عنوان پروژه

امنیت فناوری اطلاعات

پیشگفتار

مفهوم امنیت در دنیای واقعی مفهومی حیاتی و کاملاً شناخته شده برای بشر بوده و هست. در دوران ماقبل تاریخ، امنیت مفهومی کاملاً فیزیکی را شامل می شد که عبارت بود از اصول حفظ بقا نظیر امنیت در برابر حمله دیگران یا حیوانات و نیز امنیت تامین غذا. بتدریج نیازهای دیگری چون امنیت در برابر حوادث طبیعی یا بیماریها و در اختیار داشتن مکانی برای زندگی و استراحت بدون مواجهه با خطر به نیازهای پیشین بشر افزوده شد. با پیشرفت تمدن و شکل گیری جوامع، محدوده امنیت ابعاد بسیار گسترده تری یافت و با تفکیک حوزه اموال و حقوق شخصی افراد از یکدیگر و از اموال عمومی، و همچنین تعریف قلمروهای ملی و بین المللی، بتدریج مفاهیم وسیعی مانند حریم خصوصی، امنیت اجتماعی، امنیت مالی، امنیت سیاسی، امنیت ملی و امنیت اقتصادی را نیز شامل گردید. این مفاهیم گرچه دیگر کاملاً محدود به نیازهای فیزیکی بشر نمی شدند، ولی عمدتاً تحقق و دستیابی به آنها مستلزم وجود و یا استفاده از محیط های واقعی و فیزیکی بود.

لیکن جهان در دهه های اخیر و بویژه در پنج سال گذشته عرصه تحولات چشمگیری بوده که بسیاری ا زمناسبات و معادلات پیشین را بطور اساسی دستخوش تغیر نموده است. این تحولات که با محوریت کاربری وسیع از فناوری اطلاعات و ارتباطات امکانپذیر شده، از کاربرد رایانه به عنوان ابزار خودکارسازی (AUTOMATION) و افزایش بهره وری آغاز گردیده و اکنون با تکامل کاربری آن در ایجاد فضای هم افزایی مشارکتی (COLLABORATION) ، عملاً زندگی فردی و اجتماعی بشر را دگرگون ساخته است. به باور بسیاری از صاحب نظران همانگونه که پیدایش خط و کتابت آنچنان تاثیر شگرفی بر سرنوشت انسان برجای گذاشته که مورخین را بر آن داشته تا داستان زندگی بشر بر این کره خاکی را به دوران ماقبل تاریخ تقسیم نمایند، ورود به فضای مجازی حاصل از فناوری نوین اطلاعات و ارتباطات نیز دوره جدیدی از تمدن بشری را رقم زده، به نحوی که انقلاب عصر اطلاعات شیوه اندیشه، تولید، مصرف، تجارت، مدیریت، ارتباط، جنگ و حتی دینداری و عشق ورزی را دگرگون ساخته است.

این تحول بزرگ الزامات و تبعات فراوانی را به همراه داشته که از مهمترین آنها بوجود آمدن مفاهیم نوین امنیت مجازی یا امنیت در فضای سایبر می باشد. با تغییری که در اطلاق عبارت شبکه رایانه ای از یک شبکه کوچک کار گروهی به شبکه ای گسترده و جهانی (اینترنت) واقع گردیده، و با توجه به رشد روز افزون تعاملات و تبادلاتی که روی شبکه های رایانه ای صورت می پذیرد، نیاز به نظام های حفاظت و امنیت الکترونیکی جهت ضمانت مبادلات و ایجاد تعهد قانونی برای طرفهای دخیل در مبادله بسیار حیاتی است. نظام هایی مشتمل بر قوانین ،روشهای، استانداردها و ابزارهایی که حتی از عقود متداول و روشهای سنتی تعهدآورتر بوده و ضمناً امنیت و خصوصی بودن اطلاعات حساس مبادله شده را بیش از پیش تضمین نمایند.

امنیت اطلاعات در محیط های مجازی همواره بعنوان یکی از زیرساختها و الزامات اساسی در کاربری توسعه ای و فراگیر از ICT مورد تاکید قرار گرفته است. گرچه امنیت مطلق چه در محیط واقعی و چه در فضای مجازی دست نیافتنی است، ولی ایجاد سطحی از امنیت که به اندازه کافی و متناسب با نیازها و سرمایه گذاری انجام شده باشد تقریباً در تمامی شرایط محیطی امکانپذیر است. تنها با فراهم بودن چنین سطح مطلوبی است که اشخاص حقیقی، سازمانها، شرکتهای خصوصی و ارگانهای دولتی ضمن اعتماد و اطمنیان به طرفهای گوناگونی که همگی در یک تبادل الکترونیکی دخیل هستند و احتمالاً هیچگاه یکدیگر را ندیده و نمی شناسند، نقش مورد انتظار خود بعنوان گره ای موثر از این شبکه متعامل و هم افزا را ایفا خواهند نمود.

فهرست مطالب

خلاصه اجرایی

راهنمای امنیت فناوری اطلاعات، راهنمایی کاربردی جهت فهم و اجرای گامهای دستیابی به امنیت در کاربردهای حوزه فناوری اطلاعات در منزل و محل کار شما است. گرچه این پروژه بهترین و نوین ترین راهکارها را در زمینه فناوری اطلاعات ارائه می دهد، اما در اصل بری خوانندگان کشورهای در حال توسعه نوشته شده است. این پروژه علاوه بر ارائه خلاصه ای از تهدیدات فیزیکی و الکترونیکی موجود در حوزه امنیت فناوری اطلاعات، به راهکارهای مدیریتی ، محیط های ضابطه مند و الگوهای مشارکت سازماندهی همکار می پردازد که در حال حاضر در بازارهای، دولتهای، موسسات حرفه ای و سازمانهای بین المللی وجود دارند.

