعاتی که بر روی رایانه‌های شخصی دارای سیستم عامل متن باز نگهداری می‌شود نوشته شده است و آن‌ها قادر خواهند بود همانند دیگر سیستم‌های عامل با استفاده از این روش‌ها بدون گذاشتن رد پای قابل تشخیص برای کاربران به اطلاعات رایانه‌ها دسترسی داشته باشند. با توجه به تبلیغات فریبنده‌ای که در رابطه با وجود امنیت در این سیستم‌های عامل انجام شده است برخی از کاربران در تلاش می‌باشند تا برای امنیت بیش‌تر اطلاعات خود از این نوع سیستم‌های عامل

استفاده نمایند. هرچند تعداد اندکی از کاربران ممکن است با استفاده از این سیستم‌های عامل آشنایی داشته و این باعث گردد تا بیش‌تر به آن‌ها اعتماد داشته باشند لیکن باید این نکته را مد نظر بگیرند که نفوذگران بسیاری روش‌های بهره‌برداری سو از این نرم‌افزارها را به راحتی فرا گرفته و ممکن است از آن‌ها استفاده سو نمایند.

۴-۳-۲- رمز[۱] و نقش آن در امنیت رایانه‌های شخصی

در رایانه‌های شخصی نام کاربری و رمز یکی از مهم‌ترین عوامل امنیتی رایانه می‌باشد چنان چه فردی نام کاربر را بداند ولی رمز آن را نداند عملاً امکان دسترسی به اطلاعات رایانه را نخواهد داشت برای هر کدام از کاربران می‌بایست رمز جداگانه تعریف و در اختیار کاربر قرارداده شود. به اشتراک گذاشتن این رمز کاربران باعث خواهد شد تا تمام کاربران بتوانند به اطلاعات یک‌دیگر دسترسی داشته باشند درصورتی‌که فردی نام کاربری را به دست آورد دسترسی به اطلاعات برای او میسر نخواهد بود لکن اگر فردی رمز کاربر را به دست آورد با توجه به این که نام کاربرها آشکار می‌باشند می‌توانند با استفاده از آن به اطلاعات دسترسی پیدا کند.

۴-۳-۲-۱- انواع رمز در رایانه‌های شخصی

در یک رایانه شخصی در حداقل در سه مرحله امکان رمزگذاری وجود دارد. هر کدام از این مراحل سه‌گانه عمل‌کرد جدای از یک‌دیگر داشته و چنان چه رمزی یکی از آن‌ها به دست افراد غیرمجاز بیفتد در دو مرحله دیگر در صورت فعال سازی، امکان امن نگه داشتن اطلاعات وجود دارد امروزه در کتاب‌های مختلف تأکید بر رمز رایانه و نقش آن در امنیت رایانه‌های شخصی می‌گردد. چنان چه فردی نتواند به رمز دیگران دسترسی پیدا کند به اطلاعات رایانه‌ای نیز دسترسی نخواهد داشت. در این قسمت به بررسی رمز و انواع آن در رایانه‌های شخصی می‌پردازیم.

رایانه شخصی حداقل در سه مرحله دارای امنیت می‌باشد.

الف) رمز setup رایانه که مرحله آماده‌سازی سخت‌افزاری رایانه می‌باشد.

ب) رمز سیستم عامل که بر روی سیستم عامل و با توجه به نوع سیستم عامل استفاده می‌شود.

---

[۱] password

ج) رمز نرم‌افزارهای کاربردی که بر روی نرم‌افزارهای کاربردی و توسط نرم‌افزار نویس مربوطه قرار داده می‌شود.

۴-۳-۲-۱-۱- رمز در setup

این مرحله را می‌توان به اولین مرحله ایمن سازی رایانه (در صورت فعال شدن) برای کاربر در نظر گرفت . همان گونه که قبلاً گفته شد یکی از قطعات سخت‌افزاری رایانه این قسمت می‌باشد که اطلاعات اولیه برای راه‌اندازی رایانه را در خود جای می‌دهد و به صورت یک‌تراشه رایانه‌ای بر روی مادربُرد قرار گرفته است . ممکن است در کتب فنی با اسامی دیگری از قبیل بایوس و سیموس در رابطه با نام این قطعه برخورد داشته باشید. اطلاعات اولیه موجود در این قطعه را می‌توان به دو گروه متمایز از یک‌دیگر تقسیم بندی نمود:

- اطلاعات مربوط به کارخانه سازنده
- اطلاعات مربوط به کاربر

اطلاعات اولیه مربوط به کارخانه سازنده در بر گیرنده اطلاعات اولیه مربوط به سخت‌افزار و راه‌اندازی ابتدایی رایانه و شناسایی سخت‌افزارها و صحت کارکرد آن‌ها بوده و قسمت دیگر مربوط به کاربر و اطلاعات اولیه‌ای که توسط کاربر تنظیم می‌شود و یکی از این اطلاعات مربوط به رمز اولیه است که توسط کاربر در این رابطه تنظیم می‌شود . این رمز قابل تغییر بوده وتوسط هر کاربر می‌تواند به صورت دلخواه تنظیم شده و یا غیر فعال گردد.

این رمز کارکردهای مختلفی می‌تواند داشته باشد:

- ممانعت از دسترسی به تنظیمات رایانه
- ممانعت از دسترسی به‌هارد رایانه
- ممانعت از دسترسی به اطلاعات رایانه به صورت بدون رمز (اطلاعات‌هارد را به رمز تبدیل می‌نماید.)
- ترکیبی از حالات فوق

در زمان فعال سازی این رمز به مجرد روشن نمودن رایانه توسط هر فردی پس از چک کردن صحت عمل‌کرد سخت‌افزار رایانه پیغامی به شکل زیر مشاهده و بدون داشتن رمز مربوطه امکان ادامه کار با رایانه وجود نخواهد داشت:

Enter your password

بسیاری از کاربران با اطمینان از این که این رمز می‌تواند مانع از دسترسی افراد غیر مجاز به اطلاعات رایانه آن‌ها شده رایانه را در موقعیت‌های مختلف برای تعمیر و تنظیم و . . . . یا در مسافرت و هواپیما و قطار و هتل و . . . . . به شکل خواسته و یا ناخواسته در اختیار افراد غیر مجاز قرار می‌دهند.

با توجه به این که اطلاعات در این قسمت به صورت سخت‌افزاری ذخیره می‌گردد احتمال این که با جابه‌جایی رایانه و قطع برق آن اطلاعات این قسمت (ازجمله رمز) پاک گردد وجود دارد . کارخانه‌های سازنده رایانه برای این که این نقیصه را برطرف نمایند معمولاً در کنار این قطعه یک عدد باطری قابل شارژ [۱] را قرار می‌دهند تا به صورت اتوماتیک توسط برق شارژ شده و برای زمان‌های کوتاه چند ساعته که برق قطع می‌گردد برق مورد نیاز این قطعه را تامین نماید.

- **روش‌های گذر از این رمز توسط افراد غیر مجاز:**
- **قطع برق رایانه هم‌زمان با برداشتن باطری بک آپ:**

در این حالت نفوذگر پس از برداشتن درب مربوط به کیس رایانه ابتدا جریان برق رایانه را با قطع اتصال برق قطع نموده و پس از آن باطری را از محل خود خارج می‌سازد و بدین وسیله باعث می‌گردد که اطلاعات مربوط به کاربر (از جمله رمز اولیه) برداشته شود . با برداشتن رمز به راحتی نفوذگر می‌تواند از این مرحله عبور نماید.

عیب این کار برای نفوذگر این است که به مجرد این که کاربر اصلی بخواهد رایانه را روشن نماید متوجه فاقد رمز بودن رایانه شده و مشخص می‌گردد که فردی به این رایانه نفوذ نموده است. نفوذگران برای حل این مساله با توجه به این که رمز اولیه را نمیدانند با گذاشتن یک رمز دیگر تلاش دارند تا به کاربر این نکته را القا نمایند که به علت نوسانات برق یا رعد و برق یا فراموشی یا . . . . . !! این رمز به صورت اتوماتیک تغییر پیدا نموده است و حال شما می‌دانید که به هیچ عنوان با نوسانات برق و رعد و برق . . . . این رمز تغییر نخواهد کرد و تنها علت آن می‌تواند تحرکات یک نفوذگر باشد.

---

[۱] Backup battery

رمز از پیش تعریف شده:[۱]

تمام رایانه‌ها برای این قسمت دارای رمز از پیش تعریف شده (مانند شاه کلید) بوده و اگر کسی دارای این رمز باشد بدون نیاز به رمز تعریف شده توسط کاربر می‌تواند به سهولت وارد رایانه شده و این دسترسی هیچ تاثیری بر روی عمل‌کرد رمز کاربر نخواهد داشت و کاربر در مراجعه به رایانه به هیچ تغییری در رایانه خود مواجه نخواهد شد.

این رمز معمولاً در اختیار نمایندگی‌های مجاز شرکت‌های سازنده رایانه بوده و از آن برای رفع عیب و . . . در زمان ارجاع رایانه برای تعمیر استفاده می‌نمایند.

بسیاری از کاربران در این‌اندیشه هستند چون این رمز در اختیار نمایندگی‌های مربوطه می‌باشد پس هیچ خطری آن‌ها را تهدید نمی‌نماید و با کوچک‌ترین اتفاقی که در این رابطه بیفتد می‌توانند با مراجعه به عوامل انتظامی و طرح شکایت از نمایندگی‌های مربوطه دایره مظنونین را تنگ‌تر نموده و به فرد نفوذگر دسترسی داشته باشند . اما شما نیک می‌دانید که با مراجعه به سایت‌های رایانه‌ای از جمله www. passware. com می‌توان این نکته را دریافت نمود که فقط نمایندگی‌ها و تمام افراد عالم دسترسی به این رمزها را دارند زیرا تقریبا پس از ۲۴ ساعت از ارائه این رمز به نمایندگی‌ها توسط افراد سود جو این رمزها کشف شده و در سایت‌های اینترنتی قرار داده می‌شوند.

حمله به رمز:

در این حالت نفوذگران با استفاده از نرم‌افزارهایی که می‌توان آن‌ها را به راحتی در اینترنت پیدا نمود و آن‌ها را در یک فلاپی و یا سی دی bootable کپی نمود سیستم را به صورت مستقل با این سی راه‌اندازی نموده و سپس با استفاده از این نرم‌افزار به رمز حمله می‌نمایند این نوع از حمله دو کار کرد می‌تواند داشته باشد:

از کارانداختن رمز

پیدا کردن و نشان دادن رمز

در هر دو حالت نفوذگر می‌تواند با فاقد رمز نمودن و یا دانستن رمز به سیستم دسترسی داشته باشد. به نظر می‌رسد راه مقابله با این حمله گرفتن امکان دسترسی نفوذگر به سی دی و یا فلاپی به منظور ممانعت از بوت کردن سیستم باشد. این کار به دو روش صورت می‌پذیرد:

سخت‌افزاری:

---

[۱] Default password

در این روش ابزار مربوطه به صورت سخت‌افزاری از رایانه جدا می‌شود و اشکال برای کاربر اصلی این خواهد بود که دسترسی کاربر را نیز به این ابزار قطع نموده و چون کاربران اصلی با این ابزار زیاد کار دارند باعث سختی در استفاده از رایانه خواهد شد.

نرم‌افزاری:

در این روش با استفاده از روش‌های مختلف نرم‌افزاری که رایج‌ترین آن استفاده از قسمت setup می‌باشد دسترسی به این ابزار قطع می‌گردد. اشکال این روش در این است که نفوذگران می‌توانند با دسترسی به setup و دسترسی یا از کار انداختن رمز آن مجدد سیستم را به حالت اولیه برگردانند و نیت خود را عملی سازند.

استفاده از روش‌های از کار انداختن رمز از روی مادربُرد:

معمولاً بر روی مادربُردها در قسمت‌هایی علامات کوچکی که بر روی آن clrp[1] نوشته شده است وجود دارد و نفوذگران با دسترسی به این قسمت و با استفاده از ابزار رسانه برق و ایجاد اتصال کوتاه می‌توانند رمز موجود بر روی setup را پاک نموده و از این مرحله عبور کنند.

البته روش‌های فنی دیگری نیز وجود دارد که نفوذگران می‌توانند با استفاده از این روش‌ها و یاترکیبی از آن‌ها از رمز اولیه رایانه عبور نمایند.

کاربران ممکن است پس ازترک فیزیکی رایانه و مراجعه به رایانه با حالات زیر روبرو شوند:

رایانه فاقد رمز اولیه شده است:

این حالت نشان دهنده این است که نفوذگر با استفاده از روش اول رمز سیستم را از کار انداخته است.

رمز اولیه رایانه عوض شده است:

این حالت نشان دهنده این است که نفوذگر پس از از کارانداختن رمز رایانه رمز دیگری را برروی سیستم قرار داده است.

رمز اولیه رایانه عوض نشده است:

این حالت می‌تواند نشان دهنده این باشد که نفوذگر با استفاده از رمزهای از پیش تعریف شده به سیستم نفوذ کرده است و هیچ رد پایی به جا نگذاشته است.

نتیجه این خواهد شد که با هر بار دور شدن فیزیکی از رایانه این احتمال باید داده شود که به رایانه نفوذی صورت گرفته است (مخصوصا در سفرهای خارج از کشور)

---

[1] Clear password

۴-۳-۲-۱-۲- رمز در سیستم عامل

هر سیستم عامل دارای روش‌های رمز گذاری خاصی می‌باشد. قدیمی‌ترین سیستم عامل سیستم عامل داس[۱] می‌باشد که بر روی آن هیچ گونه امکان امنیت و ایمنی وجود نداشته و فاقد روش رمزگذاری می‌باشد در سیستم‌های عامل پیش‌رفته روش‌های رمزگذاری به شکل‌های مختلف وجود دارد که در مرحله قبل شیوه دسترسی عوامل غیر مجاز به آن بررسی گردید و در کل متوجه این مطلب شدیم که اطمینان به رمز در سیستم عامل عملاً باعث از دست رفتن اطلاعات خواهد شد.

با توجه به تأکیدی که امروز در کتاب‌های مختلف به اهمیت امنیت سیستم عامل می‌شود به نتیجه رسیدیم که اطمینان به رمز در سیستم عامل بدون در نظر گرفتن عوامل دیگر می‌تواند آگاهانه و یا ناآگاهانه اطلاعات ما را به دست عوامل غیر مجاز برساند.

۴-۳-۲-۱-۳- رمز در زمان فرمت کردن ابزار ذخیره ساز

در زمانی که رایانه‌ها از سیستم عامل داس استفاده می‌کردند با توجه به این که این سیستم عامل فاقد رمزگذاری بوده است برای امن نگه داشتن سیستم عامل و رایانه نرم‌افزارهای نوشته شده بود که به وسیله آن در زمان فرمت کردن ابزار ذخیره‌ساز از قبیل‌هارد رایانه آن را به درایوها و قسمت‌های مختلف تقسیم می‌کردند و بر روی هر قسمت رمز کاربری جداگانه قرار می‌دادند در همان زمان عوامل غیر مجاز نرم‌افزارهایی نوشتند که توسط آن می‌توانستند با استفاده سیستم عامل از طریق فلاپی به نام کاربری و رمز آن دسترسی پیدا کرده و نسبت به آشکارسازی و یا حذف آن اقدام نمایند و بدین وسیله بتوانند به اطلاعات رایانه دسترسی پیدا کنند.

۴-۳-۲-۱-۴- رمز در نرم‌افزارهای کاربردی

در نرم‌افزارهای کاربردی به روش‌های مختلف رمز گذاشته شده و دسترسی افراد مجاز و غیرمجاز به رایانه و اطلاعات رایانه را از طریق آن کنترل می‌نمایند نرم‌افزارهای کاربردی معمولاً دارای دو قسمت می‌باشد قسمت اول نرم‌افزاری است که به وسیله آن تولید اطلاعات می‌کنند و قسمت بعدی اطلاعات تولید شده می‌باشد. نرم‌افزار کاربردی توسط نرم‌افزار نویسان و یا شرکت‌های تولیدکننده نرم‌افزار تولید شده و در اختیار دیگران قرار داده می‌شود هر کاربری بنا به سلیقه خود و نیاز و امکانات خود می‌تواند رمزهای موجود در این نرم‌افزار را فعال نموده و رمز

---

[۱] dos

دلخواه خود را بر روی آن قرار دهد امروزه در کتاب‌های مختلف تأکید بر این می‌شود که در صورت فعال سازی رمز این گونه نرم‌افزارها می‌توان اطلاعات را محفوظ نگه داشت در قسمت‌های بعدی با هم به بررسی امنیت در نرم‌افزارهای کاربردی و شیوه اعتماد و عدم اعتماد به رمز این گونه نرم‌افزارها خواهیم پرداخت .

۴-۳-۲-۲- شرایط یک رمز خوب در رایانه شخصی

تعداد کاراکترهای بیش‌تر از ۷ کاراکتر

روانشناسان بر اثر تحقیقاتی که انجام داده‌اند به این نتیجه رسیده‌اند که اگر یک کلمه نامانوس توسط فردی دیده شود این کلمه در حافظه نزدیک فرد قرار گرفته و برای این که این کلمه ماندگاری پیدا نموده و به حافظه دور منتقل شود نیاز است که چندین بار نوشته شده و یا تکرار گردد و اگر این کار انجام نشود معمولاً فراموش می‌شود. البته کلماتی که مانوس باشند (مانند اسامی افراد، واژه‌های معنی دار و . . . .) به علت این که قبلا در حافظه دور ثبت شده‌اند شامل این بند نمی‌شوند.

عدم استفاده از کلمات لغت نامه‌ها

امروزه تقریبا تمام زبان‌های دنیا به صورت رایانه‌ای درآمده و دیکشنری آن در اینترنت قابل دست‌یابی می‌باشد. ویژگی دیگر یک رمز خوب آن است که در هیچ لغت نامه معروف و غیر معروف دنیا یافت نشود. زیرا یکی از راه‌های حمله به رمز استفاده از روش حمله لغت نامه‌ای [۱] می‌باشد که زمان حمله را به‌اندکی از ثانیه‌ها تقلیل می‌دهد.

عدم استفاده از اسامی علاقه مندی‌ها

برخی از کاربران علاقه دارند که از اسامی مورد علاقه خود شامل شخصیت مورد علاقه یا تیم فوتبال مورد علاقه یا رنگ مورد علاقه یا درس مورد علاقه یا شماره تلفن و شماره پلاک منزل یا ماشین یا تاریخ تولد و . . . . به عنوان رمز استفاده نمایند تا به یاد آوری آن راحت و آسان باشد .

در حمله به رمز حمله کنندگان با استفاده از مهندسی اجتماعی [۲] قبل از شروع حمله علاقه‌مندی‌های افراد را استخراج و آن‌ها را به عنوان یک لغت نامه لیست نموده و از آن

---

[۱] Dictionary attack
[۲] Social engineering

برای شروع حمله استفاده می‌نمایند و متاسفانه در بسیاری از مواقع این نوع حمله موفقیت آمیز می‌باشد.

۱. استفاده از هر ۴ نوع کلید صفحه کلید:

هر صفحه کلید دارای چهار نوع کلید می‌باشد:

حروف کوچک مانند ... a b c d.

حروف بزرگ مانند .... A B C D.

اعداد مانند ۱ ۲ ۳ ۴ ۵ . . . .

نمادها و علائم ویژه مانند . . . % $ # @.

برای این که یک رمز به حد کافی پیچیده گردد و تعداد حالت‌های آن حدود ۲۲۰/۰۰۰/۰۰۰/۰۰۰/۰۰۰ گردد می‌توان از این روش استفاده نمود تا حدس زدن رمز بسیار مشکل گردد.

مانند:

Skdg۲۳۴@#$SFGH

Tukl□□٪۳۴۶۷sdb

۲. عدم استفاده از دگمه‌های صفحه کلید به صورت خطی یا ضربدری

برخی از افراد برای این که اگر رمز خود را فراموش نمودند بتوانند آن را به سرعت پیدا نمایند از این روش استفاده می‌کنند مانند رمزهای زیر:

۱۲۳۴۵۶۷

۷۶۵۴۳۲۱

Zxcvbn

Nbvcxz

۱qaz۲wsx

Xsw۲zaq۱

این گونه رمزها نیز از قبل در یک لغت نامه جمع آوری و در اختیار افراد غیر مجاز قرار گرفته است.

استفاده از رمز نه بسیار ساده و نه بسیار پیچیده

یک رمز خوب نباید آنقدر ساده باشد که بتوان به راحتی آن را حدس زد و نه بسیار پیچیده که نیاز به نوشتن داشته باشد. برخی از کاربران برای این که رمز خود را فراموش نکنند آن را بر روی کیبرد و یا زیر ماوس و یا بر روی دفترچه تلفن روی میز و یا زیر میز و مکان‌های در دسترس می‌نویسند. اولین کاری که یک نفوذگر انجام می‌دهد بررسی این مکان‌ها برای دسترسی احتمالی به رمز می‌باشد (پژوهش‌ها ثابت کرده‌اند که متاسفانه در ۳۵٪ موارد این جستجو موفقیت آمیز می‌باشد)

عدم استفاده از رمز ثابت برای موقعیت‌های مختلف:

برخی از کاربران برای این که ممکن است رمز را فراموش نمایند و در مراحل مختلف نیاز به رمز دارند. به طور مثال رمز ورود به سیستم و رمز سیستم عامل و رمز کارت بانکی و رمز ایمیل و . . . . .

یک رمز را که به خوبی می‌توانند حفظ کنند و به آن عادت کرده‌اند را در همه این مکان‌ها استفاده می‌کنند و این بدان مفهوم است که اگر رمز در یکی از این مکان‌ها به هر دلیلی لو برود باعث این خواهد شد که دسترسی به تمام این مکان‌ها لو برود.

تغییر مستمر رمز

بستگی به حساسیت اطلاعات و شیوه امن نگهداشتن اطلاعات، رمزها باید به صورت مستمر و در زمان‌هایی ثابت و یا غیر ثابت توسط کاربران تعویض گردند . زیرا ممکن است بر اثر ممارست در استفاده از رمز، این رمز در سنوات گذشته در محلی لو رفته باشد و بر اثر گذشت زمان این لو رفتن باعث دسترسی غیر مجاز افراد غیر مجاز به اطلاعات کاربران گردد.

عدم استفاده از رمزهای گذشته

برخی از افراد عادت بر این دارند به رمز خاصی عادت پیدا نمایند و این باعث می‌شود در زمانی که رمز خود را تعویض می‌نمایند (به صورت آگاهانه و یا ناخودآگاه) مجدد یکی از رمزهای قبلی را به عنوان رمز جدید مورد استفاده قرار می‌دهند و اگر این رمز به هر دلیلی لو رفته باشد باعث استمرار در دسترسی غیر مجاز به اطلاعات خواهد شد.

عدم خالی گذاشتن رمز

مهم‌تر از تمام شرایط فوق این شرط می‌باشد. برخی از کاربران برای این که راحت به رایانه خود دسترسی داشته باشند نام کاربری را ایجاد نموده لیکن برای آن رمزی را تعریف نمی‌نمایند . این کار بدین مفهوم خواهد بود که هر کس که دسترسی فیزیکی به رایانه داشته باشد چون

اسامی کاربران را مشاهده می‌نمایید صرفاً با یک کلیک بر روی اسامی کاربران قادر خواهد بود به اطلاعات سیستم دسترسی پیدا کند.

۴-۳-۲-۳- روش‌های کشف رمز یک رایانه

در یک رایانه بستگی به این که کدام یک از رمزها فعال شده است روش‌های رمز مختلف وجود دارد که عوامل غیر مجاز از یکی از این راه‌ها برای دسترسی به اطلاعات استفاده می‌کنند. برخی از روش‌هایی که به کار برده می‌شود بر روی رایانه هیچ‌گونه اثر و ردپایی از خود به جای نگذاشته و در صورت مراجعت کاربری رایانه و روشن کردن و استفاده از رایانه متوجه این مطلب نخواهد شد. اگر فردی به صورت پنهانی و غیرمجاز به رایانه دسترسی پیدا نمود می‌تواند با عبور از رمزهای گذاشته شده به اطلاعات دسترسی پیدا نموده از آن‌ها کپی برداری نماید و از رایانه خارج کند در سفرهای خارج از کشور و در کشورهای بیگانه این مطلب حائز اهمیت می‌باشد اگر چنان چه فردی رایانه خود را همراه با خود به یکی از کشورهای دیگر برده باشد و در آن جا توسط افراد غیر مجاز مورد سرقت اطلاعات رایانه‌ای قرار بگیرد اگر با بررسی رایانه متوجه این که رایانه دست‌کاری شده است نگردد عملاً هیچ‌تردیدی وجود ندارد که افراد غیر مجاز با دسترسی پنهان اطلاعات رایانه را با خود برده باشد. ممکن است چندین بار این اتفاق افتاده و اطلاعات ذی قیمت تولیدی فرد توسط دیگران مورد سرقت واقع گردد برخی از روش‌های دسترسی غیرمجاز بر روی رایانه آثاری از خود به‌جا می‌گذارد و با کم‌ترین بررسی می‌توان این آثار را متوجه شد و از دسترسی آتی به اطلاعات رایانه جلوگیری نمود.

در قسمت بعد برخی از این روش‌های دسترسی غیرمجاز را با هم بررسی کرده و این که در کدام یک از این روش‌ها در صورت کاربرد توسط عوامل بیگانه می‌توان از نشانه‌های به‌جا مانده متوجه شویم که کسی به اطلاعات رایانه دسترسی پیدا کرده است یا خیر را با هم بررسی خواهیم کرد .

۴-۳-۲-۳-۱- رمزهای پیش فرض

در هر سه مرحله رمزگذاری، رایانه دارای رمزهای پیش‌فرض می‌باشد. رمزهای پیش‌فرض مانند شاه کلیدهایی می‌باشند که در اختیار سازندگان رایانه و نرم‌افزارنویسان و نمایندگان آن‌ها می‌باشد و در صورتی که در رایانه به کار برده شود هیچ گونه ردپایی از خود به جای نمی‌گذارد برخی گمان بر این دارند در صورت دسترسی فردی با استفاده از این روش به رایانه می‌توان از نمایندگی مربوط شکایت نموده و فرد مهاجم را به سرعت پیدا نمود اما امروز مشخص شده

است که بسیاری از رمزهای پیش‌فرض حداکثر ۲۴ ساعت پس از تولید شدن در اختیار نمایندگی‌ها قرار گرفته توسط افراد سودجو بر روی سایت‌های اینترنتی قرار گرفته و بسیاری از افراد غیرمجاز و تقریباً تمام افرادی که به اینترنت دسترسی دارند می‌توانند با کم‌ترین جستجو در سایت‌های مربوط به این گونه رمزها دسترسی پیدا کرده و توسط آن از موانع گذاشته شده عبور کنند با توجه به سهولت استفاده از این رمزها مشخص کردن این که چه فردی و چه زمانی به رایانه دسترسی پیدا کرده است معمولاً کاری مشکل می‌باشد و در بعضی موارد غیرقابل پیش بینی و پیگیری می‌باشد غیر قابل پیش‌گیری از این نظر که در صورت غیرفعال سازی این گونه رمزها عملاً باید در کدهای برنامه نویسی نرم‌افزار دست برد و به علت عدم دسترسی به کدهای برنامه‌نویسی این کار در بسیاری از اوقات غیر قابل اقدام می‌باشد. غیرقابل پیش‌بینی از این نظر که مشخص نیست که آیا به این رایانه و به این قسمت از رمزگذاری حمله‌ای صورت گرفته است یا خیر و اگر حمله‌ای صورت گرفته است در چه زمانی و توسط چه فردی و با استفاده از چه رمزی این کار انجام شده است زیرا پس از دسترسی افراد غیر مجاز به اطلاعات و خاموش کردن رایانه ، در رمزهای کاربران هیچ گونه آثاری از خود به جای نگذاشته و رمزهای دیگر همچنان کار خواهند نمود و اگر کاربری با رمز خود وارد رایانه شود متوجه این نکته نخواهد شد که فرد یا افرادی قبل از او به رایانه دسترسی پیدا کرده‌اند.

۴-۳-۲-۳-۲- روش لغت نامه ای

این روش حمله‌ای در زمانی صورت می‌گیرد که رمز استفاده شده ، در یکی از لغت نامه‌های زبان‌های دنیا پیدا شود (هرچند لغت بسیار بزرگی باشد) امروزه با نرم‌افزارهای رایج این حمله حداکثر ۳ ثانیه طول می‌کشد

۴-۳-۲-۳-۳- روش کنترل همه جانبه [۱]

در این روش ، حمله کننده نمیداند که رمز مربوطه از چه حروفی و با چه‌ترکیبی استفاده شده است پس سیستم حمله کننده مجبور است تمام حالتهای ممکن را مورد بررسی قرار دهد. امروزه این حمله با سرعت حدود ۱۵۰۰۰۰ مورد در ثانیه انجام می‌شود. (در برخی از کتابها نوشته شده است حالات مختلف این حمله حدود ۲۲۰۰۰۰۰۰۰۰۰ حالت می‌باشد و حمله کامل بین ۶۰ الی ۷۰ سال طول می‌کشد!!) ولی کاربران حرفه‌ای می‌دانند امروزه این کار ، برای یک کلید واژه ۴ حرفی حداکثر ۲ ساعت طول می‌کشد.

---

[۱] bruth force

۴-۳-۲-۳-۴- روش مستقیم

در نرم‌افزارهایی که الگوریتم رمز آن‌ها و محل قرار گرفتن رمز در اطلاعات فاش شده است معمولاً از این روش استفاده می‌شود . به طور مثال در جمله به اطلاعات تولید شده به اکسس زمان حمله به‌اندازه‌ای است که اینتر زده شود(صفر ثانیه).

۴-۳-۲-۴- انواع روش‌های حمله به رمز نرم‌افزارهای کاربردی

امروز چندین روش برای حمله به رمز نرم‌افزارهای کاربردی وجود دارد و به همین دلیل در تعریف رمز قابل اعتماد به این نکته اشاره می‌کنند که رمز باید دارای شرایطی باشد تا دیگران نتوانند با این روش‌ها به رمز حمله کنند روش‌های کلی حمله به رمز در نرم‌افزارهای کاربردی به شرح ذیل می‌باشند:

حمله به روش جستجوی تمام لغات

در این روش جستجوگر و مهاجم با توجه به این که نمی‌داند رمزی که مورد استفاده قرار گرفته است به چه تعداد بوده و از چه حروف یا اعدادی برای این کار استفاده شده است و برای دسترسی به رمز عملاً می‌بایست تمام حروف، اعداد ، نمادها و دگمه‌های صفحه کلید را باترکیبات مختلف آن به کار ببرد. در برخی از کتاب‌ها اشاره شده است اگر چنان چه فردی بخواهد با این روش به رمز گذاشته شده دسترسی پیدا کند می‌بایست تعداد ۲۲۰،۰۰۰،۰۰۰،۰۰۰،۰۰۰،۰۰۰ حالت را بررسی نماید و این کار ممکن است بین ۶۰ یا ۷۰ سال طول بکشد بسیاری از کاربران به این گونه نوشته‌ها اعتماد نموده و به زعم خود با گذاشتن رمز دلخواه که همه شرایط یک رمز خوب را رعایت کرده است در نظر دارد به مدت حداقل ۶۰ سال از دست مهاجمان در امان باقی بماند اما روش‌های نوین این گونه حمله به رمز متأسفانه نشان داده است که حداکثر زمانی که می‌توان یک رمز نرم‌افزار کاربردی را محفوظ نگه داشت بیش‌تر از ۴ ساعت نمی‌تواند باشد این گونه نرم‌افزارها با سرعت حدود ۱۵۰،۰۰۰ حالت در ثانیه رمز مربوطه را جستجو کرده و زمان را به شدت کاهش می‌دهد در این روش مهاجم به رمز گذاشته شده پس از گذشت مدت زمان مورد نظر دسترسی پیدا نموده و با توجه به این که رمز را به دست آورده است به راحتی به اطلاعات نرم‌افزار کاربردی دسترسی پیدا می‌کند و هیچ‌گونه اثری از خود به جای نگذاشته و بدون رد پا مهاجم می‌تواند به اطلاعات دسترسی پیدا کند .

۴-۳-۲-۴-۱- استفاده از فایل‌های دارای رمز متنی

چنان چه نرم‌افزار نویسان در زمان نوشتن برنامه خود رمزهای مربوط را در فایل‌های مستقلی در بانک اطلاعاتی قرار دهند و بستگی به این که این فایل‌ها آیا خود مجدداً رمز شده یا خیر، می‌توان با دسترسی به این فایل‌ها عملاً آن را با جابه‌جایی و یا شبیه‌سازی و یا باز کردن به وسیله نرم‌افزارهای خاص مورد بررسی قرار داد و رمز مربوطه را به دست آورد این گونه روش رمزگذاری از خطرناک‌ترین نوع در روش‌های رمزگذاری می‌باشد زیرا به مجرد دسترسی فیزیکی افراد غیرمجاز به بانک اطلاعاتی امکان این را خواهند داشت تا محل قرار گرفتن رمز را پیدا نمود و از طریق آن به اطلاعات دسترسی پیدا کنند.

۴-۳-۲-۴-۲- جایگزینی فایل‌های رمز از طریق شبیه سازی

در این روش مهاجمین با توجه به این که خود رمز را نمی‌دانند و تلاش بر این دارند تا خروجی فایل رمز را شبیه سازی نموده و با گذاشتن یک فایل به جای آن و ارائه خروجی مشابه و ادامه کار، به اطلاعات دسترسی پیدا کنند.

۴-۳-۲-۴-۳- نصب مجدد برنامه موازی

در این روش مهاجمین به اصل نرم‌افزار کاربردی و اطلاعات هیچ گونه تغییری وارد نمی‌سازند و به جای آن در یک محل دیگر یا بر روی یک رایانه دیگر برنامه نرم‌افزار کاربردی را با رمز مد نظر خود نصب نموده و صرفاً با آدرس دهی اطلاعات تولید شده توسط نرم‌افزار کاربردی را به این نرم‌افزار معرفی می‌کنند و به این روش بدون این که آسیبی به نرم‌افزار اولیه برسد می‌توانند به اطلاعات دسترسی پیدا کنند در این روش نیز هیچ گونه آثاری از رد پای مهاجم به جایی نخواهد ماند.

۴-۳-۲-۴-۴- استفاده از فایل اطلاعات د ر برنامه نصب شده مجدد

در این روش مهاجمین با نصب یک برنامه موازی در رایانه خود اطلاعات مورد نظر را کپی برداری نموده و به رایانه خود منتقل می‌نمایند و با باز کردن اطلاعات رمز شده در کنار برنامه جدیدی نصب شده به اطلاعات دسترسی پیدا می‌کنند. لازمه این کار این است که مهاجم قبلاً به روش‌های مختلف دسترسی به رایانه داشته و اطلاعات را با روشی که قبلاً بحث شد کپی برداری کرده و به رایانه خود منتقل نماید به علت این که در این روش به اطلاعات و نرم‌افزار کاربردی هیچ‌گونه آسیبی وارد نمی‌شود عملاً نمی‌توان با بررسی رایانه و اطلاعات خود متوجه ردپایی از مهاجم بر روی رایانه شد.

۴-۳-۲-۴-۵- تغییر مسیر اجرایی برنامه

در این روش مهاجمین با عوض کردن مسیر اجرای برنامه به‌منظور گرفتن نوع خروجی از ساختار و روش رمزگذاری برنامه به دنبال این خواهند بود تا با کپی سازی از خروجی برنامه و استفاده از آن در رایانه‌های دیگر به اطلاعات دسترسی پیدا کرده و از رمزها عبور نمایند.

۴-۳-۲-۴-۶- تعریف کاربر موازی

در این روش مهاجمین با تعریف کردن کاربران موازی و با استفاده از آسیب‌پذیری‌های نرم‌افزار کاربردی تلاش بر این دارند از طریق کاربر اصلی به اطلاعات دسترسی پیدا نکرده و از طریق کاربر موازی این کار را انجام دهند این کار در صورتی میسر خواهد بود که آسیب‌پذیری در نرم‌افزار نوشته شده وجود داشته باشد که معمولاً متأسفانه وجود دارد. مهاجم می‌بایست بر روی نرم‌افزار کاربردی مسیر دسترسی را تعویض نماید و در صورت دقت در مسیرهای نرم‌افزار اجرایی می‌توان به رد پاهایی از مهاجم دسترسی پیدا نمود. البته این کار صرفاً توسط نرم‌افزار نویس مربوط و یا مدیر سیستم میسر خواهد بود و کاربر استفاده کننده کم‌تر به رد پاها دسترسی پیدا خواهد کرد.

۴-۳-۲-۴-۷- استفاده از رمز شکن

امروزه رمز، شکل‌های مختلفی بر مبنای نوع حمله به رمز نوشته شده و به صورت رایگان یا با قیمت بسیاراندک بر روی اینترنت قرار داده شده است. بسیاری از این رمز شکن‌ها در زمان بهره‌برداری، قابلیت پیدا کردن رمز را دارد. این گونه رمز شکن‌ها امروز بر روی سی دی‌های مختلف کپی شده و توسط شرکت‌های مختلف پخش می‌گردد. با توجه به دسترسی همگان به این گونه نرم‌افزارها عملاً سطح مهاجمین از مهاجمین حرفه‌ای به سطح مهاجمین آماتور تقلیل پیدا کرده است و به تعبیر دیگر تعداد افرادی که به عنوان مهاجمین آماتور شانس خود را برای دسترسی به اطلاعات آزمایش کنند بسیار بیش‌تر از گذشته شده است .

۴-۳-۲-۴-۸- استفاده از ثبت کننده‌های کلید

در این روش با توجه به این که کلیه اطلاعات وارده به رایانه از طریق صفحه کلید رایانه وارد می‌شود و یکی از اطلاعاتی که وارد می‌شود همان نام کاربری و رمز مربوطه می‌باشد در صورت نصب ثبت کننده‌های کلید بر روی رایانه افراد مجاز به راحتی خواهند توانست تا کلیه کلیدهای زده شده را ثبت نموده و با تجزیه و تحلیل آن به راحتی بتوانند به نام کاربری و رمز

مربوطه دسترسی پیدا کنند. ثبت کننده‌های صفحه کلید معمولاً به دو نوع ذیل توسط مهاجمین مورد استفاده قرار می‌گیرد.

الف- این گونه ثبت کننده‌ها از یک قطعه سخت‌افزاری که مابین رایانه و صفحه کلید استفاده می‌شود تشکیل شده است برخی از آن‌ها که تجاری می‌باشند شاید به راحتی قابل تشخیص باشد اما نمونه‌های حرفه‌ای آن با توجه به این که در قسمت‌های مختلف رایانه و یا صفحه کلید به شکل یکی از قطعات اصلی رایانه پنهان شده‌اند، عملاً با نگاه سطحی و توسط کاربران معمولی و یا حتی برخی مواقع کاربران متخصص قابل شناسایی نمی‌باشد این گونه سخت‌افزار می‌تواند در زمانی که رایانه برای تعمیر و یا هر اقدام دیگر از دست فرد مجاز خارج شده و به نزد فرد غیرمجاز می‌رسد و بر روی رایانه نصب گردد.

این گونه ثبت کننده‌ها یک نرم‌افزار اجرایی می‌باشند که توسط مهاجم و به روش‌های مختلف که در رابطه با آن بحث خواهد شد و روی رایانه برای یک بار نصب شده و پس از نصب، اولین اقدام آن پنهان کردن خود نرم‌افزار ثبت کننده کلید می‌باشد و به‌راحتی نمی‌توان این گونه نرم‌افزارها را بر روی رایانه پیدا نمود زیرا اولاً حجم آن‌ها بسیار کم بود و این گونه نرم‌افزارها در محل‌هایی سرویس‌های جاری رایانه و یا نرم‌افزارهای کاربردی رایج پنهان شده و خود را به نام آنان در سیستم عرضه می‌کنند و نمی‌توان با بررسی اجمالی و کاربردی رایانه به نرم‌افزارها دسترسی پیدا نمود در صورت نصب این گونه نرم‌افزارهای مخرب اطلاعات مختلف از جمله نام کاربری و رمز مربوطه در فایلی ذخیره شده و در صورت دسترسی مجدد فرد مهاجم به رایانه می‌تواند به آن فایل دسترسی پیدا کرده و رمز را پیدا کند .

ب- در روش دیگر این فایل‌ها به مجرد اتصال رایانه قربانی به اینترنت از طریق اینترنت بدون این که تغییری در روال کار کاربر ایجاد نماید برای مهاجم ارسال شده و مهاجم از راه دور با دسترسی به این فایل محتوی رمز و نام کاربری عملاً قادر خواهد بود به اطلاعات دسترسی پیدا کند.

۴-۴- امنیت رایانه شخصی و نرم‌افزارهای مخرب

یکی از راه‌هایی که از طریق آن به اطلاعات رایانه از راه دور دسترسی پیدا کرده و آن را کپی نموده و از رایانه خارج می‌نمایند استفاده از نرم‌افزارهای مخرب می‌باشد. نرم‌افزارهای مخرب نوعی از نرم‌افزارهای اجرایی می‌باشند که توسط نرم‌افزار نویس نوشته شده و با اهداف بد

خواهانه توزیع و تکثیر می‌گردد. هدف اصلی این نرم‌افزارها دسترسی به اطلاعات و اشرافیت بر اطلاعات و مدیریت سخت‌افزار و نرم‌افزار از راه دور می‌باشد. این نرم‌افزارها انواع مختلفی دارند که به مهم‌ترین آن‌ها اشاره می‌شود.

۴-۴-۱- نرم‌افزارهای ثبت کننده صفحه کلید (keylogger)

- تمام اطلاعاتی که در بانک‌های اطلاعاتی وارد می‌شوند
- تمام اطلاعاتی که تحت عنوان یک نامه تولید می‌شوند.
- تمام اطلاعاتی که تحت عنوان گزارشات و بولتن‌ها تولید می‌شوند.
- تمام رمزهای عبور و نام کاربرانی که در ایمیل‌ها استفاده می‌شود.
- تمام شماره‌ها و رمزهای کارت‌های اعتباری که در شبکه‌های بانکی استفاده می‌شود.
- تمام نام کاربری و رمزهای عبوری که برای به روز رسانی سایت‌ها استفاده می‌شود.
- تمام اطلاعاتی که قرار است رمز شده و نگهداری شوند.
- و تمام . . . . . .
- ملاحظه می‌گردد که کم‌تر اطلاعاتی است که به صورت دیجیتال تولید شود و با این قطعه سروکار نداشته باشد.

به همین خاطر اگر کسی بتواند به اطلاعاتی که از طریق این قطعه تولید می‌شود دسترسی پیدا نماید می‌تواند ادعا داشته باشد که به تمام اطلاعات این رایانه و کاربران مرتبط با این رایانه دسترسی پیدا نموده است.

تمام نگهبانان ساختمان‌ها اسامی افراد و خودروها و لوازمی که به ساختمان وارد می‌شود و یا خارج می‌شود را یادداشت می‌نمایند تا بتوانند اطلاعات کامل ورودی‌ها و خروجی‌های ساختمان را تهیه نمایند تا در موارد ضروری بتوان از آن استفاده نمود. این کار بدین خاطر میسر است که نگهبانان در گلوگاه ورودی ساختمان مستقر شده‌اند.

کیبردها نیز در گلوگاه ورودی به رایانه‌ها قرار گرفته‌اند و می‌توانند همانند نگهبانان این کار را در فضای مجازی انجام دهند. با هر بار فشردن بر روی دگمه‌های صفحه کلید پالسی تولید می‌شود که همتای کلید وارد شده بوده و در تمام دنیا از یک استاندارد واحد برخوردار می‌باشند و با ارسال این پالس به داخل رایانه الباقی قطعات متوجه نوع اطلاعات وارد شده

خواهند شد. حال اگر فردی به صورت غیر مجاز از این پالس‌های عبوری تصویر تهیه نماید می‌تواند همگام با رایانه در جریان کلیه اطلاعات تولید شده قرار گیرد. این وسیله یا ابزار غیر مجازی چیزی نیست به جزء ثبت کننده کلیدها [۱]

۴-۴-۲- ویروس‌ها

می‌توان گفت ویروس برنامه مخفی و کوچکی است که باعث آلوده شدن برنامه‌های دیگر می‌شود و می‌توان داده‌ها را دستکاری و یا تخریب نموده سرعت سیستم را کاهش داده و باعث اغتشاش و عدم کارآیی رایانه شود.

مهم‌ترین خصوصیت ویروس قدرت تکثیر آن است ویروس‌ها برای تکثیر نیاز به یک برنامه اجرائی دارند یعنی بیش‌تر ویروس‌ها در فایل‌های اجرائی جای می‌گیرند و آن‌ها را آلوده می‌کنند و کم‌تر ویروس پیدا می‌شود که در یک فایل غیر اجرائی جای بگیرد و بتوانند از طریق آن تکثیر شود بنابراین ویروس برنامه‌ای است که می‌توان نسخه‌های اجرائی از خود را در برنامه‌های دیگر قرار دهد برنامه آلوده به ویروس می‌تواند هر برنامه سیستمی یا کاربردی باشد که شرایط مورد نیاز برای پذیرش ویروس را داشته باشد. برنامه آلوده نیز قادر است برنامه‌های دیگر را آلوده کند.

۴-۴-۳-تروجان‌ها

اگر بخواهیم برای‌تروجان [۲] یک تعریف ساده بیان کنیم می‌توانیم بگوییم:تروجان یک فایل جاسوسی می‌باشد که توسط هکر با توجه به نیاز به اطلاعات قربانی آماده می‌شود و برای قربانی فرستاده می‌شود با کمی دقت در تعریف‌تروجان در می‌یابیم که‌تروجان هیچ وقت نمی‌تواند یک ویروس باشد.

هکر با توجه به نیازهای خود به اطلاعات قربانی که می‌تواند این اطلاعات: پسورد ایمیل یا آی‌دی قربانی، اشتراک اینترنت(اکانت)، نام و پسورد رایانه قربانی و. . . است تنظیم کند. معمولاًتروجان‌ها به دو قسمت تقسیم می‌شوند:

۱) کلاینت: که تنظیمات را انجام داده و آن را با توجه به نیازهایی که بیان کردیم تنظیم می‌نمایند

---

[۱] keylogger
[۲] Trojan

۲) سرور: که بعد از تنظیمات باید این سرور برای قربانی فرستاده شود تا قربانی بعد از دریافت آن را اجرا کند.

۴-۴-۴- روت کیت‌ها[۱]

روت‌کیت‌ها برنامه‌هایی هستند که از نظر ساختار کاری بسیار شبیه‌تروجان‌ها و درب‌های پشتی‌ها۲ هستند ولی با این تفاوت که شناسایی روت‌کیت بسیار مشکل‌تر از درب‌های پشتی است زیرا روت‌کیت‌ها علاوه بر این که به عنوان یک برنامه کاربردی خارجی مثل شنونده[۳] و ابزارهای درب پشتی مثل ساب‌سون[۴] بر روی سیستم اجرا می‌شوند بلکه جای‌گزین برنامه‌های اجرایی مهم سیستم عامل و در گاهی مواقع جای‌گزین خود هسته کرنل می‌شوند و به هکرها این اجازه را می‌دهند که از طریق درب پشتی و پنهان شدن در عمق سیستم عامل به آن نفوذ کنند و مدت زیادی با خیال راحت با نصب ردیاب‌ها۵ و دیگر برنامه‌های مانیتورینگ بر روی سیستم اطلاعاتی را که نیاز دارند به‌دست آورند.

۴-۴-۵- کرم‌ها

یک کرم[۶] رایانه‌ی به طور فعال به دنبال آلوده کردن سیستم‌های دیگر است و هر ماشینی که فعال می‌شود، خود به عنوان یک پایگاه داده فعال برای حمله به ماشین‌های دیگر به کار می‌رود. یک ویروس خود را به یک برنامه می‌چسباند، اما یک کرم خود را در طول شبکه‌ها یا سیستم‌ها تکثیر می‌کند. در نتیجه می‌توان گفت، کرم‌ها به‌جای آلوده کردن عناصر خاص مثل فایل‌ها، باعث آلوده شدن محیط ، مانند محیط سیستم عامل یا سیستم پست الکترونیک می‌شوند و البته این بدان معنی نیست که ویروس‌ها نمی‌توانند در محیط شبکه‌ها حرکت کنند.

۴-۵- اختلاف بین نسل جدید و قدیم نرم‌افزارهای مخرب

---

۱ RootKit
۲ Backdoor
۳ Netcat
۴ Subv
۵ Sniffer
۶ Worm

نرم‌افزارهای نسل قدیم از نظر پیچیدگی در نوع بهره‌برداری از رایانه‌های قربانی از پیچیدگی کم‌تری برخوردار بوده‌اند و این نکته باعث می‌گردید میزان کم‌تری از اطلاعات در زمان طولانی‌تری در معرض خطر قرار گیرند و مقابله با آن نیز راحت‌تر بوده است.

روش‌های بهره‌برداری سو محدود بوده لذا روش‌های مقابله نیز به سرعت تکثیر و در اختیار دیگران قرار می‌گرفت. در نرم‌افزارهای مخرب نسل جدید با توجه به رشد علم و تکنولوژی این نرم‌افزارها نیز رشد داشته و از پیچیدگی‌های خاصی برخوردار شده‌اند که عملیات مقابله را با پیچیدگی چند برابر روبرو می‌کند. تعدد و فراوانی روش‌های آلوده سازی و افزایش انواع تکنولوژی در نوشتن این برنامه‌ها باعث شده است تا مقابله کنندگان نیز الزام داشته باشند روش‌های خود را توسعه دهند تا قادر باشند در مسابقه بین تولید کنندگان نرم‌افزارهای مخرب و استفاده کنندگان از اطلاعات ، طرفی برنده گردد که بیش‌ترین علم مربوطه را به‌کار می‌گیرد. با توجه به این که معمولاً مهاجم از مدافع جلوتر بوده و برگ برنده بیش‌تری را در دست دارد معمولاً در این مسابقه مدافع چندین قدم از مهاجم عقب‌تر بوده و این زمان از دست رفته کفایت خواهد داشت تا افراد غیر مجاز بتوانند به اطلاعات دسترسی داشته باشند.

۴-۶- انواع روش‌های آلوده سازی رایانه شخصی به نرم‌افزارهای مخرب

۴-۶-۱- نصب مستقیم :

در این شیوه فرد نفوذگر یا عوامل او به صورت مستقیمم به رایانه دسترسی پیدا نموده و نرم‌افزار را بر روی رایانه اجرا می‌نماید. به طور مثال ممکن است رایانه به علت خرابی به نزد یک مغازه و یا شرکت منتقل شود و در این مدت نرم‌افزار بر روی رایانه نصب می‌گردد.

یا ممکن است در طول سفر در داخل و یا خارج از کشور و هنگامی که رایانه در اتاق هتل و یا صندوق امانات هتل گذاشته شده است این دسترسی صورت پذیرفته و نرم‌افزار نصب گردد.

یا ممکن است به صورت صوری سرقت موقت رایانه رخ دهد و پس از زمان اندکی رایانه پیدا شود و این مدت زمان کفایت برای نصب نرم‌افزار ثبت کننده کلید خواهد داشت!

۴-۶-۲- نصب غیر مستقیم :

در این روش از طریق سی دی‌های آلوده که از بازار و از افراد ناشناخته تهیه می‌شود یا این که به صورت برنامه ریزی برای یک بار در رایانه (به هر دلیلی) اجرا شود نرم‌افزار ثبت

کننده به رایانه منتقل شود. به طور مثال گفته شود که آیا امکان دارد این سی دی را بر روی رایانه خود تست نمایید .

یا این که در قالب سی دی تبلیغاتی یا آموزشی از طریق پست و . . . به محل رایانه ارسال گردد.

یا این که یکی از سی دی‌هایی که داشته ایم مفقود می‌شود و وقتی که پیدا می‌شود این نرم‌افزار بر روی آن نصب شده است و به مجرد قرار گرفتن در داخل رایانه نرم‌افزار اجرا می‌شود.

یا این که این نرم‌افزار از طریق یکی از قطعات سخت‌افزاری که به رایانه اضافه می‌شود به رایانه منتقل می‌شود.

یا این که در زمان اتصال به اینترنت از طریق ایمیل برایمان ارسال شده باشد(خود ایمیل و یا ضمائم ایمیل).

یا این که از طریق بی‌سیم و بلوتوث به داخل رایانه منتقل شود.

۴-۷- انواع اطلاعات موجود بر روی رایانه‌های شخصی

بر روی رایانه‌های شخصی انواع و اقسام مختلفی از اطلاعات وجود دارد که در این بخش به آن پرداخته می‌شود.

۴-۷-۱- اطلاعات موجود

این اطلاعات شامل تمام اطلاعات اعم از آشکار یا پنهان که هم اکنون در داخل رایانه وجود دارد و هر فردی که بتواند رایانه را به دست آورد می‌تواند با جستجو در درون آن به اشکال مختلف به انواع اطلاعات موجود دسترسی پیدا نموده و آن را مورد استفاده قراردهد.

۴-۷-۲- اطلاعات حذف شده

برخی از کاربران به خوبی می‌دانند که اگر به‌خواهند اطلاعات به دست افراد غیر مجاز نیفتد باید پس از استفاده از آن، آن‌ها را حذف نمایند و این همان چیزی است که عناصر غیر مجاز به دنبال آن می‌باشند زیرا به خوبی می‌دانند اطلاعات مهم است که برای عدم دسترسی دیگران آن‌ها را پس از استفاده حذف می‌نمایند و عناصر غیر مجاز به خوبی می‌دانند که با چه ابزاری و یا چه روش اطلاعات حذف شده را مجدد احیا نموده و مورد بهره‌برداری قرار دهند. زمانی استنباط این بود که می‌توان اطلاعات دیجیتال را پس از استفاده حذف نمود و از بین برد امّا امروزه با توجه به انواع روش‌ها و نرم‌افزارهای کاربردی احیاء اطلاعات که با قیمت‌های بسیار

ارزان و به فراوانی در اختیار همگان می‌باشد افرادی که حتی دارای کم‌ترین سواد فنی رایانه‌ای می‌باشند به راحتی و توسط این ابزار می‌توانند به اطلاعات پاک شده دسترسی داشته باشند . نمونه آن دو پسر بچهٔ پانزده سالهٔ دانمارکی می‌باشد که با مراجعه به سایت فروش اقلام دست دوم Ebay توانستند تعداد حدود دویست عددهارد دست دوم و از رده خارج را خریداری نمایند و با استفاده از ابزار مختلف بازیابی، اطلاعات آن‌ها را تحت عنوان پروژهٔ مدرسه‌ای مورد بررسی قرار دهند و نتیجه آن دست یابی به اطلاعات اقتصادی تعداد زیادی از شهروندان و شرکت‌ها و سازمان‌های دولتی بوده است که برخی از آن را برروی اینترنت قرارداده و برخی از آن نیز به مالکان اطلاعات فروخته شد.

۴-۷-۳- اطلاعات قبل از تغییر پارتیشن

نوع دیگر از اطلاعات؛ اطلاعاتی است که با انواع روش فرمت کردن از روی این ابزار پاک می‌شود به طور مثال با فرمت کردن حافظه‌های دیجیتال دوربین‌های عکاسی و فیلمبرداری یا با فلش کردن انواع تلفن‌های همراه یا با فرمت کردن با انواع نرم‌افزارهای مختلف که بر روی‌هاردهای رایانه صورت می‌گیرد یا با از بین بردن اطلاعات درون نمابرها از طریق دکمه منوئی که بر روی آن در نظر گرفته شده است.

امروزه بسیاری از کاربران عادی و متخصص با انواع نرم‌افزارهای بازیابی، اطلاعات فرمت شده آشنایی کامل داشته و موسسات و شرکت‌هایی ایجاد شده و در قبال دریافت کارمزد نسبت به این کار اقدام می‌نمایند و به نوعی این فرضیه را عملاً به اثبات می‌رسانند که با فرمت کردن نیز نمی‌توان از دست اطلاعات خلاصی یافت.

۴-۷-۴- اطلاعات قبل از تغییر فرمت و تغییر پارتیشن و پاک کردن و . . . .

در این روش دارندگان اطلاعات تلاش می‌نمایند تا با به هم ریختن اندازه و نوع فرمت هر پارتیشن اطلاعات مربوطه را به صورت کلی از بین برده و آن را از دسترسی دیگران به دور نگهدارند . البته بسیاری از کاربران می‌دانند چگونه با ابزار و نرم‌افزاری بازیابی سکتورها مجدداً بتوانند به این اطلاعات دسترسی پیدا نمایند.

۴-۷-۵- اطلاعات پوشش داده شده یا steganography

اصطلاح «استیگانوگرافی» واژه‌ای مرکب و یونانی به معنای «پوشیده نویسی» است. در دنیای زیر زمینی نفوذگران، «استیگانوگرافی» به مکانیزمی برای مخفی کردن پیام‌های سری در

دل پیام‌ها یا اطلاعات معمولی اطلاق می‌شود. پر سابقه‌ترین روش استیگانوگرافی، جاسازی اطلاعات سری در لابلای تصاویر گرافیکی است. دقت داشته باشید که چشم انسان تفاوت‌های ناچیز بین دو رنگ را تشخیص نخواهد داد. حال فرض کنید که رنگ هر نقطه تصویر با ۲۴ بیت مشخص شود؛ (۸بیت برای قرمز، ۸ بیت برای سبز و۸ بیت برای آبی). مجموع این ۲۴ بیت،ترکیب شانزده میلیون رنگ مختلف را پدید خواهد آورد، در حالی که قدرت تشخیص چشم، این‌اندازه نیست. به بیانی دیگر اگر در بیت‌های کم ارزش از رنگ هر نقطه تصویر، تغییری ایجاد شود، چشم ما قادر به تشخیص تغییر رنگ نخواهد بود؛ برای مخفی کردن پیام‌های سری درون تصاویر از همین واقعیت استفاده شده است. حال فرض کنید تصویری به ابعاد ۲۰۴۸ در ۱۰۲۴ نقطه داشته باشیم. اگر نفوذگر کم ارزش‌ترین بیت هر رنگ را محلی برای پنهان کردن داده‌های خودش در نظر بگیرد یا در آن تغییری ایجاد کند، چشم انسان هیچ تفاوتی با تصویر اصل، احساس نخواهد گرد. بدین‌ترتیب از هر نقطه ۳ بایتی تصویر، حداقل ۳ بیت را می‌توان برای جاسازی اطلاعات در نظر گرفت. با این رویکرد در یک فریم تصویر با ابعاد فوق، فضایی معادل ۶۲۹۱۴۵۶=۳×۱۰۲۴×۲۰۴۸ بیت (۷۸۶۴۳۲ بایت) برای درج اطلاعات محرمانه به دست می‌آید! برای استفاده بهینه از این فضا معمولاً داده‌های سری فشرده شده و سپس رمز می‌شوند تا رشته این بیت‌ها در نقاط تصویر کاملاً تصادفی به نظر برسد. تاکنون انواع نرم‌افزارهای استیگانوگرافی تولید و عرضه شده است که بسیاری از آن‌ها رایگان و دارای متن باز هستند.

استیگانوگرافی را می‌توان بر روی فایل‌های صدا یا ویدئو نیز انجام داد. در این صورت فضای موجود برای مخفی سازی داده بسیار زیاد خواهد بود. (امنیت داده‌ها ، ذاکر حسینی ،۱۳۸۶)

برخی از کاربران می‌کوشند تا با پوشش دادن اطلاعات در قالب فایل‌های دیگر و به صورتی که ویژگی‌های فایل اصلی مورد تغییر واقع نشده و شک برانگیز نباشد اطلاعات مربوطه و مد نظر را پنهان نمایند. به طوری که فردی که به دنبال دسترسی به این اطلاعات می‌باشد در بررسی‌های خود با فایل پوشش دهنده روبرو گردیده و از این که اطلاعات دیگر در درون آن وجود داشته باشد بی‌خبر است لیکن عناصر غیر مجاز امروز با دست‌یابی به انواع روش‌های steganodetect راه‌های پیدا کردن فایل‌های حامل پوششی اطلاعات اصلی را به خوبی یاد گرفته و با عبور فایل‌های مشکوک از فیلترهای خاص، ابتدا این فایل‌ها را شناسائی نموده و سپس به اطلاعات آن دسترسی پیدا می‌کنند.

۴-۸- احیا اطلاعات در رایانه‌های شخصی

در رایانه‌ها شخصی و ابزار ذخیره ساز اطلاعات کاربران در بسیاری از مواقع تلاش بر این دارند تا اطلاعاتی را که به آن‌ها نیاز ندارند یا کار با آن‌ها تمام شده است را از دسترس دیگران خارج نمایند و یکی از متداول‌ترین راه‌ها پاک کردن و حذف اطلاعات می‌باشد.

در سیستم عامل‌های مختلف روش پاک کردن اطلاعات متفاوت می‌باشد لیکن تمام آن‌ها در این نکته اشتراک دارند که اطلاعات حذف شده صرفاً از دسترس کاربران به صورت موقت خارج شده است و با اندکی عملیات نرم‌افزاری مجدد می‌توان به این اطلاعات دسترسی پیدا نمود.

با توجه به رشد علم و تکنولوژی سازندگان سخت‌افزار و نویسندگان نرم‌افزار تلاش بر این دارند تا روش‌های را به کار ببرند تا در صورتی که کاربران به صورت ناخواسته اطلاعاتی را از دسترس خارج نمودند بتوان آن‌ها را در کم‌ترین زمان مجدد به دست آورد و این همان روشی است که عناصر غیر مجاز با استفاده از آن‌ها به اطلاعات حذف شده دسترسی پیدا می‌نمایند. باید این نکته را مد نظر داشت که امروز هیچ اطلاعاتی از بین نمی‌رود و صرفاً به صورت موقت از دسترس خارج می‌شود.

۴-۹- رمز نگاری اطلاعات رایانه و انواع رمز نگاری

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

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

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

رمزنگاری مخفف‌ها و اصطلاحات مخصوص به خود را دارد. برای درک عمیق‌تر به مقداری از دانش ریاضیات نیاز است. برای محافظت از دیتای اصلی (که به‌عنوان plaintext شناخته می‌شود)، آنرا با استفاده از یک کلید (رشته‌ای محدود از بیت‌ها) به‌صورت رمز در می‌آوریم تا کسی که دیتای حاصله را می‌خواند قادر به درک آن نباشد. دیتای رمزشده (که به‌عنوان ciphertext شناخته می‌شود) به‌صورت یک سری بی‌معنی از بیت‌ها بدون داشتن رابطه مشخصی با دیتای اصلی به‌نظر می‌رسد. برای حصول متن اولیه دریافت کننده آن را رمزگشایی می‌کند. یک شخص ثالث (مثلا یک هکر) می‌تواند برای این که بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمز نوشته[۱] کند. به‌خاطر داشتن وجود این شخص ثالث بسیار مهم است.

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

۴-۱۰- امنیت رایانه‌های شخصی در سفر

- حفاظت از رایانه با استفاده از رمز عبور . پیش‌نهاد می‌گردد به منظور استفاده از رایانه و Log in نمودن به آن از یک رمز عبور استفاده شود.
- نگهداری رایانه در تمامی مدت نزد خود : در زمان مسافرت ، رایانه همراه را نزد خود نگهداری نمائید . در اغلب موارد ، سارقین به دنبال فرصت‌های مناسبی می‌باشند که به‌توانند به اهداف خود نائل گردند (بررسی اطاق‌های هتل به منظور دسترسی به رایانه‌های بی مراقب) . در صورتی که قصد شرکت در یک همایش یا نمایشگاه بازرگانی را دارید ، لازم است به این موضوع دقت شود که این نوع مکان‌ها شرایط مناسب و مطلوبی را برای سارقین فراهم می‌نمایند .

---

[۱] cryptanalysis

- کم اهمیت جلوه دادن داشتن یک رایانه همراه . ضرورتی ندارد که تبلیغ داشتن رایانه همراه خود را برای سارقین انجام دهید ! سعی نمائید در مکان‌های عمومی از رایانه‌های همراه استفاده نکرده و برای جابه‌جایی آنان از کیف‌های سنتی استفاده نگردد .
- استفاده از یک قفل و یا دزدگیر : تعداد زیادی از شرکت‌ها، قفل‌ها و یا دزدگیرهایی را ارائه نموده‌اند که می‌توان با تهیه آنان ، حفاظت رایانه همراه خود را افزایش داد . در صورتی که شما اغلب مسافرت می‌نمائید یا در مکان‌های شلوغ مشغول به کار هستید ، می‌توانید از تجهیزات فوق به منظور ایمن سازی رایانه همراه خود استفاده نمائید .
- گرفتن پشتیبانی[۱] از فایل‌های موجود بر روی رایانه . به منظور پیش‌گیری در خصوص از دست دادن اطلاعات ، پیش‌نهاد می‌گردد از اطلاعات مهم موجود بر روی رایانه ، پشتیبان گرفته شده و آنان را در یک مکان جداگانه ذخیره نمائید .
- . در چنین مواردی نه تنها شما قادر به دستیابی اطلاعات خواهید بود ، بلکه در صورت سرقت رایانه ، امکان بررسی این موضوع که چه اطلاعاتی در معرض تهدید می‌باشند نیز وجود خواهد داشت .

اقدامات لازم در صورت سرقت رایانه

در صورتی که رایانه همراه شما سرقت شده است ، می‌بایست در اسرع وقت موضوع را به اطلاع سازمان‌های ذی‌ربط قانونی رسانده تا آنان مراحل و اقدامات لازم را انجام دهند . در صورتی که بر روی رایانه ، اطلاعات حساس سازمانی یا اطلاعات مربوط به مشتریان وجود داشته است ، می‌بایست بلافاصله موضوع را به اطلاع افراد مسئول در سازمان خود رسانده تا آنان سریعاً اقدامات لازم را انجام دهند . (srco. ir)

[۱] **backup**

۴-۱۱- سوالات خودآزمایی

۱. تعریف رایانه شخصی را نوشته و انواع آن را توضیح دهید.
۲. توسعه و ارتقای نرم‌افزار رایانه‌ای چه نقشی می‌تواند در امنیت داشته باشد.
۳. در زمان گارانتی و تعمیر رایانه شخصی چگونه امنیت می‌تواند به خطر افتد . توضیح دهید.
۴. سیستم عامل رایانه چه نقشی در امنیتی رایانه دارد . توضیح دهید.
۵. شرایط یک رمز خوب در رایانه را بنویسید.
۶. انواع روش‌های حمله به رمز نرم‌افزارهای رایانه‌ای را نوشته و توضیح دهید.
۷. نرم‌افزارهای ثبت کننده صفحه کلید چگونه امنیت رایانه را تهدید می‌کنند.
۸. اختلاف بین ویروس‌ها وتروجان‌ها در امنیت رایانه چیست؟
۹. انواع روش‌های آلوده سازی رایانه شخصی به نرم‌افزارهای مخرب را توضیح دهید.
۱۰. رمز نگاری چه نقشی می‌تواند در امنیت رایانه‌ای داشته باشد؟

۵

فصل پنجم : امنیت شبکه‌های رایانه‌ای

آن چه در این فصل می‌خوانید:

- **تعریف شبکه‌های رایانه‌ای**
- **تاریخچه شبکه‌های رایانه‌ای**
- **انواع بهره‌برداری از شبکه‌های رایانه‌ای**
- **استراتژی امنیتی حاکم بر شبکه‌های رایانه‌ای**

۵- امنیت شبکه‌های رایانه‌ای

۵-۱- تعریف شبکه‌های رایانه‌ای

شبکه‌های رایانه‌ای مجموعه‌ای از رایانه‌های مستقل متصل به یک‌دیگرند که با یک‌دیگر ارتباط داشته و تبادل داده می‌کنند. مستقل بودن رایانه‌ها بدین معناست که هر کدام دارای واحدهای کنترلی و پردازشی مجزا بوده و بود و نبود یکی بر دیگری تاثیرگذار نیست. متصل بودن رایانه‌ها یعنی از طریق یک رسانه فیزیکی مانند کابل ، فیبر نوری ، ماهواره‌ها و ... به هم وصل می‌باشند. دو شرط فوق شروط لازم برای ایجاد یک شبکه رایانه‌ای می‌باشند اما شرط کافی برای تشکیل یک شبکه رایانه‌ای داشتن ارتباط و تبادل داده بین رایانه‌ها است.(subnet. ir)

۵-۲- تاریخچه شبکه‌های رایانه‌ای

در اواخر سال ۱۹۶۰ اولین شبکه رایانه‌ای بین چهار رایانه که دو تای آن‌ها در MIT، یکی در دانشگاه کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه‌اندازی شد. این شبکه آرپانت نام‌گذاری شد. در سال ۱۹۶۵ نخستین ارتباط راه دور بین دانشگاه MIT و یک مرکز دیگر نیز برقرار شد. تا این سال‌ها شبکه آرپانت به امور نظامی اختصاص داشت، اما در سال ۱۹۷۲ به عموم معرفی شد. در این سال شبکه آرپانت مراکز رایانه‌ای بسیاری از دانشگاه‌ها و مراکز تحقیقاتی را به هم متصل کرده بود. در سال ۱۹۷۲ نخستین نامه الکترونیکی از طریق شبکه منتقل شد. در این سال‌ها حرکتی غیرانتفاعی به نام MERIT که چندین دانشگاه بنیانگذار آن بوده‌اند، مشغول توسعه روش‌های اتصال کاربران‌ترمینال‌ها به رایانه مرکزی یا میزبان بود. مهندسان پروژه MERIT در تلاش برای ایجاد ارتباط بین رایانه‌ها، مجبور شدند تجهیزات لازم را خود طراحی کنند. آنان با طراحی تجهیزات واسطه برای مینی رایانه ۱۱ DECPDP نخستین بستر اصلی۱ شبکه رایانه‌ای را ساختند. تا سال‌ها نمونه‌های اصلاح شده این رایانه با نام PCP نقش میزبان را در شبکه‌ها ایفا می‌کرد. نخستین شبکه از این نوع که چندین ایالت را به هم متصل می‌کرد Michnet نام داشت. روش اتصال کاربران به رایانه میزبان در آن زمان به این صورت بود که یک نرم‌افزار خاص روی رایانه مرکزی اجرا می‌شد و ارتباط کاربران را برقرار می‌کرد اما در سال ۱۹۷۶ نرم‌افزار جدیدی به نام Hermes عرضه شد که برای

---

[1] Backdone

نخستین بار به کاربران اجازه می‌داد از طریق یک‌ترمینال به صورت تعاملی مستقیماً به سیستم MERIT متصل شوند. از وقایع مهم تاریخچه شبکه‌های رایانه‌ایی، ابداع روش سوئیچینگ بسته‌ای است. قبل از معرفی شدن این روش از سوئیچینگ مداری برای تعیین مسیر ارتباطی استفاده می‌شد اما در سال ۱۹۷۴ با پیدایش پروتکل ارتباطی TCP/IP این پروتکل جایگزین پروتکل NCP شد و به پروتکل استاندارد برای آرپانت تبدیل شد. با این تغییر و تحول، شبکه‌های زیادی به بخش تحقیقاتی این شبکه متصل شدند و آرپانت به اینترنت تبدیل شد. (aftab. ir)

۵-۳- انواع بهره‌برداری از شبکه‌های رایانه‌ای

امروزه بر روی شبکه‌های مختلفی که در سیستم‌های عمومی و خصوصی استفاده می‌شود اطلاعات فراوانی وجود دارد و در صورتی که یک فرد مجاز و یا غیر مجاز به هر شکلی به این شبکه‌ها دسترسی پیدا نماید می‌تواند به بخشی و یا تمام این اطلاعات دسترسی پیدا نماید . بستگی به این که با چه روش و در چه زمانی و به چه وسیله‌ای این دسترسی صورت پذیرفته است میزان دسترسی‌ها متغیر می‌باشند . معمولاً در روش‌های دسترسی مجاز مدیر شبکه تلاش بر این دارد تا سطح دسترسی‌ها را طبقه بندی نموده و بر اساس سیاست‌های امنیتی از پیش تعریف شده کاربران را محدود به دسترسی‌های مورد نظر قرار دهد و از دسترسی آن‌ها به دیگر اطلاعات جلوگیری نماید. همینطور با استفاده از انواع روش‌ها و ابزار مختلف تلاش بر این دارد تا بر این دسترسی‌ها نظارت داشته باشد تا بتواند اشرافیت خود را بر شبکه و سمت و سوی حرکت اطلاعات و نوع اقدامات کاربران برقرار سازد .

۵-۳-۱- شبکه‌های خصوصی

با توجه به هزینه بالای شبکه نمودن اطلاعات و نیازمند بودن به سخت‌افزار و نرم‌افزارهای خاص برای این کار و همچنین نیازمند بودن به افراد متخصص برای حفظ و نگهداری از شبکه در طول زمان استفاده معمولاً برای کاربران خصوصی که به صورت انفرادی و یا در تعداد اندک از رایانه استفاده می‌نمایند این کار مقرون به صرفه نمی‌باشد. شرکت‌ها و موسسات خصوصی نیز همانند کاربران دولتی و عمومی و بستگی به تعداد کاربران و میزان

اطلاعات در حال تولید و چرخش ، از شبکه‌های رایانه‌ای استفاده می‌کنند که از نظر اصول حفظ و نگهداری اطلاعات با سیستم‌های دولتی فرق چندانی ندارد. در موسسات خصوصی حساسیت‌های امنیتی نسبت به مراکز عمومی ممکن است کم‌تر بوده و صرفاً انگیزه اقتصادی و رقابت با رقبا اصلی‌ترین انگیزه برای پرداختن به امنیت گردد. انگیزه هر چه باشد امنیت اطلاعات نیاز به روش‌های خاصی دارد که با توجه به یکسان بودن آن در کلیه شبکه‌ها دربخش مربوط به شبکه‌های عمومی به این نکته پرداخته می‌شود.

۵-۳-۲- شبکه‌های اداری و دولتی

شبکه‌های اداری جزء رایج‌ترین نوع شبکه‌ها بوده و در اکثر سازمان‌ها و وزارتخانه‌ها و شرکت‌های خصوصی برای به گردش در آوردن اطلاعات اداری و جاری سازمان‌ها مورد استفاده قرار می‌گیرد و با توجه به گستردگی و محدودیت هر سازمان اطلاعات قرار گرفته بر روی آن‌ها می‌تواند متفاوت باشد . در سازمان‌ها و شرکت‌های کوچک محدود به اطلاعات درونی سازمان‌ها بوده لیکن در وزارتخانه‌ها و نهادهای دولتی علاوه بر این که تمام اطلاعات اداری جاری و راکد وزارتخانه را در بر می‌گیرد عملاً سطح وسیعی از اطلاعات مردمی که با آن وزارتخانه برای انجام امور اداری خود در ارتباط می‌باشند را نیز در بر می‌گیرد و به نوعی درصد زیادی از اطلاعات حاکمیتی یک کشور در شبکه داخلی آن وزارتخانه مجتمع شده است . بستگی به نوع وزارتخانه میزان و درصد این اطلاعات نیز متغیر می‌باشد. با توجه به این که وزارتخانه‌ها و سازمان‌ها به صورت متمرکز و نیمه متمرکز توسط دولت هدایت و نظارت و کنترل می‌گردد علاوه بر اطلاعات فوق می‌توان اطلاعات عمومی و حاکمیتی دولت‌ها را نیز در هر کدام از وزارتخانه‌ها یافت که بر روی شبکه مربوطه قرار گرفته است.

اطلاعات زیر معمولاً در تمام شبکه‌های اداری داخلی یافت می‌شود:

- شبکه‌های پرسنلی و کارگزینی
- نام و مشخصات پرسنلی کلیه کارمندان سازمان
- رده‌های اداری و جایگاه‌های سازمانی هر شاغل و بازنشسته در سازمان
- حقوق و منابع مالی ، پرسنلی سازمان
- امورات مربوط به رفاهیات و شیوه توزیع آن‌ها در سازمان
- آدرس منازل و تلفن‌های کل پرسنل سازمان

- مشکلات شخصی و معیشتی کل پرسنل سازمان
- لیست بیماری‌ها و توانمندی‌های جسمی پرسنل سازمان
- نیازمندی‌های آتی پرسنل سازمان
- جداول سازمانی و شرح وظایف کل سازمان و تحولاتی که در سازمان در طی سالیان مختلف در این رابطه انجام شده است
- ارتباطات شغلی و طبقات رسمی و غیر رسمی ایجاد شده در سازمان
- هر فردی که به این اطلاعات دسترسی داشته باشد عملاً امکان طراحی و اجرای هرگونه عملیات اطلاعاتی و اشرافیتی در آن سازمان برای وی میسر می‌شود و تمام سازمان‌های اطلاعاتی دنیا برای به دست آوردن این نوع اطلاعات و حتی بخش بسیار کوچکی از آن، هزینه‌های بسیار گزاف صرف می‌کنند و برای شروع به جاسوسی در کشورهای دیگر یکی از اولین نوع اطلاعات که نیاز دارند تا بر اساس آن طراحی جاسوسی و شیوه جاسوسی و جذب همکاران جاسوسی نمایند این نوع اطلاعات می‌باشد.

۵-۳-۳- شبکه‌های استراتژیک

در هر کشوری شبکه‌های وجود دارد که در صورت به خطر افتادن آن‌ها کلیت نظام آن کشور به خطر افتاده و ضربات غیرقابل جبرانی به آن کشور وارد می‌شود. این شبکه‌ها معمولاً در بر گیرنده عناصر اصلی انرژی آن کشور مانند آب و برق و انرژی هسته‌ای می‌باشد. هر چه این شبکه‌ها گسترش فراوانی داشته باشند بیش‌تر در معرض خطر قرار خواهند داشت . این شبکه نیاز به حفظ پایداری و امنیت و دسترسی در شرایط عادی و بحرانی را دارند و ضمن این که می‌بایست مدیریت بر تولید و هدایت آن‌ها مدیریت بومی باشند می‌بایست در زمان ساخت و طراحی ملاحظات پدافندی در آن‌ها رعایت تا پس از اتمام قابلیت اتکا پذیری داشته باشند زیرا معمولاً هزینه انجام شده در رابطه با آن‌ها در بودجه‌های سالیانه کشورها اثرگذار بوده و اشتباهات آن‌ها غیر قابل جبران بوده و توان منابع کشور را در خود صرف می‌نماید.

۵-۳-۴- شبکه‌های مدیریت و کنترل

"جنگ فرماندهی و کنترل عبارت است از کاربرد یک‌پارچه امنیت عملیات ، فریب نظامی، عملیات روانی، جنگ الکترونیک، و تخریب فیزیکی برای تاثیرگذاری، اُفت کیفیت، یا تخریب توانمندی‌های فرماندهی و کنترل دشمن و در عین حال حفاظت از توانمندی‌های فرماندهی و کنترل خودی در برابر اقدامات مشابه دشمن. زمانی که هدف اصلی چنین جنگی چیزی بیش از فرماندهی و کنترل و ارتباطات دشمن باشد از اصطلاح عمومی‌تر جنگ اطلاعاتی استفاده می‌شود که در سطوح غیر نظامی هم‌چون جنگ دیپلماتیک و سیاسی و دیگر اشکال ارتباطات نیز کاربرد دارد. (wikipedia. com)

با توجه به این تعریف شبکه‌های مدیریت و کنترل شبکه‌های را در بر می‌گیرد که در آن سیستم فرماندهی و کنترل ارتباط مستقیمی از طریق شبکه تعریف شده با زیر مجموعه داشته و هرگونه آسیب‌پذیری به این شبکه باعث اُفت عمل‌کرد و یا از کارانداختن کل شبکه خواهد شد.

۵-۳-۵- شبکه‌های مبتنی بر پروتکل TCP/IP

TCP/IP پروتکل استاندارد در اکثر شبکه‌های بزرگ است . با اینکه پروتکل فوق کند و مستلزم استفاده از منابع زیادی است ، ولی به‌دلیل مزایای بالای آن نظیر : قابلیت روتینگ ، حمایت در اغلب پلات فورم‌ها و سیستم‌های عامل هم‌چنان در زمینه استفاده از پروتکل‌ها حرف اول را می‌زند. با استفاده از پروتکل فوق کاربران با در اختیار داشتن ویندوز و پس از اتصال به شبکه اینترنت، به‌راحتی قادر به ارتباط با کاربران دیگر خواهند بود که از مکینتاش استفاده می‌کنند.

امروزه کم‌تر محیطی را می‌توان یافت که نیاز به دانش کافی در رابطه با TCP/IP نباشد. حتی سیستم عامل شبکه‌ای ناول که سالیان متمادی از پروتکل IPX/SPX برای ارتباطات استفاده می‌کرد، در نسخه شماره پنج خود به ضرورت استفاده از پروتکل فوق واقف و نسخه اختصاصی خود را در این زمینه ارائه نمود.

پروتکل TCP/IP در ابتدا برای استفاده در شبکه ARPAnet [۱] طراحی گردید. وزارت دفاع امریکا با همکاری برخی از دانشگاه‌ها اقدام به طراحی یک سیستم جهانی نمود که دارای

---

[۱] نسخه قبلی اینترنت

قابلیت‌ها و ظرفیت‌های متعدد حتی در صورت بروز جنگ هسته‌ای باشد. پروتکل ارتباطی برای شبکه فوق، TCP/IP در نظر گرفته شد.

۵-۳-۵-۱- ساختار نرم‌افزاری

پروتکل‌های موجود در لایه Network پروتکل TCP/IP

پروتکل (TCP)[۱] ، مهم‌ترین وظیفه پروتکل فوق اطمینان از صحت ارسال اطلاعات است . پروتکل فوق اصطلاحا" Connection-oriented نامیده می‌شود. علت این امر ایجاد یک ارتباط مجازی بین رایانه‌های فرستنده و گیرنده بعد از ارسال اطلاعات است . پروتکل‌هائی از این نوع ، امکانات بیش‌تری را به منظور کنترل خطاهای احتمالی در ارسال اطلاعات فراهم نموده ولی به‌دلیل افزایش بار عملیاتی سیستم کارائی آنان کاهش خواهد یافت . از پروتکل TCPبه عنوان یک پروتکل قابل اطمینان نیز یاد می‌شود. علت این امر ارسال اطلاعات و کسب آگاهی لازم از گیرنده اطلاعات به منظور اطمینان از صحت ارسال توسط فرستنده است . در صورتی که بسته‌های اطلاعاتی به‌درستی دراختیار فرستنده قرار نگیرند، فرستنده مجدداً اقدام به ارسال اطلاعات می‌نماید .

پروتکل (UDP)[۲] . پروتکل فوق نظیر پروتکل TCP در لایه " حمل " فعالیت می‌نماید. UDP بر خلاف پروتکل TCPبه‌صورت " بدون اتصال " است . بدیهی است که سرعت پروتکل فوق نسبت به TCP سریع‌تر بوده ولی از بعد کنترل خطا تظمینات لازم را ارائه نخواهد داد. به‌ترین جایگاه استفاده از پروتکل فوق در مواردی است که برای ارسال و دریافت اطلاعات به یک سطح بالا از اطمینان ، نیاز نداشته باشیم .

پروتکل (IP) [۳]. پروتکل فوق در لایه شبکه ایفای وظیفه کرده و مهم‌ترین مسئولیت آن دریافت و ارسال بسته‌های اطلاعاتی به مقاصد درست است . پروتکل فوق با استفاده از آدرس‌های نسبت داده شده منطقی، عملیات روتینگ را انجام خواهد داد .

۵-۳-۶- اصول و مفاهیم شبکه‌های رایانه ای

امنیت شبکه‌های رایانه‌ای دارای اصول خاصی می‌باشند که در قسمت به برخی از آن‌ها پرداخته می‌شود.

---

[۱] Transmission Control Protocol
[۲] User Datagram Protocol
[۳] Internet Protocol

۵-۳-۶-۱- لایه‌های ارتباطی شبکه – مدل مرجع OSI

پروتکل ، مجموعه قوانین لازم به منظور مبادله اطلاعات بین رایانه‌های موجود در یک شبکه را مشخص می‌نماید . اکثر شبکه‌ها از "اترنت" استفاده می‌نمایند. در برخی از شبکه‌ها ممکن است از پروتکل Token Ring شرکت IBM استفاده گردد . پروتکل ، در حقیت به منزله یک اعلامیه رسمی است که در آن قوانین و رویه‌های مورد نیاز به منظور ارسال و یا دریافت داده ، تعریف می‌گردد . در صورتی که دارای دو یا چندین دستگاه (نظیر رایانه) باشیم و بخواهیم آنان را به یک‌دیگر مرتبط نمائیم ، قطعاً به وجود یک پروتکل در شبکه نیاز خواهد بود. تاکنون صدها پروتکل با اهداف متفاوت طراحی و پیاده سازی شده است .TCP/IP یکی از متداول‌ترین پروتکل‌ها در زمینه شبکه بوده که خود از مجموعه پروتکل‌هائی دیگر ، تشکیل شده است .

۵-۳-۶-۱-۱- Physical

لایه فوق در ارتباط مستقیم با سخت‌افزار بوده و خصایص فیزیکی شبکه نظیر : اتصالات ، ولتاژ و زمان را مشخص می‌نماید .

۵-۳-۶-۱-۲- Datalink

لایه دو (**Data**). در لایه فوق ، پروتکل‌های فیزیکی به داده اضافه خواهند شد. در این لایه نوع شبکه و وضعیت بسته‌های اطلاعاتی (Packet) نیز تعیین می‌گردند.

۵-۳-۶-۱-۳- Network

لایه سه (**Network**) . در لایه فوق روش ارسال داده‌ها برای دستگاه گیرنده تعیین خواهد شد. پروتکل‌های منطقی ، روتینگ و آدرس دهی در این لایه انجام خواهد شد.

۵-۳-۶-۱-۴- Transport

لایه چهار (**Transport**) . لایه فوق مسئول پشتیبانی کنترل جریان داده‌ها و بررسی خطا و بازیابی اطلاعات بین دستگاه‌های متفاوت است . کنترل جریان داده‌ها، بدین معنی است که لایه فوق در صورتی که اطلاعاتی از چندین برنامه ارسال شده باشد، داده‌های مربوطه به هر برنامه را به یک stream آماده تبدیل تا در اختیار شبکه فیزیکی قرار داده شوند .

۵-۳-۶-۱-۵- Session

لایه پنج (**Session**) . لایه فوق مسئول ایجاد ، پشتیبانی و ارتباطات مربوطه با دستگاه دریافت کننده اطلاعات است .

Presentation -۶-۱-۶-۳-۵

لایه شش (**Presentation**) . لایه فوق داده‌های مورد نظر خود را از لایه Application اخذ و آن‌ها را به‌گونه‌ای تبدیل خواهد کرد که توسط سایر لایه‌ها قابل استفاده باشد.

Application -۷-۱-۶-۳-۵

لایه هفت (Application) . این لایه با سیستم عامل و یا برنامه‌های کاربردی ارتباط دارد. کاربران با استفاده از نرم‌افزارهای کاربردی متفاوت قادر به انجام عملیات مرتبط با شبکه خواهند بود. مثلاً کاربران می‌توانند اقدام به ارسال فایل خواندن پیام ارسال پیام و . . . نمایند. (mums. ac. ir)

۵-۳-۶-۲- معرفی پروتکل‌های ارتباطی شبکه و انواع آن

●پروتکل:TCP/IP [۱]

مهم‌ترین کاربرد این پروتکل در شبکه‌اینترنت ا ست . همچنین سیستم عامل ویندوز NT از این پرتو کل استفاده می‌کند.

●پروتکل:Net BEUI[۲]

این پروتکل ساده‌ترین پروتکل ارتبا طی برای شبکه‌های محلی کوچک می‌باشد .

●پروتکلX . ۲۵:

مجموعه‌ای از پروتکل‌هایی است که در شبکه‌های سویچینگ بسته [۳]بکار می‌روند.

●پروتکل:IPX/SPX[۴]

سیستم عامل Novell برای مبادله اطلاعات از این پروتکل استفاده می‌کند.

تکنولوژی‌های ارتباطی به‌صورت‌های زیر انجام می‌گیرد:

الف)روش یکطرفه[۵]: اطلاعات فقط در یک جهت انتقال می‌یابند مثال : وقتی به صدای رادیو گوش می‌دهید عکس آن صادق نیست .

ب) روش دو طرفه غیر همزمان[۶] : داده‌ها می‌توانند در دومسیر جریان پیدا کنند ولی همزمان نمی‌توانند اطلاعات را منتقل کرد مانند دستگاه‌های بی سیم که در هر لحظه می‌توان فقط یا صحبت کرد یا گوش داد.

---

۱ Transmission Control Protocol/Internet Protocol
۲ Net BIOS Extended User Interface
۳ Packet Switchings networks
۴ Intenet Packet Exchange/Sequenced Packet Exchange
۵ simplex
۶ half – duplex

ج) روش دوطرفه همزمان : [۱]داده‌ها می‌توانند در دو مسیر همزمان جریان داشته باشند تلفن نمونه‌ای از این انتقال می‌باشد. (rangaranggroup. com)

۵-۴- استراتژی امنیتی حاکم بر شبکه‌های رایانه‌ای

در دنیایی که وجه مشخصه آن فن‌آوری سطح بالا و ارتباطات گسترده می‌باشد، هر سازمانی نیاز به استراتژی امنیتی (سیاست امنیتی) که مدبرانه تدوین شده باشند دارد. در هر لحظه خطرات مختلفی از بیرون و درون سازمان توسط هکرها، رقبا یا کشورهای خارجی منافع سازمان را تهدید می‌کند. هدف سیاست‌های امنیتی تعریف روال‌ها، راهنماها و تمریناتی است که امنیت را در محیط سازمان برقرار و مدیریت می‌نماید. با اجرای دقیق سیاست‌های امنیتی، سازمان‌ها می‌توانند تهدیدات را کاهش دهند .

استراتژی امنیتی (سیاست امنیتی) یک سازمان، سندی است که برنامه‌های سازمان برای محافظت سرمایه‌های فیزیکی و مرتبط با فن‌آوری ارتباطات را بیان می‌نماید. به سیاست امنیتی به عنوان یک سند زنده نگریسته می‌شود، بدین معنا که فرآیند تکمیل و اصلاح آن هیچ‌گاه متوقف نشده، متناسب با تغییر فن‌آوری و نیازهای کاربران به‌روز می‌شود. چنین سندی شامل شرایط استفاده مجاز کاربران، برنامه آموزش کاربران برای مقابله با خطرات، توضیح معیارهای سنجش و روش سنجش امنیت سازمان و بیان رویه ارزیابی موثر بودن سیاست‌های امنیتی و راه کار به روز رسانی آن‌ها می‌باشد. (ircert. com)

۵-۴-۱- حملات رایج

بیش‌تر حملات هدفمند، در پنج مرحله طرح ریزی و انجام می‌شوند:

- شناسایی مقدماتی شبکه و منابع آن
- پویش و جستجو در شبکه در پی رخنهٔ نفوذ
- نفوذ و حمله (شامل حملات مبتنی بر حفره‌های سیستم عامل یا برنامه‌های کاربردی، حملات مبتنی بر استراق سمع و اختلال در پروتکل‌های لایهٔ دوم و سوم شبکه و حملات اختلال در سرویس دهی[۲]
- حفظ سیطره برشبکه
- رد گم کردن ومخفی ماندن

---

[۱] full – duplex
[۲] Dos

Trojans -۱-۱-۴-۵

«اسب‌تروا» یک برنامه آلوده به کدهای اجرایی است که غالباً ظاهری فریبنده یا کاملاً معمولی دارد. این برنامه‌ها پس از نصب، همانند یک سرویس دهنده، کنترل و هدایت آن ماشین را در اختیار نفوذگر قرار می‌دهند. امروزه اکثر اسب‌های‌تروا پس از اجرا بر روی ماشین پنهان شده و خود را به گونه‌ای نصب می‌کنند که پس از هر بار ورود کاربر به سیستم، فعال شوند. آن‌ها هیچ اختلالی که باعث شود که کاربر از وجود آن‌ها مطلع گردد، ایجاد نمی‌کنند.

اسب‌های‌تروا به دو دسته «اسب‌هاتروا در سطح برنامه‌های کاربردی» و «اسب‌های‌تروا در سطح سیستم عامل»[۱] تقسیم می‌شوند.

اسب‌های‌تروا در سطح برنامه کاربردی

این گروه از اسب‌های‌تروا برنامه‌های مستقلی هستند که همانند یک برنامه معمولی بر روی سیستم قربانی اجرا می‌شوند و یک در پشتی یا رخنه درسیستم، برای ورود نفوذگر ایجاد می‌کنند. هرگاه کاربر فقط یک بار چنین برنامه‌های آلوده‌ای را اجرا کند، است‌تروا در اولین اقدام سریعاً پیکربندی سیستم عامل را تغییر می‌دهد تا ازآن به بعد هرگاه کاربر به سیستم وارد شد این برنامه هم به‌طور خودکار اجرا شود! «سرویس دهنده اسب‌تروا» به‌طور معمول یک برنامه ساکت است که روی ماشین قربانی منتظر برقراری یک ارتباط TCP یا UDP از طرف نفوذگر می‌ماند و پس از برقراری ارتباط ، مبتنی بر کدهائی که برای آن ارسال می‌شود، فرامینی را روی ماشین قربانی اجرا می‌کند. بیش از هزاران اسب‌تروای شناخته شده وجود دارد که از مشهورترین آن‌ها می‌توان به Back Orifice ۲۰۰۰ (مشهور به BO۲K) و Subseven اشاره کرد. BO۲K در بین تمام اسب‌های‌تروا، قابلیت‌های بسیار ویژه و ممتازی دارد. قابلیت‌های ویژه و انعطاف پذیری BO۲K آن را به ابزاری تبدیل کرده که واقعاً می‌توان از آن به منظور «مدیریت از راه دور» و نظارت بر کاربران و ماشین‌ها استفاده کرد، ولی پیشینه آن و سو استفاده گسترده‌ای که از آن می‌شود باعث شده که تمام ویروس یاب‌ها آن را به عنوان یک نرم‌افزار مخرب و مضر بشناسند. بخش سرویس دهنده BO۲K که بدون علائم خاص و هیچ پنجره‌ای بر روی ماشین قربانی نصب می‌شود بسیار کوچک و کم حجم است. نرم‌افزار مشتری

[۱] Rootkits

BO۲K که کنسول نفوذگر محسوب می‌شود شامل یک رابط گرافیکی و با امکانات بسیار گسترده عرضه شده است. از ویژگی‌های BO۲K می‌توان به موارد زیر اشاره کرد:

(الف) ایجاد و نمایش پنجره‌های محاوره‌ای بر روی ماشین قربانی و گول زدن کاربر برای درج اطلاعات مهم دراین پنجره با استفاده از روش‌های روان شناختی!

(ب) توانائی اخذ و ثبت کلیدهای فشار داده شده توسط کاربر.

(ج) ربودن اطلاعاتی در مورد سیستم عامل.

(د) گزارش حجم حافظه، نوع CPU، تعداد و فضای پارتیشن دیسک سخت و اطلاعاتی در مورد سیستم فایل ماشین قربانی.

(ه) جمع آوری کلمات عبور و ارسال آن‌ها برای نفوذگر.

(و) انجام عملیات لازم برای مدیریت فایل شامل بررسی و دیدن محتوای فایل، حذف ، کپی و تغییر نام فایل‌های ماشین قربانی.

(ز) امکان تغییر در فایل‌های registry از راه دور به صورت دلخواه.

(ح) فهرست گیری از پروسه‌های در حال اجرا و ارسال آن برای نفوذگر.

(ط) استراق سمع بسته‌های دریافتی ماشین قربانی و ارسال آن‌ها برای نفوذگر.

(ی) اجرای برنامه‌های کاربردی به نحوی که به یک شماره پورت تعیین شده توسط نفوذگر گوش بدهند.

(ک)کنترل ابزارهای چند رسانه‌ای.

(ل) تبدیل ماشین قربانی به یک سرویس دهنده HTTP.

(م) ارسال فایل در محیط مرورگر برای ماشین نفوذگر

(ن) مخفی کردن خود درون سیستم به گونه‌ای که در فهرست پروسه‌های فعال قرار نگیرد.

Back door -۲-۱-۴-۵

«در پشتی» ابزاری نرم‌افزاری است که به نفوذگر اجازه می‌دهد تا از راه دور به یک سیستم وارد شود، بدون آن که به تشریفات معمول و سخت گیرانه مثل اخذ کلمه عبور و احراز هویت نیاز باشد. استفاده از نرم‌افزار کوچک Net cat برای باز کردن رخنه عبور در سیستم، مثال بارزی از ایجاد یک رخنه یا در پشتی در سیستم‌های مبتنی بر یونیکس است. تفاوت «در پشتی» با «اسب‌تروا» آن است که

«در پشتی»نرم‌افزاری است که فقط راه ورود نفوذگر به سیستم را (بدون نیاز به شناسه کاربری و کلمه عبور) باز می‌کند و پس از آن نفوذگر باید از طریق سیستم عامل ماشین تحت تصرف، عملیات دلخواهش را انجام بدهد، در حالی که «اسب‌های‌تروا» به گونه‌ای نوشته می‌شوند که مجموعه‌ای از عملیات مخرب و مورد نیاز نفوذگر به‌طور مستقل انجام بدهند.

Rootkits -۳-۱-۴-۵

Root kitsها با دستکاری و تغییر در عمل‌کرد مؤلفه‌های اصلی سیستم عامل، آن‌ها را دگرگون کرده و راه حمله نفوذگر را از طریق رخنه‌هایی که در بطن سیستم عامل پدید آمده، باز می‌کنند. Root kits شدن سیستم عامل بدین معناست که نفوذگر به نحوی برنامه تحریف شده login را با برنامه اصلی جای‌گزین کرده است. این برنامه دستکاری شده، اجازه ورود نفوذگر را با عالی‌ترین مجوز، فراهم می‌کند. پس از این که نفوذگر از طریق یک Root kits نفوذ خود را سازمان‌دهی کرد، برای گسترش این نفوذ به ماشین‌های دیگر و سرویس دهنده‌های حساس، اقدام به نصب نرم‌افزارهای اسنیفر برای استراق سمع داده‌های دیگران، از جمله کلمات عبور می‌نماید. در Root kitsهای جدید برنامه‌های اجرایی مثل du (که میزان استفاده از فضای دیسک و فضای آزاد را نشان می‌دهد)، find، ifconfing، ipconfig، netstat و . . . . . به گونه‌ای تحریف و آلوده می‌شوند که مسئول شبکه به کمک آن‌ها نتواند به وجود Root kitsها در سیستم و جاسوسی آن پی ببرد. از معروف‌ترین Root kitsهای جهان می‌توان به Lrk۵ و tornkit (برای سیستم‌های لینوکس و سولاریس) اشاره کرد.

برخی از Root kitsها، قلب سیستم عامل یعنی هسته مرکزی آن را هدف قرارداده‌اند. اگر هسته مرکزی سیستم عامل، دستکاری و تحریف شود دیگر هیچ ابزاری قادر به کشف موضوع نخواهد بود. هسته سیستم عامل، اولین بخشی است که در حافظه بار می‌شود و کنترل کل سیستم را به دست می‌گیرد. بدیهی است که تمام دسترسی‌ها به ابزارهای شبکه‌ای، حافظه، دیسک و منابع سیستم، تحت نظارت و کنترل دقیق هسته انجام می‌گیرد. کاری که Root kitsهای معمولی انجام می‌دهند در حقیقت فریب هسته سیستم عامل است در حالی که Root kitsهای سطح هسته، هسته سیستم عامل را به گونه‌ای دستکاری می‌کنند که عملیات هسته به‌طور پنهانی در خدمت نفوذگر قرار بگیرد. اولین کاری که یک هسته آلوده انجام می‌دهد آن

است که تمام فراخوانی‌های سیستم که از پروسه‌ها به هسته می‌رسند را دریافت کرده و برخی از آن‌ها را به طور واقعی و برخی دیگر را به طور دروغین اجرا می‌کند. از دیگر قابلیت Root kitsهای سطح هسته، مخفی نگه داشتن پروسه‌های درحال اجراست. همچنین آن‌ها شماره پورت‌های مورد نظر نفوذگر را در خروجی ظاهر نمی‌کنند. از مشهورترین Root kitsهای سطح هسته می‌توان به Knark و Adore اشاره کرد.

اگر بخواهیم «اسب‌های‌تروا» و «Root kitsها» را با بیماری مقایسه کنیم، اسب‌های‌تروا به مثابه میکروب‌های بیرونی هستند که بدنه سیستم را آلوده می‌کنند در حالی که Root kitsها همانند سرطان، مولفه‌های اصلی سیستم عامل را بدخیم می‌نماید!!.