سازگارسازی فناوری اطلاعات و ارتباطات در حال افزایش است

این پروژه در ابتدا مروری بر رشد بخش فناوری اطلاعات و ارتباطات (ICT) دارد. این رشد و ارتقا کاربران عادی ICT را در بر میگیرد و از افزایش تعداد شبکه های خانگی و رشد سازمانهای کوچک و متوسط (SMES) که برای پشتیبانی از بازارهایی که به شدت به توسعه فناوری و بکارگیری آن در سراسر جهان وابسته اند کتکی به منابع رایانه ای می باشند- می توان به آن پی برد.

اطلاعات موجود از سوابق فعالیتهای

تامین امنیت فناوری اطلاعات

از آنجا که توسعه بازار محصولات و خدمات فناوری در دو سطح فردی و سازمانی چشمگیر است، اطلاع از مباحث امنیت فناوری اطلاعات بسیار مفید و مهم می باشد. ممکن است کاربران فردی در مورد خطراتی که هنگام استفاده از اینترنت متوجه آنها است مطلع نباشند . اگر کاربران خطرات شبکه های حفاظت نشده را تشخیص دهند، باز هم ممکن است یادگیری در مورد دیواره های آتش، ویروس یابها، رمزگذاری و نگهداری قاعده مند از

اطلاعات را به دلیل هزینه و وقتی که از آنها می گیرد و تغییری که در رفتار رایانه ای آنها ایجاد می کند به تعویق بیاندازند. علاوه بر این سازمانهای کوچک و متوسط ممکن است از یک راه حل فنی نظیر دیواره آتش استفاده نمایند و به طبقه بندی سطوح امنیت توجهی نداشته باشند و ندانند که بدون توجه به آن، امنیت سیستم به شدت دچار مخاطره است. همچنین ممکن است به دلایل مختلف ایمن ساختن سیستمهای خود را به تاخیر بیاندازند و در تدوین سیاستهای شفاف امنیتی برای کاربران و مدیران نیز کوتاهی کنند. اگر ارتباطات، آگاهی و آموزش مناسب در سازمان وجود نداشته باشد، تبهکاران ممکن است به آسانی حفاظهای فنی را پشت سر بگذارند.

فناوری در یک محیط متغیر

دستگاههای سیار، نرم افزارهای رایج کاربردی، و تهدیدهای که موجب ایجاد پیچیدگی می شوند.

در حال حاضر کاربران جدید و غیر متخصص تنها علت نقض امنیت فناوری اطلاعات نیستند. محیط فناوری اطلاعات و ارتباطات با پیدایش محصولات جدید خصوصاً دستگاههای سیار (مانند رایانه های کیفی، تلفنهای همراه و PDAها) که چالشهای متفاوتی را در زیرساخت و امنیت داده ها ایجاد می کنند بسرعت رو به تغییر می باشد. پیدایش برنامه های کاربردی رایانه ای برای سرمایه گذاری الکترونیکی و تجارت الکترونیک نیز موجب بروز پیچیدگی های در محیط های شبکه ای شده اند.

از هنگام ظهور دستگاههای خودپرداز گرفته تا زمان رواج بانکداری اینترنتی ، این قابلیتها موجب صرفه جویی مناسب در هزینه ها می شوند، اما تهدیدات و خطرات بالقوه ای نیز به همراه دارند.

آنچه که اوضاع را بدتر می کند این است که اکنون نفوذگران قادر به توسعه و گسترش تهدیدات خود می باشند: مثل ترکیبی از ویروسها، کرمها و تراواهایی که می تواند آسیبهای شدیدتری را به این سیستمها و داده ها وارد کند. این صدمات حتی می توانند از بعضی نرم افزارهای مخرب (بدافزارها) نیز خطرناکتر باشند. از آنجا که تمامی این

پیشرفتها کاربران فناوری را در سطح جهانی تحت تاثیر قرار می دهند، بهترین روشهای مقابله با تهدیدات ناشی از آنها تنها از طریق همکاری بین المللی حاصل می شود.

همکاری بین المللی و امنیت در کشورهای در حال توسعه

امنیت فناوری اطلاعات در کشورهای در حال توسعه از اهمیت شایانی برخوردار است. واضح است که اینترنت فرصتهایی طلایی برای تجارت و ارتباطات فراهم آورده که حدود ده سال قبل حتی تصور آنها مشکل بود. البته دسترسی به اینترنت همیشه هم ارزان نیست. اینترنت کاربران را قادر می سازد تا نگاهی به گستره وسیعی از موضوعات داشته باشند و با استفاده از آن ارتباط مردم از طریق پست الکترونیکی بسیار کارآمدتر از خدمات پستی سنتی شده است. اینترنت بر اصول تجارت بین المللی نیز تأثیر گذاشته است،بازارهای کشورهای در حال توسعه اکنون می توانند کالاهای خود را بصورت برخط بفروشند. اگر چه هنوز تعداد رقبا در بازار بسیار زیاد است، اما مشتریان می توانند به سادگی تواناییها و محصولات شرکتهای رقیب را ببینند و برای انجام این کار نیازی به اطلاعات وسیع در این زمینه ندارند. از آنجا که دسترسی به بازارهای آنسوی مرزهای جغرافیایی برای هر سیستم اقتصادی بسیار جذاب است، همکاری گسترده ای برای جا افتادن مدل یک نظام شبکه ای کارآمد و جهانی لازم است.

بخش اول

امنیت اطلاعات

مقدمه

اولین گام در ارائه یک استراتژی صحیح امنیتی این است که مفهوم «کاربرد صحیح» رایانه های شخصی و «حفاظت» از آنها مشخص شود. اگر شما نیز بدنبال همین مسئله هستید، اطمینان حاصل کنید که:

- داده ها و برنامه هایتان تنها در صورتی تغییر میکنند یا پاک می شوند که شما چنین خواسته ای داشته باشید.
- برنامه های رایانه بگونه ای که طراح یا برنامه نویس آنرا تعیین کرده عمل می کنند (مگر عیب و نقصهای نرم افزاری، که وجود آنها رد برنامه ها ناخواسته است).
- هیچکس نمی تواند بدون اجازه شما از داده ها، رایانه و شبکه شما استفاده کند.
- رایانه بطور ناخواسته فایلهای آلوده به ویروس را منتشر نمی کند.
- کسی قادر به مشاهده تغییراتی که رد رایانه ایجاد می کنید نیست.
- کسی توانایی دستیابی به داده های شما، چه در شبکه های بی سیم و چه در شبکه های سیمی را ندارد.
- روی سیستمها و یا پایگاه های وبی که به آنها دسترسی دارید کسی قادر به سرقت نام کاربری و رمز عبور نیست.
- چنانچه شماره کارت اعتباری و یا اطلاعات مربوط به حساب بانکی خود را از طریق شبکه اینترنت وارد کنید، داده های مربوطه از امنیت کامل برخوردار خواهند بود (مسلماً شما بر آنچه که در سوی دیگر شبکه ارتباطی رخ می دهد کنترلی نخواهید داشت).