Spoofing -۴-۱-۴-۵

spoofing ، که به آن "هویت مبهم " نیز گفته می‌شود ، به کتمان هویت واقعی بر روی شبکه اطلاق می‌گردد . در این رابطه از یک آدرس مبدا جعلی که بیانگر آدرس اولیه صادرکننده پیام نمی‌باشد ، استفاده می‌گردد . در بسیاری موارد از spoofing به منظور مخفی کردن منبع بروز یک تهاجم استفاده می‌شود. در برخی موارد که دستیابی به منابع موجود بر روی شبکه بر اساس آدرس متقاضیان انجام می‌شود ، مهاجمان با تغییر آدرس مبدا سعی می‌نمایند به این گونه از منابع دستیابی پیدا نمایند .

Man in the middle -۵-۱-۴-۵

با استفاده از این نوع حملات که به آن‌ها **session Hijacking** نیز گفته می‌شود ، مهاجمان می‌توانند از یک برنامه برای تغییر شکل ظاهری خود به عنوان یک سرویس گیرنده و یا سرویس دهنده موجه استفاده نمایند . بدین‌ترتیب ، یک سرویس دهنده و یا سرویس گیرنده واقعی فریب خورده و فکر می‌کنند که با یک host معتبر و مجاز ارتباط برقرار نموده‌اند . در واقع ، این نوع رایانه‌های میزبان متعلق به مهاجمان بوده که سعی می‌نمایند با دستکاری شبکه خود را به عنوان مقصد مورد نظر وانمود نمایند . از این نوع حملات به منظور آگاهی از اطلاعات logon و دستیابی به سیستم و سایر اطلاعات محرمانه استفاده می‌گردد .

Reply -۶-۱-۴-۵

برداشتن بسته‌های اطلاعاتی از روی خط به‌وسیله ابزارهای Sniffer و ارسال مجدد همان بسته‌ها یا بسته‌های تغییر داده شده را Reply گویند .

در این روش هکر اطلاعات مهم و نام‌های کاربری و کلمات عبور را از درون بسته‌ها استخراج می‌کند

Tcp/ip hijacking -۷-۱-۴-۵

معمولاً به آن Session Hijacking نیز گفته می‌شود که در آن هکرمی‌تواند نشست TCPبین دو ماشین را به‌دست آورد .

Dns poisoning -۸-۱-۴-۵

این حمله هنگامی است که فایل DNS شما با اطلاعات اشتباه تکمیل شود. به صورت ساده‌تر هنگامی می‌باشد که نفوذگر رکوردهای DNS را که به Hostهای صحیحی اشاره دارند، به Host موردنظر خود تغییر می‌دهد .

Denial of service(dos) -۹-۱-۴-۵

هدف بسیاری از حملات، ایجاد اختلال و وقفه در سرویس دهی یک ماشین در شبکه است. مقصود نفوذگر از چنین حملاتی، وارد کردن ضربات اقتصادی و سیاسی به گروه، سازمان، دولت یا شبکه اطلاع رسانی است؛ به این نوع حملات، حملات نوع DoS[1] یا «اختلال در سرویس دهی» می‌گویند.

هدف از حمله DoS، صرفاً درهم شکستن یک سرویس دهنده یا ابزار در شبکه، به گونه‌ای که سیستم مجبور به راه‌اندازی مجدد شود، یا مدتی از شبکه خارج بماند.

حملات DoS به دو دسته تقسیم می‌شوند: (۱) حمله‌ای که مستقیماً منجر به توقف سرویس‌های ماشین شود. (۲) حمله‌ای که منجر به اشباع یک سرویس دهنده و تلف شدن منابع آن شود.

حملات DoS گاهی از درون شبکه و گاه از بیرون شبکه آغاز می‌شود: حمله از درون بدین معناست که اگر نفوذگر به نحوی بتواند بر روی یک ماشین از شبکه برای خود حق دسترسی مجاز فراهم کند و از درون شبکه محلی به اخلال‌گری بپردازد. یک نفوذگر با سطح دسترسی کافی، قادر است به عملیاتی مانند از بین بردن یک پروسه کلیدی در حال اجرا یا تغییر در پیکر بندی ماشین، اقدام کند.

---

[1] Denial of Service

یکی دیگر از حملات نوع DoS ، ورود یک نفوذگر به سیستم و اجرای برنامه‌هائی است که منابع سیستم را تلف کنند (به‌گونه‌ای که سیستم کاملاً مختل شود یا سرویس دهنده‌های مهم را به شدت کند نماید). عملیاتی که برای اشباع منابع سیستم انجام می‌شود عبارتند از: اشباع جدول پروسه سیستم عامل (مثلاً با انجام پی در پی عمل (fork)، پرکردن پهنای باند درونی شبکه با حجم زیاد و متناوب اطلاعات بی ارزش، ارسال‌ترافیک بیهوده از درون به بیرون شبکه جهت هدر دادن پهنای باند.

در حملات DoS از بیرون، حمله با هدف ایجاد اختلال، از یک نقطه شبکه اینترنت شروع می‌شود و نفوذگر به داشتن مجوز ورود به سیستم هیچ نیازی ندارد. از شایع‌ترین این نوع از حملات، درهم شکستن سرویس دهنده با بمباران « بسته‌های ناقص و دارای اشکال» است. خطرناک‌ترین حملات از این رده عبارتند از : (۱) حمله Land (تنظیم آدرس IP و پورت مبدأ و مقصد در یک بسته با مقداری یکسان و ارسال آن برای ماشین) (۲) حمله Latierra (همانند حمله land با این تفاوت که بسته‌ها هم زمان برای چندین پورت ارسال می‌شوند). (۳) Ping of Death (ارسال بسته Ping بااندازه بیش از ۶۴KB). (۴) حمله Jolt (ارسال طولانی و وسیع از بسته‌های قطعه قطعه شده به جزء قطعه اول) (۵) حمله نوع Treadrop (ارسال بسته‌های قطعه قطعه شده IP با تنظیم غلط فیلد [۱]) (۶) حمله winnuk (ارسال داده‌های بی ارزش و بسیار طولانی به پورت شماره ۱۳۹ TCP)/ در تمام این نوع از حملات پروسه TCP یا IP ، سردرگم شده و (گاهی) در هم شکسته می‌شود و از کار می‌افتد.

هدف آن دسته از حملات DoS که به منظور تلف کردن منابع سیستم شروع می‌شوند، آن است که یک پروسه کلیدی تمام منابع اختصاص یافته به خود را تلف کرده و به اتمام برساند و بدین‌ترتیب در ادامه کارش با مشکل مواجه شود؛ یعنی یا کاملاً مختل شود یا بسیار کند و غیر قابل تحمل عمل کند.

Distributed denial of services (ddos) –۱۰-۱-۴-۵

حملات DDos در صورتی موفقیت آمیز به انجام می‌رسد که نفوذگر خطوطی با پهنای باند بالا در اختیار داشته باشد و چنین فرضی، مستلزم صرف هزینه بسیار زیاد است. درضمن طولانی بودن زمان حمله، منجر به فاش شدن هویت نفوذگر خواهد شد. در حملات DDoS نفوذگر سعی می‌کند از ماشین‌هائی که در سراسر اینترنت پراکنده هستند برای حمله به یک

[۱] Fragment offset

هدف در شکبه سو استفاده نماید. به این ماشین‌ها اصطلاحاً ماشین زامبی گفته می‌شود. نفوذگر، زیرکانه نرم‌افزار زامبی را بر روی ماشین‌های مختلف توزیع می‌کند؛ پس از توزیع گسترده و سراسری این نرم‌افزارهای آلوده، صدها یا هزاران «ماشین زامبی»، بسیج شده و برای شروع یک حمله آماده می‌شوند! نرم‌افزارهای زامبی پس از اجرا بر روی یک ماشین، منتظر صدور فرمان می‌مانند. اگر تعداد ماشین‌های زامبی زیاد باشد، نفوذگر قادر به هدایت همه آن‌ها نخواهد بود؛ به همین دلیل این ماشین‌ها گروه بندی شده و هر گروه توسط یک «سرگروه» کنترل می‌شود. در بالاترین سطح، ماشین‌های سرگروه از نفوذگر فرمان می‌گیرند. به‌عنوان مثال در یکی از حملات معروف DDoS با نام TFN۲K ، نفوذگر از طریق نرم‌افزار Netcat برای ارتباط با سرگروه‌ها استفاده می‌کند. نفوذگر به کمک Net cat فرمان حمله صادر می‌کند و آن‌ها نیز به ماشین‌های زامبی تحت فرمان خود دستور شروع حمله DoS را علیه یک هدف مشخص در شبکه صادر می‌کنند و در این حمله برای فرمان دادن به ماشین‌های زامبی از بسته‌های Echo Reply (مربوط به پروتکل ICMP) استفاده شده فلذا هیچ پورت TCP یا UDP بر روی ماشین‌هاای زامبی از بسته‌های قربانی، باز نخواهد شد و بدین‌ترتیب حضور نرم‌افزار زامبی برای مدت‌ها مخفی می‌ماند. در ضمن برای ارسال بسته‌های IP از آدرس‌های جعلی استفاده شده تا ورود و خروج بسته‌ها از دیوار آتش به راحتی انجام می‌گیرد.

متاسفانه حملات DDoS، بسیار مهلک هستند و در صورت شروع محله ، راه مقابله و واکنش سریع ندارند چراکه مبدأ این حملات در سرتاسر جهان پراکنده و عموماً از بیرون نمی‌توان خیل عظیم ماشین‌ها زامبی را خاموش کرد. به همین دلیل سرویس دهنده‌های حساس در چندین نقطه متفاوت از اینترنت به صورت آیینه‌ای[۱] مستقر می‌شوند تا در صورت مورد حمله قرار گرفتن یکی از آنها، دیگری به‌جای آن ایفای نقش کند.

Syn flood -۱۱-۱-۴-۵

در این نوع تهاجم از مزایای three-way handshake مربوط به TCP استفاده می‌گردد . سیستم مبدا اقدام به ارسال مجموعه‌ای گسترده از درخواست‌های SYN [۲] نموده بدون این که ACK[۳]نهائی آنان را ارسال نماید. بدین‌ترتیب ارتباطات نیمه فعال[۴]، ایجاد می‌گردد . با توجه به

[۱] Mirror
[۲] synchronization
[۳] acknowledgment
[۴] half-open TCP sessions

این که پشته TCP ، قبل از reset نمودن پورت ، در انتظار باقی خواهد ماند ، تهاجم فوق ، سرریز بافر اتصال رایانه مقصد را به دنبال داشته و عملاً" امکان ایجاد ارتباط وی با سرویس گیرندگان معتبر ، غیر ممکن می‌گردد .

Smurfing -۱۲-۱-۴-۵

این نوع حملات مبتنی بر تابع Reply پروتکل ICMP[۱] ، بوده و بیشتر با نام ping شناخته شده می‌باشند . (Ping ، ابزاری است که پس از فعال شدن از طریق خط دستور ، تابع Reply پروتکل ICMP را فرامی خواند) . در این نوع حملات ، مهاجم اقدام به ارسال بسته‌های اطلاعاتی Ping به آدرس‌های Broadcast شبکه نموده که در آنان آدرس مبدا هر یک از بسته‌های اطلاعاتی Ping شده با آدرس رایانه قربانی ، جای‌گزین می‌گردد . بدین‌ترتیب یک‌ترافیک کاذب در شبکه ایجاد و امکان استفاده از منابع شبکه با اختلال مواجه می‌گرد

Sniffing -۱۳-۱-۴-۵

نفوذ به شبکه در سطح لایه‌های زیرین، به دلیل انعطاف زیاد بیش‌تر مورد توجه نفوذگران حرفه‌ای است و حمله در این سطح‌ها گاهی خطرناک‌تر از حملات لایه بالاتر عمل می‌کند. یکی از ابزارهای کلیدی نفوذگر برای استراق سمع داده‌ها در سطح لایه‌های زیرین، «اسنیفر» نام دارد: Sniffer برنامه‌ای است که‌ترافیک جاری را از روی شبکه محلی استراق سمع و جمع آوری کرده و بخش‌های مفید آن را در اختیار نفوذگر قرار می‌دهد. حمله از طریق اسنیفرها یک حمله غیر فعال[۲] محسوب می‌شود و در مراحل اولیه قابل کشف و شناسایی نیست.

نفوذگر قبل از هر کاری باید در یکی از ماشین‌های شبکه محلی رسوخ کرده و یک اسنیفر بر روی آن نصب نماید. (برای این کار ممکن است از روش‌های در هم گسستن پشته، ارسال یک اسنیفر جاسازی شده در ضمیمه یک نامه الکترونیکی یا ده‌ها راه متنوع دیگر استفاده کند).

پس از نصب اسنیفر، این نرم‌افزار تمام یا بخش دلخواهی ازترافیک شبکه را دریافت و بسته‌های مورد نظر نفوذگر را پس از غربال، در یک فایل ذخیره می‌کند. اطلاعاتی که یک «اسنیفر» از کل شبکه استراق سمع می‌کند می‌تواند بنیان گذار حملات بعدی علیه ماشین‌های دیگر شبکه باشد.

---

[۱] Internet Control Message Protocol
[۲] Passive

نرم‌افزارهایی که برای محیط‌های مبتنی برهاب معمولی نوشته شده‌اند[۱] به صورت آرام و مخفیانه فریم‌های جاری بر روی LAN را استراق سمع می‌کنند. از مشهورترین این ابزارها می‌توان به Snort و Snifit اشاره کرد. Snort علاوه بر استراق سمع و ذخیره اطلاعات، قابلیت اسکریپت نویسی دارد و قابلیت انعطاف بی نظیر آن باعث شده تا بتوان از آن به عنوان IDS استفاده کرد. Sniffit مثل تمام اسنیفرها کارت شبکه را به حالت بی قید[۲] برده و سپس بسته‌های مفید را از بسته‌های دیگر غربال می‌کند؛ هم‌چنین می‌تواند تمام بسته‌های یک نشست واحد را ربوده و در یک پنجره خروجی نشان دهد .

برخلاف‌هاب که داده‌های ورودی را بر روی دیگر پورت‌ها ارسال می‌کند، سوئیچ‌ها آدرس مقصد هر فریم را بررسی کرده و آن‌ها را صرفاً بر روی پورتی می‌فرستند که ماشین مقصد بر روی آن قراردارد. بنابراین نرم‌افزارهای استراق سمع (مبتنی برهاب) نمی‌توانند بسته‌ها را از یک سوئیچ استراق سمع کنند. Dsniff یکی دیگر از اسنیفرهاست که تلاش می‌کند با اختلال در عمل‌کرد سوئیچ آن را به نحوی سردرگم کند که عمل‌کردش شبیه به یک‌هاب شود! Dsniff از دو روش برای ربودن و استراق سمع فریم‌ها از سوئیچ استفاده می‌کند: در تکنیک اول با ارسال سیل آسای فریم به سمت سوئیچ که در آن‌ها آدرس مبدأ هر فریم عددی تصادفی است، حافظه Hash Table سوئیچ را سرریز کرده و آن را از کار می‌اندازد؛ بدین نحو سوئیچ دیگر قادر به سوئیچینگ نیست و مجبور است همانند یک‌هاب معمولی عمل کند. در تکنیک دوم، Dsniff با ارسال آدرس فیزیکی ماشین خود در جواب بسته‌های ARP، خودش را به جای مسیریاب جا می‌زند! بدین‌ترتیب تمام بسته‌های خروجی از شبکه، ابتدا تحویل ماشین نفوذگر می‌شوند و سپس به سمت مسیریاب اصلی هدایت می‌شوند؛ به این روش اصطلاحاً Arp Spoofing می‌گویند.

Dsniff قابلیت گمراه کردن HTTPS را هم دارد؛ در این روش ماشین نفوذگر بین ماشین قربانی و سرویس دهنده نهایی قرار می‌گیرد. چون نفوذگر برای ارتباط داشتن با هر دو ماشین مجبور است گواهینامه دیجیتالی خود را تسلیم کند، مرورگر ماشین قربانی با دیدن تفاوت در آدرس حوزه و گواهینامه مربوطه، پیغام خطائی را نمایش خواهد داد ولی به علت بی‌توجهی بسیاری از کاربران، این مسئله جدی تلقی نمی‌شود و ارتباط ادامه پیدا می‌کند. در این مکانیزم

---

[۱] Passive Sniffer
[۲] Promiscuous

Dsniff داده‌های ارسالی از مرورگر را گرفته و با کلید خودش رمزگشایی می‌کند و پس از استراق سمع و ذخیره ، آن‌ها را مجدداً باکلید رمز دیگرش رمزنگاری نموده و به سمت سرویس دهنده اصلی ارسال می‌نماید. به این روش، اصطلاحاً[۱] PITM گفته می‌شود. (در اینجا Dsniff در نقش یک پراکسی ظاهر می‌شود که زیرکانه در میان مرورگر مشتری و سرویس دهنده قرار می‌گیرد).

برای مقابله با استراق سمع و اسنیفرها می‌توان توصیه‌های زیر را ارائه داد:

- انتقال اطلاعات به صورت رمز شده
- استفاده از IPsec در سطح لایه شبکه
- عدم برقراری نشست Tel Net از راه دور با دیوارآتش، مسیریاب یا سرویس دهنده‌های حساس
- توجه به پیغام‌های هشدار در خصوص گواهینامه‌های دیجیتالی
- استفاده از سوئیچ‌های هوشمند به جای‌هاب
- تنظیم جدول ARP به صورت دستی

۵-۴-۱-۱۴- تزریق sql –sql injection code

در این روش نفوذگر، به درون فیلدهای ورودی یک صفحهٔ وب، داده‌های غیر مجاز که قادرند کنترل اجرای دستورات SQL را دچار مشکل کنند (مثل ' و" و ; و . . . . .) وارد می‌کند. . در این حالت به محض آن که داده‌ای از طرف مرورگر مشتری برای برنامه سمت سرویس دهنده ارسال می‌شود یک رشته SQL Query ساخته شده و از طریق DBMS [۲] اجرا می‌شود. فرض برنامه نویس آن بوده که آنچه دریافت می‌شود دادهٔ خام است و طبعاً در شرائط معمولی هیچ مشکلی بوجود نمی‌آید ولی اگر کاربری اخلال‌گر به‌جای دادهٔ خام، رشته‌ای حاوی فرامین SQL (که با علامت ; تفکیک شده) برای برنامهٔ سمت سرویس دهنده ارسال کند می‌تواند هر کاری بر روی بانک اطلاعاتی انجام بدهد:

Input:۱۱۱۱۱۱۱۱۱'+or+userid٪۳d'۱۰۰۰۲;UPDATE
SELECT * FROM account WHERE (userid='۱۰۰۰۱'and
number='۱۱۱۱۱۱۱۱۱'oruserid='۱۰۰۰۲'UPDATE)

[۱] Person in the middle
[۲] Database management System

برای مقابله با این نوع حمله به هیچ وجه نباید به داده‌های ارسالی توسط کاربر اعتماد یا مستقیماً از آن‌ها Query تولید کرد، بلکه باید این داده‌ها آلوده فرض شده و آن‌ها را به دقت مورد بررسی قرارداد تا سالم بودن آن‌ها محرز شود. برای مثال باید دقت کرد که کاراکترهای کنترلی و غیر معتبر (که در SQL عمل‌کرد تعریف شده‌ای دارند) در داده‌های ارسالی وجود نداشته باشد.

۵-۴-۱-۱۵- استفاده از نرم‌افزارهای جستجو کننده‌تروجان

استفاده ازتروجان‌ها رایج‌ترین نوع حملات در شبکه‌های رایانه‌ای می‌باشد . در این نوع از حمله نرم‌افزارهای مخربی به نام‌تروجان به صورت پنهان توسط مهاجم بر روی رایانه قربانی نصب شده و با توجه به حجم بسیار پایین این نوع از نرم‌افزارها به مجرد نصب شدن در رایانه قربانی از دیدها پنهان شده و ماموریت خود را شروع می‌کند. اصلی‌ترین ماموریت این نرم‌افزارها باز کردن مسیر ارتباطی پنهان با رایانه متخاصم می‌باشد که از این مسیر اطلاعات مد نظر متخاصم از رایانه قربانی کپی گرفته شده و ارسال می‌شود. یکی دیگر از ماموریت‌های‌تروجان‌ها اجازه مدیریت پنهان بر منابع رایانه قربانی توسط متخاصم می‌باشد که با این مدیریت قادر خواهد بود تا به رایگان منابع نرم‌افزاری و سخت‌افزاری را مورد سو استفاده قرار داده و از آن‌ها برای حمله به رایانه دیگری بهره بردای سو نماید.

تروجان‌ها معمولاً به انواع آماتور و حرفه‌ای تقسیم می‌شوند و انواع آماتور آن توسط نرم‌افزارهای ضد ویروس و یا ضد بدافزار قابل تشخیص و پاک سازی بوده لیکن انواع حرفه‌ای آن‌ها توسط این نرم‌افزارهای شناسایی نشده و به کار خود ادامه می‌دهند

۵-۴-۱-۱۶- استفاده از رمزهای ذخیره شده در قسمت‌های مختلف

استفاده از کلمهٔ عبور یکی از راه‌های سنتی در جلوگیری از دسترسی غیر مجاز به منابع و سیستم‌ها بوده و هست. متاسفانه کلمات عبور ساده و پیش فرض سیستم‌ها، کشف آن‌ها را بسیار ساده می‌کند زیرا حدس زدن کلمات عبور ساده و کوتاه توسط ابزارهای خودکار به روش سعی و خطا فرآیند مشکلی نیست. بسیاری از کاربران آماتور، « کلمات عبور» پیش فرض سیستم‌ها را تغییر نمی‌دهند و این امر حدس زدن آن‌ها را به راحتی امکان پذیر می‌کند. نرم‌افزارهای زیادی برای حدس کلمات عبور به روش سعی و خطا نوشته شده‌اند و به رایگان دراختیار همه قرار دارند؛ لذا تعریف وکاربرد نامناسب کلمات عبور یک تهدید بالقوه برای سیستم‌ها به شمار می‌آید.

در هر سیستم مبتنی بر کلمهٔ عبور فایلی محلی وجود دارد که مشخصات کاربری و کلمات عبودر در آن ذخیره می‌شود. اگرچه عموماً این فایل به صورت درهم سازی شده[۱] نگهداری می‌شود ولی اگر نفوذگر بتواند این فایل را به دست آورد و تلاش برای رمزگشایی آن موفقیت آمیز باشد تمام کلمات عبور فاش خواهد شد. عملیات استخراج و کشف کلمهٔ عبور از اطلاعات رمز شده اصطلاحاً Password Crack نامیده شده است.

برای کشف کلمات عبور درهم سازی شده، ابتدا یک کلمهٔ حدسی، انتخاب و سپس درهم سازی می‌شود. اگر مقدار به دست آمده در فایل نبود یک کلمهٔ دیگر تولید و درهم سازی می‌شود و این عملیات تا کشف رمز ادامه پیدا می‌کند.

روش دیگر برای به دست آوردن کلمهٔ عبور، تولید حدس اولیه از طریق جای‌گشت‌های مختلفی است که یک کلمهٔ رمز می‌تواند داشته باشد. به این روش Brute force گفته می‌شود! خوشبختانه این روش برای شکستن کلمات عبور بزرگ بعضا ناتوان است. روش‌های تولید و آزمایش حدس‌های اولیه عبارتند از :

- تهیه یک فرهنگ غنی از کلمات معنی دار یا مصطلح و امتحان آن‌ها برای زبان‌های مختلف
- تولید حدس اولیه از جای‌گشت‌های مختلف حروف، اعداد و علائم
- روش مختلط که از تلفیق دو روش قبل به دست می‌آید و کارآیی آن بسیار بالاست.

برخی از ابزارهای حمله به کلمات عبور، به‌سادگی بسته‌های « چالش/ پاسخ»۲ را از روی کانال استراق سمع کرده و سپس تلاش در رمز گشایی آن‌ها می‌کنند. به‌عنوان یک مثال، نفوذگر برای استراق سمع رشتهٔ چالش و پاسخ، یک نامهٔ الکترونیکی جعلی تنظیم می‌کند؛ در این نامه آدرسی است که با کلیک بر روی آن، کلمه عبور در هم شدهٔ کاربر، برای احراز هویت به سمت سرویس دهنده فرستاده می‌شود. به محض ارسال، کلمه عبور درهم شده کاربر ، استراق سمع شده و تلاش برای رمزشکنی آن آغاز می‌شود و اگر این کلمه، کوتاه یا معنی‌دار انتخاب شده باشد احتمال موفقیت رمز شکن بالاست. ناگفته نماند که این مکانیزم بیش‌تر بر

---

[۱] Hashed
[۲] Challenge/Response

روی سیستم عامل ویندوز موثر می‌افتد! برای حمله به کلمات عبور در سیستم‌های عامل مبتنی بر یونیکس نفوذگران به دنبال دسترسی به فایلی به نام Shadow هستند. اگر این فایل به هر نحو در اختیار نفوذگر قرار بگیرد می‌تواند با ابزارهای خودکار برای رمزشکنی آن تلاش کند.

۵-۵- سوالات خودآزمایی

۱. شبکه‌های رایانه‌ای را به صورت کلی توضیح دهید.
۲. انواع بهره‌برداری‌هایی که از شبکه‌های رایانه‌ای در کشورمان انجام می‌شود را توضیح دهید.
۳. لایه‌های ارتباطی شبکه‌ها را در مدل مرجعosi نام ببرید.
۴. مدل انتقال اطلاعات در پروتکل TCP/IPرا بنویسید.
۵. انواع استراتژی‌های امنیتی حاکم بر شبکه‌های رایانه‌ای را نوشته و توضیح دهید.
۶. پنج نوع از حملات رایج در شبکه‌ها را نام ببرید.
۷. نقش‌تروجان‌ها در ناامنی شبکه را توضیح دهید.
۸. ضمن توضیح نقش فایروال‌ها در امنیت شبکه، ارتباط بین عادات امنیتی و فایروال‌ها را توضیح دهید.
۹. دلایل نقد پذیری ISMS در امنیت شبکه را بنویسید.
۱۰. نفوذگران در شبکه‌ها به دنبال چه چیزی می‌گردند؟ توضیح دهید.

۶

فصل ششم : امنیت بانک‌های اطلاعاتی

آن چه در این فصل می‌خوانید:

- **تعریف بانک اطلاعاتی**
- **تاریخچه بانک اطلاعاتی دیجیتال**
- **تهدیدات و فرصت‌ها در بانک‌های اطلاعاتی**
- **انواع بانک‌های اطلاعاتی دیجیتال**
- **رمز در بانک اطلاعاتی**
- **ثبت وقایع در بانک اطلاعاتی**
- **ضعف‌های مکانیزم امنیتی ثبت وقایع**
- **دسترسی به بانک اطلاعاتی**
- **رمز نگاری در بانک اطلاعاتی**
- **پشتیبان گیری از بانک اطلاعاتی**

۶- امنیت بانک‌های اطلاعاتی

۶-۱- تعریف بانک اطلاعاتی

امروزه اطلاعات دیجیتال انواع و اقسام مختلفی پیدا کرده است و علاوه تنوع میزان تولید آن نیز بسیار بیش‌تر از گذشته شده است . به منظور دسترسی طبقه بندی شده و آسان به اطلاعات ، می‌بایست به نوعی این اطلاعات را سازمان‌دهی نمود تا بتوان به اطلاعات مرتبط در زمان کوتاهی دسترسی پیدا نمود. علاوه بر دسترسی آسان و سریع به اطلاعات می‌بایست اطمینان نسبی ایجاد گردد تا اطلاعات مرتبط از قلم نیفتاده و در تصمیم گیری‌ها و تصمیم سازی‌ها دخالت نمایند. امروزه این وظیفه به فایل‌های اطلاعاتی مرتبط به هم که با هدف مشخصی این وظیفه را انجام داده و با طراحی از پیش تعیین شده اطلاعات را در اختیار افراد مجاز قرار داده و این اطمینان را برای کاربران مجاز ایجاد می‌نماید را بانک‌های اطلاعاتی به عهده دارند. در حال حاضر تقریباً تمام اطلاعات مورد نیاز در سیستم‌های عمومی و خصوصی در بانک‌های اطلاعاتی متمرکز شده و از این طریق قابل دست‌یابی می‌باشد. همان‌گونه که کاربران مجاز قادر به دسترسی به این بانک‌ها می‌باشند افراد غیر مجاز نیز با در نظر گرفتن تمهیداتی قادر خواهند بود به صورت آشکار یا پنهان به این بانک‌ها دسترسی داشته و از اطلاعات آن‌ها بهره‌برداری سو نمایند . با توجه به این که در بانک‌های اطلاعاتی ، اطلاعات به صورت طبقه‌بندی شده و آماده استفاده قرار می‌گیرند به این خاطر عناصر غیر مجاز تلاش بیش‌تری را برای دسترسی به این اطلاعات داشته و در صورت دسترسی به آن‌ها می‌توانند به انبوهی از اطلاعات مرتبط به هم دسترسی داشته باشند . به همین خاطر امنیت بانک‌های اطلاعاتی از اهمیت ویژه‌ای برخوردار است.

۶-۲- تاریخچه بانک اطلاعاتی دیجیتال

بعد از آن که استفاده از میکرو رایانه‌ها عمومیت یافت فن‌آوری اطلاعات به سمت استفاده از میکرو رایانه‌ها گرایش پیدا نمود . در ابتدای استفاده از بانک‌های اطلاعاتی سیستم‌های تک کاربره استفاده می‌شدند و سپس هنگامی که میکرو رایانه‌ها در گروه‌های کاری وسیع‌تری به هم

مرتبط شدند فن‌آوری بانک‌های اطلاعاتی نیز به سمت مجموعه‌ای از گروه‌های کاری به نام کاربردهای Client Server هدایت شدند و بالاخره تلاشی که امروزه در حال انجام است مجتمع نمودن بانک‌های اطلاعاتی متفاوت در یک شکل واحد و سازگار به نام بانک‌های اطلاعاتی توزیع شده می‌باشد. یکی از مسائلی که در بانک‌های اطلاعاتی توزیع شده وجود دارد آن است که تمام داده‌های سازمانی بین رایانه‌های بزرگ پخش شده است و این رایانه‌ها زمانی که داده‌ها را پردازش می‌کنند باهم در ارتباط هستند . از اهداف سیستم‌های بانک اطلاعاتی توزیع شده آن است که به هر کاربر این احساس القا کند که او تنها استفاده کننده سازمانی می‌باشد و در عین حال همان سازگاری و هماهنگی که در هنگام عدم استفاده از بانک‌های اطلاعاتی توزیع شده را دارا بوده داشته باشند .

از مسائل دیگر بانک‌های اطلاعاتی توزیع شده امنیت و کنترل آن‌ها می‌باشد

۶-۳- تهدیدات و فرصت‌ها در بانک‌های اطلاعاتی

بانک‌های اطلاعاتی دارای فرصت‌ها و تهدیدات مختلفی می‌باشد.

مزایا و ویژگی‌های بانک اطلاعاتی :

۱. امکان مدل سازی داده‌های عملیاتی بر اساس روابط و قواعد خاص
۲. ذخیره و بازیابی داده‌ها براساس یک کنترل متمرکز و کارا
۳. شاخص گذاری و سایر امکانات ذخیره سازی کارا
۴. اشتراک داده‌ها بین کاربران
۵. کاهش افزونگی داده
۶. سهولت دست‌یابی به داده
۷. تامین جامعیت و پیش‌گیری از تناقض و ادغام
۸. تامین امنیت داده‌ها
۹. امکان‌ترمیم داده‌ها یا ریکاوری
۱۰. تامین استدلال داده‌ای در دو سطح فیزیکی و منطقی
۱۱. بهینه سازی پرس‌وجوها
۱۲. تهدیدات بانک‌های اطلاعاتی:
۱۳. امکان دسترسی به اطلاعات متمرکز

۱۴. دسترسی پنهان به اطلاعات متمرکز
۱۵. امکان اعمال تغییرات ناخواسته در اطلاعات
۱۶. جابه‌جایی و شکست در اطلاعات
۱۷. مشکلات در تامین امنیت توزیع شده
۱۸. پنهان سازی نرم‌افزارهای مخرب در بانک‌های اطلاعاتی
۱۹. از دست دادن بخش وسیعی از اطلاعات در صورت عدم پیش بینی‌های اولیه

۶-۴- انواع بانک‌های اطلاعاتی دیجیتال

بانک‌های اطلاعاتی به لحاظ ساختاری انواع و اقسام مختلفی دارند و با توجه به نوع گستردگی با مشکلات امنیتی خاص روبرو می‌باشند. در این قسمت امنیت بانک‌های اطلاعاتی با توجه به گستره جغرافیایی آن‌ها بررسی می‌شوند.

۶-۴-۱- متمرکز

در بانک‌های اطلاعاتی متمرکز کلیه اطلاعات و پرس‌وجوها و گزارشات مرتبط با بانک اطلاعاتی در یک فایل و به صورت منسجم قرار گرفته است . در صورت دسترسی با این فایل ، کلیه اطلاعات بانک اطلاعاتی قابل دسترسی بوده و تغییرپذیر می‌باشد. از محاسن این‌گونه بانک‌ها امکان برنامه نویسی سریع و جابه‌جایی و مدیریت راحت و آسان بر آن‌ها می‌باشد و این مسئله باعث شده است تا بسیاری از کاربران خانگی یا دارندگان اطلاعات با حجم کم از این گونه بانک‌ها استفاده نمایند .

۶-۴-۱-۱- ساختار

ساختار این بانک‌های اطلاعاتی یک پارچه بوده و تمام اطلاعات و رابطه‌ها و گزارشات و دسته بندی‌ها واندیک سازی‌ها و مخصوصاً کنترل‌های امنیتی در یک فایل قرار می‌گیرند. در صورت وقوع هر گونه مشکلی برای این فایل کل اطلاعات به خطر خواهند افتاد.

۶-۴-۱-۲- نمونه‌ها

نمونه بسیار رایج این بانک اطلاغاتی ، فایل‌های اکسس می‌باشد که امروزه به صورت گسترده توسط کاربران عمومی مورد استفاده قرار می‌گیرد.

۶-۴-۱-۳- امنیت

امنیت در این گونه بانک‌های اطلاعاتی را از دو بُعد می‌توان بررسی نمود. از زاویه دید فرصت ، این گونه بانک‌های اطلاعاتی را می‌توان سریع‌تر جابه‌جا نمود و در جابه‌جایی کم‌تر با مشکل فراموشی در جابه‌جایی متعلقات بانک روبرو خواهیم بود لیکن از بعد تهدید شناسی ، در صورتی که این تک فایل به علت عدم مراقبت‌های لازم به دست عناصر غیر مجاز بیفتد ، کلیه اطلاعات قابل خدشه دار بودن می‌باشد و نمی‌توان با تمهیداتی خارج از فایل بانک اطلاعاتی را ایمن نگه داشت و صرفاً باید تلاش نمود بانک اطلاعاتی به صورت فیزیکی از دسترسی دیگران دور باشد.

۶-۴-۲- نیمه متمرکز

این‌گونه بانک‌های اطلاعاتی نیمه گسترده می‌باشند و اطلاعات بانک‌های اطلاعاتی و گزارشات و فایل‌های پرس‌وجو و فایل امنیتی مربوط به کاربران در فایل‌های مختلفی قرار می‌گیرند. ممکن است این فایل‌ها در یک محیط قرار گرفته یا این که در محیط‌های قابل دسترس متفاوت توزیع گردند.

۶-۴-۲-۱- ساختار

ساختار این گونه بانک‌های اطلاعاتی توزیع پذیر می‌باشند . اطلاعات در فایل‌های مختلف ذخیره شده و اندیکس آن‌ها در لایه‌های مختلف نگهداری می‌شوند. فایل‌ها توزیع پذیر بوده و امکان بکارگیری از ذخیره سازهای داخلی و خارجی برای حفظ و نگهداری فایل‌ها میسر می‌شوند.

۶-۴-۲-۲- نمونه‌ها

نمونه این گونه بانک‌ها ، بانک‌های اطلاعاتی مدیریت شده با SQL می‌باشد.

۶-۴-۲-۳- امنیت

با توجه به این که هر کدام از قسمت‌های بانک اطلاعاتی در فایل جداگانه و احیاناً محیط جداگانه نگهداری می‌شود در صورت دسترسی افراد غیر مجاز به این گونه بانک‌ها صرفاً بخشی از بانک اطلاعاتی مورد هجمه واقع شده و دیگر قسمت‌ها محفوظ باقی می‌مانند.

۶-۴-۳- غیر متمرکز

در دنیای به شدت رقابتی امروز، اطلاعات به عنوان یکی از فاکتورهای تولیدی مهم پدیدار شده است. در نتیجه تلاش برای استخراج اطلاعات از داده‌ها توجه بسیاری از افراد دخیل در صنعت اطلاعات و حوزه‌های وابسته را به خود جلب نموده است.

حجم بالای داده‌های دائماً در حال رشد در همه حوزه‌ها و نیز تنوع آن‌ها به شکل داده متنی، اعداد، گرافیک‌ها، نقشه‌ها، عکس‌ها، تصاویر ماهواره‌ای و عکس‌های گرفته شده با اشعه ایکس نمایان‌گر پیچیدگی کار تبدیل داده‌ها به اطلاعات است. علاوه بر این، تفاوت وسیع در فرآیندهای تولید داده مثل روش آنالوگ مبتنی بر کاغذ و روش دیجیتالی مبتنی بر رایانه ، مزید بر علت شده است. استراتژی‌ها و فنون متعددی برای گردآوری، ذخیره، سازمان‌دهی و مدیریت کارآمد داده‌های موجود و رسیدن به نتایج معنی دار بکار گرفته شده‌اند. به‌علاوه، عمل‌کرد مناسب ابرداده که داده‌ای درباره داده است در عمل عالی بنظر می‌رسد.

پیش‌رفتهای حاصله در علم اطلاع رسانی و تکنولوژی اطلاعات، فنون و ابزارهای جدیدی برای غلبه بر رشد مستمر و تنوع بانک‌های اطلاعاتی تامین می‌کنند. این پیش‌رفتها هم در بعد سخت‌افزاری و هم نرم‌افزاری حاصل شده‌اند. ریزپردازنده‌های سریع، ابزارهای ذخیره داده‌های انبوه پیوسته و غیر پیوسته، اسکنرها، چاپگرها و دیگر ابزارهای جانبی نمایانگر پیش‌رفتهای حوزه سخت‌افزار هستند. پیش‌رفتهای حاصل در نظام‌های مدیریت بانک اطلاعات در طی چهار دهه گذشته نمایانگر تلاش‌های بخش نرم‌افزاری است. این تلاش‌ها در بخش نرم‌افزار را می‌توان به‌عنوان یک حرکت پیش‌رونده از ایجاد یک بانک اطلاعات ساده تا شبکه‌ها و بانک‌های اطلاعاتی رابطه‌ای و سلسله مراتبی برای پاسخ‌گویی به نیاز روزافزون سازمان‌دهی و بازیابی اطلاعات ملاحظه نمود. بدین منظور در هر دوره، نظام‌های مدیریت بانک اطلاعاتی مناسب سازگار با نرم‌افزار سیستم عامل و سخت‌افزار رایج گسترش یافته‌اند. در این رابطه می‌توان از محصولاتی مانند، Oracle، Sybase، Unify،Dbase-IV و غیره نام برد.

داده کاوی یکی از پیش‌رفتهای اخیر در راستای فن‌آوری‌های مدیریت داده‌هاست. داده کاوی مجموعه‌ای از فنون است که به شخص امکان می‌دهد تا ورای داده پردازی معمولی حرکت کند و به استخراج اطلاعاتی که در انبوه داده‌ها مخفی یا پنهان است کمک می‌کند.

امروزه با توجه به گستردگی اطلاعات در ساختارهای عمومی و دولتی تلاش می‌نمایند تا از روش‌های غیر متمرکز برای ثبت و نگهداری اطلاعات استفاده نمایند تا علاوه بر پوشانندگی گسترده اطلاعات ، تفکیک پذیری اطلاعات را اعمال نمایند.

۶-۴-۳-۱- ساختار

ساختار در این گونه بانک‌های اطلاعاتی کاملا توزیعی می‌باشند. و منابع ذیل به شکل‌های مختلف و توزیع شده در این گونه بانک‌ها به کار گرفته می‌شوند.

- پایگاه داده‌های رابطه‌ای
- انبارهای داده
- فایل‌ها
- وب
- پایگاه‌های داده شیءگرا
- چند رسانه‌ای

۶-۴-۳-۲- نمونه‌ها

تمام بانک‌های اطلاعاتی استفاده شده در سازمان‌های بزرگ و بانک‌های اقتصادی و سیستم‌های داده کاوی اطلاعات هوشمند از این نوع بوده و رایج‌ترین نوع استفاده از بانک‌های اطلاعاتی می‌باشد.

۶-۴-۳-۳- امنیت

با توجه به این که انبوهی از اطلاعات در این‌گونه بانک‌های اطلاعاتی نگهداری شده و از سیستم‌های هوشمند برای تولید و بازیابی اطلاعات در این بانک‌ها استفاده می‌شود و معمولاً تکنولوژی بهره‌برداری از این‌گونه داده کاوی اطلاعات وارداتی بوده و تکنولوژی غیر بومی بوده و اطلاعات استراتژیک در این‌گونه ابزار جمع آوری و پردازش می‌شوند تلاش افراد و ساختارهای غیر مجاز همیشه بر این بوده است تا بتوانند با استفاده از پمپ پاژ تکنولوژی و وابسته سازی دسترسی خود را به این‌گونه بانک‌های اطلاعاتی به صوت مستمر ادامه داده و به اطلاعات در مبدا و زمان تولید دسترسی داشته باشند. امنیت در این گونه بانک‌هاترکیبی از اجزا مختلف می‌باشد و نمی‌توان با نگاه بسیط صرفاً نرم‌افزاری و یا سخت‌افزاری به آن نگاه کرد و می‌بایست عوامل دیگری همچون ارتباطات و کاربران و نوع اطلاعات را به آن اضافه نمود.

۶-۵- رمز در بانک اطلاعاتی

در بانک اطلاعاتی مهم‌ترین عامل دسترسی به بانک اطلاعاتی نام کاربری و رمز می‌باشد. نام کاربری آشکار بوده و هر کاربر مجازی که اختیار دسترسی به بانک اطلاعاتی را داشته باشد

الزاماً دارای نام کاربری می‌باشد. به منظور امکان کنترل دسترسی کاربران مختلف به بانک اطلاعاتی توصیه می‌شود از نام‌های کاربری یکسان برای کاربران مختلف استفاده نشود و هر استفاده کننده دارای نام کاربری متفاوتی باشد. در صورتی که نام کاربری فاقد رمز باشد هر فردی که به صورت فیزیکی به بانک اطلاعاتی دسترسی داشته باشد این امکان را خواهد داشت که به مجرد کلیک کردن بر روی نام کاربری به بانک اطلاعاتی دسترسی داشته و از اطلاعات آن بهره‌برداری نماید. لذا توصیه می‌شود نام کاربران همیشه همراه با رمز مورد نظر ایمن سازی گردد. رمز در بانک اطلاعاتی دارای انواع و اقسام مختلفی بوده و در مراحل مختلف به کار گرفته می‌شود.

۶-۵-۱- رمزهای پیش فرض

برخی از رمزها پیش فرض بوده و در زمان نوشتن نرم‌افزار کاربردی بر روی بانک اطلاعاتی قرار داده می‌شوند . هرکس که این رمزها را بداند بدون این که نیاز به این داشته باشد تا رمز مربوط به هر کاربر را بداند به راحتی خواهد توانست به اطلاعات دسترسی داشته و از آن‌ها کپی تهیه نموده و از سیستم خارج نماید. رمزهای پیش فرض معمولاً به دو شکل می‌تواند وجود داشته باشد :

- ایجاد شده توسط برنامه‌ای که با آن بانک اطلاعاتی نوشته می‌شود
- ایجاد شده به وسیله نویسنده نرم‌افزاری که بانک اطلاعاتی را می‌نویسد

در هر دو حالت توصیه می‌شود به مجرد تهیه یک بانک اطلاعاتی رمزهای پیش فرض را یا غیر فعال نموده و یا این که آن را با رمزهای مدنظر تعویض نمائید زیرا هر کسی که دارای این رمزها باشد عملاً مالک بانک اطلاعاتی و اطلاعاتی که به آن وارد می‌شود خواهد بود و در آینده دیگران خواهند توانست با به‌دست اوردن این رمزها به صورت پنهان و غیر مجاز به اطلاعات دسترسی داشته باشند.

۶-۵-۲- رمزهای نرم‌افزار نویسنده بانک اطلاعاتی

هر نرم‌افزاری که با آن برنامه‌های کاربردی بانک اطلاعاتی نوشته می‌شود معمولاً دارای رمزهای از پیش تعرف شده‌ای می‌باشند که برای دست‌یابی به برنامه نوشته شده مورد استفاده قرار می‌گیرد. این رمزها در حالت عادی صرفاً می‌تواند به کدهای برنامه نویسی دسترسی داشته باشند و برنامه نویسان از آن برای رفع اشکال کدهای برنامه نویسی در شرایط خاص استفاده

می‌نمایند . لیکن باید این نکته را مد نظر قرار داد که اگر کسی اختیار دست‌کاری نمودن کدهای برنامه نویسی را داشته باشد عملاً می‌تواند با کد نویسی جدید راه دسترسی به اطلاعات را هموار ساخته و به شکل دلخواه به اطلاعات تولید شده در گذشته دسترسی داشته باشد و برای آینده نیز برنامه ریزی نماید. اولین اقدام برای استفاده از بانک اطلاعاتی پیدا کردن این رمزها و تغییر آن می‌باشد.

۶-۵-۳- رمزهای کاربردی بانک اطلاعاتی

از طریق این رمزها کاربران مجاز قادر خواهند بود تا به اطلاعات مشخص شده دسترسی داشته باشند. به دست آوردن این رمزها به منزله به‌دست آوردن اطلاعات مربوطه می‌باشد لذا می‌بایست کاربران در حفظ و نگهداری آن دقت لازم را داشته باشند.

۶-۵-۴- رمزهای مدیریتی بانک اطلاعاتی

مدیران بانک‌های اطلاعاتی قادر می‌باشند به وسیله رمزهای مدیریتی به کلیه اطلاعات و عمل‌کرد و تغییرات مربوط به کلیه کاربران دسترسی داشته باشند. این رمزها یکی از قربانیان اصلی افراد غیرمجاز می‌باشد زیرا می‌دانند با به‌دست آوردن این گونه رمزها عملاً می‌توانند به کل بانک اطلاعاتی با دسترسی بالا دسترسی داشته و کلیه ردپاهای دسترسی را به روش مطلوب پاک نمایند.

۶-۵-۵- انواع رمز نگاری

۶-۵-۵-۱- رمزنگاری متقارن

یک الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند. بیش‌ترین شکل استفاده از رمزنگاری که در کارت‌های هوشمند و البته در بیشتر سیستم‌های امنیت اطلاعات وجود یا DEA [۱] دارد که بیش‌تر به‌عنوان DES شناخته می‌شود. DES یک محصول دولت ایالات متحده است که امروزه به‌طور وسیعی به‌عنوان یک استاندارد بین‌المللی شناخته می‌شود. بلوک‌های ۶۴بیتی دیتا توسط یک کلید تنها که معمولاً ۵۶بیت طول دارد، رمزنگاری و رمزگشایی می‌شوند. DES از نظر محاسباتی ساده است و به‌راحتی می‌تواند توسط پردازنده‌های کند (به‌خصوص آنهایی که در کارت‌های هوشمند وجود دارند) انجام گیرد.

---

[۱] data encryption algorithm

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

کلیدهای DES۴۰بیتی امروزه در عرض چندین ساعت توسط رایانه‌های معمولی شکسته می‌شوند و بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی اعتبار استفاده شود. کلید ۵۶بیتی عموماً توسط سخت‌افزار یا شبکه‌های به‌خصوصی شکسته می‌شوند.

۶-۵-۵-۲- رمزنگاری نامتقارن

سیستم‌های کلید نامتقارن از کلید مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. بسیاری از سیستم‌ها اجازه می‌دهند که یک جزء (کلید عمومی۱) منتشر شود در حالیکه دیگری (کلید اختصاصی[۲]) توسط صاحبش حفظ شود. فرستنده پیام، متن را با کلید عمومی گیرنده کد می‌کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری می‌کند. به‌عبارتی تنها با کلید اختصاصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی‌تواند از متن کدشده به متن اصلی دست یابد، بنابراین پیام کدشده برای هرگیرنده‌ای به‌جز گیرنده مورد نظر فرستنده بی‌معنی خواهد بود. معمول‌ترین سیستم نامتقارن به‌عنوان RSA شناخته می‌شود (بر اساس حروف اول پدیدآورندگان آن مشخص شده است) [۳] . اگرچه چندین طرح دیگر وجود دارند. می‌توان از یک سیستم نامتقارن برای نشان دادن این که فرستنده پیام همان شخصی است که ادعا می‌کند استفاده کرد که این عمل اصطلاحاً امضا نام دارد. RSA شامل دو تبدیل است که هرکدام احتیاج به بتوان‌رسانی ماجولار با توانهای خیلی طولانی دارد:

امضا، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند؛ رمزگشایی عملیات مشابه‌ای روی متن رمزشده اما با استفاده از کلید عمومی است. برای تایید امضا بررسی می‌کنیم که آیا

---

[۱] public key
[۲] private key
[۳] Rivest ،Shamir و Adlemen

این نتیجه با دیتای اولیه یکسان است؛ اگر این‌گونه است، امضا توسط کلید اختصاصی متناظر رمز شده است.

۶-۵-۵-۲-۱- کلید عمومی

کلید عمومی اعداد یا کلماتی که با یک شخص یا سازمان در ارتباط می‌باشد. کلید عمومی جزئی از جفت کلید عمومی/خصوصی می‌باشد و به صورت عمومی در دسترس کسانی که قصد انتقال اطلاعات رمز شده را دارند، می‌باشد.

۶-۵-۵-۲-۲- کلید خصوصی

کلید خصوصی اعداد یا کلماتی که با یک شخص یا سازمان در ارتباط می‌باشد. کلید خصوصی جزئی از جفت کلید عمومی/خصوصی می‌باشد. کلید خصوصی فقط در دسترس مالک جفت کلید عمومی/خصوصی می‌باشد و برای بازگشایی اطلاعاتی که توسط کلید عمومی رمزگذاری شده استفاده می‌شود.

۶-۶- سوالات خودآزمایی

۱. بانک اطلاعاتی را تعریف نمایید.
۲. تهدیدات و فرصت‌ها در بانک‌های اطلاعاتی سنتی و دیجیتال چه اختلافاتی با یک‌دیگر دارند؟
۳. انواع رمز در بانک اطلاعاتی را نوشته و توضیح دهید.
۴. ثبت وقایع بانک اطلاعاتی چه نقشی می‌تواند در امنیت آن داشته باشد.
۵. اصطلاحات زیر را توضیح دهید.
۶. ثبت وقایع اتفاقی
۷. ثبت تغییرات در بانک اطلاعاتی
۸. ثبت errors
۹. ثبت تهیه پشتیبان
۱۰. دسترسی به یک بانک اطلاعاتی از چه روش‌هایی صورت می‌پذیرد. توضیح دهید.
۱۱. رمز نگاری چه تأثیری در امنیت بانک اطلاعاتی دارد؟
۱۲. انواع شیوه‌های تهیه پشتیبان از بانک اطلاعاتی را نوشته و توضیح دهید.
۱۳. مدیریت بانک اطلاعاتی چه نقشی می‌تواند در اهمیت آن داشته باشد.

•

۷۰

فصل هفتم : امنیت اتوماسیون اداری

آن چه در این فصل می‌خوانید:

- تعریف اتوماسیون اداری
- تاریخچه اتوماسیون اداری
- انواع اتوماسیون اداری
- انواع پایلوت اتوماسیون اداری
- امنیت اتوماسیون اداری
- مدل‌های کنترل دسترسی در اتوماسیون اداری
- ثبت اطلاعات و وقایع بهره‌برداری از اتوماسیون اداری
- نظارت امنیتی و کنترل بر اتوماسیون اداری
- انواع دسترسی به اتوماسیون اداری
- استراژی حاکم بر بهره‌برداری از اتوماسیون اداری

۷- امنیت اتوماسیون اداری

۷-۱- تعریف اتوماسیون اداری

بسیاری از تکنولوژی‌های جدید بر پایه این جمله بوجود آمده‌اند "انسان فکر کند، ماشین کار کند". با وجود گذشت سال‌ها از پیاده سازی انواع سیستم‌های مکانیزه مالی و صنعتی در سازمان‌ها و موسسات اقتصادی، امور اداری و دفتری و گردش اسناد مالی اغلب این موسسات به طریقه سنتی انجام می‌گیرد. سرعت پایین، افزایش بوروکراسی، وابسته شدن سیستم به افراد و نیز عدم هماهنگی این روش با سیستم‌های مکانیزه سبب افزایش قابل ملاحظه خطاهای انسانی و کاهش بهره وری در سازمان‌ها شده است.

نتیجه اهداف،اندیشه‌ها و اقدامات انجام شده در هر سازمان به‌صورت اسناد و مدارک نگهداری می‌شود. این اسناد که با صرف وقت و هزینه‌های زیاد فراهم می‌آیند، حاوی اطلاعات و تجربیات گران‌بهایی می‌باشد که در دست‌یابی به اهداف سازمان نقش مهمی داشته و یکی از ابزارهای مهم مدیریت در تهیه برنامه‌ها و تصمیم گیری‌های استراتژیک محسوب می‌گردد.

حجم کارها و اهمیت اطلاعات در کلیه سازمان‌ها و شرکت‌ها با وجود استفاده از پرسنل متعدد شاهد رشدی روزافزون است. برنامه‌ریزی، سازمان‌دهی، کنترل و نظارت بر عمل‌کرد فعالیت‌های درون سازمانی یکی از مهم‌ترین معیارها و پیش نیازها در توسعه و کاربرد فن‌آوری اطلاعات در سازمان‌های امروزی محسوب می‌شوند. تحقیقات گروه (تحقیقات انجمن مدیریت جریان کار[۱] - ۲۰۰۶) نشان می‌دهد سازمان‌ها و شرکت‌های سنتی در محصولات و خدمات خود عملاً تنها از ۳۰٪ زمان فرآیندها ارزش افزوده دریافت می‌کنند و از ۷۰٪ زمان باقیمانده غیر از اتلاف وقت و هزینه چیزی عایدشان نمی‌شود. این آمار حتی در شرکت‌ها و بنگاه‌های اقتصادی موفق که گردش کاری سنتی را دنبال می‌کنند به‌صورتی واضح‌تر نمود پیدا می‌کند.

خودکارسازی اداری مجموعه‌ای از روش‌های کاری و نرم‌افزار و سخت‌افزار رایانه است که برای ذخیره و بازیابی و مبادله اسناد و اطلاعات اداری به کار می‌رود.

---

[۱] WFMC

۷-۲- تاریخچه اتوماسیون اداری

امروزه مدیریت برگردش کار و مکاتبات اداری و هم‌چنین مدیریت زمان در سازمان‌ها و موسسات اقتصادی به کلی متحول شده است و استفاده از روش‌های کند و مشکل ساز اداری غیرمکانیزه قابل قبول نمی‌باشد. حجم بالای اطلاعات و مکاتبات و دسترسی کُند ، مسئولین و مدیران را که به مدیریت زمان در مجموعه تحت رهبری خود بها می‌دهند، به سوی اتوماسیون اداری در ابعاد مختلف رهنمون ساخته است .

اتوماسیون اداری ، به‌ترین ابزار برای رسیدن به راه کارهای مفید در جهت صرفه جویی زمان و استفاده بهینه از وقت در سازمان می‌باشد . راه‌حل‌های مکانیزه به گردش مکاتبات سازمان سرعت بخشیده و هم‌چنین مدیریت بر گردش کارها را میسر می‌سازد. دراین فرآیند، حذف مکاتبات کاغذی ، صرفه جویی و استفاده بهینه از زمان ، عملی می‌گردد.

از زمانی که سیستم اداری متوجه گردید مشکلات فراوانی در رابطه با روش سنتی نگهداری و بازیابی و چرخش اطلاعات وجود دارد ، تلاش نمود تا با روش های نوین نسبت به حل این مشکلات اقدام نماید. ذیلاً به رئوس این مشکلات اشاره می‌گردد:

- دسترسی کُند به مکتوبات و زمان‌بر بودن فرآیندهای اداری
- عدم اطلاع از سوابق و چرخه نامه در سازمان و نداشتن ابزاری مناسب برای پی‌گیری نامه‌های مدت دار
- عدم دسترسی به گزارشات و اطلاعات جامع از نامه‌ها و مراودات سازمان
- اجرا نشدن سلسله مراتب اداری و به طور کلی سیاست‌های اداری
- عدم دسترسی و امکان رسیدگی به اطلاعات و کارها از خارج سازمان
- عدم امکان پی‌گیری یک نامه و چرخه طی شده آن درهر لحظه
- نبود نظارت بر نظام اداری ، گردش نامه و عمل‌کرد افراد
- کنترل سطح دسترسی کاربران به اطلاعات
- مشکلات بایگانی از لحاظ حجم و دسترسی کُند و محدودیت زمانی و موضوعی اطلاعات
- نگهداری و استفاده از دستگاه‌های متعدد فکس و مدون نبودن فکس‌های دریافتی

- مشکلات زمان‌بر ، بودن ارسال فکس‌های متعدد و مشخص نمودن زمان بندی ارسال
- نبودن یک محیط یک‌پارچه برای دسترسی به کل محتویات و اطلاعات مورد نظر شامل نامه‌ها، پیش‌نویس ، فکس‌ها، نامه‌های الکترونیکی ، کارهای ارجاعی ، اطلاعات پروژه‌ها و . . .
- مشکلات نظام اداری غیر مکانیزه (مدیریت کارها) به سمت خودکارسازی و اتوماسیون اداری حرکت کردند. توسعه علم و فن‌آوری رایانه‌ای به این امر کمک شایانی نمود.

۷-۳- انواع اتوماسیون اداری

اتوماسیون اداری با اهداف مختلفی در سازمان‌ها توسعه یافته‌اند که مهم‌ترین آن‌ها را می‌توان به شکل ذیل تقسیم بندی نمود:

- درگاه سازمانی
- کارتابل پرسنل
- تقویم و برنامه ریزی روزانه
- سیستم روابط عمومی
- بایگانی و آرشیو اسناد
- موتور جستجوی اسناد تحت وب
- مدیریت فرآیندهای کسب و کار
- موتور گردش کار
- طـراح گردش کار
- مدیریت صورت‌جلسات
- مدیریت دبیرخانه
- ارجاع الکترونیکی
- کتابخانه الکترونیک
- سیستم کنترل رفت و آمد اشخاص
- پردازش تصویر - تشخیص حرکت توسط دوربین مدار بسته

- تلفن گویا
- اطلاع رسانی گویا
- داشبوردهای دیجیتال مدیریت استراتژیک سازمان
- مدیریت ارسال و دریافت پیام کوتاه
- مدیریت ارسال و دریافت پیام چند رسانه‌ای
- مدیریت ارسال و دریافت فکس
- مدیریت ارسال و دریافت ایمیل
- دفترچه یادداشت روزانه
- گفتگو و تبادل پیغام
- مدیریت زمان‌بندی گزارش‌ها
- مدیریت و امنیت ۶ لایه
- گزارش ساز پویا
- تحلیل داده‌ها در کسب و کار هوشمند
- فرم ساز پویا
- دسترسی از راه دور به سیستم - تحت وب

برای دسترسی به این اهداف سازمان‌ها به یکی از سه طریق زیر نسبت به خودکارسازی اهداف اداری خود اقدام می‌نمایند:

۷-۳-۱- مستقل درون سازمانی

در این روش سازمان‌ها با استفاده از شبکه‌های مستقل رایانه‌ای خود اتوماسیون اداری را پیاده سازی می‌نمایند. چنان‌چه محدوده سازمانی این اقدام از شبکه داخلی سازمان فراتر نرفته و به شبکه‌های مخابراتی متصل نگردند می‌توان حداقل خطرات را بر آن مترتب دید و این به شرطی می‌باشد که علاوه بر نرم‌افزار و سخت‌افزار استفاده شده در شبکه با طراحی حفاظتی مسائل امنیتی کاربران و اطلاعات را نیز در نظر گرفته و برای آن راه حلی ارائه نمود. البته در این روش با توجه به عدم استفاده از ارتباطات در گسترش اتوماسیون اداری برخی از اهداف پوشیده نخواهد شد.

۷-۳-۲-ترکیبی درون سازمانی – MIS

در این روش سازمان‌های بزرگ تلاش دارند تا با استفاده از شبکه‌های مخابراتی ارتباط بین شبکه‌های مختلف درون سازمانی را با یک‌دیگر برقرار نموده و تمام سازمان را درگیر با سیستم اتوماسیون اداری نمایند . در این روش در صورت نزدیک بودن سازمان‌ها به یک‌دیگر اصلح استفاده از امکانات ارتباطی درون سازمانی که مستمرا بر آن نظارت می‌گردد می‌باشد و استفاده از سیستم‌های ارتباطی مخابراتی باعث اتصال شبکه‌های اتوماسیون اداری به سیستم مخابراتی بین‌المللی را فراهم نموده و از هر نقطه دنیا امکان تهدید اطلاعات انباشته شده در اتوماسیون اداری که به صورت MIS به هم پیوسته شده است فراهم می‌گردد. نباید این نکته را فراموش نمود که در صورت دسترسی دشمن به اطلاعات از روش پنهان و آماده به‌کار ، وی تلاش خواهد داشت این ارتباط را هرچه بیش‌تر پنهان نگهدارد تا امکان هرچه بیش‌تر استفاده سو را برای خود مهیا سازد.

۷-۳-۳-ترکیبی برون سازمانی – CBIS

در این روش سازمان‌های مختلف در گیر اداری با یک‌دیگر چاره‌ای به جزء استفاده از ارتباطات مخابراتی برای ارتباط با یک‌دیگر را ندارند . معمولاً برای یک ساختار بزرگ اداری ایجاد بستر ارتباطی موازی با سیستم مخابراتی کشور برای این کار مقرون به صرفه نخواهد بود و به همین خاطر میل سازمان‌ها در استفاده از شبکه‌های مخابراتی برای کاهش در هزینه‌ها می‌باشد. چنان‌چه در این روش ارتباطی از سیستم‌های مخابراتی بومی کشور که مرتبط با شبکه‌های بین‌المللی نمی‌باشند استفاده گردد خطرات کم‌تری اطلاعات آن سازمان‌ها را تهدید می‌کند . در صورت استفاده از سیستم‌های ارتباطی متصل به شبکه‌های مخابراتی بین‌المللی به راحتی افراد غیر مجاز خواهند توانست تا با اشرافیت بر ارتباطات به قلب سازمان‌ها که همان مراکز اسناد می‌باشند به راحتی نفوذ نموده و در مبدا تولید اطلاعات نسخه‌ای از آن را به‌دست آورند.

۷-۴- انواع پایلوت اتوماسیون اداری

همان گونه که گفته شد سازمان‌ها برای ایجاد ارتباط بین موجودیت‌های مختلف اتوماسیون اداری از سیستم‌های ارتباطی مختلفی استفاده می‌نمایند که می‌توان از آن‌ها به عنوان پایلوت و بستر ارتباطی نام برد.

۷-۴-۱- شبکه‌های سازمانی

ممکن است این بسترهای ارتباطی شبکه‌های مستقل درون سازمانی باشند. چنان‌چه این شبکه‌ها توسط طراحان بومی و با استفاده از تکنولوژی بومی طراحی شده و ارتباط آن‌ها با خارج از شبکه مسدود شده و عدم ارتباط استمرار سازمانی داشته و با تغییر در مدیریت‌ها این استراتژی حفظ گردد کم‌ترین خطرات متوجه اطلاعات سازمانی که در این بستر در حال حرکت می‌باشد متوجه خواهد شد.

۷-۴-۲- اینترنت

برخی از سازمان‌ها به علت مباحث اقتصادی یا تحت تاثیر تبلیغات نظام سلطه که همیشه اینترنت را به عنوان یک بستر مناسب و ارزان مخابراتی تبلیغ می‌نماید قرار گرفته و بدون این که متوجه خطرات بزرگ این مسئله باشند نسبت به این کار اقدام می‌نمایند و عملاً با بودجه و امکانات و هزینه خود امکان استفاده غیر مجاز دیگران از اطلاعات تولید شده را فراهم می‌شازند. با توجه به این که این دسترسی تا زمان استفاده از این پایلوت استمرار خواهد داشت می‌توان چنین نتیجه گیری نمود که نام سلطه با تبلیغات وسیع خود مدیران را تشویق به این کار خواهد نمود تا بتواند هرچه بیش‌تر با اشرافیت اطلاعاتی بر اینترنت به اطلاعات مورد نظر دسترسی داشته باشد.

۷-۵- امنیت اتوماسیون اداری

امنیت اتوماسیون اداری را نمی‌توان امری بسیط فرض نمود که صرفاً با تامین امنیت وارداتی بر روی شبکه و یا سخت‌افزار به آن دست یافت . امنیت سیستم‌های اتوماسیون اداری مسئله مرکبی است که عوامل بسیاری بر آن دخالت دارند.

۷-۵-۱- امنیت اتوماسیون اداری در مرحله طراحی

مرحله طراحی اولین مرحله شروع یک اتوماسیون اداری می‌باشد . در این مرحله سازمان کل اقداماتی را که انجام می‌دهد و انواع اطلاعاتی را که تولید می‌کند و افرادی را که اطلاعات تولید می‌کنند را به ریزه کاری‌های مربوطه به طراح سیستم معرفی می‌نماید.

۷-۵-۲- امنیت اتوماسیون اداری در مرحله برنامه نویسی

در مرحله برنامه نویسی بر مبنای طراحی انجام گرفته شده نرم‌افزار نویسان روش‌ها را تبدیل به برنامه نموده و ارتباط بین ساختارها را با کدهای برنامه نویسی تنظیم می‌نمایند.

۷-۵-۳- امنیت اتوماسیون اداری در مرحله بهره‌برداری

در مرحله بهره‌برداری کاربران مجاز به بهره‌برداری از اتوماسیون اداری صرفاً در چهارچوب برنامه نوشته شده قادر خواهند بود و خارج از آن هیچ اقدامی را نمی‌توانند انجام دهند و هرگونه درخواست تغییر می‌بایست مجدد طراحی و پیاده سازی گردد.

۷-۵-۴- امنیت اتوماسیون اداری در مرحله انتقال اطلاعات

در این مرحله کلیه اطلاعات تولید شده از طریق سیستم‌های ارتباطی که اجزا مختلف اتوماسیون اداری را به هم متصل می‌نماید صورت می‌پذیرد و عملاً هیچ اطلاعاتی خارج از این روش‌های ارتباطی نمی‌توانند مبادله گردند.

۷-۶- مدل‌های کنترل دسترسی در اتوماسیون اداری

برای کنترل دسترسی در اتوماسیون اداری مدل‌های مختلفی ارائه شده است. لیکن باید در استفاده از مدل، موارد ذیل را مد نظر قرار داد:

- بایستی مدلی ارائه شود تا تعیین گردد که چه دسترسی‌هایی مجاز و چه دسترسی‌هایی غیر مجاز است.
- پایگاه‌های داده با توجه به متمرکزسازی داده‌ها در آن بیش‌تر مورد توجه قرار می‌گیرند.
- مدل کنترل دسترسی نقش- مبنا به عنوان یک مدل کنترل دسترسی بسیار مرسوم و پرکاربرد مطرح است.

۷-۷- ثبت اطلاعات و وقایع بهره‌برداری از اتوماسیون اداری

دسترسی به اطلاعات در سیستم اتوماسیون اداری در زمان‌های مختلف و توسط کاربران مختلف و با استفاده از ابزار مختلف و برای بهره‌برداری‌های مختلف صورت پذیرفته و اقدامات مختلفی بر روی آن انجام می‌پذیرد . درصورت ثبت شدن این وقایع می‌توان با بررسی آن‌ها تحلیل جامعی در رابطه با اعتبار و روایی کار انجام شده ارائه نمود و اگر کلیه وقایع مرتبط با اتوماسیون اداری و دسترسی‌های مجاز و تلاش به منظور دسترسی غیر مجاز ثبت نگردند عملاً نمی‌توان هیچ کنترلی بر روند استفاده از این سیستم داشت . لذا سازمان‌های استفاده

کننده می‌بایست با طراحی دقیق و مشخص نمودن مسئول انجام این کار ، وقایع را ثبت و بهره‌برداری نمایند.

۷-۸- نظارت امنیتی و کنترل بر اتوماسیون اداری

با توجه به این که در اتوماسیون اداری کلیه اطلاعات مهم سازمان تجمیع شده و مسیر حرکت اطلاعات و نوع بهره‌برداری از آن و شیوه استفاده و قیمت آن برای سازمان در این سیستم متمرکز می‌گردد برای سازمان از اهمیت وافری برخوردار می‌باشد لذا می‌بایست به‌صورت دائم توسط ساختار مشخص شده‌ای در سازمان که در قبال اختیار داده شده دارای مسئولیت پاسخ‌گویی باشد نظارت و شیوه‌های دسترسی و بهره‌برداری از آن مورد دقت قرار گیرد.

۷-۹- انواع دسترسی به اتوماسیون اداری

برای استفاده از اتوماسیون اداری نیاز به دسترسی به اجزا اتوماسیون اداری می‌باشد که این دسترسی معمولاً به دو روش می‌تواند انجام شود:

۷-۹-۱- دسترسی مجاز

در این روش دسترسی ، توسط مدیر یا مدیران اتوماسیون اداری سطح دسترسی مورد نیاز هر فرد مشخص شده و بنابر وظیفه اداری و نیاز سازمانی و حیطه دسترسی کاربر مربوطه، سطح دسترسی وی تعریف شده و کاربر در حیطه تعریف شده مجاز به دسترسی به سیستم و استفاده از آن می‌باشد. کاربران قادر خواهند بود صرفاً در حیطه‌ای که برای آنان مشخص شده است حرکت نمایند و اختیار تولید اطلاعات و اعمال تغییرات در محدوده‌ای که برای آنان مشخص شده است را دارا می‌باشند و خارج از آن نمی‌توانند اقدامی انجام دهند . کلیه اقدامات انجام شده توسط کاربران مجاز ثبت شده و در قبال آن به لحاظ حقوقی پاسخ‌گو می‌باشند و با توجه به عدم انکارپذیری که در سیستم تعبیه شده است موظف به پاسخ‌گویی در قبال اقدامات انجام شده می‌باشند.

۷-۹-۲- دسترسی غیر مجاز

در دسترسی غیر مجاز کابران به صورت غیر مجاز و خارج از چهارچوب تعیین شده امکان دسترسی به سیستم را برای خود مهیا می‌سازند . در این نوع دسترسی که یا به‌وسیله کاربران کنجکاو برای ارضا حس کنجکاوی انجام شده یا این که توسط عوامل غیر مجاز برای اشرافیت بر اطلاعات تولید شده و دسترسی غیر مجاز به اطلاعات و بهره‌برداری سو از اطلاعات انجام می‌شود . در بسیاری از مواقع افراد غیر مجاز اولین اقدام خود را با استفاده از ضعف در مدیریت سیستم سو استفاده نموده و برای خود ایجاد نموده و به مرور نسبت به گسترش سطح دسترسی اقدام می‌نمایند. مهم‌ترین مطلب برای این گونه افراد عدم متوجه شدن مدیر سیستم یا سیستم کنترل کننده شیوه‌های دسترسی می‌باشد و تلاش دارند خود را به عنوان کاربر مجاز به سیستم معرفی نمایند تا در کنترل‌ها کم‌ترین مشکوکیت را ایجاد نموده و به این کار خود ادامه دهند.

نوع دیگر این سو استفاده کنندگان تولید کنندگان غیر بومی سخت‌افزار و نرم‌افزارهای استفاده شده در سیستم اتوماسیون اداری می‌باشد که با اهداف سلطه جویانه از ابتدای تولید این ابزار راه‌های نفوذی را تحت عنوان درپشتی[۱] یا نکات مدیریتی پنهان بر روی این سخت‌افزار و نرم‌افزار قرار داده‌اند تا ضمن هم‌خوانی با اقدامات آن‌ها و به مجرد استفاده در هر سیستمی خود را با آن هماهنگ نموده و نسبت به ارسال اطلاعات مد نظر و یا مدیریت پنهان بر سیستم استفاده نمایند این همان نیمه پنهان استفاده از ابزار غیر بومی و ناشناخته در مهم‌ترین قسمت‌های سازمان که همان مراکز اسناد و مراکز تولید اطلاعات هستند می‌باشد.

۷-۱۰- تهدیدات و فرصت‌های امنیت شبکه در امنیت اتوماسیون اداری

نرم‌افزارهای اتوماسیون اداری دارای فرصت‌ها و تهدیدات بی‌شماری می‌باشند . با توجه به این که در ابتدای فصل به فرصت‌های آن اشاره گردید در این قسمت به برخی از تهدیدات آن اشاره می‌گردد.

۷-۱۰-۱- آسیب‌پذیری استفاده از اتوماسیون اداری در بسته

برای مراکز مهم و حیاتی استفاده از این گونه نرم‌افزارها (هرچند تولید داخل کشور باشد) توصیه نمی‌شود و پیش‌نهاد می‌گردد با فرض تولید داخل بودن یک‌بار به صورت کامل با مهندسی مجدد کد خوانی شده و پس از تایید مورد بهره‌برداری قرار گیرد و به هیچ وجه نباید

---

[۱] backdoor

در مقابل شرکت‌های که اجازه دسترسی به منبع نرم‌افزاری را به مصرف کننده نمی‌دهند در این گونه مواقع کوتاه آمد.

۷-۱۰-۱-۱- اتوماسیون‌های اداری تولید داخل کشور

نرم‌افزارهای اتوماسیون اداری تولید داخل کشور به دو نوع می‌باشد . در نوع اول نرم‌افزار مربوطه توسط طراحان بومی داخل کشور طراحی شده و سپس نرم‌افزار نویسان داخل کشور با استفاده از تجربیات خود آن‌ها را تبدیل به کدهای نرم‌افزاری نموده و با توجه به نیازهای داخل کشور تولید شده و در اختیار مصرف کنندگان قرار می‌گیرد . این‌گونه نرم‌افزارهای نوشته شده درصدی از مشکلات امنیتی را نداشته و نسبت به دیگر انواع از مشکلات کم‌تری برخوردار می‌باشند.

۷-۱۰-۱-۲- اتوماسیون‌های اداری تولید خارج از کشور

این‌گونه نرم‌افزارها توسط دیگر کشورها با اهداف اقتصادی و بسیاری اوقات با داشتن پشت پرده اطلاعاتی نوشته شده و بیش‌تر با هدف اشرافیت اطلاعاتی بر اطلاعات تولید شده توسط دیگر کشورها با پوشش‌های علمی و اقتصادی و شرکتی به کشورهای مد نظر ارسال می‌گردد. این گونه نرم‌افزارها را شاید بتوان با قیمت کم‌تر خریداری یا به‌دست آورد لیکن این نکته را باید مدنظر داشت که نرم‌افزارهای آماده خریداری شده از خارج از کشور را نمی‌توان حتی با بررسی‌های مو شکافانه فنی بررسی کامل نموده و اختیار اطلاعات سازمان را به دست آن داد. این نرم‌افزارها معمولاً حلقه مفقوده طرح‌های اشرافیتی نظام سلطه مانند طرح اشلون را تکمیل می‌نمایند.

۷-۱۱- کنترل‌های در مسیر طراحی و برنامه نویسی اتوماسیون اداری

اگر چنان‌چه در سازمان اجازه شروع و اتمام طراحی و نوشتن نرم‌افزار اتوماسیون را به فرد و یا گروه یا شرکتی داده و انتظار این را داشت که در انتهای آماده سازی می‌توان آن را تست و کنترل امنیتی نمود ، معمولاً این کار امکان‌پذیر نمی‌باشد و در صورت امکان پذیر بودن توان و زمان لازم برای این کار وجود نخواهد داشت چون همیشه با فشار سازمان برای شروع کار روبرو خواهیم بود . پیش‌نهاد می‌گردد تیم کنترل کننده هم زمان با تیم طراحی و برنامه نویسی کار خود را شروع نموده و حتی یک قدم از آنان جلوتر حرکت نماید تا از موضع انفعالی خارج شده و با موضع بالاتری نسبت به این کار اقدام نماید.

۷-۱۲- تاثیر اتوماسیون اداری در تغییر حساسیت‌های امنیتی سازمان

یکی از آثار طبیعی استفاده از اتوماسیون اداری در یک سازمان چرخش کار از فضای سنتی به سمت دیجیتال می‌باشد و با توجه به فرآیندهای تعریف شده در سیستم برخی از فرآیندهای اداری دچار تحول می‌گردند. هر چند که بسیاری از تحولات ممکن است به نفع سازمان باشد لیکن در بررسی تحولات انجام شده می‌بایست نکات امنیتی مد نظر را مورد توجه قرار داد و با بصیرت و چشم باز آن‌ها را شناسایی کرده و پس از اشرافیت کامل بر محاسن آن و ممانعت از ایجاد تهدیدات جدید آن را قبول نمود.

۷-۱۳- سئوالات خودآزمایی

۱. تعریف اتوماسیون اداری را از دیدگاه امنیتی بنویسید.
۲. انواع اتوماسیون اداری را نوشته و توضیح دهید.
۳. مراحل ایمن سازی اتوماسیون اداری را نام ببرید.
۴. امنیت اتوماسیون اداری در مرحله بهره‌برداری را توضیح دهید.
۵. انواع مدل‌های کنترل دسترسی در اتوماسیون اداری را نوشته و توضیح دهید.
۶. انواع دسترسی به اتوماسیون اداری را نوشته و توضیح دهید.
۷. استراتژی‌های امنیتی حاکم در بهره‌برداری از اتوماسیون اداری را توضیح دهید.
۸. انواع خلاهای امنیتی در اتوماسیون اداری را نام ببرید .
۹. ارتباط تهدیدات و فرصت‌های امنیت شبکه با اتوماسیون اداری را توضیح دهید.
۱۰. نقش لایه‌های مختلف را در امنیت اتوماسیون اداری بنویسید.

•

۸

فصل هشتم : امنیت اینترنت

آن چه در این فصل می‌خوانید:

- **تعریف اینترنت**
- **تاریخچه اینترنت**
- **استراتژی نظام سلطه در طراحی اینترنت**
- **ساختار و پیکربندی کاربردی اینترنت**
- **نیمه پنهان ساختاری اینترنت از دیدگاه نظام سلطه**
- **جنگ اینترنتی**
- **اینترنت به عنوان اصلی‌ترین روش بر اشرافیت بر اطلاعات**
- **همکاری و هماهنگی بین سه عنصر اینترنت اشلون و فن‌آوری‌های هوشمند**
- **اطلاعات تبادلی از طریق اینترنت**

۸- امنیت اینترنت

۸-۱- تعریف اینترنت

با توجه به این که اصلی‌ترین و گران قیمت‌ترین کالا در عصر اطلاعات ، اطلاعات می‌باشد بهره‌برداران تلاش می‌نمایند تا با استفاده از شبکه‌های مختلف اطلاعات را با دیگران به اشتراک بگذارند تا افراد بیش‌تری بتوانند از آن‌ها در زمان واحد استفاده نمایند. یکی از راه‌های به اشتراک گذاشتن اطلاعات به هم پیوستن شبکه‌ها از طریق انواع روش‌های ارتباطی بوده که امروزه از آن با نام شبکه شبکه‌ها و یا اینترنت نام می‌برند.

امروزه حدود دو میلیارد کاربر در سراسر جهان از طریق این شبکه گستره به یک‌دیگر متصل شده و از اطلاعات هم‌دیگر استفاده می‌نمایند. با توجه به این که تمام افراد مرتبط با اینترنت قادر خواهند بود به شکل مجاز و غیر مجاز از اطلاعات دیگران بهره‌برداری مجاز و یا سو نمایند در این قسمت به نکات امنیتی که می‌بایست در بهره‌برداری از اینترنت مد نظر قرار گیرد، خواهیم پرداخت.

۸-۲- تاریخچه اینترنت

هفتاد سال پیش ، موشکی با نام «اسپونیک[۱]» با هدف قدرت نمایی توسط شوروی سابق به فضا ارسال و نشان می‌دهد دارای قدرتی است که می‌تواند شبکه‌های ارتباطی آمریکا را توسط موشک‌های بالستیک و دوربرد خود از بین ببرد. آمریکایی‌ها در پاسخ گویی به این اقدام روس‌ها، موسسه پروژه‌های تحقیقی پیش‌رفته[۲] را به‌وجود آوردند. هدف از تاسیس چنین موسسه‌ای، پژوهش و آزمایش برای پیدا کردن روشی بود که بتوان از طریق خطوط تلفنی، رایانه‌ها را به هم مرتبط نمود. به طوری که چندین کاربر بتوانند از یک خط ارتباطی مشترک استفاده کنند. در اصل شبکه‌ای بسازند که در آن داده‌ها به صورت اتوماتیک، بین مبدا و مقصد حتی در صورت از بین رفتن بخشی از مسیرها جابه‌جا و منتقل شوند. در اصل هدف "ARPA" ایجاد یک شبکه اینترنتی نبود و فقط یک اقدام احتیاطی در مقابل حمله احتمالی موشک‌های

---

[۱] Spotnik
[۲] ARPA

اتمی دوربرد بود. هر چند اکثر دانش امروزی ما درباره شبکه به‌طور مستقیم از طرح آرپانت[۱] گرفته شده‌است. شبکه‌ای که هم‌چون یک تار عنکبوت باشد و هر رایانه آن از مسیرهای مختلف بتواند با همتایان خود ارتباط داشته باشد و اگر یک یا چند رایانه روی شبکه یا پیوند بین آن‌ها از کار بیافتد بقیه باز هم بتوانند از مسیرهای تخریب نشده با هم ارتباط بر قرار کنند.

این ماجرا با وجودی که بخشی از حقایق به‌وجود آمدن اینترنت را بیان می‌کند اما نمی‌تواند تمام واقعیات مربوط به آن را تشریح کند. باید بگوئیم افراد مختلفی در تشکیل اینترنت سهم داشته‌اند. آقای باران[۲] یکی از مهم‌ترین آنهاست. آقای باران که در دوران جنگ سرد زندگی می‌کرد می‌دانست که شبکه سراسری تلفن آمریکا، توانائی مقابله با حمله اتمی شوروی سابق را ندارد. مثلاً اگر رئیس جمهور وقت آمریکا حمله اتمی متقابل را دستور دهد، باید از یک شبکه تلفنی استفاده می‌کرد که قبلاً توسط روس‌ها منهدم شده بود. در نتیجه، طرح یک سیستم مقاوم در مقابل حمله اتمی روس‌ها ریخته شد. آقای باران تشکیل و تکامل اینترنت را به ساخت یک بنا تشبیه کرد و معتقد بود، طی سال‌های اخیر هر کس، سنگی به پایه‌ها و سنگ‌های قبلی بنا اضافه می‌کند و انجام هر کاری وابسته به کارهای انجام شده قبلی است. بنابراین نمی‌توان گفت، کدام بخش از کار مهم‌ترین بخش کار بوده است و در کل پیدایش اینترنت نتیجه کار و تلاش گروه کثیری از دانشمندان است. داستان پیدایش اینترنت با افسانه و واقعیت در هم آمیخته شده‌است. (wikipedia. com)

پیدایش اینترنت به دهه ۱۹۶۰ برمی گردد. زمانی که دولت ایالات متحده براساس طرحی موسوم به "Arpa" مخفف " آژانس تحقیق پروژه‌های پیش‌رفته" که در آن زمان برای کارکردهای دفاعی به وجود آمده بود، این طرح را اجرا نمود. طرح این بود که رایانه‌های موجود در شهرهای مختلف (در آن زمان چیزی بنام رایانه شخصی وجود نداشت بلکه سازمان‌های بزرگ و دانشگاه‌ها و مراکز دولتی معمولاً دارای سیستم‌های رایانه بزرگ [۳] بودند) که هر کدام اطلاعات خاص خود را در آن ذخیره داشتند بتوانند در صورت نیاز با یکدیگر اتصال بر قرار نموده و اطلاعات را به یک‌دیگر منتقل کرده یا در صورت ایجاد بستر مناسب، اطلاعات را در حالت اشتراک[۴] قرار دهند. در همان دوران سیستم‌هایی به‌وجود آمده بودند که امکان ارتباط

---

[۱] ARPPA NET
[۲] Paul Baran
[۳] MainFrame
[۴] Share

بین رایانه‌های یک سازمان را از طریق مختص همان سازمان فراهم می‌نمودند به‌طوری که رایانه ای موجود در بخش‌ها یا طبقات مختلف با یک‌دیگر تبادل اطلاعات نموده و امکان ارسال نامه بین بخش‌های مختلف سازمان را فراهم می‌کردند که اکنون به این سیستم ارسال نامه یا پست الکترونیک می‌گویند. اما برای اتصال و ارتباط دادن این شبکه‌های کوچک و پراکنده که هر کدام به روش و استانداردهای خودشان کار می‌کردند استانداردهای جدید و مشخصی که همان پروتکل‌ها[۱] هستند توسط کارشناسان وضع شد. سرانجام درسال ۱۹۶۱ تعداد ۴ رایانه در ۲ ایالت مختلف با موفقیت ارتباط بر قرار کردند و با اضافه شدن واژه نت[۲] به طرح اولیه، نام آرپانت[۳] برای آن منظور شد. در دهه ۱۹۷۰ با تعریف پروتکل‌های جدیدتر از جمله "TCP" که تا به امروز رواج دارد و نیز مشارکت رایانه‌های میزبان[۴] بیش‌تر به آرپانت و حتی گسترده شدن آن به برخی نواحی فراتر از مرزهای ایالات متحده، آرپانت شهرت بیش‌تری یافت و ایده اینترنت همراه با جزئیات بیش‌تر راجع به شبکه‌های رایانه‌ی مطرح گشت تا این‌که طی سال‌های پایانی دهه ۱۹۷۰ شبکه‌های مختلف تصمیم گرفتند به صورت شبکه‌ای با یک‌دیگر ارتباط بر قرار نمایند و آرپانت را به‌عنوان هسته اصلی انتخاب کردند. بعدها در سال ۱۹۹۳ نام اینترنت۵ روی این شبکه بزرگ گذاشته شد. وب یا همان "www"که مخفف " تار جهان گستر۶" می‌باشد توسط آزمایشگاه اروپایی فیزیک ذرات ۷ به‌خاطر نیاز آن‌ها به دسترسی مرتب‌تر و آسان‌تر به اطلاعات موجود روی اینترنت ابداع گشت. در این روش اطلاعات به صورت مستنداتی صفحه‌ای۸ بر روی شبکه اینترنت قرار می‌گیرند و به‌وسیله یک مرورگر وب۹ قابل مشاهده هستند و هم اکنون کارکردهای بسیاری دارند. (wordpress. com)

---

[۱] Protocol
[۲] Net
[۳] ArpaNet
[۴] Host
[۵] Internet
[۶] World Wide Web
[۷] Cern
[۸] Page
[۹] WebBrowser

بنابراین وزارت دفاع آمریکا در یک پروژه نوع جدید از شبکه‌های بزرگ را طراحی کرد که حتی اگر یکی از بخش‌های آن از کار می‌افتاد باز هم می‌توانست به کار خود ادامه دهد. آن چه که کل این شبکه عظیم را به هم ارتباط می‌داد. مجموعه‌ای از قوانین ارتباطی یا به اصطلاح «پروتکل» بود که آنرا TCP/IP نامیدند.

اصولاً هر شبکه‌ای که از قوانین TCP/IP استفاده کند می‌تواند با هر شبکه دیگری که آن هم با قوانین TCP/IP کار می‌کند ارتباط برقرار کند و اگر در شبکه بزرگی که هر یک از شبکه‌های کوچک‌تر داخل آن از قوانین TCP/IP استفاده می‌کنند یک شبکه کوچک از کار بیافتد مابقی شبکه به کار خود ادامه خواهد داد.

نتیجه این پروژه پس از چندین سال همان شبکه جهانی اینترنت کنونی است که اکنون به صورت غیرنظامی گردیده و تمامی عرصه گیتی را تحت پوشش خود قرار داده است. (roshd. com)

۸-۳- استراتژی نظام سلطه در طراحی اینترنت

- شروع اینترنت یک اقدام تدافعی در جنگ سرد بین شوروی و آمریکا بوده است و در تقابل با اقدام نظامی شوروی که ارسال موشک به فضا بوده است صورت گرفته است و اصل آن برای پیدا کردن راهی نظامی – فنی برای اقدام تهاجمی شوروی‌ها علیه سیستم‌های مخابراتی امریکا بوده است.
- اولین بار ایده استقبال از اینترنت در نیروی هوایی امریکا و پنتاگون پشتیبانی گردید و با اهداف کاملاً نظامی شکل گرفت.
- ایده استفاده ازتحلیل‌گران و دانشمندان غیر نظامی برای کمک به اهداف نظامی شکل گرفت و این ایده به عنوان ایده غالب در بین اندیشمندان و سیاستمداران امریکایی به عنوان ایده برتر قبول شد .

- در دهه ۱۹۷۰ استراتژیست‌های نظام سلطه به این نتیجه رسیدند که بدون نقاب غیر نظامی زدن به اینترنت نمی‌توانند آن را در بین عامه مردم و نخبگان و دانشمندان و دانشگاهیان و . . . رایج سازند و به همین خاطر در این دهه تصمیم گرفتند ظاهر آن را از حالت نظامی خارج ساخته و در بین مردم رایج ساخته و پروتکل‌های ساده‌ای را که می‌توان با آن اعتماد مردم را جلب نمود ایجاد نمایند.

۸-۴- ساختار و پیکربندی کاربردی اینترنت

اینترنت امروزه به شبکه‌ی شبکه‌ها معروف گشته است و هر شبکه را می‌توان جزئی از اجزا اینترنت دانست و هر شبکه نیز از موجودیت‌های کوچک‌تری تشکیل شده است که با شناخت خطرات هر کدام از این موجودیت‌ها می‌توان خطرات کل سیستم را جمع بندی نمود. هر چند که از در کنار هم قرارگرفتن این موجودیت‌ها در بسیاری از مواقع خطرات با استفاده از هم گرائی‌های ایجاد شده بعضاً به صورت تصاعدی افزایش می‌یابد.

هر رایانه که به شبکه اینترنت متصل می‌گردد ، بخشی از شبکه تلقی می‌گردد. مثلاً می‌توان با استفاده از تلفن (منزل) به یک مرکز ارائه دهنده خدمات اینترنت[۱] متصل و از اینترنت استفاده کرد. در چنین حالتی رایانه مورد نظر به‌عنوان بخشی از شبکه بزرگ اینترنت محسوب خواهد شد. برخی از کاربران در ادارات خود و با استفاده از بستر ایجاد شده ، به اینترنت متصل می‌گردند. در مدل فوق ، کاربران در ابتدا از شبکه محلی نصب شده در سازمان استفاده می‌نمایند. شبکه فوق با استفاده از خطوط مخابراتی خاص یا سایر امکانات مربوطه به یک مرکز ارائه دهنده خدمات اینترنت متصل شده است . مرکز ارائه دهنده خدمات اینترنت نیز ممکن است به یک شبکه بزرگ‌تر متصل شده باشد. اینترنت ، شبکه‌ای است که از شبکه‌های بی‌شماری تشکیل شده است.

در اینترنت ، هزاران مرکز ارائه دهنده سرویس اینترنت بزرگ از طریق NAP در شهرهای متفاوت به یک‌دیگر متصل می‌گردند. در نقاط فوق (NAP[۲]) روزانه میلیاردها بایت اطلاعات جابه‌جا می‌گردد. اینترنت ، مجموعه‌ای از شبکه‌های بسیار بزرگ بوده که تمام آن‌ها از طریق

---

[۱] ISP
[۲] Network Access Points

NAP به یک‌دیگر مرتبط می‌گردند. در چنین حالتی هر رایانه موجود در اینترنت قادر به ارتباط با سایر رایانه‌های موجود در شبکه خواهد بود.

۸-۵- نیمه پنهان ساختاری اینترنت از دیدگاه نظام سلطه

با بررسی تاریخچه اینترنت مشخص می‌گردد که از ابتدا اینترنت با اهداف نظامی و توسط کشور امریکا به منظور افزایش سلطه و تسلط علمی و غیر علمی بر دیگر نقاط جهان و از طریق وزارت دفاع آمریکا شکل گرفته و به دیگر نقاط دنیا تسری پیدا نموده است .

۸-۵-۱- زیرساخت فنی و امنیتی اینترنت

هر ماشین موجود در اینترنت دارای یک شماره شناسائی منحصر به فرد است. این شماره شناسائی ، آدرس (IP)[۱] نامیده می‌گردد. پروتکل فوق مشابه یک زبان ارتباطی مشترک برای گفتگوی رایانه‌های موجود در اینترنت است . پروتکل ، به مجموعه قوانینی اطلاق می‌گردد که با استناد به آن گفتگو و تبادل اطلاعاتی بین دو رایانه میسر خواهد شد. IP دارای فرمتی به طور مثال :۲۱۱. ۲۷. ۶۵. ۱۳۸ است . به خاطر سپردن آدرس‌های IP به منظور دست‌یابی به رایانه مورد نظر، مشکل است . بدین منظور هر رایانه دارای نام انحصاری خود شده و از طریق سیستمی دیگر ، آدرس IP به نام درنظر گرفته شده برای رایانه ، نسبت داده می‌شود.

۸-۵-۲- دسترسی به سخت‌افزار محلی از طریق اینترنت

در یک شبکه سخت‌افزارها به انواع ذیل قابل تقسیم می‌باشد.

الف) انواع ابزار سخت‌افزاری نگهدارنده اطلاعات مانند رایانه سرور، تین کلاینت

ب) انواع سخت‌افزارهای ارتباطی مانند کابل کشی‌ها،هاب‌ها، سوئیچ‌ها، روترها

ج) انواع ابزار سخت‌افزاری کمکی مانند پرینترها، اسکنرها، پلاترها

در رابطه با ابزار ارتباطی می‌توان دو روش ارتباط با سخت‌افزار رایانه را در نظر داشت.

- ابزار ارتباط با رایانه به شکل محلی[۲]
- ابزار ارتباط با رایانه به روش از راه دور [۳]

---

[۱] Internet Protocol
[۲] LOCALLY
[۳] REMOTE

در روش محلی چنان‌چه فرد غیر مجاز بتواند به صورت فیزیکی به شبکه و اجزا آن دسترسی داشته باشد می‌تواند به روشی که در رابطه با رایانه‌های PC گفته شد به اطلاعات دسترسی پیدا کند

۸-۵-۳- دسترسی به اطلاعات محلی از طریق اینترنت

با توجه به این که اینترنت سیستم ارتباطی اتصال بین کلیه سخت‌افزارهای محلی بوده و سخت‌افزارها از طریق سیستم‌های ارتباطی به یک‌دیگر پیوند خورده و جزئی از موجودیت اینترنت محسوب می‌شوند و کلیه پروتکل‌های ارتباط بر این نکته تاکید دارند که در صورت اتصال یک سخت‌افزار به شبکه‌ای مانند اینترنت می‌بایست از قوانین عمومی آن تبعیت نماید تا دیگران قادر به ارتباط با آن باشند یا بتوانند به درخواست‌های آن پاسخ دهند می‌توان این نتیجه گیری را داشت که اطلاعات محلی نیز جزئی از اطلاعات اینترنت بوده و همان‌گونه که مالک اطلاعات می‌تواند به آن‌ها دسترسی داشته باشد دیگران نیز می‌توانند به این اطلاعات دسترسی داشته و از آن‌ها بهره‌برداری نمایند.

۸-۵-۴- تغییر وظایف امنیتی ابزار ارتباطی اینترنت از قبیل سویچ‌ها و روترها و مسیریاب‌ها

با توجه به این که تمام اطلاعات یک شبکه از طریق یکی از این ابزار در جریان افتاده و به دیگر اجزا شبکه منتقل می‌شود در صورت دسترسی فرد غیر مجاز به این سخت‌افزارها می‌تواند به روش مستقیم یا غیر مستقیم از طریق این سخت‌افزارها علاوه بر این که به اطلاعات تعاملی دسترسی پیدا می‌کند به اطلاعات شبکه نیز دسترسی پیدا نموده و بر کل شبکه اشرافیت داشته باشد.

۸-۶- اینترنت به عنوان اصلی‌ترین روش بر اشرافیت بر اطلاعات

بسیاری از کاربران گمان بر این دارند که فضای اینرنت محدود به فضایی است که سرویس‌های مختلف از قبیل جستجوی اطلاعات ، ایمیل ، وبلاگ و . . . . در آن ارایه شده و کاربران به صورت مستقیم از آن‌ها استفاده می‌نماید . این مقدار از فضا صرفاً بخش بسیار کوچکی از فضای اینترنت بوده و شاید یک ده هزارم فضای واقعی را تشکیل دهد. بسیاری از فضای اینترنت استفاده زیر ساخت‌های حیاتی کشورها مانند ارتباطات مخابراتی و ارتباطات سیستم‌های اقتصادی که بانک‌ها بخشی از آن می‌باشد و سیستم‌های ماهواره‌ای و فرودگاه‌ها و

انواع روش‌های ارتباطی و حمل و نقل و پالایشگاه‌های نفتی و فرآورده‌های نفتی و کارخانجات تولید انرژی هسته‌ای و برق و سدها و . . . . بخشی از آن می‌باشد.

امروزه با توجه به جمع‌بندی که در سال ۲۰۰۲ میلادی انجام گرفت ۹۸ درصد از اطلاعات بشریت بر روی ابزار نوین که توسط اینترنت به یک‌دیگر متصل شده است تولید و نگهداری و پردازش و توسط این ابزار توزیع می‌گردد. هر ساختاری بتواند به این ابزار دسترسی پیدا نموده یا بر روی آن اشرافیت داشته باشد عملاً مالک آشکار یا پنهان کل اطلاعات جهان بوده و روند دسترسی به آن را رقم می‌زند.

کاربران اولیه اینترنت و فن‌آوری اطلاعات بر اثر تبلیغات مختلفی که صورت گرفته و هر روز این تبلیغات با استفاده از سیستم‌های هدایت اطلاعات برای کاربران عادی بیش‌تر توسعه می‌یابد به این باور رسیده‌اند که باید برای بیسواد قلمداد نشدن کل اطلاعات خود را بر روی ابزار و شبکه‌های که به نوعی با اینترنت در ارتباط می‌باشند قرار دهند. بسیاری از کاربران از خصوصی‌ترین اطلاعات خود تا اطلاعات عمومی خود را بر روی این ابزار قرار می‌دهند.

بسیاری از سازمان‌ها تحت عنوان ایجاد paperless و یا lesspaper اطلاعات طبقه بندی شده عادی خود را با استفاده از نرم‌افزارهای مختلف مکانیزه کرده و بر روی سیستم قرار می‌دهند و چون اینترنت را به لحاظ اقتصادی به‌ترین وسیله انتقال اطلاعات و سریع‌ترین وسیله تشخیص داده‌اند از آن استفاده می‌نمایند.

با توجه به این که امروزه ۹۸درصد از اطلاعات بشریت برروی ابزار دیجیتال تولید ، ذخیره ، پردازش و توزیع می‌گردد تمام نیازمندان رسمی و غیر رسمی به اطلاعات به دنبال راه‌هایی می‌باشند تا بتوانند به این سهم عظیم اطلاعات دسترسی پیدا نموده و نیاز اطلاعاتی خود را مرتفع سازند.