فصل اول

امنیت اطلاعات چیست؟

امنیت اطلاعات نمی تواند ایمنی را صد در صد سازماندهی اطلاعاتی سیستم کامپیوتری شما ضمانت نماید. به عبارت دیگر امنیت اطلاعات قادر به نگهداری اطلاعات شما نیست. هیچ سحر و جادویی را نمی توان یافت تا امنیت کاملی برای اطلاعات ایجاد نمود. مفاهیم موجود در امنیت اطلاعات، علم نظامی و فنی هم نیست که واضح و آشکار باشد.

در واقع امنیت اطلاعات نوعی طرز فکر است. طرز فکری که در آن انواع تهدیدهای ممکن و راههای ضربه زدن به سازماندهی اطلاعاتی بررسی می شود و مدیریت مناسبی برای آن پیشنهاد می گردد. شاید به تعداد زیادی از تولید کنندگان برخورد کرده باشید که هر یک ادعا می کنند محصول تولیدی آنها بهترین راه حل برای رفع مشکلات امنیتی است .

در این فصل سعی بر آن است تا مسائل مربوط به امنیت اطلاعات تشریح گردد و در نهایت استراتژی مدیریتی مناسبی برای سازماندهی اطلاعاتی پیشنهاد گردد.

تعریف امنیت اطلاعات

بنا بر فرهنگ Merrian- Webster (که به صورت زنده در آدرس www.m-w.com موجود است) کلمه «اطلاعات» بصورت زیر تعریف شده است:

اطلاعات دانشی است که از طریق تحقیق، مطالعه، آموزش، فهم مطلب، اخبار، حقایق، دیتا، سیگنال یا کارکتری که حاوی دیتا باشد (مانند سیستمهای مخابراتی یا کامپیوتری)، چیزی که نحوه ایجاد تغییرات در یک ساختار را بیان می کند (مانند طرح یا تئوری) و چیزهایی از این قبیل بدست آمده باشد.

در همین فرهنگ نامه امنیت بصورت زیر تعریف شده است :

رهایی از خطر ، وجود ایمنی ، رهایی از ترس یا نگرانی

اگر دو کلمه فوق را در کنار هم قرار دهیم ، به تعریفی از «امنیت اطلاعات» بصورت زیر خواهیم رسید:

امنیت اطلاعات میزان اجازه و اختیاری است که استفاده از یک سرویس ، عدم استفاده از آن، و مقدار ایجاد اصلاحات توسط آن تعریف می شود و جلوگیری از بکارگیری دانش، حقایق ، دیتا یا قابلیت ها را باعث می شود .این تعریف حوزه وسیعی را شامل می شود که دانش ، حقایق ، دیتا یا قابلیت ها در برابر اتفاقات بد محافظت شود.

علاوه بر این در تعریف فوق محدودیتی روی شکل اطلاعات قرار ندادیم بطوریکه می تواند بصورت دانش یا قابلیت های یک سیستم باشد.

اما تعریفی که از امنیت شبکه ارائه شد ضمانتی روی حفاظت از اطلاعات ندارد . زیرا اگر بزرگترین قلعه نظامی دنیا بسازیم باز هم یک نفر پیدا خواهد شد که با ابزار جنگی قوی تر و بزرگتری آن قلعه را فتح خواهد کرد.

امنیت اطلاعات نامی است که به اقدامات پیشگرانه اطلاق می شود بطوریکه این اقدامات قادر است از اطلاعات و قابلیت هایمان نگهبانی نماید. بدین ترتیب می توانیم اطلاعات را در برابر حملات خارجی و بهره برداری های غیر مجاز محافظت نماییم.

تاریخچه مختصری از امنیت

امنیت اطلاعات در طول زمان و بتدریج سیر تکاملی خود را پیموده است بطوریکه این روند تکاملی از رشد تکنولوژی و مسائل اجتماعی متأثر بوده است . فهمیدن روند رشد امنیت اطلاعات در این جهت مهم است که می توانیم احتیاجات خود را بهتر درک کرده و مطابق نیازهای روز آنرا ایجاد نمائیم . علاوه بر دانستن تاریخچه امنیت اطلاعات ، باید بر جنبه های مختلف آن نیز اشراف داشت بدین ترتیب اشتباهاتی که افراد قبل از ما انجام داده اند تکرار نخواهد شد . در ادا مه به این موارد خواهیم پرداخت .

امنیت فیزیکی

از جهت تاریخی می توان گفت اولین شکل اطلاعاتی که بشر آنها را نگهداری می کرد به صورت فیزیکی بودند بطوریکه در ابتدا آنها را روی سنگ و بعداً روی کاغذ ثبت می کرد. (بسیاری از کتابهای راهنمای تاریخی در مکان امن و مناسبی قرار نداشته اند تا اطلاعات حیاتی آنها در امان بماند . به همین دلیل امروزه اطلاعات بسیار کمی درباره علم کیمیا وجود دارد. علاوه بر این کسانی که اطلاعات مهم در اختیار داشتند آنرا فقط در برخی شاگردان خاص خود قرار می دارند چنانکه ضرب المثلی معروف میگوید دانش همان قدرت است . شاید این روش بهترین روش باشد . یک ضرب المثل معروف می گوید: رازی که بیش از یکنفر آنرا بداند دیگر راز نیست). بهر حال برای محافظت از این سرمایه ها امنیت فیزیکی بصورت دیوار ، خندق و نگهبان بکار می رفت.