۸-۶-۱- شبکه‌های اجتماعی اینترنت و بهره‌برداری از آن در کنترل و براندازی حاکمیت‌ها

شبکه اجتماعی ساختاری اجتماعی است که از گره‌هایی(که عموماً فردی یا سازمانی هستند) تشکیل شده است که توسط یک یا چند نوع خاص از وابستگی به هم متصل‌اند، برای مثال: قیمت‌ها، الهامات، ایده‌ها و تبادلات مالی، دوست‌ها، خویشاوندی، تجارت، لینک‌های وب، سرایت بیماری‌ها (اپیدمولوژی) یا مسیرهای هواپیمایی. ساختارهای حاصل اغلب بسیار پیچیده هستند. تحلیل شبکه‌های اجتماعی روابط اجتماعی را با اصطلاحات رأس و یال می‌نگرد. رأس‌ها

بازیگران فردی درون شبکه‌ها هستند و یال‌ها روابط میان این بازیگران هستند. انواع زیادی از یال‌ها می‌تواند میان رأس‌ها وجود داشته باشد. تحقیق در تعدادی از زمینه‌های آکادمیک نشان داده است که شبکه‌های اجتماعی در بسیاری از سطوح به کار گرفته می‌شوند از خانواده‌ها گرفته تا ملت‌ها و نقش مهمی در تعیین راه حل مسائل، اداره کردن تشکیلات و میزان موفقیت افراد در رسیدن به اهدافشان ایفا می‌کند.

آنالیز شبکه‌های اجتماعی(مرتبط با نظریه شبکه‌ها) به عنوان یک تکنیک کلیدی در جامعه شناسی، انسان شناسی، جغرافیا، روانشناسی اجتماعی، علوم ارتباطات، علوم اطلاعات، مطالعات سازمانی، اقتصاد و زیست شناسی مدرن همانند یک موضوع محبوب در زمینه تفکر و مطالعه پدیدار شده است.

در دهه ۱۹۷۰ و در پی اصلاحات گورباچف مبنی بر ایجاد فضای باز سیاسی و تغییر در قوانین اقتصادی شوروی سابق، کمیته‌ای متشکل از اساتید برجسته علوم سیاسی و مدیران سابقه دار سیا و پنتاگون تشکیل و با منتفی دانستن جنگ سخت برای رویارویی با شوروی ، تنها راه به زانو درآوردن این کشور را جنگ نرم و فروپاشی از درون دانستند و بدین وسیله برای اولین بار لغت جنگ نرم در دنیا به کار گرفته شد.

جنگ نرم شامل هرگونه اقدام روانی ، تبلیغاتی ، رسانه‌ای و فرهنگی است تا بتواند جامعه هدف را نشانه گرفته و بدون درگیری سخت‌افزارانه آن را منفعل ساخته و به شکست وا دارد.

مقام معظم رهبری می‌فرمایند" امروز جنگ نظامی با ما خیلی محتمل نیست – نمی‌گوئیم بکلی منتفی است، اما خیلی محتمل نیست - لکن جنگی که وجود دارد، از جنگ نظامی اگر خطرش بیش‌تر نباشد، کم‌تر نیست؛ اگر احتیاط بیش‌تری نخواهد، کم‌تر نمی‌خواهد. در جنگ نظامی دشمن به سراغ سنگرهای مرزی ما می‌آید، مراکز مرزی ما را سعی می‌کند منهدم بکند تا بتواند در مرز نفوذ کند؛ در جنگ روانی و آن چه که امروز به او جنگ نرم گفته می‌شود. در دنیا، دشمن به سراغ سنگرهای معنوی می‌آید که آن‌ها را منهدم کند؛ به سراغ ایمان‌ها، معرفت‌ها، عزم‌ها، پایه‌ها و ارکان اساسی یک نظام و یک کشور؛ دشمن به سراغ این‌ها می‌آید که این‌ها را منهدم بکند و نقاط قوت را در تبلیغات خود به نقاط ضعف تبدیل کند؛ فرصت‌های یک نظام را به تهدید تبدیل کند. این کارهائی است که دارند می‌کنند؛ در این کار تجربه هم دارند، تلاش هم زیاد دارند می‌کنند، ابزار فراوانی هم در اختیارشان هست. باید ابعاد دشمن و ابعاد دشمنی را بدانیم تا بتوانیم بر او فائق بیائیم. البته ما مدد الهی داریم، کمک غیبی داریم بدون

شک؛ این را انسان دارد مشاهده می‌کند؛ لکن ما مادامی که هوشیارانه، آگاهانه در میدان نباشیم، تدبیر لازم را به کار نبریم، کمک الهی به سراغ ما نخواهد آمد. "(مقام معظم رهبری)
کشورهای سلطه جو تلاش بر این دارند تا با استفاده از ویژگی‌هایی هم‌چون:

- خسارت کم‌تر برای مهاجم
- پنهانی بودن عملیات
- گستره وسیع نتایج اقدامات
- به حداقل رسانیدن امکان مقابله‌ای
- مساعد بودن زمینه عمومی موفقیت
- ماهیت تفرقه انگیزانه بودن این اقدام

و با استفاده از:

- شیوه‌های اقناع و فریب و اختلال و جذابیت به جای زور و خشونت
- استفاده از ظرفیت‌های قانونی و حقوقی کشور هدف
- گسترش حوزه عمل در لایه‌های فرهنگی و فکری
- به صورت تدریجی و زمان بندی شده

و بدون استفاده از عامل خشونت به نتیجه خود که همان فروپاشی از درون است دست یابند.

در روش‌های جنگ نرم، تلاش بر این دارند تا با استفاده از عملیات روانی شامل تبلیغات روانی و شایعه سازی و فریب استراتژیک و استفاده از ظرفیت‌های دیپلماسی و . . . . . هم‌چنین به کارگیری اعتراض و تبلیغ نافرمانی مدنی، مانند عدم همکاری با حکومت رسمی و قانونی و جذب مخالفین حکومت‌ها به روش‌های مختلف اهداف خود را عملی سازند.

امروزه روش رایج دیگری برای این کار به کار گرفته شده است که عبارت است از روش‌های شبکه‌ای که با استفاده از فن آوری‌های نوین و انواع ابزار الکترونیک در حال گسترش می‌باشد.

امروزه روش‌های شبکه‌ای مورد استفاده در جنگ نرم با عنایت به گسترش در فن‌آوری‌های نوین، ابعاد تازه‌ای به خود گرفته است . با گسترش علوم و نوآوری این روش‌ها ، ابزار مورد استفاده نیز در حال رشد و تکامل می‌باشد. میزان نفوذ این ابزار در بین جوامع مختلف این زمینه را ایجاد می‌نماید تا بتوان سهل‌تر و آسان‌تر از این ابزار در راستای جنگ نرم بهره‌برداری نمود.

امروزه کشورهای سلطه‌گر تلاش بر این دارند تا از انواع ابزار فرهنگی مانند سینما و فیلم سازی و اسباب بازی و بازی‌های رایانه‌ای و ماهواره‌ها و حتی موسیقی در رابطه با نفوذ فرهنگی خود استفاده نمایند.

به دنبال این هستند تا با استفاده از انواع رسانه‌های نوین و سنتی از قبیل مطبوعات و رادیوها و تلویزیون‌های در حال گسترش و خبرگزاری‌ها در این رابطه استفاده نمایند و هر زمان که لازم دیدند به توسعه کیفی و کمی این ابزار، برای نیل به اهداف خود بپردازند.

امروزه تلاش بر این دارند تا با استفاده از انواع سرویس‌هایی که در اینترنت ارائه می‌گردد از قبیل :

- سایت‌های خبری و خبرگزاری‌ها
- رسانه‌های اجتماعی
- سایت‌های ارتباطی و شبکه‌های اجتماعی
- وبلاگ‌ها و میکرو بلاگ‌ها
- ویکی‌ها
- فروم‌ها
- سایت‌های اشتراک گذاری
- انواع چت روم‌های متنی و صوتی و تصویری
- سیستم‌های ایمیل

به اهداف خود رسیده و با تبلیغ این که هرکس امروز نتواند از این ابزار استفاده نماید بی سواد است، دیگران را تشویق و ترغیب به استفاده از این ابزار نموده و به اهداف خود برسند.

مقام معظم رهبری، جنگ نرم را چنین تعریف می‌فرمایند:" همه این را امروز فهمیده‌اند و دانسته‌اند که مواجهه‌ی استکبار با نظام جمهوری اسلامی، دیگر از نوع مواجهه‌ی دهه‌ی اول انقلاب نیست. در آن مواجهه، زورآزمائی کردند؛ شکست خوردند. مواجهه‌ی سخت بود؛ ایجاد جنگ بود، کودتا بود. در اول انقلاب کودتا راه انداختند، شکست خوردند؛ شورش‌های قومی راه انداختند، سرکوب شدند و شکست خوردند؛ جنگ تحمیلی را به راه انداختند که هشت سال به طول انجامید، شکست خوردند؛ پس دنبال این راه‌ها نخواهند رفت، یعنی احتمالش ضعیف است. البته باید همیشه هشیاری نسبت به همه‌ی جوانب باشد. اما این، اولویت استکبار در مواجهه‌ی با نظام اسلامی نیست. اولویت، آن چیزی است که امروز به آن می‌گویند جنگ نرم؛

یعنی جنگ به وسیله‌ی ابزارهای فرهنگی، به وسیله‌ی نفوذ، به وسیله‌ی دروغ، به وسیله‌ی شایعه‌پراکنی؛ با ابزارهای پیش‌رفته‌ای که امروز وجود دارد، ابزارهای ارتباطی‌ای که ده سال قبل و پانزده سال قبل و سی سال قبل نبود، امروز گسترش پیدا کرده. جنگ نرم یعنی ایجادتردید در دل‌ها و ذهن‌های مردم .

یکی از ابزارها در جنگ نرم این است که مردم را در یک جامعه نسبت به یک‌دیگر بدبین کنند، بددل کنند، اختلاف ایجاد کنند؛ یک بهانه‌ای پیدا کنند، با این بهانه بین مردم ایجاد اختلاف کنند؛ مثل همین قضایای بعد از انتخابات امسال که دیدید یک بهانه‌ای درست کردند، بین مردم ایجاد اختلافی کردند. خوشبختانه مردم ما بابصیرتند. این جور کاری در کشورهای دیگر اوضاع کشور را بکلی عوض کرد؛ در جاهای دیگر، تردیدافکنی در دل‌های مردم نسبت به یک‌دیگر؛ یک بهانه‌ای مثل بهانه‌ی انتخابات را پیش بکشند، ایجادتردید کنند، دل‌ها را نسبت به یک‌دیگر چرکین کنند، مردم را در مقابل هم قرار بدهند؛ بعد در میانه، عناصر دست‌آموزِ مغرضِ معاند را به کارهای خلاف وادار کنند و مسئولین کشور نتوانند تشخیص بدهند کی بود، چی بود، چه شد. این جزو طرح‌های اساسی است. این جور کاری را دنبال می‌کنند"(مقام معظم رهبری)

۸-۷- همکاری و هماهنگی بین سه عنصر اینترنت اشلون و فن‌آوری‌های هوشمند

امروزه فن آوری‌های هوشمند به عنوان یکی از توانمندی‌های تکنولوژی نوین در اختیار تمام کاربران قرار گرفته است . در این فن‌آوری کلیه امکانات و اطلاعات مورد نیاز به صورت هوشمندانه و به صورت پیش تعریف شده در سیستم قرار داده شده و هر سخت‌افزار و نرم‌افزاری که به کار گرفته می‌شود این قابلیت را خواهد داشت تا محیط را شناسایی نموده و خود را به محیط به عنوان یک ابزار مجاز شناسایی نموده و در آن محیط قادر به انجام ماموریت از پیش تعریف شده باشد و برای انجام این ماموریت در کوتاه‌ترین زمان ممکن و بدون استفاده از هرگونه عامل بیرونی غیر از پیش تعریف شده به عامل جدیدی نیاز نداشته باشد و برای به روز رسانی خود به صورت هوشمندانه عوامل محیطی و محاطی را شناسایی نموده و خود را با شرایط جدید تنظیم و به روز رسانی نماید.

از طرف دیگر در طرح اشلون با استفاده از ماهواره‌ها و ارتباطات زمینی که در پایگاه‌های مختلف در اقصی نقاط جهان به کار گرفته می‌شوند نظام سلطه به دنبال این می‌باشد تا هر چه بیش‌تر این امکانات را به صورت هوشمندانه توسعه داده و ماموریت از پیش تعریف شده و استراتژی خود را که همان اشرافیت کامل بر ارتباطات و اطلاعات جهان می‌باشد به خوبی انجام داده و تمام اطلاعات در مبدا تولید را به دست آورده و با کلید واژه‌های از قبل تعریف شده آن‌ها را شناسایی و در راستای نیات پلید نظام سلطه به کار گرفته و بیش از پیش تلاش در گسترش این سلطه بر تمام دنیا دارد.

این دو مولود نابهنجار به دنبال این بوده و هستند تا بتوانند ارتباطات خود را از روش‌های که خود عاملین شوق در به کارگیری آن داشته باشند را گسترش دهند .

با این شرایط همکاری و هماهنگی بین سه عنصر اینترنت و اشلون و فن آوری‌های هوشمند شکل می‌گیرد . یکی از این عوامل تلاش می‌نماید تا هر چه بیش‌تر در زندگی انسان‌ها نفوذ نموده و در مبادی تولید اطلاعات قرار گرفته و شیوه و نوع اطلاعات تولید شده را به آسان‌ترین روش و مقبول‌ترین روش مدیریت نماید و دیگری به دنبال این می‌باشد که به اطلاعات تولید شده اشرافیت داشته و با طبقه بندی اطلاعات آن‌ها را به صورت موضوع بندی شده و مرتبط با یک‌دیگر به کار بگیرد و سومی مسیر ارتباط بین این دو مولود را برای ارتباط هرچه به‌تر و سریع‌تر و ارزان‌تر و مورد علاقه‌مندتر فراهم سازد.

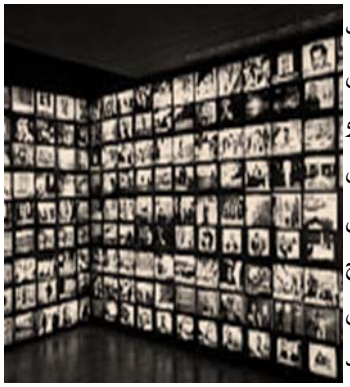
۸-۸- اینترنت و جنگ روانی

امروزه انسان‌ها شاهد فراگیری بی‌سابقه رسانه‌ها و وسایل ارتباطات جمعی مدرن و نوین هستند. بالطبع آن‌ها در معرض شدیدترین امواج رسانه‌ها قرار دارند. گرچه رسانه‌ها ذاتاً کارکردی دوطرفه و دو سویه دارند، اما بیش‌ترین حجم بهره‌گیری از آن در دست نظام سلطه قرار دارد؛ چنان‌چه می‌توان با جرأت گفت حفظ و گسترش قدرت استکباری نظام سلطه به حضور و ظهور رسانه‌ها وابسته است. رسانه‌ها پل ارتباطی و بلکه وسیله‌ی تسلط بر افکار، اراده و احساسات بشر دوران معاصر به شمار می‌آیند. مراکز رسانه‌های استکبار که به مدرن‌ترین فن‌آوری جهانی مجهزند، از یک سو ابزاری برای اجرای "عملیات روانی" قدرت‌ها علیه ملت‌ها و دولت‌های مستقل هستند و از سوی دیگر وسیله‌ای برای کنترل، تضعیف، جهت‌دهی و هدایت جوانان در سراسر جهان محسوب می‌شوند.

۸-۹- ارتباط بین سیاست‌های توسعه‌ای استراتژی سلطه و توسعه فنی و عمومی اینترنت

مارک پالمر* از استراتژیست‌های معروف آمریکایی است که از او به عنوان یکی از نوآوران سیاست خارجی ایالات متحده نام می‌برند. پالمر در دولت‌های نیکسون، کارتر، ریگان و بوش در وزارت خارجه مشغول بوده و اکنون علاوه بر این‌که مدیر دپارتمان تحقیقاتی مرکز سیاست خارجی سابان در مؤسسه‌ی "بروکینگز" می‌باشد، عضو کمیته‌ی خطر جاری است که اخیراً و در پی تحولات پیش آمده پس از یازده سپتامبر ۲۰۰۱ گزارشی تحت عنوان "ایران- آمریکا، رهیافت جدید" را به نگارش درآورد. کمیته‌ی خطر جاری در اوج جنگ سرد و در دهه ۱۹۷۰ میلادی و با مشارکت اساتید برجسته‌ی علوم سیاسی و مدیران سابقه‌دار سازمان سیا و پنتاگون تأسیس شد و یکی از موفقیت‌آمیزترین اقدامات در جریان رقابت دو ابرقدرت شرق و غرب، طراحی و اجرای مراحل مختلف سناریوی فروپاشی ابرقدرت شرق از طریق جنگ نرم[۱] در سال‌های پایانی دهه‌ی ۱۹۸۰ بود. (afand. blogfa. com)

۸-۱۰- جنگ‌های نوین



هیچ انسانی بدون امنیت نمی‌تواند به ادامه‌ی حیات خود امیدوار باشد؛ چه در دنیای واقعی چه در دنیای مجازی. موضوع امنیت یکی از اصلی‌ترین شاخصه‌ها و نیازهای بشری است و این خصوصیات، امروزه در دنیای سایبر نیز محسوس و ملموس است. اخبار و آمار امنیتی شدن فضای سایبر مدت‌هاست که جزء اخبار اول صبح رسانه‌ها شده و بسیاری نیز بر این عقیده‌اند که این آغازی است بر" جنگ سایبر "بین دولت‌ها و نام آن را گذاشته‌اند جنگ جهانی سوم.

امروزه انسان‌ها شاهد فراگیری بی‌سابقه رسانه‌ها و وسایل ارتباطات جمعی مدرن و نوین هستند. بالطبع آن‌ها در معرض شدیدترین امواج رسانه‌ها قرار دارند. گرچه رسانه‌ها ذاتاً کارکردی دوطرفه و دو سویه دارند، اما بیش‌ترین حجم بهره‌گیری از آن در دست نظام سلطه

---

[۱] Soft War

قرار دارد؛ چنان‌چه می‌توان با جرأت گفت حفظ و گسترش قدرت استکباری نظام سلطه به حضور و ظهور رسانه‌ها وابسته است. رسانه‌ها پل ارتباطی و بلکه وسیله‌ی تسلط بر افکار، اراده و احساسات بشر دوران معاصر به شمار می‌آیند. مراکز رسانه‌های استکبار که به مدرن‌ترین فن‌آوری جهانی مجهزند، از یک سو ابزاری برای اجرای "عملیات روانی" قدرت‌ها علیه ملت‌ها و دولت‌های مستقل هستند و از سوی دیگر وسیله‌ای برای کنترل، تضعیف، جهت‌دهی و هدایت جوانان در سراسر جهان محسوب می‌شوند.

۸-۱۰-۱- جنگ اطلاعات

جنگ اطلاعاتی یک اصطلاح نسبتاً جدید است که طی سال‌های گذشته به واژه نامه اصطلاحات نظامی وارد شده است . البته مفهوم استفاده از اطلاعات در جنگ قدمت طولانی دارد. ظهور اصطلاح جنگ اطلاعاتی و اهمیت روزافزون آن احتمالا با انقلاب اطلاعات ارتباط مستقیم دارد. باور همگانی به این صورت است که چنین انقلابی آن قدر قدرتمند و دامنه تاثیر آن آنقدر گسترده است که می‌تواند بُعد جدیدی در جنگ یا اصلاً سبک جدیدی از جنگ را تعریف کند.

در خلال نیمه دوم دهه ۱۹۹۰ اصطلاح جنگ اطلاعاتی مطرح و بعدا توجه به آن کم رنگ شد. هیچ کارشناس نمی‌توانست تعریف روشنی برای آن ارائه دهد ، چه رسد به این که کارشناسان نظامی در باره یک تعریف مشخص به تفاهم برسند . غالبا به نظر می‌رسد اصطلاح جنگ اطلاعاتی طیف بسیار گسترده‌ای را در بر گرفته و شامل موارد سنتی مانند جنگ فرماندهی و کنترل[۱] و جنگ الکترونیک می‌شود . این حوزه‌های سنتی عملیات نظامی ارتباط دو طرفه با انقلاب اطلاعات برقرار کرده‌اند. انقلاب اطلاعات از یک سو باعث تکامل هر چه بیش‌تر و به‌تر آن‌ها شده است و از سوی دیگر خود آن‌ها جزء پیش رانه‌های انقلاب اطلاعات محسوب می‌شوند . به هر حال ، در حوزه عمومی جنگ اطلاعاتی یک مفهوم مشخص اهمیت روز افزون یافته است. این احتمال وجود دارد که دشمنان بالقوه آینده با استفاده ، یا به‌تر بگوئیم سو استفاده ، از ابزار و تکنیک‌های مرتبط با انقلاب اطلاعات ، دارائی‌های استراتژیک ملی یک‌دیگر را مانند عناصر اولیه وجهه نظامی یا زیرساخت‌های ملی را در معرض خطر قرار دهند. یعنی

[۱] Command and control warfare (C۲W)

هدف عمده از چنین حملاتی تخریب و انفجار نیست بلکه ایجاد اختلال بزرگ مقیاس یا گسترده در دارائی‌های استراتژیک ملی هدف مطلوب می‌باشد.

مگان برنز در سال ۱۹۹۹ تلاش کرد که مولفه مشترک همه تعاریف صاحب نظران را در یک مجموعه گردآوری کند ، وی نتیجه می‌گیرد:

"جنگ اطلاعاتی طبقه یا مجموعه‌ای از تکنیک‌ها شامل جمع آوری ، انتقال ، حفاظت ، ممانعت از دسترسی ، ایجاد اغتشاش و اُفت کیفیت در اطلاعات است که از طریق آن یکی از طرفین درگیر بر دشمنان خود به مزیتی چشم‌گیر دست یافته و آن را حفظ می‌کند "

لغت نامه دانشگاه پرینستون ، که از جمله معتبرترین مراجع اینترنتی است ، جنگ اطلاعاتی را به صورت "کاربرد اطلاعات یا فن‌آوری اطلاعات در خلال بحران یا درگیری برای تحقق یا پیشبرد اهداف مشخص علیه یک یا چند دشمن" تعریف می‌نماید.

فرماندهان ارشد نیروی هوائی در سندی رسمی تحت عنوان "سنگ بنای جنگ اطلاعاتی " تعریف زیر را مطرح کردند:

"جنگ اطلاعاتی عبارت است از هر اقدامی در راستای ممانعت از دسترسی ، بهره‌برداری (سواستفاده) ، ایجاد اختلال، و نهایتاً تخریب و حذف اطلاعات دشمن و کارکردهای آن و هم‌چنین حفاظت در برابر اقدامات مشابه دشمن"

دکتر جان الگر در یکی از سمینارهای در معرفی جنگ اطلاعاتی تعریفی ارائه داد که علاوه بر دیدگاه‌های کاملاً نظامی ، دیدگاه‌های غیرنظامی را نیز تحت پوشش قرار می‌دهد :

"جنگ اطلاعاتی یعنی اقدامات اتخاذ شده برای تحقق برتری اطلاعاتی از طریق تاثیر گذاشتن بر اطلاعات ، فرآیندهای بر پایه اطلاعات ، و سیستم اطلاعاتی دشمن و در عین حال دفاع از اطلاعات ، فرآیندهای بر پایه اطلاعات ، و سیستم‌های اطلاعاتی خودی"

وزارت دفاع آمریکا در اواخر دهه ۱۹۹۰ یک تعریف رسمی به صورت زیر منتشر کرد:

"جنگ اطلاعاتی عبارت است از اقدامات اتخاذ شده برای تحقق برتری اطلاعاتی که از طریق تاثیرگذاری بر اطلاعات و سیستم‌های اطلاعاتی دشمن از استراتژی نظامی ملی پشتیبانی کرده و در عین حال اطلاعات و سیستم‌های خودی را ارتقا بخشیده و از آن‌ها دفاع می‌کند ".

دانشگاه دفاع ملی آمریکا نیز در تعریف خود ، ضمن تاکید بر نقش فن‌آوری پیش‌رفته اطلاعات ، بازیگران این عرصه چنگی را فقط نظامیان می‌دانست:

"جنگ اطلاعاتی یعنی کاربرد اطلاعات و سیستم‌های اطلاعاتی به عنوان یک سلاح در درگیری‌هائی که اطلاعات و سیستم‌های اطلاعاتی یک هدف نظامی به شمار می‌روند ".

مارتین لیبیکی ضمن وفادار ماندن به تعریف کاملاً نظامی از جنگ اطلاعاتی ، هفت شکل مختلف جنگ اطلاعاتی را به شرح زیر نام می‌برد:

- جنگ فرماندهی و کنترل ، که هدف آن قطع کردن سر دشمن ، یعنی از بین بردن مغز متفکر دشمن است .
- جنگ بر پایه اطلاعات که متشکل از طراحی ، حفاظت و ممانعت از دسترسی به سیستم‌هائی است که برای برتری در فضای نبرد در جستجوی دانش کافی هستند.
- جنگ الکترونیک که شامل تکنیک‌های رادیوئی ، الکترونیک و رمزنگاری می‌باشد.
- جنگ روانی که در آن اطلاعات برای تغییر ذهنیت و طرز فکر دوستان ، بی طرف‌ها ، و دشمنان استفاده می‌شود.
- جنگ هکرها که در آن به سیستم‌های رایانه‌ای حمله می‌شود.
- جنگ اقتصادی که ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی می‌باشد.
- جنگ سایبر که ترکیبی از موارد شش گانه فوق می‌باشد.

در سال ۱۹۹۷ چارلزهاوکینز در سخنرانی خود در مرکز اطلاعات علم و فن‌آوری دفاعی چین خاطر نشان می‌کند که تعدادی از کارشناسان نظامی جوان مایلند تعریف زیر را برای جنگ اطلاعاتی ارائه دهند:

"استفاده از ابزارها و سیستم‌های برخوردار از فن‌آوری برتر[۱] برای حس‌گری ، پردازش و ارتباط اطلاعات دیجیتالی و تبدیل آن به اطلاعات مفید برای استفاده در یگان توپخانه ، موشک‌انداز و دیگر سیستم‌های تسلیحاتی ، یا برای بهبود فرماندهی و کنترل عملیات نظامی".

در حال که کارشناسان قدیمی‌تر و افسران ارشد بازنشسته دیدگاهی سنتی‌تر داشته و از دریچه فن‌آوری معمولی (یا سطح پایین)[۲] به موضوع نگریسته و جنگ اطلاعاتی را شامل

---

[۱] High tech
[۲] Low tech

"تبلیغات ، عملیات روانی ، و عملیات فریب با هدف بازدارندگی ، گیج کردن ، به تاخیر انداختن اقدامات ، یا شگفت زده کردن دشمن " می‌دانند.

در بین جنگ‌های اطلاعاتی، این نوع رویارویی (در فضای مجازی) طیف بسیار وسیعی را در بر می‌گیرد که شامل مواردی از قبیل‌تروریسم اطلاعاتی، تهاجم از طریق اختلال در منطق حاکم بر یک نرم‌افزار و شبیه‌سازی تمام عیار یک نبرد می‌باشد. در تهاجم از طریق تغییر در مفهوم یا منطق حاکم بر یک نرم‌افزار، سعی می‌شود ماموریت یک نرم‌افزار به گونه‌ای تغییر داده شود تا نتایج نهایی، بر خلاف انتظار باشد. به عنوان مثال، با تزریق ویروس در سامانه ناوبری یک هواپیما می‌توان زمینه‌ی نمایش اطلاعات خطا (ولو به ظاهر طبیعی) مانند ارتفاع هواپیما از سطح دریا یا فاصله واقعی باند پرواز تا هواپیما را فراهم نمود.

جنگ سایبر به معنی استفاده از فضای تبادل اطلاعات و رایانه‌ها به عنوان یک اسلحه یا به عنوان ابزاری برای انجام کارهای خشونت بار جهت‌ترساندن یا تغییر عقیده، تغییر فرهنگ و تغییر سیاست یک کشور می‌باشد. جنگ سایبر به قصد کارهای سیاسی انجام می‌گیرد و مکان‌ها و تاسیسات حیاتی مانند انرژی، حمل و نقل ،ارتباطات و سرویس‌های خدماتی ضروری را هدف قرار می‌دهد و از شبکه‌های رایانه‌ی به عنوان بسترهایی جهت انجام این اعمال خرابکارانه استفاده می‌کند.

این دسته از جنگ‌ها اگرچه در فضای مجازی اتفاق می‌افتد ولی هدف‌های اصلی آن بر اثر عوارضی در فضای حقیقی ایجاد می‌شود.

جنگ سایبر ایده‌ی جدیدی را در زمینه‌ی جنگ فراهم آورده که جنگ شبکه‌ای نامیده می‌شود. در جنگ شبکه‌ای گروه‌های مختلفی با یک‌دیگر ارتباط و هماهنگی برقرار می‌کنند.

اگرچه نیت و انگیزه‌ی بروز جنگ‌های مختلف انگیزه‌های سیاسی است و اساساً جنگ اطلاعات با همین هدف بین قدرت‌ها بروز می‌کند، اما ابزارهایی که پیش از این اشاره شد، با هدف‌های مالی و با انگیزه‌ی سرقت از افراد در اختیار مجرمان نیز قرار دارد. این دسته از فعالیت‌ها که هدف آن الزاماً سیاسی نیست، جرم سایبری می‌نامیم.

جنگ سایبری شامل کلیه اقدامات مخاصمه آمیز در فضای تبادل اطلاعات و ارتباطات است که با به کارگیری ابزارهای تخصصی حوزه فن‌آوری اطلاعات و ارتباطات و در بستر شبکه‌ها و سامانه‌های اطلاعاتی، ارتباطی و مدیریتی اجرا می‌گردند.

جنگ سایبری در حوزه‌های عملیاتی ذیل برنامه ریزی و اجرا می‌شود :

۱. جنگ اطلاعات
۲. جنگ مدیریت/ فرماندهی و کنترل
۳. جنگ نرم (فرهنگی، اعتقادی، اجتماعی، سیاسی، روانی و . . .)

با توجه به آن‌چه در خصوص تعریف و حوزه‌های جنگ سایبری ارائه شد، می‌توان ویژگی‌های مختلفی در خصوص این دسته از جنگ‌ها بیان کرد که آن را از جنگ‌های دیگر متمایز می‌سازد. برخی از این خصوصیت‌ها عبارتند از:

۱. امکان توسعه جنگ (رفتارهای خصمانه) در همه حوزه‌ها و عرصه‌های زیرساختی و عمومی
۲. پیچیدگی و دشواری استفاده از حمایت‌ها و پوشش حقوقی و انتظامی
۳. همکاری پنهان و نامحسوس تجهیزات دفاعی و غیردفاعی کشور هدف با سازمان تهاجمی کشور مهاجم (نقش تجهیزات هوشمند و حفره‌های امنیتی، اینترنت، اشلون و ارتباط نظام مند و هدفمند بین آن‌ها که به‌وسیله سازندگان و صاحبان آن‌ها بر جهان تحمیل شده است.)
۴. امکان درگیر کردن کشورها و یا مراجع بی اطلاع در جنگ علیه کشور هدف

هدف این نوع جنگ اطلاعاتی، روش‌های تهاجم به بخش غیرنظامی یک کشور است؛ چرا که تهاجم به بخش‌های نظامی در قالب روش‌های جنگ فرمان و کنترل صورت می‌پذیرد. در این نوع جنگ، سارقین اطلاعات یا نفوذگران رایانه‌ای اقدام به شناخت نقاط آسیب‌پذیر ساختار یک سامانه نموده و از آن نقاط، تهاجم خود را آغاز می‌کنند. زمینه‌های این تهاجم می‌تواند بسیار متنوع باشد. برای نمونه هدف از تهاجم ممکن است ساقط کردن یک سامانه، تعطیلی و توقف مکرر یک سامانه، ایجاد خطاهای اتفاقی در داده‌ها، سرقت خدمات (انجام مکالمات تلفنی رایگان، ورود و بهره‌برداری از اطلاعات پایگاه‌ها بدون پرداخت هزینه) ، جعل هویت (استفاده از امضای دیجیتالی و یا کارت اعتباری دیگران) ، گردآوری اطلاعات برای سرویس‌های امنیتی (رمز شکنی و دست یابی به رمز ورود به پایگاه‌های نظامی و فروش این رمزها به سرویس‌های اطلاعاتی) ، ارسال پیام‌های ساختگی غیرمجاز و دست یابی به اطلاعات شخصی افراد به منظور اخاذی از آن‌ها باشد. در این رابطه از نرم‌افزارهای متعددی نیز بهره گرفته می‌شود.

۸-۱۰-۲- جنگ سایبر

جنگ سایبر عبارت است از انجام یا آماده شدن برای انجام عملیات نظامی مطابق با اصول مربوط به اطلاعات. جنگ سایبر یعنی ایجاد اختلال، اگر نگوئیم نابودی کامل، در سیستم‌های اطلاعاتی و ارتباطی که دشمن برای دانستن خود به آن‌ها تکیه می‌کند یعنی این که او کیست ؟ چه کاری را در چه زمانی می‌تواند انجام می‌دهد ؟ چرا می‌جنگد؟ چه تهدیداتی در اولویت قرار دارد؟ و غیره. در جنگ سایبر تلاش می‌شود تا همه چیز در باره دشمن بدانیم و در عین حال نگذاریم او هیچ چیزی در باره ما بداند. به بیان دیگر هدف اصلی در جنگ سایبر بر هم زدن موازنه اطلاعات و دانش به نفع نیروهای خودی است به ویژه اگر موازنه توان رزمی وجود نداشته باشد. بنابراین در جنگ سایبر می‌توان با بهره گیری از دانش برتر ، ضعف سرمایه و نفرات کم‌تر را جبران کرده و به پیروزی قاطع دست یافت.

جنگ سایبر اشکال متعددی داشته و از انواع فن‌آوری‌های پیش‌رفته بهره می‌جوید. سیستم‌های سلاح‌های هوشمند، ماهواره‌های جاسوسی ، پرنده‌های بدون سرنشین با مداومت پرواز بالا، فن‌آوری موقعیت یاب جهانی[۱] و غیره نمونه‌هائی از فن‌آوری‌های مورد استفاده در جنگ سایبر هستند. هم‌چنین می‌توان به توان‌مندی‌های کور کردن الکترونیک ، جمینگ ، فریب، بیش بارگذاری و نفوذ به مدارهای ارتباطی و اطلاعاتی دشمن اشاره کرد. جنگ سایبر صرفاً یک مجموعه از اقدامات بر پایه فن‌آوری محسوب نمی‌شود و نباید آن را با تعاریف قدیمی در باره جنگ رایانه‌ای ، جنگ خودکار، جنگ روباتی، یا جنگ الکترونیک اشتباه گرفت، زیرا جنگ سایبر در برگیرنده اشاراتی مربوط به سازمان نیز می‌شود. همان طور که اشاره شد انقلاب اطلاعات منجر به نوآوری‌های درون سازمانی می‌شود به گونه‌ای که ادارات مختلف یک سازمان شبیه اجزا یک شبکه به هم پیوسته در کنار یک‌دیگر قرار دارندتا به صورت ادارات تابع سلسله مراتب. بنابر این جنگ سایبر با الزاماتی همراه است که موجب طراحی مجدد سازمانی، چه درون سازمانی و چه برون سازمانی، می‌شود. حرکت به سمت ساختارهای شبکه‌ای مستلزم تمرکز زدائی از فرماندهی و کنترل است. مفهومی که برداشت‌های قبلی را مبنی بر این که فن‌آوری نوین اطلاعاتی موجب تقویت هرچه بیش‌تر فرماندهی متمرکز می‌شود، کاملاً نقض می‌کند. البته تمرکز زدائی تنها بخشی از تصویر کلی است، آنچه مهم‌تر است این که فن‌آوری نوین موجب تقویت هر چه بیش‌تر نگاه از بالا می‌شود. یعنی این که مانند بازی فوتبال ، بازیگران می‌توانند از جای‌گاه تماشاگران نیز صحنه نبرد را مشاهده کرده و موقعیت نیروهای

---

[۱] GPS

خودی و دشمن را به‌تر شناخته و در نتیجه پیچیدگی‌های فوق‌العاده میدان نبرد را به‌تر مدیریت کند. در زمینه جنگ سایبر تعداد زیادی فقط بر لزوم طراحی مجدد سازمانی و تمرکززدائی در تصمیم گیری تاکید می‌کند، در حالی که مفهوم نگاه از بالا درترکیب با تمرکز زدائی فرماندهی ثمرات چشم‌گیر و بالقوه تعیین کننده جنگ سایبر را به ارمغان می‌آورد.

رموند پارکز و دیوید دوگان از پژوهشگاه ملی ساندیا در نیومکزیکو در تعریف جنگ سایبر می‌نویسد:

"جنگ سایبر زیر مجموعه‌ای است از جنگ اطلاعاتی که شامل اقداماتی می‌شود که در دنیای سایبر رخ می‌دهد. دنیای سایبر هرگونه واقعیت مجازی[۱] است که توسط مجموعه رایانه‌ها و شبکه‌ها ایجاد می‌شود . در بین دنیای سایبر متعدد و مختلف ، اینترنت و شبکه‌های مرتبطی که حاوی مطالب چند رسانه‌ای هستند ، بیش‌ترین ارتباط را با جنگ سایبر دارند".

۸-۱۰-۳- جنگ شبکه‌ای

جنگ شبکه‌ای عبارت است از منازعات و بحران‌های مرتبط با اطلاعات که در سطح کلان بین دو کشور یا دو جامعه رخ می‌دهد. هدف از آن مختل سازی، تخریب، یا دست‌کاری دانش جمعیت هدف درباره خود و محیط پیرامونی‌اش است. در جنگ شبکه‌ای شاید بر افکار نخبگان یا افکار عمومی یا هر دو تمرکز شود. جنگ شبکه‌ای معمولاً در برگیرنده روش‌های دیپلماتیک ، تبلیغات مسموم ، عملیات روانی، فریب یا مداخله در امور رسانه‌ای گروهی، نفوذ به شبکه‌های رایانه‌ای و سایت‌های اینترنتی و نهایتاً حمایت آشکار و همه جانبه از جنبش‌ها و گروه‌های مخالف رژیم هدف می‌شود. بنابراین در جنگ شبکه‌ای تعدادی از اقدامات که پیش‌تر از این به طور جداگانه استفاده می‌شدند به صورت مرکب، یک‌پارچه به کار می‌روند. به عبارت دیگر ، جنگ شبکه‌ای مفهومی تازه وارد در طیف گسترده جنگ سیاسی ، جنگ اقتصادی، جنگ اجتماعی، و نهایتا جنگ تمام عیار نظامی می‌باشد. با توجه به این که امروزه تمام جوامع در بین دو شبکه به هم تنیده رایانه‌ای زندگی می‌کنند (شبکه ارتباطی و شبکه اطلاعاتی رایانه‌ای) و زندگی بدون این دو شبکه عملاً قابل فرض نمی‌باشد. امروزه بستر جنگ شبکه‌ای عملاً یک یا هر دو این شبکه‌ها می‌باشد . جنگ رسانه‌ای خود را در این دو شبکه نشان می‌دهد. توسعه رسانه‌های مختلف رادیوئی و تلویزیونی از طریق اینترنت، دسترسی به همه شبکه‌های رسانه‌ای

---

[۱] Virtual reality

از طریق تلفن همراه، دست‌یابی به هزاران شبکه ماهواره‌ای از طریق گیرنده‌های معمولی ، امکان افزایش لحظه‌ای هرکدام از شبکه‌ها این امکان را فراهم نموده است تا تاثیر گذاران با استفاده از این پهنه گسترده برای جنگ شبکه‌ای تعریف جدیدی داشته باشند و آن استفاده از فضای اینترنت در جنگ شبکه‌ای می‌باشد.

۸-۱۰-۴- تفاوت بین جنگ و جرم سایبری

یکی از مسایلی که در حوزه‌ی دفاع غیرعامل مطرح می‌گردد، دفاع در برابر جنگ‌هایی است که بدون جنگ‌افزار فیزیکی صورت می‌پذیرد.

با پیشرفت فن‌آوری و ظهور فن‌آوری‌های نوین از جمله فن‌آوری اطلاعات و ارتباطات، ارزش اطلاعات در افزایش قدرت بازدارندگی یا ایجاد برتری در جنگ بالاتر رفته است. این افزایش ارزش اولاً به دلیل افزایش بسیار زیاد حجم اطلاعات تولید شده در دنیای کنونی از یک سو و ثانیاً به دلیل ایجاد قابلیت‌های پردازش و تحلیل دقیق اطلاعات به وجود آمده است. به همین دلیل است که به اذعان همه‌ی متخصصان، اطلاعات به عنوان مهم‌ترین منبع لازم برای کلیه‌ی فعالیت‌ها در سطوح مختلف اعم از فردی، سازمانی و ملی معرفی گردیده است. بنابراین حفظ برتری در سطح سیاسی کشورها، چه در شرایط صلح چه در جنگ رابطه‌ی مستقیمی با برتری اطلاعاتی آن‌ها دارد.

با توجه به آن‌چه در خصوص ارزش اطلاعات برای افراد، سازمان‌ها و کشورها گفته شد، طبیعی است تخاصماتی بین رقبا، در همه‌ی سطوح، نه به صورت سابق که با رویکرد جمع‌آوری اطلاعات یا ارائه‌ی اطلاعات مخدوش به حریف در می‌گیرد.

در یک تعریف جنگ‌هایی این‌گونه که در شکل سنتی صورت نمی‌گیرد، جنگ اطلاعاتی نامیده شده است. در تعریف دیگری ایده‌ها و نظریه‌های مرتبط با اثرگذاری و روش تفکر انسان‌ها و از آن مهم‌تر، روش بهره‌گیری از اطلاعات برای دست‌یابی به اهداف ملی یک کشور نیز جنگ اطلاعاتی نامیده می‌شود. این اهداف ممکن است در زمینه‌های سیاسی، اقتصادی یا نظامی باشند. در استراتژی جنگ اطلاعاتی، اعتقاد بر این است که به جای تسلیحات با حجم تخریب زیاد، باید از تسلیحات به صورت دقیق علیه نقاط ضعف و آسیب‌پذیر سیستم استفاده شود. جنگ اطلاعات شامل عملیات معین برای حفظ یک‌پارچگی سیستم اطلاعات خودی در برابر تخریب، گسیختگی یا بهره‌برداری دشمن است، در حالی که به طور هم‌زمان بهره‌برداری،

انهدام یا تخریب یک سیستم اطلاعاتی دشمن و فرآیند کسب برتری اطلاعاتی را در به کارگیری نیروها نیز انجام می‌دهد.

۸-۱۰-۵- سلاح‌های سایبری

رسانه‌های جمعی در معنای وسیع شامل تمامی وسایل ارتباطی است که در سطحی گسترده به انتشار اطلاعات، اخبار، عقاید، نظرات، آموزش، عملیات روانی، تبلیغات، توجیه، جهت‌دهی، ارشاد، انحراف و. . . می‌پردازند.

آنچه مسلم است جنگ رسانه‌ای غیر از ابزارهای فنی و هنری، به ملزومات مختلفی از جمله آگاهی، آموزش، علم و تخصص نیز نیاز دارد. حامی، پشتیبان و سرمایه از دیگر نیازهای جنگ رسانه‌ای است.

ابزارهای رسانه‌ای تنوع فراوانی دارند که در گروه‌های مختلف همچون دیداری، شنیداری، نوشتاری، ارتباطی، الکترونیکی، دسته‌بندی می‌شوند. در هر یک از این گروه‌ها تعداد بسیاری از ابزارها مورد استفاده قرار می‌گیرند. ابزارهای دیداری و شنیداری شامل گروه‌های ماهواره‌ای، سینما، تلویزیون، هنرهای نمایشی و تجسمی، خبرگزاری‌ها، بازی‌های رایانه‌ای، فرستنده‌های پرتابل؛ ابزارهای شنیداری شامل رادیو با موج‌های کوتاه، بلند، موسیقی، آهنگ؛ ابزارهای نوشتاری شامل کتب، نشریات، روزنامه‌ها، شب‌نامه، اعلامیه، اوراق تبلیغی، ابزارهای ارتباطی، شامل تلفن، بی‌سیم، فکس، تلکس، تلگراف و ابزارهای الکترونیکی شامل اینترنت، تلفن همراه و.... هر یک از این وسایل و ابزار با کاربردهای مختلف، وظیفه اساسی انتقال پیام از مبدا پیام به گیرنده پیام (مخاطب) را برعهده دارند

۸-۱۰-۶- نقض حاکمیتی سایبری

یکی از مؤلفه‌های اصلی جهانی شدن، رسانه‌ها و فن‌آوری‌های نوین ارتباطی – اطلاعاتی است و پیامدهای آن در عرصه سیاست کشورها گواه تأثیر رسانه‌ها بر شکل‌گیری جریاناتی چون انقلاب‌های رنگی در اروپای شرقی و آسیای مرکزی و نقش آن‌ها در صدور این جریانات سیاسی بدون خشونت به دیگر نقاط جهان است. در ادامه این تأثیرگذاری می‌توان به انتخابات اخیر برمه، کنیا، زیمبابوه و رخدادهای تبت که هم‌چنان هم ادامه دارد، اشاره کرد. از یک منظر و مطابق آن‌چه که از پیامدهای رسانه‌های الکترونیک جدید مطرح است، جهان وارد عصر دوم رسانه‌ها شده است که بر خلاف دوره مدرن و عصر اول رسانه‌ها، آینده آن به طور کامل قابل

پیش‌بینی نیست، زیرا عصر دوم رسانه‌ها که در آن بحث رسانه‌های الکترونیک جدید، حاکمیت دارند و اطلاعات حرف آخر را می‌زنند، پدیده‌ها کم‌تر قابل پیش‌بینی شده‌اند (جنگ نرم ۲، ۱۳۸۷: ۲۷۸)

در حال حاضر، «پیشرفت سیستم‌های ارتباطی جدید دنیایی را پدید آورده است که در آن ویژگی‌های مکان و فردیت همواره از طریق شبکه‌های ارتباطی منطقه‌ای و جهانی بازنمایی و دوباره تفسیر می‌شوند. اما وابستگی این سیستم‌ها به فراسوی این موارد می‌رود. زیرا برای احتمال سازمان‌دهی عمل سیاسی و اعمال قدرت سیاسی در فواصل دوردست بنیادی تلقی می‌شوند» (دیبرت، ۱۹۹۷)

علاوه بر این ملت‌ها، مردم و سازمان‌ها به وسیله انواع جدید ارتباطات در مرزهای کشورها به یک‌دیگر متصل‌اند. انقلاب دیجیتالی در میکروالکترونیک، در فن‌آوری اطلاعات و در رایانه‌ها موجب برقراری تماس‌های تقریباً آنی در سراسر جهان شده، که همواره با فن‌آوری تلفن، تلویزیون، کابل، ماهواره و حمل و نقل با هواپیمای جت، ماهیت ارتباطات سیاسی را به طور چشم‌گیری دگرگون کرده‌اند. پیوند عمیق میان «محیط فیزیک»، «موقعیت اجتماعی» و سیاست که مشخصه بیش‌تر کانون‌های سیاسی از دوران ماقبل مدرن تا مدرن بود، از هم گسیخته است (هلد و مک‌گرو، ۱۳۸۲: ۲۱)

مهم‌ترین تأثیرات سیاسی فن‌آوری‌های ارتباطی – اطلاعاتی تضعیف دولت‌های ملی، اشاعه اطلاعات سیاسی و درگیرسازی مدنی با مشارکت سیاسی افراد و گروه‌هاست. در حقیقت، فن‌آوری‌های نوین ارتباطی و اطلاعاتی، موتور اصلی جهانی شدن بود و تمام ابعاد حیات سیاسی، اجتماعی، فرهنگی و اقتصادی را تحت‌تأثیر قرار داده است. شاید، هیچ تحولی را در عصر حاضر نتوان سراغ گرفت که از حیث ایجاد تغییر در حیات سیاسی و اجتماعی بتواند با این فن‌آوری‌ها برابر می‌کند. کنترل اطلاعات در عصر جدید اهرم اصلی قدرت بازیگران جهانی، ملی و محلی است (سردارنیا، ۱۳۸۶: ۱۰۴).

۸-۱۰-۷- جنگ رسانه‌ای و اینترنت

جنگ رسانه‌ای کارکردهای مختلف منفی و مثبت دارد که از آن در جهت تحقق جامعه مدنی به‌عنوان رکن چهارم دمکراسی نام می‌برند. بهره‌گیری نظام سلطه و در رأس آن امریکا از رسانه‌ها در جهت تسلط بر ملت‌ها نمونه‌های فراوانی دارد که می‌توان بر راه‌اندازی جنگ رسانه‌ای در ویتنام، گرانادا، بالکان، کارائیب، افغانستان، جنگ اول و دوم خلیج فارس و. . . اشاره

نمود و از حجم وسیع اقدامات رسانه‌ای در جنگ اخیر به عنوان استراتژی نظام سلطه در به کارگیری روش‌ها، تکنیک‌ها و ابزارهای نوین یاد نمود، در این خصوص می‌توان به استفاده از خبرنگاران همراه که بیش از پانصد تن از آنان در یگان‌های عمل‌کننده همراه نیروها وارد جنگ شدند، اشاره کرد. واقعیت آنست که در پشت صحنه عملیات رسانه‌ای، راهبردی به عنوان سیاست رسانه‌ای قدرت‌ها قرار گرفته است که به صورت رسمی و سازمان یافته اما پنهان با بودجه‌های سری توسط سازمان‌های اطلاعاتی و امنیتی و سرویس‌های جاسوسی راهبردی می‌شود. فرماندهان جنگ رسانه‌ای استراتژیست‌های عملیات روانی و متخصصان تبلیغاتی و عملیات روانی و کارگزاران رسانه‌ای بین المللی می‌باشند. جنگ رسانه‌ای از ویژگی‌هایی هم‌چون توجیه و اجرای عملیات روانی از طریق بحران‌سازی، سیاه‌نمایی و تحریک افکارعمومی مخاطبین و جامعه در جهت رسیدن به اهداف برخوردار است. صاحبان قدرت برای اجرای سیاست‌های خود روش‌هایی را در جهت انحصاری نمودن رسانه‌ها به اجرا می‌گذارند و در این رابطه از روش‌های پنهان‌کاری، حمله و انهدام هدف، برچسب‌زدن، فرض و تصور پیش‌گیرانه، ظاهرسازی، کوچک‌نمایی، توازن نادرست و عدم پی‌گیری استفاده می‌کنند. رسانه‌ها ویژگی‌های خاصی نیز دارند، از جمله این که گفتمان را حیاتی‌ترین حوزه و سلاح می‌دانند و متقاعد ساختن یک نفر برای پیوستن به خودی، را بسیار ارزان‌تر از کشتن او می‌دانند و کلمات را کم‌هزینه‌تر از گلوله می‌پندارند. در این راستا، از ابزارهای متنوع و مدرن رسانه‌ای در گروه‌های مختلف دیداری، شنیداری و نوشتاری بهره می‌برند.(afand. blogfa. com)

۸-۱۰-۸- جنگ اقتصادی و اینترنت

جرایم و خسارات اقتصادی به صورت بالقوه در حملات شبکه‌ای وجود دارند. خسارات اقتصادی وارد شده ممکن است از هزینهِ صرف شده برای یک حملهِ شبکه‌ای بسیار بیش‌تر باشند. گردباد اندرو، که بزرگ‌ترین بلای طبیعی در تاریخ امریکا محسوب می‌شود، ۲۵ میلیارد دلار خسارت در بر داشت. در شرایط طبیعی، هزینهِ خسارات سالانه طوفان‌ها، گردبادها و سیل در این کشور حدود یازده میلیارد دلار برآورد شده است، در حالی که تخمین زده می‌شود که ویروس لاو باگ در سراسر جهان هزینه‌ای معادل سه تا پانزده میلیارد دلار را به کاربران رایانه تحمیل کرده باشد. در اینجا، قصد نداریم به پرسش دربارهِ چگونگی برآورد خسارت‌های وارد شده از سوی این ویروس بپردازیم. اما چنان‌چه مشاهده می‌شود خسارت‌های یک حملهِ شبکه‌ای، بسیار بیش‌تر از خسارت‌های طبیعی در یک سال است. در این زمینه، می‌توان به

هزینه‌های‌اندک یک حملهِ شبکه‌ای اشاره کرد. یک دانش‌جوی فیلیپینی با استفاده از رایانه و چند نرم‌افزار توانست خسارت درخور توجهی را به یک شرکت اقتصادی وارد آورد. توان یک دانش‌جوی فیلیپینی برای وارد آوردن خساراتی به این گستردگی با استفاده از تجهیزات نه چندان گران‌بها، نشان دهندهِ خطر بالقوه‌ای است که حملات شبکه‌ای می‌توانند به اقتصاد جهانی وارد آورند.

خسارات مالی‌ای که حملات شبکه‌ای به اقتصاد وارد می‌آورند، می‌تواند از دست دادن دارایی‌های فکری و معنوی، اختلاس مالی، لطمه به اعتبار، کاهش تولید و افزایش بدهی به اشخاص دیگر را شامل شود. خسارات وارده در اثر از دست دادن فروش و کاهش تولید، درصد عمده‌ای از خسارات حملات شبکه‌ای و ویروس‌ها را تشکیل می‌دهند، اما این خسارت‌ها به معنی وارد آمدن خسارت به اقتصاد ملی نیست. برای نمونه، اگر یک فروشندهِ کتاب در اینترنت هدف حملهِ شبکه‌ای قرار بگیرد و نتواند خدمات خود را ارائه دهد، مشتریان به یک فروشندهِ دیگر مراجعه می‌کنند. هرچند بازار فروشندهِ اول کساد خواهد شد، اما این امر در اقتصاد ملی تأثیر چندانی نخواهد داشت. در صورت در دسترس نبودن فروشندهِ اول، ممکن است تنها تعداد بسیار اندکی از مشتریان به سایت دیگری مراجعه نکنند، اما فروش‌های از دست رفته با مراجعه‌های بعدی همان مشتری جبران خواهند شد. خطرها و زیان‌های ناشی از اختلاس‌های مالی و سرقت دارایی‌های فکری و معنوی از طریق اینترنت بیش از هر چیزی، تجارت را تهدید می‌کنند؛ جرائمی که تعداد آن‌ها روز به روز در حال افزایش است.

ماهیت فراملی مسائل مربوط به امنیت شبکه‌ای باید بیش از این مورد توجه و تأکید قرار بگیرد. در چند سال گذشته، ظهور گروه‌های جنایتکار بسیار ماهری را شاهد بوده‌ایم که به شبکه‌های تجاری خساراتی را وارد آورده‌اند. هدف آنها، نه ایجاد رعب و وحشت، بلکه اختلاس یا جمع آوری اطلاعاتی است که از نظر اقتصادی ارزشمندند. طبق گزارش‌های شرکت‌های بزرگ در این زمینه، سرقت اطلاعات خصوصی، هنوز هم بستر بسیاری از زیان‌های جدّی و وخیم می‌باشد. باید بین این جرایم و حملاتی که قطع سرویس دهی را باعث می‌شوند و هم‌چنین، حمله با ویروس‌ها تمایز قائل شد. هرچند دو حملهِ اخیر، برای امور تجاری خطرهای بالقوه‌ای دارند، اما به‌اندازهِ حمله به شبکه‌های تجاری خطرناک نیستند. (afand. blogfa. com)

۸-۱۱- سئوالات خودآزمایی

۱. تاریخچه مختصر اینترنت را از دیدگاه نظام سلطه بنویسید.
۲. جنگ اینترنتی چیست؟ توضیح دهید.
۳. دسترسی به اطلاعات محلی از طریق اینترنت را توضیح دهید .
۴. نقش شبکه‌های اجتماعی موجود در اینترنت را در براندازی حاکمیت‌ها را توضیح دهید.
۵. پنج نوع از اطلاعات تبادلی از طریق اینترنت را نام برده و توضیح دهید.
۶. جنگ سایبری را توضیح دهید.
۷. تفاوت بین جنگ و جرم سایبر را توضیح دهید.
۸. مبانی و اصول امنیت رایج در اینترنت را بنویسید.
۹. نقش شخصیت مجازی در ناامنی اینترنت را توضیح دهید.
۱۰. انواع روش‌های اخذ اطلاعات پنهان از طریق روش‌های رایج در روی اینترنت را بنویسید.

۹

فصل نهم :ماهواره‌ها

آن چه در این فصل می‌خوانید:

- **ماهواره؛ بیم‌ها و امیدها**
- **تنّوع کار کرد و افزایش بیم**
- **مدارهای ماهواره‌ای**
- **استقرار ماهواره‌ها**
- **شبکه ماهواره‌ای جاسوسی اشلون**
- **کاربرد نظامی ماهواره‌ها**

۹- ماهواره‌ها

اهمیت کسب اطلاعات بر هیچ‌کس پوشیده نیست. توانایی کنترل اطلاعات نیز پایه اصلی و اساسی حیات دولت‌ها و شرکت‌های بازرگانی در جهان کنونی است. این امر عنصر اساسی روابط بین‌المللی، دادوستدهای بازرگانی، قدرت اقتصادی، نیروی دفاعی و پیوندهای صلح و دوستی است و در یک جمله "اطلاعات یعنی‌قدرت" و هر کشوری که به اطلاعات علمی، فنی، دفاعی، بازرگانی و. . . دسترسی دارد، می‌تواند از رقیبان خودپیشی بگیرد.

در جهان کنونی، ملاحظات ژئوپلتیکی، ژئواستراتژیکی و ژئواکونومیک به واسطه انقلاب حقیقی ناشی از تکنیک‌های نوین انتشاراتی ـ اطلاعاتی، عمیقاً تأثیر گرفته‌اند و داده‌های جدیدی را خلق کرده‌اند. دیروز "پیک‌پیاده" یا سواره وجود داشت و اخبار توسط اسب، "کشتی" یا "کبوتر نامه‌بر" و غیره. . . انتقال می‌یافت؛ اما امروز وسایل الکترونیکی جای آنها را گرفته‌اند. به‌طور نمونه به کمک ماهواره امکان بهبود بخشیدن به شناخت منابع‌طبیعی، امکان پیش‌بینی هوا یا ایجاد روابط مخابراتی با فاصله‌های دور فراهم شده است. دیگر احتیاجی به‌ایجاد زیربناهای ثابت بین این نقاط وجود ندارد. لذا معلوم می‌شود که برخلاف تکنیک‌ها و فنون کابل‌سازی، استفاده از ماهواره‌های مخابراتی این امکان را می‌دهند تا در فضا بین دستگاه‌های گوناگون پخش و دریافت ثابت یا متحرک روی کره زمین زمینی یا دریایی برقرار شود.

امروزه ثانیه‌ها به مثابه قرن‌ها هستند. در عرض کم‌تر از یک ثانیه بین دو نفر، دو دستگاه، دو بنگاه و. . . ارتباط ایجاد شده و اطلاعات ردوبدل می‌شود. (prr. ir)

امروزه با استفاده از فاکس، تلفن، اینترنت و. . . در عرض چند دقیقه یا چند ثانیه پیام‌ها ردوبدل می‌شود.

بدین‌ترتیب به‌خوبی می‌توان به اهمیت تغییرات ژرف و پایه‌ای که ناشی از کاربرد تکنیک‌های جدید پخش اطلاعات است، پی‌برد. اهمیت این موضوع مخصوصاً هنگامی آشکار می‌شود که مسایل مربوط به دفاع از امور لشکری، به اولین و مهم‌ترین مسایل اطلاعاتی تبدیل گردند. اگر چه سیستم‌های دفاعی همواره محتاج اطلاعات بوده‌اند، اما اهمیت این اطلاعات در زمان ما از لحاظ کمی و کیفی متفاوت است.

اطلاعات در جهان کنونی به صورت یکی از مهم‌ترین عناصر شکل‌دهنده عهد "جدید" اجتماعی ـ اقتصادی در آمده است و به همین دلیل در بسیاری موارد سخن از جامعه اطلاعاتی به میان می‌آید.

اطلاعات انسان را به شیوه‌های جدید و روش‌های نوین زندگی راهنمایی می‌کند و او را به ارایه تعریف جدیدی از روابط با فضا، به عنوان جزیی از زندگی روزمره (نظیر استفاده از تلفن‌های همراه) وا داشته است.

از آغاز قرن نوزدهم شاهد جهانی شدن[۳] اقتصاد و انکار فضا و مکان (با وسایل حمل‌ونقل و ارتباط جمعی‌سریع) هستیم. دو عامل الکتریسته وترانزیستور، موجب تسهیل ارتباطات در سطح کره زمین شده، به روند آن‌سرعت بخشیده است.

ژ. گوتمن[۴] معتقد است سرعت ارتباطات، مفهوم سنتی مرزها را در هم نوردیده و دیگر برای گذر از مرزها احتیاج به ویزا نیست؛ تلفن مرزها را شکسته است، رایانه حد و مرزی نمی‌شناسد و اینترنت فراگیر شده است. در واقع امروزه "جهان بیش از یک کالئدوسکوپ[۱] متحرک‌ها، شبکه‌ها، سلسله مراتب و سطوح سیاسی است. شرکت‌های چند ملیتی غول‌آسا، روابط بین‌المللی فرد با فرد، نقشی بیش از پیش فراگیرتر را بازی می‌کنند. در چنین جهانی است که ملت‌ها باید بیش از پیش به حرکات و اعمال خود و دیگران توجه داشته‌باشند. زیرا در این جهان امکان جذب دیگران فراهم آمده است و می‌توان با ظرافت، فرهنگ و تمدن خود را جهانی ساخت. آمریکا و کشورهای غرب، از این وسایل به نحو عاقلانه و گاه مزدورانه‌ای استفاده می‌کنند. آنها با بهره‌گیری از تبلیغات علمی و فنی را مسخ کرده و مفتون و شیدای فرهنگ خود سازند.

با در نظر گرفتن اهمیت انتقال اطلاعات و تحولاتی که در شیوه‌ها و وسایل ارتباطی پدید آمده، باید توجه داشت که ارتباطات فضایی (ماهواره‌ای)، شریانی بزرگ و اساسی ایجاد کرده است که مرزها را از بین می‌برد. در این زمینه باید به دو نکته توجه کرد:

۱. قدرت سیاسی و ایجاد شبکه‌های اطلاع‌رسانی

---

۳. Mondialisation

۴. J. Gothman

۱- Keleidoscope : استوانه‌ای که در طول آن چند آیینه گذاشته‌اند و اشیایی کوچک و رنگین که در وسط لوله است، به شکل مختلف قرینه‌وار جلوه می‌کند.

۲. شبکه‌های اطلاعاتی دولتی (تلگراف، تلفن و. . .)

اکنون اطلاعات و ارتباطات را در رابطه با اقتصاد و مسایل مالی نمی‌توان نادیده گرفت. آینده در دست این قدرت‌هاست و دولت‌های غربی در این مورد سیاست‌های خاصی دارند و از استراتژی‌های اطلاعاتی مخصوصی در قالب بحث اطلاعات و قدرت اقتصادی استفاده می‌کنند.

در عصر ما که به عقیده باکیسا [۱] و گان [۲] عهدی است که در آن، نه تنها تحولات خاصی رخ داده؛ بلکه گسستی در رابطه جهان امروز با گذشته اقتصادی، ارتباطی و مفهومی دنیای غرب (از قرون وسطی تا اولین انقلاب صنعتی و تا سال‌های ۱۹۶۰) پدید آمده است (باکیسا و گان، ۱۹۸۵)

۹-۱- ماهواره؛ بیم‌ها و امیدها

پرتاب نخستین ماهواره به فضا شادی‌ها ونگرانی‌های هم‌زمانی را در بشر موجب شد ؛ شادی از این بابت که آرزوی دیرین انسان برای دست‌یابی به آسمان پر رمز و راز، جامه عمل و تحقق می‌پوشید و دروازه‌های دنیایی شگفت و بس پهناور به روی او گشوده می‌شد.

بلند پروازی و فزون خواهی همیشگی فرزند آدم به او نوید می‌داد که با بهره‌مندی از منابع ناشناخته موجود در سیارات و ستارگان دیگر می‌تواند به فردایی به‌تر بیندیشد و بر دیگران برتری جوید .

در مقابل ، نگرانی‌ها نیز کم نبود ؛ نگرانی از این که باز هم آدمیان فرصت‌ها را به تهدید تبدیل کنند و از نو یافته‌های خویش بهره‌برداری‌هایی کنند که آرامش موجود را نیز بر هم زند . این هراس ،در آن زمان که هنوز آثار وحشتناک جنگ جهانی دوم در گوشه و کنار به راحتی دیده می‌شد ، بی جا هم نبود . مردم شاهد آن بودند که چگونه برتری جویی و سیری ناپذیری هواداران قدرت ، همه هستی آنان را به کام خود کشید و خسارت‌هایی باور نکردنی بر جان و مال آنان تحمیل کرد . همین مردم اینک می‌دیدند که از یک سوی کار زار گامی بلندتر برداشته شده و ((اسپوتنیک یک)) راهی فضای ناشناخته گردیده است . طبیعی است که آن خاطره‌های هراسناک همگان را در اندیشه فرو برد که مبادا فضا هم نا امن شود و استفاده‌های نظامی از آن بر ابعاد خطر بیفزاید . این دلهره ، به‌ویژه آنگاه جدّی‌تر می‌نمود ، که با پایان جنگ

---

۱. Baquisat
۲. Ganne

جهانی دوم ، جنگ سرد تبلیغاتی اندک اندک جای‌گزین قدرت نمایی‌های فیزیکی می‌شد و هر بازیکنی در میدان سیاست می‌کوشید تا با اشاره به توانمندی‌های ناشناخته و ویرانگر خویش قدرت مانور را از طرف مقابل گرفته و نتیجه را از پیش به سود خود اعلام کند .

۹-۲- تنّوع کار کرد و افزایش بیم

اگر دغدغه‌های ناشی از تولد ماهواره در حدّ تهدیدات نظامی هم باقی می‌ماند ، چاره‌ای جزء ورود حقوق به این عرصه وجود نداشت ؛ چه رسد به آن که این پدیده بشری با شتابی باور نکردنی تکامل یافت و روز به روز بر قابلیت‌ها و کارکردهای خود در حوزه‌های مختلف زندگی افزود . امروزه نه تنها عرصه‌های ((نظامی و امنیتی))، که زمینه‌های ((ارتباطی و علمی)) ، ((اقتصادی و تجاری)) و بالاخره ((سیاسی و فرهنگی)) نیز به شدّت تحت تاثیر توانمندی‌های ماهواره قرار گرفته‌اند . حضور این فن‌آوری در هر یک از این عرصه‌ها موجب پیدایش موضوعات و مسائل جدیدی شد که نیازمند قانون‌گذاری در ارتباط با آن‌ها است و به همین دلیل ((حقوق بین‌الملل ارتباطات)) که عهده‌دار مبحث ((حقوق ماهواره‌ها)) نیز می‌باشد از گستره و عمق فراوانی برخوردار شده است

در این نوشتار تلاش می‌شود تا با اشاره‌ای بسیارگذرا به کارکردهای ماهواره درهر یک از عرصه‌های یاد شده، دور نمایی از نیازها و مباحث حقوقی نیزترسیم شود .

۹-۲-۱- کارکرد((نظامی و امنیتی))

دیدیم که نقطه آغاز گفتگوهای حقوقی پیرامون ماهواره‌ها ،نگرانی قابل درک دولت‌ها و ملت‌ها از شیوه و اهداف به‌کارگیری این فن‌آوری نو پیدا بود و به همین جهت محور اصلی همه مذاکرات و اسنادی که بر جای مانده است ، همان ((صلح آمیز)) بودن استفاده از فضای آزاد است . با این حال طبیعی است که میزان و نوع تهدید در این ۵۰ سال تغییر عمده کرده باشد سلاح‌های کشتار جمعی و موضوع خلع سلاح هنوز از مسائل اصلی و مورد توجه جامعه بشری است و همه می‌کوشند تا ، دست کم در شعار و قانون ، به دنبال تضمین‌های حقوقی برای جلوگیری از تکرار فجایع انسانی وگسترش آن به رقابت‌های فضایی باشند.

همه از دیدار دوباره با صحنه‌های مشابه جنگ جهانی هراسناک هستند . اما در همان حال برای رقابت با دیگران روز به روز بر قدرت نظامی و امنیتی خود می‌افزایند . جمع آوری اطلاعات مورد نیاز در عملیات‌های نظامی ، عکس‌برداری از نقل و انتقال‌های تجهیزات و نیروی انسانی ،

استراق سمع و شنود ارتباطات تلفنی و رادیویی و جاسوسی به شیوه‌های مختلف نمونه‌هایی از بکار گرفتن ماهواره در حوزه‌های نظامی و امنیتی است .

افزون بر این‌ها ممکن است از ماهواره در مسیر اهداف تروریستی نیز بهره‌برداری شود و برای مثال پیام‌های ناشناخته یا آموزش‌های غیر مستقیم از طریق صدا یا تصویر به هر جای دنیا ارسال گردد. پیشتیبانی تبلیغاتی و روانی ازتروریست‌ها ، تشویق آنان به ادامه فعالیت‌های ضد بشری ، پنهان کردن ابعاد جنایت‌های آنان و بدتر ، توجیه آن نمونه‌های دیگری از کارکرد ماهواره‌ها بر ضد امنیت و صلح جهانی است که هر روزه شاهد تداوم آن در جریان پوشش خبری و اطلاعاتی جنایات اسرائیل علیه مردم محروم فلسطین از سوی رسانه‌های وابسته به سلطه خبری جهان هستیم. ترویج نفرت و خشوت ، نقض و تهدید صلح از جرایم بین‌المللی رسانه‌ها است که می‌تواند پیامدهایی بسیار وسیع‌تر ازجنگ‌های رودرروی تاریخی داشته باشد .

بنابر این نه تنها گذشت زمان و مشاهده آثار ویران‌گر مسابقات تسلیحاتی در گذشته ، تهدیدات نظامی و امنیتی را منتفی نساخته و کاهش نیز نداده است ، که به دو جهت دغدغه‌های بشر در این حوزه‌ها بیش‌تر و متنوع‌تر شده است ؛ نخست از آن جهت که مفهوم و تعریف صلح و جنگ در شرایط نوین پس از جنگ جهانی دوم دگرگون شد و نتایج درگیری‌های بی امان و خونین همگان را به این نتیجه رساند که سلطه بر دیگران را به نوعی دیگر ببینند و بخواهند. این‌گونه بود که جنگ تبلیغاتی و روانی جای تهاجم‌های نظامی را گرفت و دوران جنگ سرد آغاز شد . در این نوع جنگ ، هم تهاجم و هم دفاع معنایی دیگر یافت و طبیعتاً شیوه‌ها و ابزارهای خاص خود را طلب کرد ؛ که اتفاقا" دست یابی به فضا و تکنولوژی ماهواره به‌ترین زمینه‌ها را در این باب فراهم می‌ساخت .

از جهت دیگر هم پیشرفت حیرت انگیزه و پر شتاب دانش ، تسخیر فضا و بکارگیری موثر و علمی‌تر شیوه‌های ارتباطی قابلیت ماهواره را برای بهره‌برداری‌های برتری جویانه بارورتر می‌کرد .

این عوامل مجموعاً سبب شده است که مباحث حقوقی مربوط به تهدیدات نظامی و امنیتی فعالیت در فضا و ماهواره هنوز هم ضروری و زنده باشد و البته ادبیات حقوقی در این زمینه متناسب با تحولات عمیق مفاهیم جنگ و صلح دگرگون و وسیع‌تر شود .

۹-۲-۲-کارکرد((ارتباطی و علمی))

یکی از کارکردهای مثبت و شناخته شده ماهواره‌ها انقلابی است که در حوزه ارتباطات و دانش بشری به وجود آورد و البته به نوبه خود مباحث حقوقی نوینی را مطرح ساخت . گرچه اولین ماهواره‌ها با مقاصد عمدتا" نظامی به فضا پرتاب شدند ، امّا تا روزی که همین ابزار برای بهره‌برداری ارتباطی آماده شد زمان چندانی فاصله نداشت . نخستین ماهواره شوروی در روز چهارم اکتبر ۱۹۵۷ به آسمان رفت و حدود ۵ سال بعد ، یعنی ۱۰ جولای ۱۹۶۲ اولین ماهواره مخابراتی آمریکا هم راهی فضا گشت . این ماهواره ارتباطی می‌توانست برنامه‌های زنده برای منطقه اروپا ارسال کند . اکنون که چهل سال از آن روزها می‌گذرد ؛ قدرت شگرف ماهواره در کسب و ارسال خبر از دورترین نقطه‌ها و با بالاترین سرعت ممکن امری نیست که بر کسی پنهان مانده باشد .

امروز آژانس‌های خبری به ابزاری کار آمد برای رشد و توسعه همه جانبه کشورها و تسلط آنان بر دولت‌های ضعیف‌تر تبدیل شده است . اشتیاق پایان ناپذیر قدرتمندان برای کسب اطلاعات بیش‌تر به منظور سلطه قوی‌تر ، آنان را به نادیده گرفتن حریم خصوصی دیگران تحریک کرده و کار را به آنجا رسانده است که رسانه‌های خبری مرز روشنی برای ورود خود به زندگی مردم قائل نیستند . این واقعیت هم به نوبه خود فصل جدیدی را به روی حقوقدانان و مصلحان اجتماعی گشوده است و آنان را وادار داشته تا به شفاف سازی حریم خصوصی افراد و تعبیه ضمانت اجراهای کارآمد برای تجاوز به آن رو آورند .

در هر صورت انقلاب یا انفجار اطلاعات که خود منشا قدرت و ابزاری برای سلطه است باید خود را وام‌دار فن‌آوری‌های نوین فضایی بداند که توانسته است چشمان تیز بین بشر را به پنهان‌ترین نقاط جهان پهناور باز کند . اگر در چند دهه پیش آدمیان از تحولات بزرگ در همسایگی خویش نیز بی خبر باقی می‌ماندند، امروز به یاری دانش و صنعت چنان بر وسعت و سرعت اطلاعات افزوده شده که مشکل اصلی بشر چگونگی گزینش و انتخاب اطلاعات است نه دست‌یابی به آن .

این دگرگونی در حوزه سیاست از اهمیتی بزرگ برخوردار است ، امّا منحصر در آن نیست و از جمله باید مسائل حقوقی ناشی از دست‌یابی دیگران به دستاوردهای علمی و صنعتی را در نظر گرفت . در کنار پیشرفت علم و ارتقا سطح زندگی عمومی انسان‌ها در اثر این تبادلات علمی، البته از دیدگاه حقوقی جنبه‌های ((حقوق مالکیت‌های معنوی)) نیز بسیار مهم است . ماهواره ، به‌ویژه با توجه به فن‌آوری‌های رایانه‌ای ، موجب شده است که دیگر نتوان از حفظ و

حبس دست‌آوردها و اطلاعات سخن گفت . ممکن است در یک لحظه محصول سال‌ها تلاش علمی و هنری و صنعتی افراد ، سازمان‌ها و کشورها به یغما رود و مثلاً هزاران هزار صفحه تحقیقات و داده‌های ارزشمند ، و احتمالاً محرمانه ، در لوحی فشرده جابه‌جا شود .

این‌گونه است که اشاره به حقوق مالکیت معنوی در همه اسناد مهم جهانی به صورت مقررات حمایت از حقوق خالقان آثار به چشم می‌خورد و برای حمایت از آن ، معاهدات و ساز و کارهایی در نظر گرفته شده که به دو بخش کلی قابل تقسیم است ؛ یک بخش حقوق مالکیت‌های صنعتی و تجارتی و بخش دیگر حقوق مالکیت‌های ادبی و هنری . اینک سازمان جهانی مالکیت معنوی که اختصاراً ((وایپو)) گفته می‌شود نقش اساسی را در هدایت این جنبه از حقوق بین‌الملل بر عهده دارد .

۹-۲-۳-کارکرد ((اقتصادی و تجاری))

کارکرد دیگر ماهواره‌ها ، اقتصادی است . گرچه همان کسب و انتقال اخبار و اطلاعات هم پیامدهای تجاری و اقتصادی را به دنبال داشته و دارد ، امّا فعالیت‌های دیگری هم برای ماهواره‌ها قابل انجام است که به تقویت این کارکرد می‌انجامد . توان عکس‌برداری ، فیلم‌برداری ،تهیه گزارش و ارائه خدماتی نظیر پیش بینی آب و هوا و تغییرات جوّی در دنیای ما مشتری‌های خاص خود را دارد. این توانمندی‌ها هم اکنون مبنای فعالیت بسیاری از صنعت‌های بزرگ اقتصادی است که صنعت هواپیمایی و نیز حمل و نقل دریایی و زمینی از جمله آن‌ها است. اگر رواج و گسترش تجارت الکترونیکی را هم در کنار این مجموعه لحاظ کنیم ، آنگاه اهمیت موضوع روشن‌تر می‌شود .

تبلیغات بازرگانی را می‌توان بارزترین جلوه کارکرد تجاری ماهواره‌ها دانست که البته در جای خود آثار سیاسی و فرهنگی نیز داشته و دارد . فن‌آوری قدرتمند ماهواره‌ای امکان دور زدن مقررات و ضوابط تعیین شده ملی در داخل کشورها را فراهم می‌کند و زمینه ارسال پیام به داخل کشورهایی را هموار می‌سازد که در مقابل پیام‌های ارسالی خارجی به داخل محدوده سرزمینی خویش ممانعت می‌کنند. در بُعد رسانه‌ها ، عامل دیگر موثر در فرآیند جهانی شدن ، ظهور شرکت‌ها و واحدهای غول آسای رسانه‌ای و فیلم سازی است که حاصل ادغام شرکت‌های دیگر هستند . پیدایش غول‌های جدید در همه حوزه‌ها ، از جمله صنعت ۱۲۵ میلیارد دلاری تبلیغات و آگهی نیز قابل مشاهده است . واشنگتن نیز حمایت از رسانه‌های تجارتی آمریکایی و فراهم آوردن زمینه رقابت و جلوگیری از انحصار را وظیفه خود می‌داند ، ولی . . . .))

بیهوده نیست که((آمریکا با ۶ ٪ جمعیت کل جهان ، ۷۵ ٪ تبلیغات دنیا را انجام می‌دهد . تولیدکنندگان سالانه بیش از ۴۵ میلیارد دلار صرف تبلیغات و بیش از ۶۰ میلیارد دلار هزینه به معرفی کالا از طریق کوپن تخفیف ، نمونه‌های مجانی ، تخفیف بعد از فروش و موارد مشابه اختصاص می‌دهند . این مبلغ تبلیغاتی معادل ۲۰۰ دلار برای هر آمریکایی است ؛ رقمی که بیش از در آمد سرانه یک شهروند متعارف جهان سومی است))

این واقعیت‌ها موجب شده است که ((در دهه‌های آخر قرن بیستم ، بر اثر کاربرد گسترده تبلیغات بازرگانی در برنامه‌های تلویزیونی و به‌خصوص برنامه‌های پخش مستقیم ماهواره‌ای در سراسر جهان ، علاوه بر مقررات گذاری‌های خاص این تبلیغات در سطح بین‌المللی و منطقه‌ای همکاری کشورها نیز به ضرورت برخی مقررات گذاری‌های ویژه در مورد تبلیغات بازرگانی توجه پیدا شده است و به همراه آن مطالعات حقوقی تبلیغات مذکور در گستره جهانی خارج از حوزه حاکمیت دولت‌ها نیز اهمیت یافته است .))

تاثیر ماهواره‌ها بر گسترش صنعت گردش‌گری و تاثیرات عمیق و همه جانبه آن هم موضوع قابل توجه دیگر در حقوق مربوط به کارکرد تجاری ماهواره‌هاست که پرداختن به آن فرصت دیگری می‌طلبد .

۹-۲-۴-کارکرد ((سیاسی و فرهنگی))

به رغم آن چه در باره کارکردهای مهم ماهواره در زمینه‌های مختلف گفته شد ، هیچ کس نمی‌تواند نگرانی ویژه خود از کارکردهای سیاسی و فرهنگی ماهواره‌ها را پنهان کند ؛ دغدغه‌ای که شاید همه نگرانی‌های پیشین نیز به نوعی به آن بازگردند . دلیل پیوند سیاست و فرهنگ در این‌جا و طرح آنها در کنار یک‌دیگر رابطه دو سویه و تنگاتنگی است که میان آنها وجود دارد . این پیوند و ارتباط ، اگر هم در گذشته کم‌تر مورد توجه بوده باشد ، نزد پژوهش‌گران و دانشمندان امروز حوزه‌های مختلف علوم اجتماعی به عنوان ((اصل موضوعه)) و مسلّم پذیرفته شده است .

باورها وارزش‌های فرهنگی مورد احترام ملت‌ها اساس تصمیم گیری‌ها و اقدامات سیاسی آنهاست و به همین دلیل سرچشمه تغییرات اجتماعی را باید در تغییرات درونی و فرهنگی ملت‌ها جست‌وجو کرد . انگیزه اصلی حمایت ملت‌ها از دولت‌های خویش یا دست کشیدن از حمایت و پیدایش شکاف میان مردم و حاکمیت‌ها ، همین احساس درونی مردم است که آیا

دولت حاکم حافظ ارزش‌های مورد احترام آن‌ها و در صدد تحکیم و توسعه منافع ملی هست یا نه .

اینجاست که نقش رسانه‌های خارجی در تغییر گفتمان ملی و در نتیجه اثرگذاری در بخش سیاست و حاکمیت به خوبی آشکار می‌شود . ((منافع ملی یک حقیقت عینی نیست (که افراد یک ملت آن را درک کرده یا نکرده باشند) بلکه بیش‌تر مجموعه‌ای متکثر ترجیحات ذهنی است که هرگاه نیازمندی‌ها و تمایلات اعضا ملتی تغییر کند ، آن‌ها نیز دگرگون می‌شوند .))

ماهواره‌ها با توانایی‌های خاص خود در این زمینه نقشی تعیین کننده دارند و می‌توانند با تبلیغات جهت‌دار برای تغییر فرهنگ و سرانجام تغییر دولت‌ها اقدام نمایند . به همین جهت در دوران کنونی تبلیغات هم می‌تواند ابزاری برای مداخله در حاکمیت کشورها و براندازی دولت‌ها محسوب شود . ((تبلیغات بر اندازانه)) دیگر اصطلاحی شاعرانه و ناشناخته تلقی نمی‌شود .

پیدایش اصطلاح ((تهاجم فرهنگی))هم بر همین اساس مبتنی بر واقیعتی است که جهانیان با همه وجود آن را درک و لمس می‌کنند و عجیب اینکه فهم آن برای برخی از مدعیان فرهنگ در کشور ما گران آمده است . (۱۴۹ .۳۲ .۱۱ .۸۴)

۹-۳- استقرار ماهواره‌ها:

ماهواره‌های عملیاتی که برای دریافت و ارسال سیگنال‌ها از زمین مورد استفاده قرار می‌گیرند، از نقطه‌ای روی زمین پرتاب می‌شوند و در یک مدار خاص و ثابت قرار می‌گیرند.

پس از آن که ماهواره در مدار ثابت قرار گرفت ، دستگاه فرعی دیگری هم در ماهواره فعال می‌شود تا قدرت الکتریکی مورد نیاز تکرار کننده‌ها و دیگر دستگاه‌های ماهواره را تولید و تنظیم کند.

۹-۳-۱- مدار ژئوسنکرون :

مداری که برای ارتباط ماهواره‌های محلی از اهمیت بیش‌تری برخوردار است ، مدار ژئوسنکرون نام دارد. ماهواره باید حدالامکان در نقطه‌ای از مدار ژئوسنکرون قرارگیرد که نیروی جاذبه زمین روی آن اثری نداشته باشد این مدار دایره‌ای شکل روی صفحه‌ای قرار دارد که از خط استوا می‌گذرد. در این حالت ، سرعت زاویه‌ای ماهواره و زمین با هم برابر است. ارتفاع ماهواره از سطح زمین در این مدار ۳۵۷۸۸ کیلومتر است.

۹-۳-۱-۱- مزایای مدار ژئوسنکرون :

ماهواره نسبت به زاویه‌ای که ایستگاه زمینی آن را می‌بیند، ثابت است ، درنتیجه احتیاجی به تغییر جهت آنتن نیست ولی تنظیم آن ضروری است تعداد زیادی از ایستگاه‌های زمینی می‌توانند پوشش یک ماهواره در این مدار قرار گیرند به طوری که آنتن هر ماهواره می‌تواند حداکثر ۴۲/۴ درصد سطح کره زمین را بپوشاند.

۹-۳-۱-۲- معایب مدار ژئوسنکرون :

نواحی قطبی یعنی مناطقی که دارای عرض جغرافیایی بیش‌تر از ۴۱/۳ درجه‌اند ، زیر پوشش قرار نمی‌گیرند. زمان تاخیر انتشار به علت بعد مسافت رفت وبرگشت ، زیاد است .

۹-۴- شبکه ماهواره ای جاسوسی اشلون

ایستگاه‌های گیرنده شبکه جاسوسی اشلون در تمام دنیا مستقر است آژانس امنیت ملی ایالات متحده (NSA) سیستم جاسوسی جهانی با اسم رمز اشلون۱ را طراحی کرده است. این شبکه به کلیه تماس‌های تلفنی، فاکس‌ها و پیام‌های تله تکس و پست‌های الکترونیکی که در هر نقطه از دنیا رد و بدل می‌شوند، دسترسی دارد و آن‌ها را بررسی می‌کند. شبکه اشلون از سوی آژانس امنیت ملی آمریکا کنترل می‌شود و با همکاری سازمان‌هایی چون، ستاد ارتباطات کل در انگلیس، مقر امنیتی ارتباطات در کانادا، ریاست امنیت دفاعی استرالیا و دایره‌ی امنیت ارتباطات کل در نیوزلند، فعالیت می‌کند. این سازمان‌ها تحت یک توافق‌نامه خیلی محرمانه در سال ۱۹۴۸ آغاز به کار کرد. نحوه فعالیت سیستم اشلون به این گونه است که ایستگاه‌های گیرنده داخلی خود را در همه نقاط دنیا مستقر می‌کند تا کلیه ماهواره‌ها، طول موج‌های کوتاه، ترافیک‌های ارتباطاتی سلولی و فیبرنوری را به دام بیاندازد و سپس آن را به رایانه‌های انبوه و با قابلیت بالای آژانس آمریکایی مزبور برای تجزیه و تحلیل و بررسی دقیق ارسال کند. این پیام‌های مختلف پس از دریافت توسط ایستگاه‌های شنود، شامل مکالمات و مکاتبات هستند که توسط یک سیستم تحلیلی هوشمند به دقت بررسی می‌شوند. هدف اصلی از فعالیت آژانس مزبور ردیابی و کشف گروه‌های سیاسی ناشناس و فعالیت‌های آنها است. سیگنال‌های بسیار اندکی می‌توانند از دام این گیرنده‌های الکترونیکی فرار کنند. بهره‌گیری از ایستگاه‌های گیرنده

---

[۱] ECHELON

زمینی، کشتی‌های هوشمند در آب‌های هفتگانه‌ی دنیا و ماهواره‌های سری قوی در ارتفاعات ۲۰ هزار مایلی از سطح زمین قدرت فعالیت آژانس امنیت ملی آمریکا و اعضای پیمان UKUSA را افزایش داده است. مناطق جغرافیایی مختلف در سرتاسر دنیا بین اعضای این پیمان تقسیم شده است؛ به طوری که آمریکا در بخش بررسی سیگنال‌های ارتباطاتی قاره آمریکا، انگلیس در بخش اروپا، آفریقا و غرب روسیه، استرالیا در بخش آسیای جنوب شرقی، جنوب غربی اقیانوسیه و مناطق شرقی اقیانوس هند، نیوزلند در بخش شرکت‌های غربی اقیانوس آرام و بالاخره کانادا در بخش بررسی سیگنال‌های شمال روسیه، اروپای شمالی و هم‌چنین ارتباطات آمریکایی، فعالیت می‌کنند. روش کار اشلون به این نحو است که می‌تواند بخش زیادی از ارتباطات را با استفاده از رایانه ردیابی کند این کار به‌صورت خودکار و با استفاده از کلید واژها مورد نظر صورت می‌گیرد . که کلید واژه‌ها می‌توانند نظامی، سیاسی، امنیتی و حتی اقتصادی باشند. به‌عنوان مثال اتحادیه اروپا در سال ۸۱ اعلام کرد جاسوسی صنعتی بین سیزده تا یک‌صد و چهل و پنج میلیارد دلار به شرکت‌های اروپایی صدمه زده است. (hamshahri. org)

۹-۵- سئوالات خودآزمایی

۱- ماهواره ها به لحاظ امنیتی چه تاثیری در زندگی انسان ها دارند؟
۲- کارکرد نظامی و امنیتی ماهواره ها را توضیح دهید.
۳- آیا در کنار کارکرد ارتباطی و علمی ماهواره ها , می توان انتظار عملکرد امنیتی داشت؟ چرا؟
۴- لایه های استقرار ماهواره ها را نام برده و توضیح دهید.
۵- نوع بهره برداری طرح اشلون از ماهواره های غیر نظامی را توضیح دهید.

۱۰

فصل دهم:امنیت محیطی و فیزیکی

آن چه در این فصل می‌خوانید:

- تعریف امنیت محیطی و فیزیکی
- خصوصیات فیزیکی محل نگهداری دیتا سنتر
- خصوصیات توپولوژیک محل نگهداری دیتا سنتر
- امنیت فیزیکی محل نگهداری سرور شبکه‌های ناامن
- امنیت فیزیکی محل نگهداری شبکه‌های مهم حساس و حیاتی
- کنترل دسترسی فیزیکی به محل نگهداری شبکه‌ها
- نکات ایمنی کابل کشی شبکه
- رعایت امنیت ابزار دیجیتال در زمان ارسال برای گارانتی و تعمیر
- بازرسی دوره‌ای از محل نگهداری فیزیکی رایانه و چک لیست‌های لازم
- رعایت اصول پدافند غیر عامل در جایابی شبکه‌های رایانه‌ای

۱۰- امنیت فیزیکی

۱۰-۱- امنیت فیزیکی محل نگهداری شبکه‌های مهم حساس و حیاتی

به منظور تعریف اقدامات پدافند غیرعامل ابتدا باید سطوح امنیتی تعریف شوند. در این خصوص یک نوع طبقه بندی برگرفته از سیستم بدن انسان مراکز را به سه دسته حیاتی، حساس و مهم تقسیم می‌کند.

در این تقسیم‌بندی 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 در سراسر کشور می‌گردد.

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.

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.

معیارهای اولویت بندی مراکز

معیارهای زیر در اولویت‌بندی مراکز مختلف باید رعایت شود.

- اهمیت راهبردی نقطه
- میزان ، نوع وپایداری تهدید نسبت به آن
- گستردگی حوزه نفوذ مراکز از نظر جغرافیا و جمعیت
- عمق تاثیرگذاری مرکز از نظر اهمیت در تامین نیازهای حیاتی کشور.
- بازدهی بیشتر با زمان و هزینه کم‌تر برای اجرای طرح پدافند غیرعامل.
- انحصاری بودن مکان یا تجهیزات و عدم امکان تجدید پذیری.
- عدم امکان استفاده از خدمات جای‌گزین و موازی

- ارزش اقتصادی مراکز و تأسیسات و تجهیزات

۱۰-۲- کنترل دسترسی فیزیکی به محل نگهداری شبکه‌ها

نیازمندی کاری برای کنترل دسترسی :

هدف : کنترل دسترسی به اطلاعات

کنترل‌ها در خصوص دسترسی به اطلاعات و فرآیندکاری باید بر اساس ضرورت‌های حفاظتی و کاری باشد. این کنترل‌ها باید سیاست‌های مربوط به تعیین صلاحیت و توزیع اطلاعات را تأمین نماید.

کنترل‌های مربوط به تردد فیزیکی :

مناطق امن باید از دسترسی افراد غیر مجاز با کنترل‌هایی چون موارد ذیل محافظت گردد :

- کنترل امضاهایی که برای تعیین صلاحیت ورود به مناطق دارای اطلاعات طبقه بندی شده، از جمله اماکن پردازش اطلاعات، انجام می‌شود.
- رسیدگی حفاظتی به پی‌آمد ترددات
- برخی لباس‌های شناسایی که امکان دیدن دارد و همه‌ی کارکنان می‌پوشند.
- سیاست‌های برخورد با غریبه‌های فاقد فرد همراه و هر کس که لباس شناسایی را نپوشیده است.
- بازنگری مستمر و به روز کردن حق‌تردد به مناطق امن
- کنترل میهمانان :
- نظارت یا صدور مجوز خاص برای اهداف مجاز
- آموزش اضطراری دستورالعمل‌ها و نیازمندی‌های حفاظتی
- ثبت روز و ساعت ورود و خروج آنها

نیاز کاری به سیستم کنترل‌تردد :

کنترل‌های مناسب و دقیق دسترسی به حفظ اطلاعاتی که در سیستم‌های رایانه‌ای پردازش و ذخیره می‌شوند، کمک می‌کند. اصل «دفاع در عمق» باید بر مبنای مدیریت آسیب‌پذیری دنبال شود و هر کجا مناسب بود از طبقات مختلف برای حفظ اطلاعات حساس استفاده کرد.

خط مشی حفاظتی سیستم سازمان باید به طور واضح نیازهای هر کاربر یا گروهی که به سیستم‌ها، تجهیزات و داده‌ها دسترسی دارند مشخص نماید.

دسترسی کاربر یا گروه کاربران به فایل‌ها باید مطابق نیازهای کاری و اصل «اطلاع در حد نیاز» محدود شود.

دستورالعمل‌های رسمی باید کنترل نماید چگونه دسترسی به خدمات سیستم اطلاعات اعطا می‌شود یا چگونه این دسترسی عوض می‌شود تا این که از دسترسی غیرمجاز به داده‌ها یا منابع سیستم جلوگیری شود.

نقشه‌ی کاری که جزئیات حقوق دسترسی و حقوق ویژه را دربر دارد باید به هر کاربر تخصیص یابد. توجه خاص به حقوق دسترسی مرجع که می‌تواند کنترل‌های سیستم را باطل سازد، داشته باشید. گزارش‌های مدیران باید به دقت کنترل شود و در معرض بررسی خاص توسط افسر حفاظتی اداره قرار گیرد.

سیاست ثبت کاربر باید :

- رسماً صلاحیت کسی را که ID کاربری ارائه می‌کند، تعیین کند.
- سطوح دسترسی را که می‌توان ارائه کرد، کنترل کند.
- سوابق رسمی کاربران ثبت شده را نگه داری کند.
- اطمینان دهد که تمام گزارش‌های کاربران اضافی پاک شده است.
- مرتب حقوق ویژه کارکنان بازنگری شود.

قوانین سیستم کنترل :

کنترل دسترسی با دادن دسترسی به هر چیز شروع و سپس دسترسی به هر نوع سیستم و انبار اطلاعات یا تجهیزات که کاربر نیاز ندارد لغو می‌شود. به هر حال به‌تر است کنترل با رد دسترسی به هر چیز شروع و سپس دسترسی را فقط به اطلاعات مورد نیاز کاربر محدود کرد.

دستورالعمل‌های حفاظتی می‌تواند دسترسی به سیستم‌های اطلاعات را کنترل نماید. دستورالعمل‌ها باید حداقل اطلاعات را راجع به سیستم افشا نماید تا مانع استفاده افراد فاقد صلاحیت گردد.

کم‌ترین امتیاز برای صدور مجوز (اطلاع در حد نیاز) :

اصل کم‌ترین امتیاز را در نظر داشته باشید. بیش‌تر از سطح دسترسی لازم برای انجام وظیفه، اجازه‌ی دسترسی به هیچ کاربری ندهید.

این اصل می‌تواند برای دسترسی کاربران به کار گرفته شود. مثلاً این که آیا امتیاز خواندن یا نوشتن دریافت نمایند.

موانع ورود به سیستم و علائم هشدار دهنده :

ممکن است یک دفاعیه و پی‌گرد قانونی برای حملات مرتبط با رایانه وجود داشته باشد که هشدار دهد چگونه از سیستم اطلاعات استفاده می‌شود. برای به کارگیری چنین دفاعی، یک سازمان باید هشدارهایی در خصوص موانع ورود به سیستم که موارد زیر را در بر دارد، ارائه نماید :

- سیستم فقط برای کاربران مجاز است.
- استفاده از آن اعلام می‌شود.
- سند سو استفاده ممکن است در مسیر قانونی ارائه شود.
- با استمرار دسترسی به سیستم پس از مشاهده‌ی هشدار، افراد خود را کاربر مجاز می‌دانند.

کنترل سیستم‌های فایلی :

سیستم‌های فایلی سرور باید مکانیسم کنترل دسترسی داشته باشد تا مانع دسترسی غیرمجاز یا تفسیر در داده‌ها شود. این امر تا وقتی که سیستم‌های فایل ـ سرور به اینترنت وصل شود، حتی با نصب دیواره آتش (فایروال) ضروری است.

کنترل‌های دسترسی فایل ــ سرور باید محدود کند :

- دسترسی نوشتاری مستقیم به بخش‌های سیستم
- اضافه کردن نرم‌افزار یا خدمات
- دسترسی به فایل‌های کاربران دیگر

مدیریت و دسترسی کاربر :

هدف : ممانعت از دسترسی به سیستم‌های اطلاعاتی

دستورالعمل‌های رسمی باید اعطای حق دسترسی به سیستم‌ها و خدمات اطلاعاتی را کنترل نماید.

این دستورالعمل‌ها باید تمام عرصه دسترسی کاربر از ثبت کاربر جدید تا پاک کردن نام کاربر که دیگر نیازی به دسترسی ندارد پوشش دهد. توجه خاص به حق دسترسی ویژه که به کاربر اجازه اشراف بر کنترل سیستم می‌دهد، معطوف گردد.

کنترل دسترسی به سیستم‌های اطلاعاتی و خدمات باید تمام زمینه‌های چرخه‌ی حیات دسترسی کاربر را پوشش دهد : از ثبت کاربر جدید تا لغو دسترسی کاربری که دیگر بدان نیاز ندارد. هر کجا ممکن است سیاست‌های کاربر باید با سیستم عامل یا نرم‌افزار دیگر عملی شود.

ثبت کاربر :

مدیریت دسترسی و حساب :

کاربران باید فقط به اطلاعاتی دسترسی داشته باشند که برای کارشان بدان نیاز دارند.

محاسبات مدیریت سیستم باید فقط هر زمان که نیاز است مورد استفاده قرار گیرد. وارد محاسبات مدیر سیستم نشوید. برای مثال وقتی از سیستم به عنوان کاربر همیشگی استفاده می‌کنید، وظایف مدیر را انجام ندهید.

مدیریت کارکنان باید دستورالعمل‌های مستند که چرخه کامل محاسبات کاربر را توضیح می‌دهد در بر گیرد.

مدیریت کلمات عبور کاربر :

کلمات عبور :

اولین خط دفاع برای سیستم رایانه معمولاً شناسایی کد کاربر و برخی اشکال شناسایی مانند کلمه عبور می‌باشد.

کلمات عبور باید امن ولی قابل حفظ باشند. کاربران باید از طریق فرآیند مدیریت رسمی کلمه‌ی عبور را دریافت و به حفظ و نگهداری آن از حیث محرمانه بودن تعهد دهند.

کلمات عبور یک بار مصرف و علامت‌ها:

علامت‌ها، وسایلی هستند که کلمات عبور یک بار مصرف یا شماره‌ی شناسایی کارمندان را به وجود می‌آورند. از آنجا که آن‌ها گران هستند، معمولاً فقط روی سیستم‌های حفاظتی بالاتر نصب می‌شوند.

هر جا کلمات عبور ایجاد شود، آن را باید با **شماره شناسایی پرسنل** به کار برد تا در صورت سرقت یا گم شدن از دسترسی افراد فاقد صلاحیت جلوگیری نماید. **شماره شناسایی پرسنل** باید مانند کلمات عبور حفظ و محافظت گردد.

علامت‌های دیجیتالی :

علامت‌های دیجیتالی می‌توانند استفاده شوند تا صحت و سقم تهیه کنندگان گزارش، پیام اسناد و نرم‌افزار را مشخص نمایند. ظهور کلید عمومی رمز (PKC)، علامت‌های دیجیتالی را برای کنترل دسترسی، شناسایی و شناسایی کاربر ایجاد کرده است.

اطلاعات علامت دیجیتالی باید در مقابل ویروس یا گم شدن محافظت گردد.

علامت دیجیتالی ممکن است به عنوان یک نشانه ارائه شود.

بیومتریک‌ها :

ابزار و تجهیزات بیومتریک می‌تواند حفاظتی به‌تر از نشانه‌ها یا کلمات عبور ارائه کند. آن‌ها می‌توانند مسائل مهندسی بیش‌تری ارائه کنند. سازمان‌هایی که قصد استفاده از ابزار بیومتریک دارند باید از اداره حفاظت ارتباطات دولتی راهنمایی بگیرند.