برای ارسال این نوع اطلاعات از یک پیام رسان استفاده می شد که اغلب نگهبانی هم او را همراهی می کرد. خطر موجود در این حالت کاملاً فیزیکی است چون راهی وجود ندارد که بدون بدست آوردن آن شئ اطلاعاتش را بدست آورد. در اکثر موارد سرمایه موجود به سرقت می رفت (این سرمایه پول یا اطلاعات مکتوب بود) و مالک اصلی آنرا از دست می داد.

امنیت مخابراتی

متأسفانه امنیت فیزیکی دارای نقص عمده ا ی است و آن اینکه اگر هنگام جابجایی اطلاعات، پیام به سرقت رود اطلاعات آن قابل استفاده و یادگیری برای دشمن خواهد بود . این نقیصه توسط ژولیس سزار شناسایی شده بود. راه حل این نقص در امنیت مخابراتی است. ژولیس سزار برای رفع این مشکل رمز سزار را ایجاد کرد. این نوع رمز باعث میشد تا اطلاعات در حال انتقال حتی اگر به سرقت برود توسط کسی قابل خواندن و استفاده نباشد .

این مسئله در جنگ جهانی دوم ادامه پیدا کرد. آلمانی ها از ماشینی به نام Enigma استفاده کردند که پیام های ارسالی به واحدهای نظامی توسط آن رمز میشد. آلمانی ها ادعا می کردند اگر از ماشین Enigma بدرستی استفاده شود نمی توان قفل آنرا شکست . اما استفاده درست از آن کار بسیار سختی بود، به همین دلیل برخی اپراتورها هنگام استفاده از این ماشین دچار اشتباه می شدند و در نتیجه طرف مقابل قادر بود برخی پیامها را بخواند (بعد از آنکه مقادیر قابل توجهی از منابع رمز این ماشین بدست آمد مشکل خواندن پیام های آن نیز حل شد).

ارتباطات نظامی برای ارسال پیام به واحدها و مکان های نظامی از کلمات کد استفاده می نمایند. ژاپن در طول جنگ از کلمات کدی استفاده می کرد که درک درست پیام ها را برای آمریکایی ها ، حتی اگر کدها را کشف می کردند بسیار مشکل می ساخت . زمانیکه جنگ به نبرد Midway کشیده شد، کد شکن های آمریکایی سعی می کردند هدف ژاپنی ها پیدا کنند. این هدف در پیام های ژاپنی ها بصورت " AF " دیده می شد. سرانجام آمریکایی کاری می کردند تا Midway عمداً پیامی درباره کمبود آب ارسال نماید. ژاپنی ها مجبور شدند در پاسخ و یک پیام کد ارسال کنند. در پیام کد شده معلوم گردیده که AF مخفف آب است . از انجام که آمریکایی ها پیام ژاپنی ها را خواندند لذا قادر بودند که بفهمند AF در واقع همان Midway است.

پیام ها تنها نوع ترافیکی نبود که کد می شدند . واحدهای ارتش آمریکا از یک زبان محلی استفاده می کردند تا دشمن نتواند به پیام های مخابره شده گوش کند . این افراد محلی برای ارسال پیام ها استفاده می کردند به همین دلیل اگر دشمن به این پیام ها گوش می داد نمی توانست از آن چیزی بفهمد.

بعد از جنگ جهانی دوم جاسوسان اتحاد جماهیر شوروی برای ارسال اطلاعات از یک سیستم خاص استفاده می کرد که one- time pads (الگوی یکبار مصرف) نام داشت. این سیستم در واقع از چند صفحه کاغذ ادبی تشکیل شده بود که هر صفحه از آن دارای یک عدد تصادفی بود. هر صفحه فقط و فقط برای یک پیام بکار می رفت . چنانچه از این روش رمز نگاری بدرستی استفاده می شد، غیر قابل شکست بود اما در اینجا هم اشتباهات انسان باعث شد تا برخی از پیام ها قابل رمز گشایی شود.

امنیت تشعشع

صرف نظر از اشتباهاتی که باعث لو رفتن یک پیام رمز شده می شود، استفاده از یک رمز کننده خوب باعث می شود که شکستن آن رمز بسیار مشکل گردد. به همین دلیل تلاش ها به سمت دیگری معطوف گردید تا بوسیله آن بتوان اطلاعات رمز شده برای ارسال را به چنگ آورد. در سال ۱۹۵۰ کشف گردید اگر سیگنالهای الکتریکی که از طریق خطوط تلفن عبور می کنند تحت نظر قرار گیرند می توان به پیام اصلی دست پیدا کرد.

تمام سیستم های الکترونیکی از خود تشعشع الکترونیکی صادر می کنند. این پدیده در دستگاه تله تایپ و دستگاه رمز کننده ای که برای ارسال پیام های رمز شده بکار می رود نیز وجود دارد .

وظیفه دستگاه رمز کننده این است که سر راه پیام قرار داده شود و پس از رمز نمودن پیام، آنرا روی خط تلفن ارسال کند. اما نکته جالب این است که سیگنالهای الکتریکی که پیام اصلی و رمز نشده را در خود دارند بدلیل تشعشع ، اندکی روی خط تلفن دیده می شود. در واقع اگر از تجهیزات خوبی استفاده شود می توان پیام را از روی خط تلفن بازیابی کرد.

این مشکل ایالات متحده آمریکا را بر آن داشت تا برنامه ای به نام TEMPTEST ایجاد کند. وظیفه این برنامه ایجاد استاندارد های تشعشع الکتریکی برای سیستم های کامپیوتری است که در محیطهای بسیار حساس استفاده می شوند . نتیجه این بود که با کاهش تشعشعات ، امکان به سرقت رفتن اطلاعات کاش یافت .