مسئولیت‌های کاربر :

هدف: ممانعت از دسترسی کاربران غیرمجاز هم‌کاری کاربران مجاز برای یک حفاظت کارآمد ضروری است. کاربران باید به وظایف خود در خصوص حفظ کنترل‌های مربوط به دسترسی به خصوص رمز ورود و تجهیزات کاربر آشنا باشند.

تعیین صلاحیت کاربر :

وقتی کاربران وارد سیستم می‌شوند، سازمان‌ها باید ماهیت آن‌ها را شناسایی کنند. چگونگی اثبات ماهیت عمدتاً به ارزیابی ریسک و هزینه بستگی دارد. سه نوع اثبات اطلاعات وجود دارد :

- چیزی که کاربر می‌داند معمولاً یک رمز ورود یا عبارت عبور می‌باشد.
- چیزی که کاربر دارد، مانند کارت رمز مغناطیسی یا کارت هوشمند.
- هر کجا ممکن و عملی است دو اصل اثبات را به کار بندید.
- چیزی که کاربرد دارد مانند اثر انگشت که به‌وسیله‌ی آزمایشات شیمیایی درستی آن اثبات شده است.
- اولین خط دفاع برای سیستم رایانه معمولاً شناسایی کد کاربرد مانند کلمه عبور می‌باشد.
- علامت‌ها، وسایلی هستند که کلمات عبور یک بار مصرف یا شماره‌ی شناسایی کارمندان را به وجود می‌آورند. از آن جا که آن‌ها گران هستند، معمولاً فقط روی سیستم‌های حفاظتی بالاتر نصب می‌شوند. هرجا کلمات عبور ایجاد شود، آن را باید با شماره شناسایی پرسنل به کار

برد تا در صورت سرقت یا گم شدن از دسترس افراد فاقد صلاحیت جلوگیری نماید. شماره شناسایی پرسنل باید مانند کلمات عبور حفظ و محافظت گردند.

آسیب‌های سیستم می‌تواند از طریق موارد زیر کاهش یابد :

- یک مهندسی محافظتی دقیق که مناسب با اصول دفاع در عمق طراحی شده باشد.
- حفاظت فیزیکی برای محل کاری که کسی در آن نیست.
- رمزنگاری و بهره گیری از دیگر فنون مسیر ارتباطی.
- «فایروال‌ها» دیواره آتش مورد تأیید، هر کجا ارتباطات مجاز به وصل شبکه‌های عمومی باشد.
- سیستم‌های مزاحم یاب که با اتصال به فایروال به کار می‌رود.
- کنترل‌های دقیق دسترسی سیستم فعال.

۱۰-۳- سوالات خودآزمایی

۱. امنیت محیطی و فیزیکی را تعریف نمایید.
۲. امنیت فیزیکی محل نگه داری دیتا سنتر را توضیح دهید.
۳. انواع کنترل دسترسی به محل نگهداری شبکه‌ها را توضیح دهید.
۴. اصول پدافند غیر عامل در جایابی شبکه‌های رایانه‌ای را بنویسید.
۵. جست‌جوی زباله‌های فیزیکی چه نقشی در امنیت رایانه دارند. توضیح دهید.

۱۱

فصل یازدهم: سیاست‌ها و استانداردها و مدیریت امنیتی

آن چه در این فصل می‌خوانید:

- سیاست‌های امنیتی
- راهبردهای میان مدت و بلند مدت
- تعیین سطوح طبقه بندی اطلاعاتی که نمی‌توان بر روی ابزار دیجیتال قرار داد
- سیستم‌های امنیتی
- مدیریت ریسک
- مدیریت بحران و تصمیم گیری
- استانداردها و گواهی نامه‌های امنیتی
- نقد استانداردهای رایج و محدودیت پذیری آن‌ها
- نظام مدیریت امنیت اطلاعات
- سیاست‌های امنیتی
- OSINT جمع آوری آشکار و جاسوسی

۱۱- سیاست‌ها و استانداردها و مدیریت امنیتی

۱۱- ۱- سیاست‌های امنیتی

سیاست امنیتی یک سازمان سندی است که برنامه‌های سازمان برای محافظت سرمایه‌های فیزیکی و مرتبط با فن‌آوری ارتباطات را بیان می‌نماید . به سیاست امنیتی به عنوان یک سند زنده نگریسته می‌شود ، بدین معنا که فرآیند تکمیل و اصلاح آن هیچ گاه متوقف نشده ، متناسب با تغییر فن‌آوری و نیازهای کاربران به روز می‌شود . چنین سندی شامل شرایط استفاده مجاز کاربران ، برنامه آموزش کاربران برای مقابله با خطرات ،توضیح معیارهای سنجش و روش سنجش امنیت سازمان و بیان رویه ارزیابی موثر بودن سیاست‌های امنیتی و راه کار به روز رسانی آن‌ها می‌باشد.

هر سیاست امنیتی مشخص کننده اهداف امنیتی و تجاری سازمان است ولی در مورد راه کارهای مهندسی و پیاده سازی این اهداف بحثی نمی‌کند . سند سیاست امنیتی سازمان باید قابل فهم ، واقع بینانه و غیر متناقض باشد، علاوه بر این از نظر اقتصادی امکان پذیر ، از نظر علمی قابل انعطاف و متناسب با اهداف سازمان و نظرات مدیریت آن سطح حافظتی قابل قبولی را ارائه نماید.

در دنیایی که وجه مشخصه آن فن‌آوری سطح بالا و ارتباطات گسترده می‌باشد ،هر سازمانی نیاز به سیاست‌های امنیتی که مدبرانه تدوین شده باشند دارد. در هر لحظه خطرات مختلفی از بیرون و درون سازمان توسط هکرها ، رقبا یا کشورهای خارجی منافع سازمان را تهدید می‌کند . هدف سیاست‌های امنیتی تعریف روال‌ها ، راهنماها و تمریناتی است که امنیت را در محیط سازمان برقرار و مدیریت می‌نماید . با اجرای دقیق سیاست‌های امنیتی ، سازمان‌ها می‌توانند تهدیدات را کاهش دهند.

۱۱-۱-۱- سرمایه‌های دیجیتال که نیاز به سیاست امنیتی دارند

- سخت‌افزارها:

- ✓ ایستگاه‌های کاری
- ✓ سرویس دهنده‌ها
- ✓ خطوط ارتباطی
- ✓ تجهیزات شبکه
- ✓ تجهیزات انتقال داده‌ها
- ✓ لینک‌های ارتباطی
- ✓ اینترفیس‌ها
- ✓ سیستم‌های ارتباطی

- نرم‌افزارها:
  - ✓ سیستم‌های عامل
  - ✓ نرم‌افزارهای کاربردی عمومی
  - ✓ نرم‌افزارهای کاربردی اختصاصی
  - ✓ نرم‌افزارهای مدیریت شبکه
  - ✓ ابزارهای نرم‌افزاری
- اطلاعات
  - ✓ اسناد و اطلاعات ذخیره شده در شبکه
  - ✓ اسناد و اطلاعات پشتیبان
  - ✓ اسناد و اطلاعات در حال انتقال
- ارتباطات:
  - ✓ ارتباطات داخلی سازمان
  - ✓ ارتباطات شبکه سازمان با دیگر شبکه‌های موجود مانند:
  - ✓ شبکه سراسری
  - ✓ شبکه سایر سازمان‌ها
  - ✓ شبکه اینترنت
- کاربران
  - ✓ مدیران
  - ✓ کارشناسان فنی

- ✓ کاربران عادی
- ✓ مدیر فنی
- ✓ کارشناسان تیم فنی
- ✓ پیمانکاران مرتبط با شبکه
- ✓ سایر کاربرانی که به نوعی با شبکه ارتباط دارند

۱۱-۱-۲- ارزش گذاری سرمایه‌های سازمان برای سیاست گذاری

• ارزش سرمایه گذاری روی تجهیزات سخت‌افزاری و برنامه‌های نرم‌افزاری

نکته قابل توجه این است که رایانه‌ها و بسته‌های نرم‌افزاری بسیار گران قیمت هستند و جای‌گزینی آن‌ها پرهزینه و دشوار است . حتی اگر دریک رخداد امنیتی نرم‌افزارها و سخت‌افزارها کاملاً از بین نروند ممکن است مشکلات امنیتی ما را وادار به نصب مجدد همه نرم‌افزارها کنند و متعاقبًا لازم شود کلیه نیازهای اساسی مجددًا تعریف گردند . این امر مستلزم صرف زمان بسیار زیادی است؛ خصوصًا اگر فرد مسئول، اطلاعات فنی کافی در این زمینه نداشته باشد.

• ارزش داده‌های سازمانی

با ارزش‌ترین محتویات بر روی یک رایانه ، اطلاعات و داده‌های ایجاد شده توسط کاربر می‌باشد و شاید وجود همین اطلاعات که ضرورت استفاده از رایانه یا شبکه را توجیه می‌نماید. سیستم‌های عامل و نرم‌افزارها را در بسیاری از موارد و هم‌زمان با بروز مشکل در سیستم می‌توان مجددا نصب نمود ولی داده ایجاد شده در نوع خود منحصر به فرد بوده و در صورت از دست دادن برخی داده‌های مهم می‌تواند در نهایت منجر به زیان‌های عمده و غیر قابل جبران گردد.

• ارزش داده‌های فردی

ممکن است داده‌های فردی ارزش مادی چندانی نداشته باشند ولی از دست دادن آن‌ها بسیار زیان آور باشد و برای ایجاد دوباره اطلاعات زمان بسیار زیادی لازم باشد.

• تهدیدات جنایتکاران رایانه‌ای

همگام با پیشرفت‌های فن‌آوری، گروهی از خراب‌کاران که از دزدی داده‌های رایانه‌ای سود می‌برند نیز به‌وجود آمده‌اند . در مواردی این کار صرفاً برای لذت و سرگرمی صورت می‌گیرد و برخی افراد نیز تنها به‌خاطر خودنمایی در برابر دوستان خود دست به چنین کارهایی می‌زنند؛

اما در بعضی موارد این کار برای دستیابی به منافع شخصی و سازمانی انجام می‌گیرد. در تمامی موارد مذکور این اشخاص باعث ایجاد خسارت و گسترش بی اعتمادی می‌شوند و در حد گسترده‌تر مشکلات بحرانی به‌وجود می‌آورند که به اشخاص و موقعیت‌های شغلی صدمه وارد می‌کند. باید گفت از زمانی که اینترنت در مقیاس جهانی در اختیار کاربران قرار گرفته، تعقیب و متوقف کردن مهاجمین هرچند هم‌چنان امکان‌پذیر می‌باشد ولی بسیار پیچیده شده است.

۱۱-۱-۳- مدون نمودن سیاست‌های امنیتی

به‌ترین روش برای دست‌یابی به امنیت اطلاعات ، فرموله نموده سیاست امنیتی است. مشخص نمودن سرمایه‌های اصلی که باید امن شوند و تعیین سطح دسترسی افراد (به عبارت دیگر این که چه افرادی به چه سرمایه‌هایی دسترسی دارند)

در اولین گام باید انجام شود. هدف اصلی از سیاست امنیتی این است که کاربران بدانند مجاز به چه کارهایی هستند.

۱۱-۲- مدیریت ریسک

مدیریت ریسک فرآیند شناسایی ، تجزیه و تحلیل ، نظارت و اعلام ریسک‌ها را برقرار می‌کند. این ریسک‌ها، ممکن است سازمان را از نیل به اهداف خود باز دارد و یا این که فرصت کسب منافع بیش‌تر را پیش روی سازمان قرار دهد. مدیریت ریسک ، کنترل و انعطاف پذیری سازمانی را فراهم می‌آورد. مدیریت ریسک، غالباً با نگاهی از بیرون ، نقش سازمان را مورد بررسی قرار می‌دهد و آن‌را تقویت می‌کند. از این طریق، توجه به مشتریان و ارباب رجوع افزایش می‌یابد و تأکید بیش‌تری بر نتایج مبذول می‌شود و بر اولویت‌های منافع و ارزیابی عمل‌کرد به‌عنوان بخشی از تصمیم گیری مدیریت تمرکز می‌شود.

برای این که فرآیند مدیریت ریسک کارآمد باشد باید دقیق ، ساختارمند و سیستماتیک باشد. مدیریت ریسک کارآمد نیازمند سازمانی است که از فرهنگ ارزیابی ریسک برخوردار باشد.

نخستین گام در مدیریت ریسک شناخت ماهیت و تقسیم بندی‌های گوناگون ریسک از دیدگاه اقتصادی است، پس از این منظر ، نوبت به ارتباط مبحث راهبردی مدیریت ریسک با اقتصاد پایه کشورها که مرتبط با امنیت غذایی به عنوان دیگر موضوع استراتژیک اقتصاد سیاسی است می‌رسد که در حوزه اقتصاد مهندسی نیز بدان پرداخته می‌شود و مورد مکیال قرار

می‌گیرد که نمود آن در کارآمدی و توفیق مندی بیمه کشاورزی به عنوان یگانه ابزار کارآمد در تحکیم پایه‌های امنیت غذایی کشورها است.

به‌طور کلی، مدیریت ریسک فرآیند سنجش یا ارزیابی ریسک و سپس طرح استراتژی‌هایی برای اداره ریسک است. در مجموع، استراتژی‌های به‌کار رفته شامل: انتقال ریسک به بخش‌های دیگر، اجتناب از ریسک، کاهش اثرات منفی ریسک، و پذیرش قسمتی یا تمامی پیامدهای یک ریسک خاص هستند. مدیریت ریسک سنتی، تمرکزش روی ریسک‌های جلوگیری کننده از علل قانونی و فیزیکی بود (مثل حوادث طبیعی یا آتش سوزی‌ها، تصادفات، مرگ و میر و دادخواهی‌ها). مدیریت ریسک مالی، از سوی دیگر، تمرکزش روی ریسک‌هایی بود که می‌تواند استفاده از ابزار مالی و تجاری را اداره کند. مدیریت ریسک ناملموس، تمرکزش روی ریسک‌های مربوط به سرمایه انسانی، مثل ریسک دانش، ریسک روابط و ریسک فرآیندهای عملیاتی است. بدون توجه به نوع مدیریت ریسک، تمامی شرکت‌های بزرگ دارای تیم‌های مدیریت ریسک هستند و شرکت‌ها و گروه‌های کوچک به‌صورت غیر رسمی، در صورت عدم وجود نوع رسمی آن، مدیریت ریسک را مورد استفاده قرار می‌دهند.

در مدیریت ریسک مطلوب، یک فرآیند اولویت بندی منظور گردیده که بدان طریق ریسک‌هایی با بیش‌ترین زیان‌دهی و بالاترین احتمال وقوع در ابتدا و ریسک‌هایی با احتمال وقوع کم‌تر و زیان‌دهی پایین‌تر در ادامه مورد رسیدگی قرار می‌گیرند. در عمل، این فرآیند ممکن است خیلی مشکل باشد و هم‌چنین در اغلب اوقات ایجاد توازن میان ریسک‌هایی که احتمال وقوع شان بالا و زیان‌دهی شان پایین و ریسک‌هایی که احتمال وقوع شان پایین و زیان‌دهی شان بالاست، ممکن است به‌طور مناسبی مورد رسیدگی قرار نگیرند. در نتیجه می‌توان ریسک‌های موجود در سازمان را از این دو بعُد نیزطبقه بندی کرد که در شکل ۳ نشان داده شده است.

ریسک استراتژیک ریسکی است که سازمان برای تحقق اهداف تجاری خود می‌پذیرد.

در دنیای کسب و کار پرتحول امروز، مدیریت ریسک از اهمیت روزافزونی برخوردار شده است.

مدیریت ریسک ناملموس، یک نوع جدید از ریسک را معرفی می‌کند، ریسکی که احتمال وقوع‌اش ۱۰۰ درصد است، ولی در سازمان‌ها به‌خاطر فقدان توانایی تشخیص، نادیده گرفته می‌شود. برای مثال ریسک دانش، زمانی رخ می‌دهد که دانش دارای ضعف و نقص به‌کار برده

شود. ریسک روابط، زمانی رخ می‌دهد که هم‌کاری بی‌اثر و نتیجه‌ای اتفاق افتد. ریسک فرآیند عملیاتی، زمانی رخ می‌دهد که عملیات بی‌ثمری اتفاق افتد. این ریسک‌ها به‌صورت مستقیم بهره‌وری دانش کارکنان را کاهش داده، و باعث نزول مقرون به صرفه بودن از نظر اقتصادی، سودآوری، خدمات، کیفیت، شهرت، ارزش مارک و کیفیت درآمدها می‌شود. در واقع مدیریت ریسک ناملموس باعث می‌شود در مدیریت ریسک به‌واسطه شناسایی و کاهش ریسک‌هایی که عامل نزول بهره وری می‌باشند، ارزش‌های آنی و مستقیمی خلق شود.

۱۱-۵-۱- معرفی مدیریت ریسک

گمان می‌رود بیمه دانان جهان براین مفهوم اتفاق نظر داشته باشند که اساس بیمه ریسک است، اما تعاریف متعددی برای ریسک در فرهنگ‌ها و کتاب‌ها آمده است که از آن جمله می‌توان به تعریف ویلیامز وهنیز

اشاره کرد که بیان می‌کند :

«ریسک به عنوان تفاوت در نتایجی ست که در یک دوره معین می‌توانست رخ دهد.»

واژه ریسک ممکن است ریشه عربی داشته باشد یا از عبارت Riscum لاتینی ریشه گرفته باشد، اما آن چه که در کمیته اصطلاح شناسی انجمن بیمه و ریسک آمریکا مورد اجماع قرار گرفته و منتشر شده است \"عدم اطمینان از پیامد حادثه‌ای که دو احتمال یا بیش‌تر دارد\" را به عنوان تعریف نموده است .

۱۱-۲-۱- نقاط بحرانی در مدیریت ریسک

۱۱-۲-۲- واژه شناسی در مدیریت ریسک

مراجعه به منابع مختلف علمی، تعاریف متعددی از ریسک می‌توان یافت که البته هر کدام از این تعاریف بسته به بعد یا زاویه دید خود، تعاریف متفاوتی از ریسک در ارایه کرده‌اند و ستون و بیگام در تعریف ریسک می‌نویسند:

(ریسک عبارتست از تغییر احتمالی بازده آتی ناشی از شکست یا تهدید سازمان)

نیکلز مفهوم ریسک را از ابعاد مختلف مد نظر قرار داده و آن را از نظر مفهومی به دو دسته تقسیم می‌کند. وی معتقد است واژه ریسک به احتمال ضرر، درجه احتمال ضرر و میزان احتمال ضرر اشاره دارد. در این راستا ریسک احتمال خطر هم احتمال سود و هم احتمال زیان

را در بر می‌گیرد. درحالی که ریسک خالص صرفاً احتمال زیان را در بر می‌گیرد و شامل احتمال سود نمی‌شود، مانند احتمال وقوع آتش .

لذا با توجه به مجموعه تعاریف فوق می‌توان ریسک را به صورت زیر تعریف کرد :

(ریسک عبارت است از احتمال تغییر در مزایا و منافع پیش‌بینی‌شده برای یک تصمیم، یک واقعه و یا یک حالت در آینده)

منظور از احتمال این است که اطمینانی به تغییرات نیست. در صورتی که اطمینان کافی نسبت به تغییرات وجود داشت، تغییرات مطمئن در چارچوب منافع و مزایا پیش‌بینی‌شده پوشش پیدا می‌کرد، در حالی که عدم امکان پیش‌بینی ناشی از احتمالی بودن تغییرات، آن را به ریسک حاکم بر منافع و مزایا تبدیل کرده است. تغییر ، اشاره و هر گونه کاهش یا افزایش در منافع دارد به این معنا که صرفاً تأثیرات نامطلوب نیست که در چارچوب ریسک پوشش پیدا می‌کند، بلکه تغییرات مطلوب نیز در این معنا در چارچوب ریسک قرار دارد .

تصمیم، واقعه یا حالت، اشاره به ارادی و غیر ارادی بودن شرایطی دارد که دیسک بر آن حاکم می‌شود. ممکن است تصمیمی به صورت ارادی گرفته شود، مزایا و منافع آن ارزیابی شود، و بر مزایا و منافع آن ریسک خاصی حاکم باشد. از طرف دیگر ممکن است واقعه یا حالتی در آینده به صورت غیر ارادی پیش آید و پیش‌بینی‌های مزایا و منافع آن تحت لوای احتمال تغییر قرار گیرد .

ریسک‌ها را به دو قسمت اقتصادی و غیراقتصادی تقسیم می‌شوند:

۱. ریسک اقتصادی ناشی از زندگی اقتصادی است.
۲. ریسک غیراقتصادی پیامد فعالیت‌های اقتصادی نیست.

۱۱-۲-۲- طبقه بندی ریسک

۱. ریسک‌های تخریبی که بر اثر بروز خطرهای فیزیکی ایجاد می‌شوند
۲. ریسک‌های ناشی از عدم اطمینان در فرآیند تولید
۳. ریسک‌های ناشی از تغییرات بازار
۴. ریسک‌هایی که از «ناهنجاری‌های» رفتار اجتماعی ایجاد می‌شوند
۵. ریسک‌های برخاسته از ضعف استفاده از دانش موجود.

ریسک‌های پویا ریسک‌هایی هستند که از امکان تغییرات پویا ناشی می‌شوند. این ریسک‌ها بر اثر تغییر در شرایط اقتصادی، مانند تغییرات در سطح قیمت‌ها، سلیقه مصرف کنندگان، رفتار پس‌انداز و تکنولوژی به وجود می‌آیند و معمولاً در بلند مدت کل جامعه را منتفع می‌کنند .

ریسک‌های ایستا متضمن خسارت‌هایی هستند که حتی اگر هیچ تغییری در شرایط اقتصادی روی ندهد، باز اتفاق خواهند افتاد، مانند خسارت‌های ناشی از تصادفات، آتش سوزی و سایر خطرهای طبیعی. این خسارت‌ها گاهی نیز ناشی از اقدامات غیرعادی یا اشتباهات انسانی است. ریسک‌های ایستا ممکن است منبع کسب منفعت برای فرد باشند اما خسارت‌های ایستا معمولاً متضمن از بین رفتن اموال و دارایی‌اند و منبع کسب منفعت برای جامعه نیستند .

تقسیم و تفکیک بین ریسک‌های سوداگرانه و خالص را معمولاً به موبری نسبت می‌دهند. پروفسور موبری در نخستین کتابی که انجمن اقتصادی آمریکا منتشر کرده بین ریسک‌های تولید و ریسک‌های سوداگرانه تمایز قایل شده است. در این اثر، ریسک‌های تولید تعریف نشده‌اند اما در تعریف ریسک‌های سوداگرانه آمده است :

«ریسک‌هایی هستند که از نوسان‌های قیمت ایجاد می‌شوند و کل بازار را تحت تأثیر قرار می دهند» .

ریسک‌های سوداگرانه وضعیتی را که در آن ، هم احتمال خسارت و هم امکان سود وجود دارد توصیف می‌کنند. فعالیت‌هایی که موجب چنین ریسک‌هایی می‌شوند معمولاً به امید کسب سود منجر می‌شود. بازی شانسی یا شرط بندی مثال خوبی برای ریسک سوداگرانه است. گرچه سرمایه گذاری در دارایی‌های پر ریسک به طور اختیاری انجام می‌گیرد، نوسان‌های قیمت ممکن است مالک آن را منتفع یا متضرر کند .

ریسک‌های خالص ریسک‌هایی هستند که فقط احتمال خسارت دارند. بنابراین، خطرهای طبیعی یا پیامدهای ناشی از اشتباهات انسانی معمولاً فقط ریسک‌های خالص هستند.

بعضی از ریسک‌ها موارد بینابینی هستند و به راحتی نمی‌توان آن‌ها را طبقه‌بندی کرد، زیرا که فرآیند آن‌ها پویاست و نتیجه آن ممکن است در کوتاه مدت خسارت و در بلندمدت سود باشد. برای مثال، نتیجه اعتصاب برای کارگران و بنگاه خسارت است اما در واقع پیامد آن، قرارداد کار جدیدی است که چشم‌انداز شرایط کار به‌تر یا دستمزدها و بهره‌وری مورد انتظار بالاتر و سود بیش‌تر را برای بنگاه به ارمغان می‌آورد. عواقب جنگ را نیز می‌توان به طرق متفاوتی ارزیابی کرد. نتایج ملی کردن به دلیل تحولات پویایی که در کشور روی می‌دهد

خسارتی است که به اموال و دارایی‌ها وارد می‌شود اما در واقع این امر سبب می‌شود که ریسک سرمایه گذاری افزایش یابد و سرمایه گذار نرخ بازده به مراتب بالاتری از نرخ بازده مورد نیاز سرمایه گذاری در شرایط عادی را بطلبد .

وقتی که ریسک‌ها شناسایی و ارزیابی شدند، تمامی تکنیک‌های اداری ریسک در یک یا چند طبقه از چهار طبقه اصلی قرار می‌گیرند:

* انتقال
* اجتناب
* کاهش (یا تسکین)
* پذیرش (یا نگهداری)

۱۱-۲-۴- ارزیابی ریسک

محاسبه ریسک آخرین مرحله نیست. حال باید در مورد پذیرش یا عدم پذیرش ریسک، تصمیم گیری نمود. یا این که سیستم را طوری تغییر دهیم که تأثیر ریسک‌ها آن کاهش یابد. ارزش‌یابی ریسک بدین معنی است که ریسک را بر اساس یک سری معیارها یا شاخص‌های مشخص، اولویت بندی شوند. البته یک معیار جهانی در مورد پذیرش ریسک وجود ندارد زیرا آن‌چه که براساس آن‌ها در مورد ریسک تصمیم‌گیری می‌شود، ممکن است مسائل سیاسی ، قانونی اجتماعی یا بشر دوستانه باشد که همه این موارد بستگی به اهداف شرکت یا سازمان مربوط دارد .

۱۱-۲-۵- کاهش ریسک

استراتژی کاهش، یعنی به‌کارگیری شیوه‌هایی که باعث کاهش شدت زیان می‌شود. به‌عنوان مثال می‌توان به کپسول‌های آتش نشانی که برای فرونشاندن آتش طراحی گردیده‌اند، اشاره کرد که ریسک زیان ناشی از آتش را کاهش می‌دهد .این شیوه ممکن است باعث زیان‌های بیش‌تری به‌واسطه خسارات ناشی از آب شود و در نتیجه امکان دارد که مناسب نباشد. سیستم هالوژنی جلوگیری کننده از آتش ممکن است آن ریسک را کاهش دهد، ولی هزینه آن امکان دارد، به‌عنوان یک عامل بازدارنده از انتخاب آن استراتژی جلوگیری کند .

۱۱-۲-۶- اجتناب از ریسک

استراتژی اجتناب، یعنی انجام ندادن فعالیتی که باعث ریسک می‌شود. به‌عنوان مثال ممکن است که یک دارایی خریداری نگردد یا ورود به یک کسب و کار مورد چشم پوشی قرار گیرد، تا از مشکلات و دردسرهای آن‌ها اجتناب شود. مثال دیگر در این زمینه، پرواز نکردن هواپیماست، تا از ریسک سرقت آن اجتناب شود. استراتژی اجتناب به‌نظر می‌رسد راه حلی برای تمامی ریسک‌هاست، ولی اجتناب از ریسک هم‌چنین به معنی زیان‌دهی در مورد سودآوری‌های بالقوه‌ای است که امکان دارد به‌واسطه پذیرش آن ریسک حاصل شود .داخل نشدن به یک بازار به منظور اجتناب از ریسک، هم‌چنین احتمال کسب سودآوری را ضایع می‌کند .

۱۱-۲-۷- انتقال ریسک

استراتژی انتقال، یعنی موجب شدن این که بخش دیگری ریسک را قبول کند، معمولاً به‌وسیله بستن قرارداد یا انجام اقدامات احتیاطی. بیمه کردن، یک نوع از استراتژی‌های انتقال ریسک با استفاده از بستن قرار داد است. در موارد دیگر این امر به‌واسطه قراردادهای کلامی انجام می‌گیرد که ریسک را به بخش‌های دیگر بدون پرداختی بابت حق بیمه، انتقال می‌دهد. معمولاً بار مسئولیت در میان سازندگان ساختمان یا دیگر سازندگان بدین صورت انتقال می‌یابد. از سوی دیگر، استفاده از وضعیت‌های تعدیل کننده در سرمایه‌گذاری‌های مالی، یک نمونه از چگونگی انجام اقدامات احتیاطی توسط شرکت‌ها، به منظور اداره ریسک از نظر مالی است.

بعضی از روش‌های اداره نمودن ریسک، در تمامی طبقات جای می‌گیرند. پذیرش جمعی ریسک از لحاظ فنی یعنی تحمل ریسک توسط گروه، ولی توزیع آن در کل گروه، یعنی انتقال ریسک در میان افراد عضو در گروه. که این وضعیت متفاوت از بیمه سنتی است، که در آن هیچ حق بیمه‌ای پیشاپیش میان اعضای گروه مبادله نمی‌شود، ولی در عوض زیان حاصله به حساب تمام اعضای گروه گذاشته می‌شود.

۱۱-۲-۸- عوامل موفقیت در مدیریت ریسک فن آوری

پیاده سازی موفقیت آمیز پروژه مدیریت ریسک‌ها امنیتی به عوامل متعددی بستگی خواهد داشت :

- **ضمانت اجرائی** : مدیران ارشد سازمان ، می‌بایست از پروژه مدیریت ریسک‌ها امنیتی حمایت نمایند . بدون وجود ضمانت‌های اجرائی لازم ، کارکنان یک سازمان ممکن است در مقابل استفاده از توصیه‌ها و راهکارهای ارائه شده در

خصوص نحوه انجام فعالیت‌ها ، با آنان مقاومت نموده و مرگ فرسایشی آنان را باعث گردند .

- **تعریف یک لیست مشخص از افرادی که در مقوله امنیت ذی‌نفع می‌باشند** . در هر سازمان افرادی وجود دارند که از نتایج و دست‌آوردهای مدیریت ریسک‌ها امنیتی بیش از سایر افراد ذی‌نفع می‌باشند . گروه مدیریت ریسک امنیتی ، می‌بایست نسبت به شناسائی این افراد در سازمان اقدام و آنان را با فرآیندهای موجود به منظور حفاظت از سرمایه‌ها و از دست ندادن منابع مالی در درازمدت آشنا نماید .
- **وجود بلوغ سازمانی در ارتباط با مدیریت ریسک‌ها امنیتی**: مدیریت ریسک‌ها امنیتی صرفاً" در سازمان‌هائی که دارای یک بلوغ سازمانی مناسب می‌باشند ، قابل پیاده سازی است . بلوغ سازمانی و اطلاعاتی ، می‌بایست در تعداد زیادی از سطوح مدیریتی یک سازمان وجود داشته باشد .
- **وجود یک فضای فکری باز برای کارگروهی** : پروژه مدیریت ریسک‌ها امنیتی نیازمند یک رویکرد باز و صادقانه ارتباطی است (هم بین اعضای گروه و هم با سایر افراد شاغل در سازمان که مدیریت ریسک‌ها امنیتی برای آنان دستاوردهای ارزشمندی را به دنبال خواهد داشت) . وجود یک تفکر ارتباطی مثبت و اعتقاد عملی به کار گروهی در ذهن یکایک اعضا گروه ، علاوه بر استفاده مفید از زمان، ضریب موفقیت پروژه را در زمان مواجهه با مسائل و مشکلات ناخواسته افزایش می‌دهد (مشارکت و همکاری به منظور حل مسائل) .
- **دید سیستماتیک نسبت به سازمان** : در زمان پیاده سازی پروژه مدیریت ریسک‌ها امنیتی ، می‌بایست بررسی تمام سازمان بدون هیچ‌گونه افراط یا تفریطی در دستور کار قرار گیرد . در برخی موارد ممکن است یک واحد خاص در سازمان پروژه را به سمتی هدایت نماید که بیش‌تر در جهت تامین اهداف یک بخش باشد و نه تمامی سازمان (نگرش سیستماتیک نسبت به مسائل و یافتن راه حل آنان) .
- **اختیارات لازم برای گروه مدیریت ریسک‌ها امنیتی** : مشارکت در پروژه مدیریت ریسک‌ها امنیتی به منزله قبول مسئولیت به منظور شناسائی و کنترل

مهم‌ترین تهدیدات امنیتی است که سرمایه‌های یک سازمان را در معرض ریسک قرار می‌دهد . با توجه به اهداف مهم پروژه ، می‌بایست این گروه دارای اختیارات کافی و منابع مورد نیاز به منظور انجام وظایف قانونی خود باشند.

۱۱-۳- مدیریت بحران و تصمیم گیری

۱۱-۳-۱- تعریف مدیریت بحران

قبل از پرداختن به ویژگی‌های موقعیت بحرانی و معرفی رویکرد سیستماتیک رویارویی موثر، باید توجه کرد که در هر حال بحران یا مستقیماً در یک سیستم به‌وجود آمده یا تاثیر عوامل خارجی سیستم را مختل ساخته است. در هر دو حالت می‌توان تجزیه و تحلیل خود را به‌صورت ملاحظات سیستماتیک پیش برد. زیرا در نهایت وظیفه مدیریت بحران، اتخاذ تصمیمات موثر براساس اطلاعات صحیح در جهت کاهش خسارات و کنترل سریع بحران است. این پروسه در نهایت با شناخت کنش‌ها و واکنش‌های سیستماتیک انجام می‌شود. در غیر این‌صورت تصمیمات چیزی جزء آزمون و خطا نخواهد بود و باتوجه به سه عامل، محدودیت زمان، تهدید و غافل‌گیری نمی‌توان انتظار داشت جایی برای چنین رویکردی باشد. مسلماً در تمام برنامه‌ریزی‌های بحران جایی برای موقعیت‌های پیش‌بینی نشده درنظر گرفته خواهد شد. بنابراین می‌توانیم بحران را براساس تعریف سیستم چنین بیان کنیم: اجزأ تشکیل‌دهنده سیستم در چارچوب معین براساس ضوابط و معیارهای سنجیده و تنظیم شده روابطی به‌صورت کنش و واکنش با هم برقرار می‌کنند. در هر سیستم عناصر متغیر تشکیل‌دهنده آن باید در حدود و قلمرو معینی نگهداری و محافظت شود، در غیر این‌صورت حالت تعادل سیستم به‌هم می‌خورد. تا جایی که امکان محو کامل آن وجود دارد. بحران عبارت است از وضعیتی که نظم سیستم اصلی یا قسمت‌هایی از آن را مختل کرده و پایداری آن را بر هم زند. به‌بیان دیگر بحران وضعیتی است که تغییری ناگهانی در یک یا چند قسمت از عوامل متغیر سیستم به‌وجود می‌آورد. شدت و ضعف بحران‌ها بستگی به عوامل تشدیدکننده یا عناصر کاهش‌دهنده بحران و تکنیک‌های موجود برای مدیریت و بالاخره مهار آن دارد.

از نظر عملیاتی نیز بحران را می‌توان به‌صورت یک سیستم، تجزیه و تحلیل کرد که در آن دو سری عوامل مختلف یکی محیط و ساختار سیستم و دیگری عواملی که موجد بحران هستند، وجود دارد. تعیین این که کدام یک از عوامل و عناصر تشکیل‌دهنده سیستم در مقابل

بحران آسیب‌پذیری و تاثیرپذیری بیش‌تری دارد، یکی از وظایف اولیه تحقیق و پژوهش مدیریت بحران است. تعیین آسیب‌پذیرترین بخش سیستم در عمل به بخشی از سیستم برمی‌گردد که بالاترین رسیدگی را نیاز دارد.

اگر در گذشته بخشی از سازمان‌ها، شاید روابط عمومی، مسئولیت رویارویی با بحران را به‌عهده داشت، اکنون کل سازمان آن‌را مهم دانسته و پیچیدگی و پیشرفت این برنامه‌ها سبب شده، دولت‌ها، نهادهای مالی شرکت‌های خدماتی و. . . به شناخت روش‌های برخورد با تغییرات ناگهانی و پیش بینی نشده رو آورده و مدیریت بحران واقعاً بخشی از تمام برنامه‌های استراتژیک سازمان‌ها گردد. بزرگترین اشتباه می‌تواند تصور مصون بودن سازمان از بحران توسط مدیران آن باشد. شرکت‌ها به‌دلیل انتخاب استراتژی‌ها و سیاست‌های مختلف و عواقب آن، در مقابل اقشار مختلف مردم جوابگو و مسئول هستند. شرکت‌هایی که توجه خود را به برنامه‌ریزی‌های علمی و مدیریت سازمان‌دهی شده معطوف کرده‌اند ممکن است در مقابله با یک بحران بازدارنده به‌طرز تاسف باری شکست بخورند. هر تصمیمی در جاده اشتباه باتوجه به تصورات غلط گذشته اتخاذ می‌شود. جملات زیر بیان‌گر قرارداشتن در جاده اشتباه است: «حال که تااینجا پیش رفته‌ایم مسلماً دیگر نمی‌توانیم برگردیم. » «تا به حال پول زیادی صرف این پروژه کرده‌ایم، اگر آن را متوقف کنیم، تمام زحماتمان به‌هدر خواهد رفت. »

راهکارهای شرایط بحرانی به‌صورت روشن و مشخص وجود ندارند. اگر هم باشد همگان به‌طور یک‌سان با کیفیت و محاسن و مضار آن‌ها هم‌نظر نیستند. هنگامی که صحبت از انتخاب می‌شود. مسئله جنبه ارزش و قضاوت پیدا می‌کند. بنابه طبیعت و عوامل روحی عاملان تصمیم‌گیری نتایج آن متفاوت است. در اینجا ممکن است تضاد منافع گروه‌های درگیر در تصمیم تاثیر بگذارد. تصمیم که عملی ناشی از اراده انسان‌هاست باید اهداف و مقاصد را نیز درنظر بگیرد. به‌طور کلی در هر تصمیم باید به این دو سوال پاسخ داده شود: «باتوجه به هدفی که تصمیم‌گیرنده دنبال می‌کند، چه رابطه‌ای بین ارزش موضوع و میزان ریسک یا احتمال خطر وجود دارد؟» و «چه تناسبی بین مقاصد دنبال شده و وسایلی که در اختیار است وجود دارد؟» معمولاً رابطه اول را در چارچوب استراتژی و رابطه دوم را در قلمرو تاکتیک بحث و مطالعه می‌کنند.

مدیریت بحران علمی است کاربردی که با شناخت مشاهدت و تجزیه و تحلیل داده‌ها به‌صورت سیستمی جهت یافتن ابزار و راه حل‌هایی که به‌وسیله آن از یک سو بتوان از وقوع

فاجعه پیش‌گیری کرد یا مقابله نمود و از سوی دیگر در صورت وقوع آن نسبت به امداد رسانی و بهبود اوضاع اقدام نمود .

۱۱-۳-۲- ویژگی‌های بحران

بررسی بحران‌های گذشته نشان می‌دهد، افراد در این گونه موارد دچار سردرگمی می‌شوند، ساده‌ترین و در عین حال اساسی‌ترین اشتباهات در لحظات بحرانی رخ می‌دهد، معمولاً سخن و عمل‌کرد مسئولان خلاف جهت منافع خود و سازمان آن‌هاست، دست‌پاچگی و عکس‌العمل‌های غیرمنطقی در چنین شرایطی بسیار دیده می‌شود، جلوگیری از ازدحام خبرنگاران کنجکاو، حفظ اعتبار، کاهش عوارض و بازتاب‌های منفی آن بر آینده و افکار عمومی مسائلی هستند که گاه از کنترل خود بحران برای مسئولان مشکل‌تر می‌شود. تضادی که بین کنترل بحران و تسلط بر شایعات و اعصاب ایجاد می‌گردد، دقیقاً نمایان‌گر عدم آمادگی است. تعجب و غافل‌گیری اولین عامل مخرب در بحران‌هاست. در حقیقت دوباره به‌دست گرفتن اوضاع یا شکست درهمان ساعات اول مشخص می‌شود.

۱۱-۳-۳- فرآیند مدیریت بحران

داشتن برنامه‌ای سنجیده توانی ایجاد خواهد کرد تا مسئولان با روشی صحیح به‌سرعت دست به‌کار شوند. زیرا کلیه موارد عمومی، سازمان‌دهی، تقسیم کارها، تخصیص منابع و تعیین مسئولیت‌ها و اختیارات انجام شده و کانال‌های ارتباطی نیز تعیین شده است. بنابراین کلیه موارد فوق می‌تواند از مکانیسم‌های کنترل بحران حذف شود و به‌سرعت برنامه تغییرات متناسب با شرایط خاص آغاز گردد. به‌همین دلیل پیش‌بینی، بررسی و ارزیابی بحران و خطرات آن قبل از وقوع از ضروریات مدیریت بحران است، برای تدوین چنین برنامه‌هایی می‌توان:

- از آرأ عمومی، نظر مشترکان، نظر کارکنان برای تجزیه و تحلیل بحران‌ها کمک گرفت؛
- در سمینارهای داخلی، ارتباطات دوره بحران را مشخص و آمادگی در سطوح مختلف ایجاد کرد؛
- برای ایجاد تیم‌های خبره، متخصص و هم روحیه تحقیقاتی انجام داد؛
- یک لیست از مدت زمان و منابع ضروری جهت آمادگی برای بحران، تهیه کرد؛

O بادرنظر گرفتن مسائل مربوط به آموزش و ارتباط، شناخت درازمدتی از بحران به‌دست آورد؛

O یک استراتژی کلی برای مقابله با وضعیت‌های بحرانی در مدیریت بهینه سازمان گنجانید.

توجه به نکات زیر می‌تواند برخی از سوء تفاهمات را از بین ببرد. هر ریالی که به‌طور صحیح قبل از بحران خرج می‌شود، باعث صرفه‌جویی هزاران ریال در پایان بحران خواهد شد. ضمناً آمار و ارقام مربوط به هزینه‌های احتمالی تنها در صورت برنامه‌ریزی قابل محاسبه هستند. نقطه شروع برنامه‌های اضطراری، ایجاد نگرشی وسیع در مورد مشکلات بالقوه‌ای است که ممکن است در تمامی سازمان‌ها به‌وجود آید. باید به کارمندان سطوح پایین در مورد شناسایی بازتاب‌های بحران آموزش داد تا وقایعی که ممکن است از دید مدیریت کل سازمان پنهان بماند را گوشزد کنند.

برنامه عملیات اضطراری شامل فعالیت‌هایی برای پشتیبانی از اصول عملیاتی و اهداف سازمان است. می‌توان سیستم پژوهش برنامه‌ریزی را در روند استاندارد عملیاتی که سازمان برای نیل به اهداف خود دنبال می‌کند قرار دهیم. به‌عنوان مثال قراردادن یک پرسشنامه برای تعیین اثرات یک سانحه، لیستی از نقاط آسیب‌پذیر شرکت را مشخص می‌کند. چنین تحقیق سیستماتیکی مشخص می‌کند در تخمین دینامیک یک مسئله خاص، سازمان چه چیزهایی را می‌داند و چه چیزهایی را نمی‌داند. (system. parsiblog. com)

۱۱-۴- استانداردها و گواهی نامه‌های امنیتی

منشاء استاندارد BS۷۷۹۹ [۱]به زمان تاسیس مرکز CCSC [۲] و شکل‌گیری بخش DTI [۳] در سال ۱۹۸۷ برمی گردد. این مرکز به منظور تحقق دو هدف تشکیل گردید. اول تعریف معیارهایی بین‌المللی برای ارزیابی میزان امنیت تجهیزات تولید شده توسط سازندگان تجهیزات امنیتی، به منظور ارائه تاییدیه‌های مربوطه بود و دوم کمک به کاربران برای این منظور مرکز CCSC در سال ۱۹۸۹ اقدام به انتشار کدهایی برای سنجش میزان امنیت نمود که به "Practice Users Code of" معروف گردید. چندی بعد، اجرایی بودن این کدها از دیدگاه کاربر، توسط مرکز محاسبات بین‌المللی NCC و

---

[۱] British Standard
[۲] Commercial Computer Security Center
[۳] Industry UK Department of Trade and

یک کنسرسیوم از کاربران که به طور کلی از صاحبان صنایع در انگلستان بودند مورد بررسی قرار گرفت. اولین نسخه این استاندارد به عنوان مستندات راهبری ۰۰۰۳ PD در انگلستان منتشر گردید. در سال ۱۹۹۵ این استاندارد با عنوان BS۷۷۹۹ منشر گردید و قسمت دوم آن نیز در فوریه سال ۱۹۹۸ به آن اضافه گردید. این قسمت مفهوم سیستم مدیریت امنیت اطلاعات ISMS ۱را به‌وجود آورد. این سیستم ISMS به مدیران این امکان را می‌دهد تا بتوانند امنیت سیستم‌های خود را با حداقل نمودن ریسک‌های تجاری کنترل نمایند. نسخه بازنگری شده این استاندارد در سال ۱۹۹۵ به عنوان استاندارد ISO ثبت گردید. در مجمعی که رای موافق به ثبت این استاندارد به عنوان استاندارد ISO داده بودند، کشورهایی نظیر استرالیا و نیوزلند بااندکی تغییر، آن را در کشور خود با عنوان AS/NZS۴۴۴۴ منتشر نمودند. طی سال‌های ۱۹۹۹ تا ۲۰۰۲ بازنگری‌های زیادی روی این استاندارد صورت پذیرفت. در سال ۲۰۰۰ با افزودن الحاقیه‌هایی به استاندارد BS۷۷۹۹ که به عنوان یک استاندارد ISO ثبت شده بود، این استاندارد تحت‌عنوان استاندارد ISO/IEC۱۷۷۹۹ به ثبت رسید. نسخه جدید و قسمت دوم این استاندارد در سال ۲۰۰۲ به منظور ایجاد هماهنگی بین این استاندارد مدیریتی و سایر استانداردهای مدیریتی نظیر ISO ۹۰۰۱ و ISO ۱۴۰۰۱ تدوین گردید. این قسمت برای ارزیابی میزان موثربودن سیستم ISMS در یک سازمان مدلPDCA۲ را ارائه می‌نماید. در سال ۱۹۹۰ براساس حساسیت‌ها و نیازمندی‌های امنیتی موجود، یک گروه کاری خاص برای امنیت اطلاعات در BSI تشکیل شد. این گروه در سال۱۹۹۲ ، اولین نتیجه تحقیقات خود را تحت عنوان آیین‌نامه مدیریت امنیت اطلاعات ۳منتشر نمود. موسسه استاندارد انگلستان اولین نسخه BS۷۷۹۹ را در سال ۱۹۹۵ براساس این تحقیق تدوین و منتشر نمود. ۴

نسخه اول از BS ۷۷۹۹، استانداردی سطح بالا و ماهیتاً مفهومی است. این ویژگی‌ها سبب می‌شود که بتوان از آن برای انواع مختلف سیستم‌ها و کاربردها در تکنولوژی اطلاعات استفاده نمود. تا سال ۱۹۹۸ موسسه استاندارد انگلستان (BSI) مراحل اعطای گواهی۵ را برای این استاندارد طی نمود و در سال ۱۹۹۹ نسخه دوم از استاندارد BS ۷۷۹۹ با عنوان "توصیف سیستم مدیریت امنیت اطلاعات" توسط این موسسه تدوین و منتشر شد. ۶

---

[۱] Information Security Management System
[۲] Plan-Do-Check-Act
[۳] "Code of Practice for Information Security Management"
[۴] Part ۱: Code of Practice for Information Security Management

[۵] Certificate
[۶] Part ۲: Specification of Information Security Management System

بخش دوم BS۷۷۹۹ به بیان جزئیات برقراری، پیاده‌سازی و مستندسازی مربوط به یک سیستم مدیریت امنیت اطلاعات و یا به اختصارISMS [۱] می‌پردازد. ISMS جهت مشخص نمودن کنترل‌های امنیتی یک سازمان براساس اهداف کاری و نیازمندی‌های امنیتی آن شکل می‌گیرد. به عبارتی از آن‌جا که ممکن است تمامی کنترل‌های امنیتی مشخص شده در بخش اول BS۷۷۹۹ برای همه سازمان‌ها در جهت نیل به امنیت لازم نباشد، با ایجاد یکISMS ، وظیفه تشخیص و انتخاب کنترل‌های امنیتی مورد نیاز، مدیریت و نگهداری آن‌ها به این سیستم محول می‌شود. بخش اول BS۷۷۹۹ مجموعه‌ای کامل از همه کنترل‌های امنیتی لازم در حالت کلی را مطرح می‌سازد، در حالی‌که BS۷۷۹۹ روش پیاده‌سازی و انتخاب کنترل‌های لازم را بیان می‌کند.

با این که سازمان‌های زیادی BS ۷۷۹۹ را به عنوان استاندارد امن‌سازی خود مورد استفاده قرار دادند ولی نیاز شدیدی به وضع یک استاندارد بین‌المللی معتبر از طرف یک مؤسسه شناخته شده بین‌المللی حس می‌شد. در ماه دسامبر سال ۲۰۰۰ میلادی، مؤسسه بین‌المللی استاندارد یا ISO بخش اول از استاندارد BS ۷۷۹۹ را بررسی نموده و تحت استاندارد ISO/IEC ۱۷۷۹۹ منتشر نمود. بنا براین بخش اول استاندارد BS ۷۷۹۹ معادل استاندارد ISO/IEC ۱۷۷۹۹ می‌باشد. در سال ۲۰۰۲ موسسه استاندارد انگلستان ویرایش دیگری از بخش دوم استاندارد BS ۷۷۹۹ منتشر نمود. در این استاندارد، ISMS به‌صورت متدولوژیک و براساس مفاهیم مدیریت مبتنی بر فرآیند توصیف شده است

برای پیش‌گیری از تهدیدهای امنیتی ، متدها و استانداردهای مختلفی تا به حال ارائه شده است. تاریخچه ورود این استانداردها با BS ۷۷۹۹ شروع شده است که در دوره خود کامل‌ترین و معروف‌ترین استاندارد در این زمینه بوده است . این استاندارد در سال ۱۹۸۷ توسط موسسه CCSC [۲] بخش DTI [۳] تدوین گردیده سپس با توجه به گذشت زمان و تجارب مختلف از سنجش میزان امنیت اطلاعات توسط CCSC و مرکز محاسبات بین المللی NCC و یک کنسرسیوم از کاربران یک نسخه استاندارد امنیت با عنوان مستندات راهبری PD۰۰۳ در انگلستان منتشر شد و نسخه بازنگری شده این استاندارد در سال ۱۹۹۵ با عنوان استاندارد ISO ثبت گردید . در فوریه سال ۱۹۹۸ نسخه دوم این استاندارد (BS ۷۷۹۹)تحت عنوان سیستم مدیریت امنیت اطلاعات ISMS منتشر شد. در سال ۲۰۰۰ با افزودن الحاقیه‌ای

---

[۱] Information Security Management System
[۲] Commercial Computer Security Center
[۳] UK Department of trade and industry

به استاندارد BS۷۷۹۹ که به‌عنوان ISO ثبت شده بود این استاندارد تحت عنوان راهنمای اجرای استاندارد امنیت اطلاعات ISO/IEC ۱۷۷۹۹ به ثبت رسید. استاندارد BS۷۷۹۹ در سال ۲۰۰۲ مجدداً مورد بازنگری قرار گرفت و نها یتاً آخرین ویرایش استاندارد ISMS در ۲۸ ژوئن سال ۲۰۰۵ تحت عنوان (Draft BS۷۷۹۹-۲:۲۰۰۵) ISO/IEC FDIS ۲۷۰۰۱:۲۰۰۵ توسط کمیته IST/۳۳ سازمان ISO چاپ و منتشر شد. با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش سیتماتیک به مقوله ایمن سازی اطلاعات و به تبع آن فضای تبادل اطلاعات شکل گرفت.