امنیت کامپیوتری

اگر از سیستم تله تایپ برای ارسال پیام استفاده شود، کافی است برای محافظت پیام امنیت مخابراتی و امنیت تشعشع رعایت شود. اما با ورود کامپیوتر به عرصه زندگی انسان چشم اندازهای جدیدی در نحوه ذخیره و ارسال

اطلاعات ایجاد گردید و فرمت های جدیدی برای سیگنالهای الکتریکی حاوی پیام ابداع گردید . با گذشت زمان استفاده از کامپیوتر آسانتر شد و مردمان بیشتری امکان استفاده و برقراری ارتباط دو طرفه با آنرا پیدا کردند. بدین ترتیب اطلاعات موجود روی سیستم کامپیوتر ی برای هر کسی ک بتواند از این وسیله استفاده کند قابل استفاده می شود.

در سال ۱۹۷۰ دو نفر به نامهای Leonard La Padula و Davd Bel مدلی برای عملکرد ایمن کامپیوتر ابداع کردند. این مدل بر اساس یک مفهوم حکومتی بنا شده است که در آن اطلاعات بصورت طبقه بندی شده وبا سطوح مختلف قرار می گیرد و مجوزهایی با سطوح مختلف برای استفاده از اطلاعات وجود دارد . (در این سیستم اطلاعات به چهار فرم طبقه بندی نشده ، محرمانه ، سری و بسیار سری تقسیم بندی می شود) . بدین ترتیب اگر کسی یا سیستمی دارای مجوزی باشد که سطح آن از سطح طبقه بندی اطلاعات بالاتر باشد می تواند به آن فایل دسترسی پیدا کند.

مدل فوق اساس استاندارد ۵۲۰۰/۲۸ در آمریکا گردید که به نام TCSEC شناخته می شود (البته به نام کتاب نارنجی هم شناخته می شود). کتاب نارنجی سیستم های کامپیوتری را بر طبق معیار زیر تعریف می کند :

حداقل محافظت (و یا خارج از محدوده)	D
محافظت امنیتی از روی احتیاط	C1
محافظت بصورت دسترسی کنترل شده	C2
محافظت امنیتی طبقه بندی	B1
محافظت ساختار یافته	B2
حوزه های امنیتی	B3
طراحی بازبینی	A1

برای هر یک از تقسیم بندی های فوق کتاب نارنجی وظایف خاصی را به عنوان پیش نیاز معین کرده است تا اطمینان و ضمانت لازم حاصل شود. بنابراین برای آنکه سیستمی به سطح خاصی از اطمینان برسد و مورد تصدیق قرار گیرد باید این وظایف و خصوصیات را بدرستی رعایت نماید.

فراهم کردن ملزومات سیستمی کاملاً امن و مطمئن ، نیاز به دقت بسیار و هزینه بالا دارد. به همین دلیل سیستم های کمی وجود دارند که از تقسیم بندی C2 بالاتر باشند (تاکنون فقط یک سیستم توانسته به A1 برسد و آن سیستم Honeywel Scomp است. معیار های دیگری که وجود دارند سعی کردهاند وظایف یک سیستم را از اطمینان و ضمانت آن جدا نمایند. برای نمونه می توان به German Green Book در سال ۱۹۸۹، Canadian Criterid در سال ۱۹۹۰ ، CISE یا Criteria Information Security Evaluation در سال ۱۹۹۱ و بلاخره Federal Criteria در سال ۱۹۹۲ اشاره کرد. هر یک از این معیارها تلاش کرده اند برای امنیت بخشیدن به سیستم های کامپیوتری روشی را پیشنهاد دهند.

در آخر باید گفت سیستم های کامپیوتری به سرعت به طرف برنا مه های تضمین شده و مطمئن در حرکتند . این حرکت آنقدر سریع است که قبل از آنکه نسخه های قدیمی سیستم عامل و سخت افزار کامپیوتر بتواند مورد تائید واقع شوند، نسخه های جدید به بازار می آید.

امنیت شبکه

از جمله مشکلات موجود در هنگام ارزیابی معیار های امنیت کامپیوتری فقدان درک مفهوم شبکه بود. هنگامی که کامپیوترها به هم شبکه شدند مفاهیم جدیدی از امنیت هم پدیدار شد و مفاهیم قبلی امنیت دیگر مفید نبود. به عنوان مثال هنگام استفاده از مخابرات، شبکه ای محلی وجود دارد و نه یک شبکه گسترده، علاوه بر این در یک شبکه کامپیوتری از سرعت های بالاتری استفاده می شود و تعداد زیادی ارتباط از طریق یک واسطه ایجاد می شود. در این حالت استفاده از یک رمز کننده خاص به هیچ عنوان جوابگوی نیاز امنیتی نمی باشد. علاوه بر این مسئله تشعشع

الکتریکی از سیم هایی که در یک اتاق یا ساختمان کامپیوترها را به هم شبکه کرده است نیز وجود دارد و سرانجام این که در یک شبکه کامپیوتری کاربرانی وجود دارند که از سیستم های بسیار متنوع به سیستم ما دسترسی دارند بدون اینکه توسط یک کامپیوتر واحد، کنترل مرکزی روی آنها اعمال گردد.

در کتاب نارنجی به مفهوم کامپیوتر های شبکه شده اشاره ای نشده است . به عبارت دیگر دسترسی از طریق شبکه قادر است اعتبار کتاب نارنجی را زیر سؤال ببرد. جواب این مشکل در کتاب آورده شده است که به شرح شبکه امن در TCSEC می پردازد و به TNI یا کتاب قرمز معروف است. مفاد کتاب قرمز در سال ۱۹۸۷ تنظیم شده است . کتاب قرمز تمام نیازهایی که کتاب نارنجی به آن اشاره کرده است را در خود دارد و علاوه برآن سعی کرده است به محیط شبکه ای کامپیوترها هم بپردازد . متأسفانه کتاب قرمز بیشتر به مسائل وظیفه ای پرداخته است به همین دلیل سیستم های کمی توانسته اند تحت TNI یا کتاب قرمز ارزیابی گردند که البته هیچکدام از آنها به موفقیت تجاری نرسیدند.

امنیت اطلاعات

به نظر شما تاریخچه ای که تا اینجا از امنیت ارائه شد ما را به چه چیز راهنمایی می کند ؟ از این تاریخچه معلوم می شود هیچ یک از انواع امنیتی که به آن اشاره شد به تنهایی قادر نیستند مشکلات امنیتی ما را حل نماید. امنیت فیزیکی خوب زمانی نیاز است که بخواهیم سرمایه ای مانند کاغذ یا یک سیستم ثبت اطلاعات را محافظت کنیم. امنیت مخابراتی برای محافظت اطلاعات به هنگام ارسال آنها مفید است . امنیت تشعشع زمانی مفید است که دشمن بتواند با استفاده از منابع کافی که در اختیار دارد تشعشعات الکتریکی حاصل از سیستم کامپیوتری را بخواند . امنیت کامپیوتری برای کنترل دسترسی دیگران به سیستم های کامپیوتری نیاز است و بلاخره امنیت شبکه برای امنیت شبکه محلی نیاز است .

جمع بندی تمام مفاهیم فوق و استفاده از تمام آنها در کنار هم، امنیت اطلاعات را تحقق می بخشد.

هر آنچه ما انجام می دهیم نمی تواند نوعی پروسه اعتبار بخشی به سیستم های کامپیوتری باشد. تکنولوژی به سرعت در حال پیشرفت است و بسیاری ا ز این پروسه ها را پشت سر می گذارند. اخیراً آزمایشگاه بیمه گر امنیتی پیشنهاد شده است . در این آزمایشگاه میزان امنیت انواع محصولات موجود مورد ارزیابی قرار گرفته و تصدیق می‌شود . اگر محصولی نتواند گواهی لازم را کسب کند در آن صورت کاربر، تولید کننده آن محصول را بی دقت خواهد دید چون ممکن است سایت یا اطلاعات کاربر در معرض تهاجم قرار گیرد . متأسفانه این ایده دو مشکل دارد:

- تکنولوژی با سرعت رو به جلو در حرکت است و در نتیجه دلیل چندانی وجود ندارد چنین آزمایشگاهی شانس بهتری برای گواهی کردن محصولات داشته باشد. چون ممکن است قبل از تصدیق یک محصول نسخه جدیدتر آن وارد بازار گردد.
- ثابت کردن این مسئله که برخی چیزها امن و مطمئن هستند، اگر غیر ممکن نباشد بسیار سخت است . شما به سادگی تحت تاثیر گواهی چنین آزمایشگاهی به یک حصول اعتماد می کنید و آنرا غیر قابل نفوذ خواهید پنداشت در حالیکه یک پیشرفت جدید و یک توسعه جدیدتر می تواند تمامی گواهی های امروز را بی اعتبار کند.

در حالیکه صنایع در حال جستجو برای یک جواب نهایی هستند ، ما سعی می کنیم تا امنیت را به بهترین حالتی که بتوانیم پیاده کنیم . این کار از طریق ممارست و پشتکار دائم حاصل می شود.

امنیت یک پروسه است ، نه یک محصول خاص

برای محافظت از اطلاعات سازمان نمی توان به نوع خاصی از امنیت اکتفا کرد. به همین طریق نمی توان به یک محصول اعتماد کرد و انتظار داشت که تمام احتیاجات امنیتی برای کامپیوترها و سیستم های شبکه ای را فراهم کند . متأسفانه برخی از فروشندگان محصولات امنیتی برای کسب

درآمد و جلب مشتری ادعا می کنند که محصول کاملی را ارائه کرده اند، اما حقیقت امر آن است که هیچ محصولی نمی تواند به تنهایی امنیت سازمان را تأمین نماید. برای آنکه از سرمایه های اطلاعاتی سازمان بطور کامل محافظت شود به تعداد زیادی از این محصولات و انواع گوناگونی از آن نیاز می باشد. در چند پاراگراف بعد خواهیم دید چرا چند محصول برجسته و معروف امنیتی نمی توانند به تنهایی راه حل نهایی و کاملی باشند.

نرم افزار ضد ویروس

نرم افزار ضد ویروس بخش لازمی از یک برنامه خوب امنیتی می باشد. با نصب و تنظیم درست نرم افزار ضد ویروس می توان حملات وارده به سازمان را کاهش داد. اما برنامه های ضد ویروس فقط قادرند با برنامه های نرم افزاری بدخواهانه مقابله کنند (هر چند با همه آنها هم نمی توانند).

چنین برنامه ای قادر نیست در برابر مزاحمی که قصد سوء استفاده از برنامه های مجاز یک سازمان را دارد از یک سازمان محافظت کند. علاوه بر این نرم افزار ضد ویروس نمی تواند سازمان را در برابر کسی که قصد دارد به فایل های آن سازمان دسترسی پیدا کند (در حالیکه چنین اجازه ای ندارد) محافظت نماید.

کنترل دسترسی

هر سیستم متعلق به سازمان باید قادر باشد دسترسی به فایل ها را بر اساس نوع ID که به کاربر داده شده است محدود نماید چنانچه این سیستم بطور صحیح پیکر بندی شود قادر خواهد بود تا دسترسی کاربران مجاز را محدود نماید و بدین ترتیب روی دسترسی کاربران کنترل داشته باشد . با استفاده از کنترل دسترسی ، کسی که ا ز یک سیستم آسیب پذیر قصد دسترسی به فایل های سیستم را دارد

نمی تواند مدیر سیستم آن فایل ها را مشاهده کند. حتی سیستم کنترل دسترسی که اجازه پیکره بندی کنترل دسترسی روی سیستم را صادر می کند نمی تواند این فایل ها را مشاهده کند. بنابراین در چنین سیستمی ، مهاجم سعی میکند تا به عنوان یک کاربر مجاز از نوع مدیر به سیستم نگاه کند تا مجوز دسترسی به فایل را بدست آورد .