۱۱-۴-۱- دستورالعمل‌های امنیتی و نظارتی ابزار دیجیتال

سیاست امنیتی یک سازمان سندی است که برنامه‌های سازمان برای محافظت سرمایه‌های فیزیکی و مرتبط با فن‌آوری ارتباطات را بیان می‌نماید . به سیاست امنیتی به عنوان یک سند زنده نگریسته می‌شود ، بدین معنا که فرآیند تکمیل و اصلاح آن هیچ گاه متوقف نشده ، متناسب با تغییر فن‌آوری و نیازهای کاربران به روز می‌شود . چنین سندی شامل شرایط استفاده مجاز کاربران ، برنامه آموزش کاربران برای مقابله با خطرات ،توضیح معیارهای سنجش و روش سنجش امنیت سازمان و بیان رویه ارزیابی موثر بودن سیاست‌های امنیتی و راه کار به روز رسانی آن‌ها می‌باشد.

هر سیاست امنیتی مشخص کننده اهداف امنیتی و تجاری سازمان است ولی در مورد راه کارهای مهندسی و پیاده سازی این اهداف بحثی نمی‌کند . سند سیاست امنیتی سازمان باید قابل فهم ، واقع بینانه و غیر متناقض باشد، علاوه بر این از نظر اقتصادی امکان پذیر ،از نظر علمی قابل انعطاف و متناسب با اهداف سازمان و نظرات مدیریت آن سطح حافظتی قابل قبولی را ارائه نماید.

۱۱-۴-۱-۱-تدوین سیاست

به‌ترین روش برای دست‌یابی به امنیت اطلاعات ، فرموله نموده سیاست امنیتی است.

مشخص نمودن سرمایه‌های اصلی که باید امن شوند و تعیین سطح دسترسی افراد (به عبارت دیگر این که چه افرادی به چه سرمایه‌هایی دسترسی دارند)

در اولین گام باید انجام شود. هدف اصلی از سیاست امنیتی این است که کاربران بدانند مجاز به چه کارهایی هستند.

۱۱-۴-۱-۲-استانداردها و روال امنیتی

سیاست‌های امنیتی در بر دارنده کلیه انتظارات ، برنامه‌ها و اهداف عملیاتی مدیریت سازمان می‌باشد . برای عملیاتی و قابل اجرا بودن ، سیاست امنیتی باید با استفاده از استانداردها ، راهنماها و رویه‌های شناخته شده تعریف شود که اطمینان از سازگاری کلیه عملیات اجرایی با سیاست‌های امنیتی حاصل گردد.

استانداردها، راهنماها و روال‌ها تفسیر خاصی از سیاست را ارائه می‌کنند و کاربران ، مشتریان و مدیران سازمان را برای پیاده سازی سیاست آماده می‌نمایند.

۱۱-۴-۱-۳- ساختار سیاست امنیتی

ساختار سیاست امنیتی مرکب از اجزای زیر می‌باشد:

۱. عبارتی در رابطه با موضوع سیاست
۲. چگونگی اجرای سیاست در محیط سازمان
۳. نقش و مسئولیت افراد مختلف تاثیر گذار در سیاست
۴. سیاست به چه میزان انعطاف پذیر است؟
۵. اعمال ، فعالیت‌ها و فرآیندهای مجاز و غیر مجاز موارد سخت گیری و عدم انعطاف سیاست

۱۱-۵- سئوالات خودآزمایی

۱. سرمایه‌های دیجیتال که نیاز به تأمین امنیت دارند را نام برده و توضیح دهید.
۲. در یک سازمان متولی بررسی و تصویب سیاست‌های امنیتی چه ساختاری می‌باشد؟
۳. راهبردهای میان مدت را در سیاست‌های امنیتی دیجیتال بنویسید.
۴. نظریه جهانی‌سازی چه نقشی در امنیت دیجیتال دارد آن را توضیح دهید.
۵. نظریه نسبی بودن امنیت اطلاعات دیجیتال را توضیح دهید.
۶. انواع روش‌های مدیریت ریسک را نوشته و توضیح دهید.
۷. ارزیابی مستمر و شناسایی مداوم ریسک‌های مربوط به فاوا چه نقشی می‌تواند در امنیت آن داشته باشد.
۸. مدیریت بحران را تعریف کرده و نقش آن را در امنیت دیجیتال بنویسید.
۹. OSINT چیست؟ و چه نقشی در امنیت اطلاعات دارد؟
۱۰. چک لیست‌های حفاظتی به چه روشی می‌تواند به افزایش امنیت کمک نماید؟

•

۱۲

فصل دوازدهم: تست نفوذ و ابزارهای امنیتی

- **آن چه در این فصل می‌خوانید:**
-

- **نفوذ و تست نفوذ**
- **حمله به نرم‌افزارهای کاربردی**
- **اسکن شبکه‌ها**
- **اسب‌های‌تراوا و نرم‌افزارهای مخرب نفوذ**
- **ثبت کننده‌ای صفحه کلید**
- **اجزا و آناتومی هک**
- **اطلاع از شیوه‌های نفوذ از داخل و خارج شبکه**
- **روش‌های شناسایی و ممانعت از حملات**
- **نرم‌افزارهای ضد ویروس و استفاده هکرها**
- **تست نرم‌افزار و سخت‌افزار خریداری شده**

•

۱۲- تست نفوذ و ابزارهای امنیتی

۱۲-۱- نفوذ و تست نفوذ

۱۲-۱-۱- حمله به امنیت SETUP

این مرحله از امنیت رایانه اولین مرحله امن سازی رایانه می‌باشد در صورتی که فردی بتواند از این مرحله عبور نماید و رمز اولیه آن را به دست بگیرد قادر خواهد بود تا به رایانه دسترسی پیدا نماید. امروزه اقدامات مختلفی توسط نفوذگردان انجام می‌شود تا بتوانند از این مرحله عبور نمایند. بخشی از اقدامات آن‌ها دارای رد پای نفوذ بوده و برخی دیگر از اقدامات اثر گذاشتن هیچ گونه رد پایی قادر به گذر از این مرحله خواهد بود .

اقدامات زیر از جمله اقداماتی است که توسط نفوذگران برای گذر از این مرحله انجام می‌شود :

قطع برق رایانه هم‌زمان با برداشتن باطری پشتیبان

استفاده از نرم‌افزارهای حمله کننده به رمز

استفاده از نرم‌افزارهای آشکار کننده رمز

استفاده از رمزهای از پیش تعریف شده

استفاده از روش‌های نرم‌افزاری دور زدن رمز

استفاده از این روش‌ها و روش‌های مشابه باعث خواهد شد نفوذگران از امنیت این مرحله عبور نموده و بتوانند وارد مراحل دیگر رایانه شوند. برخی از این اقدامات مانند استفاده از رمزهای از پیش تعریف شده هیچ‌گونه ردپایی از خود به جای نمی‌گذارد لذا کاربران اصلی رایانه

پس از مراجعه به رایانه و استفاده از آن متوجه این که فردی به صورت غیرمجاز به رایانه دسترسی پیدا نموده است نخواهد شد .

۱۲-۱-۲- حمله به سیستم‌های عامل

سیستم عامل به عنوان دومین مرحله امن سازی رایانه به کار گرفته می‌شود همان‌گونه که می‌دانید وظیفه اصلی سیستم عامل مدیریت برمنابع سخت‌افزاری و نرم‌افزاری رایانه می‌باشد امروزه از سیستم‌های عامل مختلف بر روی رایانه استفاده می‌گردد قدیمی‌ترین نوع سیستم عامل سیستم عامل داس بوده است که امروز کاربرد فراوانی در امور اداری ندارد. با مطالعه در کتاب‌های میکروسافت مشخص می‌شود که سیستم عامل داس فاقد امنیت بوده است و هر ساختاری که از این سیستم عامل بر روی رایانه خود استفاده نماید عملاً امنیت را نیاز نداشته است اطلاعات تو لیدی او به راحتی در اختیار دیگران قرار می‌گیرد

۱۲-۱-۲-۱- حمله به سیستم عامل ویندوز گروه ۹X

این گروه از سیستم عامل دارای دواشکال امنیتی اساسی می‌باشد که نفوذگران با استفاده از این ۲ اشکال امنیتی به راحتی قادر خواهند بود تا کنترل سیستم عامل را به دست گرفته و بر آن مدیریت نمایند ، اشکالات امنیتی فوق به شرح ذیل می‌باشند:

وجود دکمه ESC بر روی صفحه کیبرد و دکمه CANCEL بر روی صفحه ورودی کاربر

این کلیدها باعث می‌گردد چنان‌چه فردی رمز کاربری را نداند بتواند با استفاده از یکی از این ۲ کلید بدون این که هیچ رمزی ارائه نماید وارد رایانه شده و به محیط عمومی رایانه دسترسی پیدا نماید و هر کس که وارد محیط عمومی رایانه گردد می‌تواند بااندکی جستجو در داخل رایانه اطلاعات مربوط به هر کدام از کاربران را پیدا نمود و آن‌ها را کپی و از رایانه خارج نماید .

اشکال امنیتی دوم وجود فایل‌هایی با نام کاربرو پسوند PWL می‌باشد این فایل‌ها زمانی که مدیر رایانه برای کاربران رمز دسترسی تعریف می‌کند به صورت اتوماتیک ایجاد می‌شود. محل این فایل‌ها در همان محلی است که سیستم عامل در آنجا نصب شده است یعنی در هر فولدری که سیستم عامل نصب شده باشد این فایل‌ها در همان‌جا ایجاد می‌شوند .

افراد غیرمجاز با استفاده از اشکال امنیتی اول وارد سیستم شده و با تغییر محل این فایل‌ها و دوباره راه‌اندازی رایانه بدون این که نیازی به رمز عبور داشته باشند وارد رایانه شده و با نام کاربر مورد نظر اطلاعات مربوطه را کپی نموده و از رایانه خارج می‌نمایند و بعد از این که

اقدامات خود را انجام دادند مجدد فایل مربوطه را که تغییر محل داده بودند به محل اصلی کپی می‌نمایند و با انجام این اقدامات بدون این که هیچ ردپایی بر روی رایانه به جای بگذارد به صورت غیر مجاز وارد سیستم شده واقدامات مد نظر خود را انجام می‌دهند. درصورتی‌که مالک رایانه که همان کاربراصلی می‌باشد به رایانه دسترسی پیدا نمود و به صورت عادی بخواهد کار خود ادامه دهد متوجه هیچ گونه تغییراتی در رایانه نخواهد شد و استنباط این که نفوذ غیر مجاز به رایانه انجام شده است را نخواهد داشت .

۱۲-۱-۲-۲- حمله به سیستم عامل ویندوز گروه NT

شرکت میکروسافت پس از این که متوجه شد این اشکالات امنیتی گروه ۹۸ آشکار شده است و کاربران از خریداری این سیستم‌های عامل خودداری می‌نمایند و کم‌کم بازار و فروش مربوطه کاهش پیدا نموده است با استفاده از تعداد زیادی کارشناس در نقاط مختلف دنیا سیستم عامل جدیدی را نوشته و نام این سیستم عامل را ویندوز گروه NT نامید انواع سیستم‌های عاملی مانند XP و NT ازجمله این سیستم عامل می‌باشد .

در سیستم عامل جدید اشکالات گروه ۹۸ حل شده بود و شرکت میکروسافت تبلیغات فراوانی را در این رابطه انجام داد و به کل دنیا این مطلب را القا نمود که سیستم عامل جدید دارای امنیت بوده و می‌تواند امنیت مربوط به کاربران را تأمین نماید .

امروز عناصر غیرمجاز با استفاده از انواع نرم‌افزارهای حمله کننده به رمز سیستم عامل ویندوز گروه NT در کم‌تر از یک دقیقه قادر خواهند بود تا رمز گذاشته شده بر روی سیستم عامل را از بین برده یا تعویض نمایند و به راحتی دسترسی به اطلاعات رایانه پیدا نمایند یا این که با استفاده از انواع سی دی‌های live و بدون این که هیچ ردپایی از خود به جای بگذارند به راحتی قادر خواهند بود رمز رایانه را دور زده و وارد رایانه شده و اطلاعات مورد نظر خود را کپی نموده و از رایانه خارج نمایند متأسفانه در این حالت هیچ‌گونه ردپایی از نفوذگر در داخل رایانه به جای نخواهد ماند و کاربر مربوطه حتی گمان این را نخواهد برد که به رایانه دسترسی غیرمجاز صورت گرفته و اطلاعات مربوطه از سیستم خارج شده است .

۱۲-۱-۲-۳- حمله به سیستم عامل انواع دیگر ویندوز

انواع دیگر سیستم عامل ویندوز مانند سیستم عامل ویندوز ویستا و ۷ امروزه توسط شرکت مایکروسافت به دنیا ارائه شده است تمام این سیستم‌های عامل در مقابل استفده از سی دی‌های live ناامن بوده و به راحتی افراد غیرمجاز قادر خواهند بود تا با استفاده از این گونه ابزار رمز

مربوطه به کاربران را دور زده و از آن عبور نمایند بدون این که ردپایی از خود به جای بگذارند و علاوه بر آن نرم‌افزارهای مختلفی که قادر خواهد بود در کم‌تر از ۱ دقیقه رمز مربوطه را حذف نموده و یا جای‌گزین نماید نوشته شده و بر روی اینترنت قرار داده شده است افراد غیرمجاز با استفاده از این گونه نرم‌افزارها به راحتی به رایانه‌هایی که توسط این سیستم‌های عامل امن شده است دسترسی پیدا می‌نمایند .

۱۲-۱-۳- حمله به سیستم‌های عامل OPEN SOURCE

سی دی‌های live در رابطه با سیستم‌های عامل منبع باز نیز عمل نموده و بدون این که نیاز به رمزهای گذاشته شده باشد از این سیستم عامل عبور نموده و وارد رایانه می‌شوند البته نرم‌افزارهای گوناگونی نوشته شده است و با توزیع آن‌ها بر روی اینترنت افراد غیرمجاز به راحتی دسترسی به این نرم‌افزارها پیدا نموده و با راه‌اندازی رایانه توسط آن‌ها وارد سیستم شده و رمز مربوط به سیستم‌های عامل منبع باز را ازرده خارج یا جای گزین می‌نمایند.

۱۲-۲- حمله به نرم‌افزارهای کاربردی

عالیه نرم‌افزارهای کاربردی دارای ۲ قسمت می‌باشند قسمت اصلی آن‌ها نرم‌افزار کاربردی در قسمت دوم آن‌ها اطلاعاتی است که توسط این نرم‌افزارها تولید می‌شود قسمت اصلی نرم‌افزار معمولاً فقط ارزش اقتصادی داشته و ارزش و اهمیتی ندارد و معمولاً می‌توان با پرداخت مبلغی آن‌ها را تهیه نمود لذا قسمت اصلی که می‌بایست در نرم‌افزارهای کاربردی ایمن شوند اطلاعاتی است که توسط آن‌ها تولید می‌شود برای کم کردن اطلاعات کاربردی رمزهای مختلفی را بر روی این اطلاعات گذاشته و مانع از این می‌شوند تا افراد غیر مجاز بتوانند این اطلاعات دسترسی پیدا نمایند .

نرم‌افزارهای حمله کننده به رمز به یکی از ۳ روش زیر می‌توانند به امنیت گذاشته شده بر روی فایل ها حمله کنند:

۱ - استفاده از روش را حمله لغت‌نامه‌ای :

در صورتی که رمز استفاده شده در نرم‌افزار کاربردی کار می‌باشد که در یکی از لغت نامه‌های رایج دنیا وجود داشته باشد این کلمه با استفاده از این گونه حمله در کم‌تر از ۱ دقیقه آشکار شده است و به راحتی قابل دسترسی خواهد بود.

۲- استفاده از روش حمله brute force

در صورتی که رمز استفاده شده از رمزهای پیچیده‌ای که در هیچ لغت‌نامه نیز استفاده نشده است باشد مهاجمان از این روش برای پیدا کردن رمز استفاده می‌نمایند در این روش کلیه حروف ، اعداد در دور نهایی صفحه کلید توسط نرم‌افزار خاصی به صورت انفرادی وترکیبی مورد کنترل و آزمایش قرار می‌گیرد دسترسی به رمز در این روش هر چند که نیاز به زمان بیش‌تری دارد اما در نهایت با توجه به نوع رایانه و نرم‌افزار هیچ مورد استفاده قرار می‌گیرد رمز مربوطه استخراج شده و مورد بهره‌برداری سو قرار می‌گیرد امروز نرم‌افزارهایی وجود دارند که در هر ثانیه ۱۵۰٬۰۰۰ رمز را چک در کنترل می‌نمایند.

۳- استفاده از روش حمله مستقیم :

در این روش با توجه به این که الگوریتم رمز و محل نگهداری آن از قبل توسط مهاجمین شناسایی شده است برای پیدا کردن آن برنامه نرم‌افزاری خاصی نوشته شده و به مجرد این که اطلاعات مربوط توسط این نرم‌افزار مورد بازرسی قرار می‌گیرند بدون صرف هرگونه زمانی رمز مربوطه را پیدا نموده و آشکار می‌سازد.

۱۲-۳- اسب‌های‌تراوا و نرم‌افزارهای مخرب نفوذ

تروجان چیست ؟ به عبارت ساده یک فایل مخرب و جاسوسی است که توسط یک هکر به رایانه قربانی ارسال و در رایانه تعبیه می‌شود ،تروجان وظیفه جمع آوری ، گردآوری و ارسال کلیه اطلاعات مورد نیاز نفوذگر ار رایانه کاربر قربانی را برعهده دارد.

اسب تروجان خود را به شکلی غیر از آنچه که هست به تصویر می‌کشد. اسب تروجان خود را به سایر فایل‌ها الصاق نمی‌کند و از خود کپی ایجاد نمی‌نماید بلکه موجب آسیب به سیستم رایانه‌ای یا ایجاد حفره امنیتی در رایانه می‌گردد.

اسب تروجان برای انتقال باید توسط شخص یا برنامه‌ای ارسال شود. اسب تروجان ممکن است توسط برنامه‌های جذاب تفریحی و خنده‌آور یا روش‌های دیگری به سیستم‌های رایانه‌ای منتقل شود.

عمل‌کرد اسب‌تروا می‌توان هرگونه فعالیت نامطلوب برای کابر باشد؛ مانند تخریب اطلاعات کاربر و یا ایجاد روشی برای عبور از سد کنترل‌های معمول جهت دسترسی غیر مجاز به رایانه آلوده.

معمولاً تروجان‌ها به دو قسمت تقسیم می‌شوند:

۱-کلاینت:که تنظیمات را انجام داده و آن را با توجه به نیازهایی که بیان کردیم تنظیم می‌نمایند

۲-سرور:که بعد از تنظیمات باید این سرور برای قربانی فرستاده شود تا قربانی بعد از دریافت آن را اجرا کند.

۱۲-۴- ثبت کننده‌ای صفحه کلید

اما اخیرا هکرهای اینترنتی و رایانه‌ای به نرم‌افزارهای پیش‌رفته روی آورده‌اند که به کلید ثبت کننده[۱] معروف شده‌اند و می‌توانند هر کلیدی که کاربری بر روی صفحه کلید ضربه می‌زند را در حافظه خود نگهداری و آنرا برای هکر مورد نظر ارسال نماید . اوج استفاده این نوع از نرم‌افزارها سرقت کلمه کاربری و رمزعبور حساب‌های اعتباری و مالی است که زیان‌های مالی و اقتصادی زیادی را برای کاربر به همراه خواهد داشت . از نمونه حمله‌های موفق که در طول ماه جولای به وقوع پیوسته است و در آن‌ها از نرم‌افزارهای ثبت کلید استفاده شده می‌توان به حمله به بانک‌های اطلاعاتی سازمان حمل و نقل آمریکا ، سرقت اطلاعات شرکت بزرگ رایانه‌ای هیولت پاکارد (HP)و شبکه ماهواره‌ای HSN اشاره کرد .

خروجی برنامه‌های ثبت کننده کلید یک فایل است که برای کنترل کننده اصلی ارسال می‌شود. این فایل می‌تواند یک فایل متنی باشد که تمام کلیدهای ضربه خورده در روی صفحه کلید در آن ثبت شده است . (iranew. com)

۱۲-۵- روش‌های کلی نفوذ هکرها

هکرها معمولاً از یکی از دو روش زیر برای دست یابی به اهداف خود استفاده می‌کنند:

- اجرای نرم‌افزار مخرب
- استفاده از آسیب‌پذیری‌های نرم‌افزاری و یا سخت‌افزاری

۱۲-۶- نفوذ در سیستم‌ها به‌وسیله سازندگان

اغلب سازندگان سخت‌افزاری و نرم‌افزاری برای دسترسی به سیستم ساخته شده در مواقع مورد نیاز دریچه‌های را به صورت پنهان در آن تعبیه می‌نمایند که این دریچه‌ها به درب‌های

---

[۱] keylogger

پشتی[۱] معروف می‌باشند. این دریچه‌ها برای دسترسی و پنهان از راه دور و یا نزدیک به سخت‌افزار و نرم‌افزار مد نظر استفاده می‌شود . یکی از رایج‌ترین راه‌های اشرافیت بر اطلاعات دسترسی به اطلاعات از این طریق می‌باشد.

۱۲-۷- ابزارهای امنیتی

ابزارهای امنیتی نرم‌افزارهایی می‌باشند که از آن‌ها می‌توان هم برای تأمین امنیت و هم برای نفوذ در امنیت استفاده نمود. در این قسمت به بررسی برخی از این نرم‌افزارها از بعُد تأمین امنیت خواهیم پرداخت . نام بردن از نرم‌افزار خاص به معنی تأیید و یا عدم تأیید آن نمی‌باشد و صرفاً عمل‌کرد آن مدنظر بوده و شیوهٔ استفاده از آن در تأمین امنیت مدنظر می‌باشد .

Accesspv

امروز یکی از نرم‌افزارهای رایج برای ایجاد بانک اطلاعاتی نرم‌افزارaccess می‌باشد. در سازمان‌های مختلف علت سهولت در استفاده از این نرم‌افزار و هم‌چنین با توجه به آموزش دیدن بسیاری از کارکنان سازمان‌ها از این نرم‌افزار برای ایجاد بانک‌های اطلاعاتی کوچک در سازمان‌ها استفاده می‌شود و به منظور امن نمودن اطلاعات تولید شده بر روی بانک اطلاعاتی ایجاد شده رمز گذاشته می‌شود . از این نرم‌افزار می‌توان برای رویت رمز گذاشته شده بر روی بانک اطلاعاتی استفاده نمود و به مجرد کلیک کردن بر روی هم فایل مربوط رمز گذاشته شده بر روی آن هر چقدر هم پیچیده باشد رؤیت خواهد شد . منظور از ارائه این نرم‌افزار این است که نمی‌توان به رمز گذاشته شده بر روی نرم‌افزارهای کاربردی اعتماد داشت و فایل‌های آن را در اختیار افراد غیرمجاز قرار داد.

Active password changer

یکی از راه‌های محافظت از رایانه‌هایی که سیستم عامل ویندوز بر روی آن نصب شده است تعریف کاربر همراه با رمز می‌باشد. در کتاب‌های مربوط به امنیت شبکه و رایانه که توسط شرکت‌های تولیدکننده سیستم عامل ویندوز نوشته شده است اشاره می‌گردد که در صورت گذاشتن رمز بر روی کاربر افراد غیرمجاز قادر به دسترسی به اطلاعات رایانه نخواهند بود این مسئله باعث می‌گردد تا بسیاری از کاربران به این رمز اعتماد نموده و رایانه خود را پس از گذاشتن رمز در اختیار دیگران از جمله تعمیر کنندگان رایانه یا نویسندگان نرم‌افزار قرار دهند.

---

[۱] Back doors

این نرم‌افزار قادر خواهد بود تا در دقایق اندکی به کلیه رمزهای کاربران دسترسی پیدا نموده و آن را با رمز مدنظر تعویض نماید . با تعویض رمز کاربر اصلی قادر به دسترسی به اطلاعات نخواهد بود و کسی که رمز راعوض کرده است می‌تواند به اطلاعات دسترسی داشته باشد.

Administrative tools

در یک رایانه، مدیر رایانه به همه قسمت‌های آن دسترسی دارد و قادر خواهد بود به اطلاعات همه کاربران دسترسی داشته باشد . به منظور تعیین حیطه دسترسی برای کاربران دیگر، مدیر سیستم از ابزار خاصی استفاده می‌نماید. برخی از این ابزار توسط سیستم عامل در اختیار او قرار داده می‌شود. و برخی دیگر از ابزار با استفاده از نرم‌افزارهای کمکی تامین می‌شود. این نرم‌افزار قادر خواهد بود بدون استفاده از نرم‌افزارهای موجود به مدیریت سیستم دسترسی پیدا نموده و همانند مدیر سیستم رایانه را در اختیار داشته باشد و بر آن مدیریت نماید.

Anm

در زمانی که یک رایانه به شبکه متصل می‌شود مدیر شبکه می‌تواند به رایانه‌های متصل شده مدیریت داشته باشند ، در صورت اتصال شبکه‌ای به چندین شبکه مدیران مختلف و هم‌چنین کاربرانی که به این شبکه‌ها دسترسی فیزیکی دارند می‌توانند به اطلاعات رایانه‌های دیگر دسترسی داشته باشند . بسیاری از کاربران تصور می‌نمایند که با اتصال به شبکه امنیت رایانه تنها توسط مدیر شبکه تأمین می‌شود اما این نرم‌افزار نشان می‌دهد که با اتصال فیزیکی یک رایانه به شبکه کاربر مربوطه قادر خواهد بود کلیهٔ رایانه‌ها و شبکه‌های متصل به شبکه مربوطه را شناسایی و از اطلاعات آن‌ها بهره‌مند گردد.

Aports

در شبکه برای تعاملات اطلاعاتی بین اجزاء مختلف شبکه موجودیت‌ها از پورت‌های مجازی استفاده می‌نمایند از هر پورت که برای ارسال یا دریافت یک نوع اطلاعات استفاده می‌شود . در هر شبکه تعداد ۶۵،۵۳۵ پورت وجود دارد . با شناسایی این پورت‌ها می‌توان بر سر راه آن‌ها قرار گرفت و از اطلاعاتی که از طریق آن‌ها رد و بدل می‌شود بهره‌برداری سوء نمود. از این نرم‌افزار برای شناسایی پورت‌های باز و بسته استفاده می‌شود .

Dialpass

کاربرانی که به اینترنت متصل می‌شوند با استفاده از شماره تلفن و رمز و نام کاربری مربوطه از طریق شرکت‌هایی که خدمات اینترنت ارائه می‌دهند به اینترنت متصل می‌شوند ،

اطلاعات مربوط به شماره تلفن و نام کاربری و رمز مربوطه در رایانه ذخیره می‌گردد . این نرم‌افزار قادر خواهد بود تا به کلیه این اطلاعات دسترسی و آن‌ها را نمایش دهد.

Getdataback

بر روی ابزار ذخیره‌سازی اطلاعات اطلاعات مختلفی تولید و پس از استفاده از بین می‌روند و این اطلاعات در طی سال‌های مختلف همین روند را طی می‌نماید . رایانه‌ای که چندین سال برای کار شخصی یا اداری استفاده گردد می‌تواند صدها هزار فایل را تولید و آن‌ها را پس از استفاده حذف نماید ، در صورت دسترسی به اطلاعات گذشته افراد غیرمجاز قادر خواهند بود به اطلاعات انبوهی دسترسی داشته باشند . این نرم‌افزار برای احیا اطلاعات پاک شده استفاده می‌شود .

Iecv

در زمان استفاده از اینترنت یا استفاده جاری از رایانه اطلاعات با ارزشی مانند دسترسی به سایت‌های مختلف، زمان دسترسی، نوع استفاده و دیگر اطلاعات درون رایانه ذخیره می‌شود. در صورت دسترسی به این اطلاعات می‌توان به عادات امنیتی افراد مختلف دسترسی پیدا نمود. این نرم‌افزار قادر خواهد بود تا کلیه این گونه اطلاعات ذخیره شده را به نمایش بگذارد.

Ipscan

درشبکه رایانه‌ها با استفاده از شماره‌های خاصی که آی‌پی نامیده می‌شوند با یک‌دیگر تماس گرفته و تعامل اطلاعات دارند . با این نرم‌افزار می‌توان کلیه شماره‌های آی‌پی شبکه را شناسایی و نوع استفاده آن‌ها از منابع شبکه را تشخیص داد .

۱۲-۸- سئوالات خودآزمایی

۱. انواع روش‌های حمله به SETUP رایانه را نوشته و توضیح دهید.
۲. ارتباط بین سیستم عامل ویندوز و امنیت را توضیح دهید.
۳. اجزاء آناتومی هکرها نوشته و توضیح دهید.
۴. تست نرم‌افزار و سخت‌افزار خریداری شده، چه نقشی می‌تواند در امنیت رایانه داشته باشد.
۵. در زمان ارسال رایانه برای تعمیر و تنظیم چه مشکلات امنیتی ممکن است ایجاد شود؟
۶. سیستم‌های IDS وIPS چه نقشی در امنیتی رایانه دارند؟
۷. نفوذ در سیستم‌ها به وسیله سازندگان به چه روش‌هایی انجام می‌شود؟
۸. نقش اسکنرها در امنیت رایانه و شبکه را توضیح دهید.

لغت نامه:

administrative	به‌طور اداری
algorithm	الگوریتم ، مجموعه ی دستورات تعیین شده
analytical	ماهر در به کار بردن تجزیه و تحلیل ، تحلیل گر
application	نرم افزار کاربردی
appraisal	ارزیابی کردن ، برآورد کردن ، ارزشیابی کردن ، تقویم کردن ، ورانداز کردن
archive	بایگانی
arpanet	آرپانت
assessment	ارزیابی
attack	حمله
availability	قابلیت ارائه
backdoor	درب پشتی (نرم افزار مخرب)
biometrics	زیست سنجی
broadband	پهنای باند وسیع
broadcast	پخش کردن (رادیو تلویزیونی)

bug	حشره (منظور اختلالات در برنامه نویسی)
ciphertext	متن رمز شده
confidentiality	محرمانگی
conflict	تداخل
cryptanalysis	تجزیه و تحلیل رمز
cyber	فضایی
cyberwarfare	ابزار جنگی فضایی
database	پایگاه اطلاعاتی
datagram	چارت اطلاعاتی
datalink	ارتباط اطلاعاتی
demodulate	پیاده سازی - دمادوله کردن
implementation	بکارگیری
implication	مطلق
infrastructures	زیرساختار
keylogger	ثبت کننده صفحه کلید
lesspaper	استفاده کمتر از کاغذ در سیستم اداری

mainframe	رایانه اصلی و مادر
mitigation	تعدیل کننده
packet	بسته کوچک نرم افزاری
paperless	سیستم اداری بدون استفاده از کاغذ
passive	غیر فعال
password	رمز عبور
plaintext	متن آشکار
policy	سیاست
secret	رمز و راز
sector	قسمت - بخش - سکتور
secure	امن کردن
security	امنیت
security_policy	سیاست امنیتی
steganography	رمز نگاری - پوشش نگاری
synchronization	متقارن سازی
token	ابزاری برای رمزنگاری در رایانه

virtual	مجازی
wireless	بیسیم

اندیکس:

فهرست منابع

منابع فارسی

۱. اظهری علی – رازهای پنهان هیپنوتیزم – انتشارات میر – ۱۳۷۷
۲. ایلداری، س، "تاثیر تجارت الکترونیک بر بانک‌داری خرد، ماهنامه بانک صادرات، ۳۰.
۳. باطنی محمدرضا – ساخت و کار ذهن – انتشارات واژه – ۱۳۶۹
۴. بانک مرکزی و بانک‌داری الکترونیک"، بانک‌داری الکترونیک، ۱۳۸۷، ۳، ۲۲.
۵. پورابراهیمی و بنابی– آشنایی با اصول امنیت محیطی در حوزه فن‌آوری اطلاعات و ارتباطات – پدافند غیرعامل کشور -۱۳۸۹
۶. ترجمه بخشی از کتاب : security risk assessment and management
۷. جمالیان سید رضا – قدرت خود هیپنوتیزم – انتشارات اسپرک – ۱۳۶۸
۸. جمالیان سید رضا – هیپنوتیزم‌هارتلند –انتشارات جمال الحق– ۱۳۷۵
۹. جنگ و دفاع سایبر
۱۰. جهانگیری، ف، ۱۳۸۶"بررسی عوامل موثر در آمادگی الکترونیکی برای بانک‌داری الکترونیکی در بانک صادرات"پایان نامه کارشناسی ارشد، دانشگاه‌تربیت مدرس۱۳۸۶
۱۱. چالش‌های تحول الکترونیکی"پرتو ملت، ۲۰و۲۱، ۱۳۸۶، ۵۲-۴۹.
۱۲. خدادادی مهدی – مصاحبه تشخیص – انتشارات مدبر – ۱۳۸۵
۱۳. دهستانی مهدی – آسیب شناسی روانی – انتشارات طیف نگار – ۱۳۸۶
۱۴. دو مانع پیش روی بانک‌داری الکترونیک"ماهنامه بانک‌داری الکترونیک" ۱۳۸۷، ۵، ۱۰.
۱۵. ذاکر حسینی، دکتر علی- امنیت داده‌ها ، ،۱۳۸۶
۱۶. رشیدی، د، زادگان باوی، ه، "بانک‌داری متمرکز؛پیش نیازی برای تحول در ارائه خدمات بانکی"تازه‌های اقتصاد، ۳۱-۲۵-
۱۷. سی آرتور ویلیامز ،دیچارد دام . هینز – مدیریت ریسک – ترجمه : دکتر داور ونوس و گودرزی

۱۸. سید محمدی یحیی – آسیب شناس روانی – انتشارات نشر روان – ۱۳۸۶
۱۹. سید محمدی یحیی – روانشناس عمومی – انتشارات نشر ارسباران – ۱۳۸۶
۲۰. طاووس شعبان – روانشناس هیپنوتیزم – انتشارات کابوک – ۱۳۵۶
۲۱. عزبدفتری بهروز – ذهن و جامعه – انتشارات فاطمی – ۱۳۷۲
۲۲. 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.
۲۳. فرس پل – روانشناسی تجربی – سازمان انتشارات آموزش انقلاب اسلامی - ۱۳۶۹
۲۴. فرمایشات مقام معظم رهبری در دیدار اعضا مجلس خبرگان رهبری – ۱۳۸۸/۰۷/۰۲
۲۵. فرمایشات مقام معظم رهبری در دیدار جمع کثیری از بسیجیان – ۱۳۸۸/۰۹/۰۴
۲۶. فصلنامه میثاق بسیج متخصصین، سال سوم، شماره ۱۱، پاییز ۸۹
۲۷. فکور ثقیه، ا. م، "تاثیر فن‌آوری اطلاعات بر صنعت بانک‌داری"مدیریت، ۱۸، ۱۳۸۵، ۱۰۸-۱۰۷.
۲۸. کریستااسون – حافظه مجرمان از جرایم خشونت بار – انتشارات نشر آگاه – ۱۳۸۸
۲۹. کلمان ژاگوپل – روش‌های علمی مانیتیسم، هیپنوتیسم، تلقین – انتشارات ققنوس – ۱۳۸۳
۳۰. کیمیایی، پ، ۱۳۸۱"بانکداری سنتی و بانک‌داری الکترونیکی تقابلی اجتناب ناپذیر" فصلنامه بانک، شماره۲۲.
۳۱. گنجی حمزه – مصلحی زیبنده – ایزد دوست یوسف – روان شناسی – چاپ و نشر ایران – ۱۳۷۲
۳۲. اللهیاری فرد، م، "ارزیابی گسترش بانک‌داری الکترونیک در کشورهای اسلامی"، تازه‌های اقتصاد.

۳۳. مجوز عبدالله – دنیای خود هیپنوتیزم و بهبودی با تلقین – موسسه فرهنگی انتشاراتی حیان – ۱۳۷۶
۳۴. محمدزاده علی اکبر – ولیزاده صمد – روانشناس هیپنوتیزم – انتشارات تلاش
۳۵. مدیریت ریسک - سایت اینترنتی هیراد انجمن ایرانیان
۳۶. مقاله مدیریت ریسک - نوشته‌ی دکتر محمد علی بابایی و حمید رضا وزیر زنجانی
۳۷. مقاله مدیریت ریسک استراتژیک – نویسنده : آلن ورینگ و حسن مهدی زاد
۳۸. مقاله نقش فن‌آوری اطلاعات در مدیریت ریسک ، نشریه جهان اقتصاد
۳۹. مک فی نیل –تری راجر – هنر مخفی مصاحبه با افراد – انتشارات نشر آگاه – ۱۳۸۸
۴۰. منجمی علیرضا – روش‌های تقویت حافظه – نشر آزاد مهر – ۱۳۸۸
۴۱. نگاهی به بانک‌داری خرده فروشی درآینده- ترجمه جندقی، م، ماهنامه آموزشی، خبری بانک ملی ایران، ۱۳۸۶، ۲۱-۱۹. ۱۳۵. by betty E. biringer rodolph
۴۲. هیپنوتیزم‌هارتلند – جمالیان سید رضا – انتشارات جمال الحق– ۱۳۷۵
۴۳. دباغ رضایی، ی ، س، پزشکی، ۱۳۸۴"نقش فن‌آوری اطلاعات و ارتباطات در رشد اقتصادی"، تدبیر، ۱۳۸۴، ۱۶۳

منابع لاتین

۱. Agence France Press ،Mar ،۲۸ ،۲۰۰۱
۲. Air Force ،Operation Iraqi Freedom ،Information Operation Lessons Learned: Frist Look
۳. Airpower Journal ،July ،۱۹۹۶
۴. Appraisal: The Changing Role of Information in Warfare ، RAND ،۱۹۹۹ ،
۵. CANADIAN FORCES COLLEGE ،ADVANCED MILITARY STUDIES

۶. Carrington ،M ،۱۹۹۷ ،" The banking Revolution : how Technology in creating winners and losers " ،Great Britain ، pitman publishing company.
۷. Center ،Beijin Special Lecture ،Mar ،۱۹۹۷ ،
۸. Charles F. Hawkins ،China Defense Science & Technology Information
۹. Col. Andrew Borden ،USAF ،What is Information Warfare? The Information
۱۰. Col. Timothy Thomas ،Russian Views on Information-Based Warfare ،
۱۱. Communication Networks ،John Wiley and Sons Publishing ، ۲۰۰۳.
۱۲. Conflict in the Information Age ،RAND ،۱۹۹۷ ،
۱۳. Costas Courcoubetis and Richard Weber ،Pricing
۱۴. David Fulghum ،Sneak Attack ،Aviation Week & Space Technology ،June ۲۸ ،۲۰۰۴
۱۵. David Ruppe ،Directed-Energy Weapons: Possible U. S. Use Against Iraq
۱۶. DoD dictionary of Military and Associated Terms ،
۱۷. Dorothy Denning ،Information Warfare and Security ،Addison-Wesley ،۱۹۹۹
۱۸. Durhin ،M. ،Howcroft ،B. ،۲۰۰۳ ،" Relationship marketing in the banking sector " ،marketing Intelligence and planning ،vol ۲۷.
۱۹. Elaine Grossman ،Officials: Space ،Info Targets largely Cobbled on-the-fly for
۲۰. Frenchelon ،The large ears made in France
۲۱. Giampiero Giacomello ،Measuring digital wars: Learning from the experience

۲۲. IAnewsletter ،Vol. ۳ ،No. ۴

۲۳. InfoWarCon ،۲۰۰۰ ،Sep ۱۲ ،۲۰۰۰ ،Washington D. C.

۲۴. Iraq ،Inside Pentagon ،May ۲۹ ،۲۰۰۳

۲۵. ITU-toolkit page\ICT Regulation Toolkit. htm

۲۶. Jack Moteff ،Critical Infrastructures: Background & Early Implementation of PDD-۶۳-۱۳۵

۲۷. James Mulvenon ،The PLA and Information Warfare

۲۸. John Arquilla and David Ronfeldt (Ed) In Athena's Camp: Preparing for

۲۹. Joint Information Operations Planning Handbook ،

۳۰. Kajaluoto. h ،Kaoivumaki. t ،and Salo. j ،۲۰۰۳ ،"Individual difference in privat banking:empirical evidence from finlandhngs of the ۳ ،th hawii international conference on system sciences(H۱CSS) ،big island ،Hawaii ،p۱۹۶.

۳۱. Lester W. Grau and Timothy L. Thomas ،A Russian View of Future War:

۳۲. LU. J. ،L iu ،c. ،Yao ،J. ،۲۰۰۳ ،" Technoloyy Acceptance Model for wireless internet " ،Electronic Networking Applications and policy ،vol ۱۳ ،No۳.

۳۳. Megan Burns ،Defining Information Warfare: Easier Said than Done ،۱۹۹۹ ،

۳۴. Mesic ،Strategic Information Warfare Rising ،RAND ،۱۹۹۸ ،

۳۵. Military Strategic Research Center ،Beijing ،May ،۱۹۹۶

۳۶. Network Centric Warfare ،Department of Defense Report to Congress ،

۳۷. News Release ،US Space Command ،Sep ۲۹ ،۲۰۰۰ ،

۳۸. of peace research and arms control ،The Information Warfare Site ،

۳۹. Other countries developing cyber attack capability ،CIA says ، Feb ،۲۰۰۰ ،
۴۰. Peter Cartwright ،Interconnect Costing ،BWCS ltd ،United Kingdom ،۲۰۰۱.
۴۱. Proceeding of the ۲۰۰۱ IEEE Workshop on Information Assurance and
۴۲. Raymond C. Parks and David Duggan ،Principles of cyber-warefare ،
۴۳. Roger C. Molander ،Peter W. Wilson ،David A. Mussington ، Richard F.
۴۴. Ronald Fogleman and Sheila Widnall ،Cornerstones of Information Warfare ،
۴۵. Security ،Untied States Military Academy ،West Point ،NY ،۵-۶ June ،۲۰۰۱
۴۶. Smart Card Security and Applications”، Mike Hendry ، ۲nd Edition، ©ARTECH House INC Jr۰۲-۲۰۰۹ tracking ghostnet
۴۷. The White House ،A National Security Strategy for a New Century ،Dec ،۱۹۹۹
۴۸. Theory and Direction ،The Journal of Slavic Military Studies ، Issue ۹. ۳ ،Sep۱۹۹۶
۴۹. Threaten International Regims ،Global Security Newswire ، Agust ۱۶ ،۲۰۰۲،
۵۰. U. S Military concerned about China's cyberwarfare capabilities: General ،
۵۱. WIK-Consult ،Analytical Cost Model Broadband Network ،۲۰۰۵
۵۲. Will Dunham ،U. S may debut secret microwave weapons versus Iraq ،Reuters ،

۵۳. Y. P Baqwisat at R. Ganne, Kafrance dans Ia bataile des Technologie del inteligence, Paris, ed: La Documentation Fran Cise ۱۹۸۵ P. ۷.

۵۴. Yiu. c. s ،Grant. k ،Adgar. d ،۲۰۰۷ ،Factors affecting the adoption of Internet Banking in Hong kong-implication for the banking sector"International Journal of Informetion management ،۲۷ ،۳۳۶-۳

۵۵. Zalmay Khalizad ،John P. White ،Andrew W. Marchal (Ed) ، Strategic

منابع اینترنت

۱. David Alexander ،http://www. davidalexanderbooks.Com
۲. http // www. articles. com
۳. http // www. bashg. net
۴. http // www. beheshtnet. . blogfa. com
۵. http // www. daneshnameh. roshd. ir
۶. http // www. duzli-oghlan. blogfa. com
۷. http // www. fa. wikipedia . org
۸. http // www. farya. com
۹. http // www. firooz . ir
۱۰. http // www. forun. manuatoo. com
۱۱. http // www. giganews. ir
۱۲. http // www. iricap. Com
۱۳. http // www. noorportal. net
۱۴. http // www. social. iran-emrooz. net
۱۵. http // www. tebyan-ardebill. ir
۱۶. http //www. ahmady aghma. blogfa. com
۱۷. http://۸٤. ۱۱. ۳۲. ۱٤۹/NSite/FullStory/News/?Id=۱٦٦
۱۸. http://afand. blogfa. com/post-٤۹. aspx
۱۹. http://afand. blogfa. com/post-٦٤. aspx
۲۰. http://dehckade-danesh. mihanblog. com/post/۱۰
۲۱. http://dehckade-danesh. mihanblog. com/post/۹
۲۲. http://emmaf۲. isuisse. com/emmaf۲/iw/what. htm
۲۳. http://en. wikipedia. org/wiki/Command_and_control_warfare

۲۴. http://padafand-gh-amel. persianblog. ir
۲۵. http://parsifa. wordpress. Com
۲۶. HTTP://RANGARANGGROUP. COM/ARTICLES/۱۰۵۲٤
۲۷. http://system. parsiblog. com/Archive٤۱۲٤٦. htm
۲۸. http://www .erfan۲۰۰۰. persiangig. ir
۲۹. http://www. af. mil/lib/corner. html
۳۰. HTTP://WWW. AFTAB. IR/LIFESTYLE/VIEW/۱۲٦۹۷۱
۳۱. http://www. cs. cmu. edu/~burnsm/InfoWarfare. html
۳۲. http://www. daneshju. ir/forum/f۳٥۰/t۳۷۱٤۸. html
۳۳. http://www. daneshju. ir/forum/sitemap/t-٤٦۰٤۰. html
۳۴. http://www. dod. mil/nii/NCW/
۳٥. http://www. dtic. mil/doctrine/jel/doddict/data/i/index. html
۳٦. http://www. ege. eslsca. fr
۳۷. http://www. globalsecrutiy. org/org/news
۳۸. http://www. hamshahri. org
۳۹. http://www. herolibrary. org/iwa٤web. htm
۴۰. http://www. infoguerre. com
۴۱. HTTP://WWW. IRCERT. COM/ARTICLES/SECURITY_POLICY۱. HTM
۴۲. http://www. iwar. org. uk/infocon
۴۳. http://www. iwar. org. uk/iwar/resources/jiopc/io-handbook. pdf
۴۴. HTTP://WWW. MUMS. AC. IR/HIT/FA/OSI
۴٥. http://www. networkworld. com/news/۲۰۰۰/۰۲۲٤cia. html
۴٦. http://www. peace. ca/canadianinformationoperations. htm
۴۷. http://www. prr. ir/files/۷۰۰۳accfc٦۰ac۷۹۱e۲٦۸۹b۷۳۳۲۸٦۷b۰a. doc
۴۸. http://www. rand. org/publications/MR/MR۹٦٤/MR۹٦٤. pdf
۴۹. http://www. rand. org/pubs/monograph_reports/MR۱۰۱٦/
٥۰. http://www. rand. org/pubs/monograph_reports/MR۸۸۰/index. html
٥۱. http://www. sans. org/newlook/resources/IDFAQ /solar_sunrise. htm
٥۲. http://www. spacecom. af. mil/usspace/re۱۱٥-۰۰. htm
٥۳. http://www. srco. ir/Articles/TipsView. asp?ID=۲۹۱
٥۴. http://www. thefreedictionary. com/IWCOURSE ۲ ،NOV ،۱۹۹۹ ،
٥٥. http://www. zdnet. fr/actu/tech/secu/a۰۰۱٤۷٦۸/html
٥٦. http://www.georgetown.edu/sfs/programs/stia/students/vol.۰۳/Johnson_IW. htm
٥۷. http://www.insidedefense.com/secure/data_extra/pdf۳/dplus۲۰۰٤_۲٦٥. pdf

۵۸. http://www.shabakeh-ag.com/articles/Show.aspx?n=۱۰۰۳٤۱٤
۵۹. http://www.shabakeh-mag.com/articles/Show.aspx?n=۱۰۰۳٤۱٤&p=۳
۶۰. US Strategic Command Fact File ،http://www. stratcom. af. Mil /factsheet. shtml
۶۱. USAF Doctrine of Information Operations.http://www. iwar. org. uk/iwar/resources/usaf/maxwell/students/۲۰۰۱/۰۱-۰۲۸. pdf
۶۲. Warfare Site ،http://www. iwar. org. uk /iwar /resources /airchronicles /borden. htm
۶۳. Wordnet Princeton University ، http://www. wordnet. princeton. Edu,
۶۴. www. berkley. com
۶۵. www. berkley. Com
۶۶. www. forum. silvapc. com/index. php?topic=۲٦۷٦. ۰%۳bwap۲
۶۷. www. hamedbanaei. com
۶۸. www. imi. ir/tadbir/tadbir-۱۳٤/article-۱۳٤/٤. asp
۶۹. www. iranew. com
۷۰. www. itirn. com
۷۱. www. microsoft. com
۷۲. www. p۳۰lords. com/forum/archive/index. php/t-۹۲٦۳. html
۷۳. www. ponemonen. com
۷۴. www. roshd. com
۷۵. www. srco. ir/articles/docview. asp۲id=۱۸۲
۷۶. www.tebyan.net/science_technology/computermagazine/interview_report/۲۰۰٤/۱۳/٥۸۰۲. html
۷۷. www//informat. htm