دیوار آتش، Firewall

دیوار آتش نوعی ابزار کنترل دسترسی به شبکه است، بطوریکه می تواند شبکه داخلی سازمان را در برابر حملات خارجی محافظت کند. با توجه به ماهیت دیوار آتش، این ابزار از نوع تولیدات امنیت حاشیه ای می باشد، معنای این جمله آن است که بین شبکه داخلی و شبکه خارجی حاشیه اطمینان قرار داده می شود. با پیکر بندی صحیح ، دیوار آتش توانسته است به یکی از ابزارهای لازم امنیتی تبدیل شود. اما دیوار آتش نمی تواند در برابر مهاجمی که دارای مجوز اتصال به شبکه است محافظتی به عمل آورد. برای مثال چنانچه یک سرور وب مجاز به برقراری تماس از خارج شبکه باشد و چنانچه آن سرور در برابر حمله نرم افزاری دیگری آسیب پذیر باشد، در آن صورت دیوار آتش به این نرم افزار مهاجم اجازه کار خواهد داد. علاوه بر این دیوار آتش نمی تواند در برابر کاربر داخلی سازمان محافظتی به عمل آورد، چون این کاربر از قبل در داخل شبکه قرار داشته است.

کارت های هوشمند

به رسمیت شناختن یک نفر را می توان با ترکیبی ا ز آنچه آن شخص می داند، آن چیزی که آن شخص دارد یا بر پایه آنچه که هست انجام داد. یکی از روش های اعتبار سنجی افراد که سابقه زیادی هم دارد استفاده از کلمه عبور یا Password است تا با استفاده از آن هویت افراد برای کامپیوتر تعیین گردد. این نوع اعتبار سنجی بر پایه آن چیزی که شخص می داند انجام می گیرد . اما با گذشت زمان معلوم گردید اعتبار سنجی بر پایه آنچه یک شخص

می داند روش چندان مطمئنی نیست چون ممکن است کلمه عبور توسط افراد دیگر کشف گردد یا هنگام تایپ لو برود. برای مقابله با این مشکل، امنیت به سمت روش های دیگر اعتبار سنجی حرکت کرد بطوریکه این کار بر پایه آنچه یک شخص دارد و آنطوری که آن شخص هست انجام می شود.

از کارت های هوشمند می توان برای اعتبار سنجی استفاده کرد (اعتبار سنجی بر پایه چیزی که شخص دارد) و خطر لو رفتن کلمه عبور را کاهش داد. اما اگر آن کارت به سرقت رود یا مفقود گردد یک نفر دیگر می تواند با کتمان هویت اصلی خود و با استفاده از کارت هوشمند ، به عنوان فردی مجاز وارد شبکه گردد. به عبارت دیگر هنگامیکه کاربری از مسیر درست و با استفاده از کارت هوشمند وارد شبکه میشود، سیستم قادر نخواهد بود خود را در برابر حمله او محافظت کند.

بیومتری

بیومتری یکی ا ز روش های اعتبار سنجی است (بر پایه آن چیزی که یک شخص هست) و می تواند خطر لو رفتن کلمه عبور تا حد زیادی کاهش دهد. برای آنکه روش بیومتری بتواند همانند دیگر روش های قدرتمند اعتبار سنجی کار کند باید دسترسی به این سیستم از طریق روش ورود مناسبی انجام گیرد . اگر مهاجم روشی برای پیشدستی کردن بر روش بیومتری پیدا کند، این روش نخواه د توانست امنیت سیستم را تأمین کند.

تشخیص ورود غیر مجاز

سیستم تشخیص ورود غیر مجاز یکی از محصولاتی است که ادعا می کند مشکلات امنیتی را بطور کامل حل می کند. در این سیستم نیازی به محافظت فایل و سیستم نمی باشد بلکه در این سیستم وقتی یکنفر وارد سیستم می شود و قصد دارد کار خطایی را انجام دهد از ادامه کار ا و جلوگیری می شود. در واقع برخی از سیستم های تشخیص ورود غیر مجاز که توانسته اند بازاری بدست آورند دارای این قابلیت هستند که قبل از آنکه مهاجم بتواند کاری انجام دهد او را متوقف می سازند. هیچ یک از سیستمهای تشخیص ورود غیر مجاز کاملاً ایده آل نیستند لذا نمی توان آنرا یک برنامه امنیتی خوب تعریف کرد. علاوه بر این چنین سیستمی قادر به تشخیص کاربران مجازی که احتمالاً دسترسی نادرست به اطلاعات دارند نمی باشد.

مدیریت سیاسی

در یک برنامه خوب امنیتی ، سیاست و رویه ای که در پیش گرفته شده است جزء مهمی می باشد و مدیریت سیستم کامپیوتری اهمیت زیادی دارد. با استفاده از مدیریت سیاسی، سازمان مقتدر خواهد بود خود را از سیستم های دیگر که خط مشی متفاوتی دارند دور نگه دارد. اما توجه کنید که از مدیریت استفاده کرد و هریک از این موارد می تواند باعث نفوذ موفق دشمن گردد. علاوه براین برای کاربرانی که کلمه عبور خود را در اختیار افراد غیر مجاز قرار می دهند یا به طریقی کلمه عبور آنها لو می رود نمی توان از این سیستم استفاده کرد.

جستجوی راه های نفوذ

یکی از بخشهای مهم یک برنامه امنیتی خوب آن است که به دنبال راه های نفوذ در سیستم کامپیوتری خود باشد و آنها را بیابد. به کمک این جستجو سازمان می تواند پتانسیل های موجود برای ورود مزاحمین را پیدا کند البته این

سیستم به تنهایی قادر به حفاظت سیستم کامپیوتری شما نخواهد بود و باید بعد از یافتن را ه های نفوذ آنها را مسدود کرد. یکی از نقائص این روش آن است که کاربران مجازی که دسترسی نادرست به اطلاعات دارند را کشف نمی کند و همچنین مزاحمینی که از قبل وارد سیستم شده اند را نمی تواند پیدا کند.

رمزنگاری

رمزنگاری از جمله اولین مکانیزمهای امنیت مخابراتی می با شد و قطعاً اطلاعات را به هنگام ارسال محافظت می کند برای محافظت اطلاعاتی که به صورت فایل ذخیره می شوند نیز می توان از سیستم رمز نگاری استفاده کرد. البته کاربران مجاز باید قادر به دسترسی به این فایل ها باشند. چنانچه کلید استفاده شده در الگوریتم رمزنگاری در اختیار افراد قرار گیرد، سیستم رمزنگاری نمی تواند تفاوتی میان افراد مجاز و افراد غیر مجاز قائل شود. بنابراین رمزنگاری به تنهایی نمی تواند امنیت لازم را فراهم کند و باید روی کلید رمزنگاری کنترل دقیقی اعمال شود.

مکانیزم های امنیت فیزیکی

امنیت فیزیکی یکی از طبقه بندی های محصولات امنیتی می باشد و می تواند محافظت کاملی برای سیستم های کامپیوتری و اطلاعات فرا هم کند. این سیستم را می توان با هزینه نسبتاً ارزان ایجاد کرد. بدین ترتیب که حفره ای به عمق ده متر ایجاد گردد، تمام سیستم ها و اطلاعات مهم در آن قرار داده شوند و پس از آن روی حفره با بتون پوشانده شود. بدین ترتیب سیستم و اطلاعات در امان خواهد ماند و هیچ کس قادر به دسترسی نخواهد بود. اما این کار راه حل معقولی برای مشکلات امنیتی نمی باشد چون برای آنکه سازمان وظایف خود را انجام دهد لازم است پرسنل آن سازمان به کامپیوترها و اطلاعاتش دسترسی داشته باشند. از طرفی سیستم امنیت فیزیکی که روی مکان قرار گیری اطلاعات اعمال کردیم باعث خواهد شد فقط مقدار کمی از مردم به آن دسترسی داشته باشند و در

نتیجه بحث شبکه کردن سیستم منتفی خواهد شد. علاوه بر این امنیت فیزیکی قادر نخواهد بـود سیسـتم را در برابـر حملات افرادی که به ظاهر دارای مجوز دسترسی می باشند حفظ کند.

فصل دوم

انـــواع حمـــلات

راههای زیادی وجود دارد تا برای اطلاعات و سیستم های کامپیوتری سازمان اتفاقات ناگوار رخ دهد. برخی از این اتفاقات از روی عناد و بدخواهی صورت می گیرند و برخی هم بطور تصادفی حادث می شوند. طرف نظر از نوع اتفاق، آنچه مهم است از بین رفتن اطلاعات و خساراتی است که به سازمان وارد می آید. به همین دلیل تمام این اتفاقات را حمله نامیده و کاری به عمدی یا غیر عمدی بودن آن نداریم. در این راستا حملات را به چهار دسته اساسی تقسیم می کنیم:

- دسترسی (accessattacks)
- دستکاری (modification attacks)
- جلوگیری از سرویس دهی (denial-of-serveice attacks)
- انکار (repudication attacks)

هر یک از موارد فوق در بخش های بعد به تفصیل مورد بررسی قرار خواهد گرفت.

حملات وارده به یک سازمان از طریق ابزارهای تکنیکی (همانند راه های نفوذ سیستم کامپیوتری) یا از طریق مهندسی اجتماعی می باشد. منظور از مهندسی اجتماعی استفاده از ابزارهای غیر تکنیکی برای رسیدن به دسترسی غیر مجاز می باشد. به عنوان مثال فردی را در نظر بگیرید که از طریق خط تلفن یا قدم زدن وارد سازمانی می شود و چنان وانمود می کند که واقعاً عضو آن مجموعه است. حملاتی که از طریق مهندسی اجتماعی صورت می گیرد بسیار مخرب و زیان آور می باشد.

حمله به اطلاعاتی که دارای فرم الکتریکی هستند دارای خاصیت جالبی است و آن اینکه می توان این اطلاعات را کپی کرد در حالیکه ظاهراً چیزی به سرقت نرفته است به عبارت دیگر مهاجم می تواند غیر مجاز به اطلاعات دسترسی پیدا کند در حالیکه مالک اصلی آن اطلاعات چیزی را از دست نداده است. پس از آن مالک اصلی هر

دو طرف خواهند بود. نیم خواهیم بگوییم در این حالت خساراتی وارد نشده است. کشف این حمله بسیار مشکل است چرا که مالک اصلی از اطلاعات بی بهره نشده است تا حمله را تشخیص دهد.

حمله برای دسترسی

منظور از حمله برای دسترسی تلاشی است که مهاجم برا یدست یافتن به اطلاعاتی که نباید مشاهده کند انجام میدهد. این حمله ممکن است به اطلاعات ثابت در یک محل یا اطلاعات در حال انتقال صورت پذیرد. این نوع حمله برای بدست آوردن اطلاعات محرمانه انجام می گیرد. این حمله بصورتهایی که رد ادامه توضیح داده شده است انجام میشود.

جاسوسی

منظور از جاسوسی، جستجو در بین فایل های اطلاعاتی است به امید آنکه مطلب جالب توجهی در بین آنها پیدا شود. اگر اطلاعات بر روی کاغذ ثبت شده باشد، جاسوس مجبور است رد بین تمام پرونده ها و کمدها بایگانی جستجو کند. چنانچه اطلاعات بصورت فایل های کامپیوتری باشد جاسوس مجبور است فایلها را یکی پس از دیگری باز کند تا به اطلاعات مورد نظر دست پیدا کند.

استراق سمع

زمانیکه فردی به یک مکالمه گوش می دهد رد حالیکه جزء افراد مکالمه نیست استراق سمع کرده است . برای آنکه مهاجم بتواند بطور غیر مجاز به اطلاعات دیت یابد خود را در مکانی قرار می دهد که اطلاعات مورد علاقه اش از آن مکان عبور می کند. این مورد بیشتر بصورت الکترونیکی انجام می شود.

حائل شدن

برخلاف استراق سمع حائل شدن حمله ای فعال در مقابل اطلاعات است. زمانیکه مهاجم در برابر اطلاعات حائل می شود، خود را در مسیر عبور اطلاعات قرار داده و قبل از رسیدن اطلاعات به مقصد آنها را بر می دارد. پس از آنکه مهاجم از محتوای اطلاعات آگاه شد و آنها را بررسی نمود، شاید دوباره اجازه دهد اطلاعات مسیر خود را ادامه دهند و شاید هم این کار را نکند.

حمله برای دسترسی چگونه انجام می گیرد؟

حمله جهت دسترسی دارای شکلهای متفاوتی است . شکل حمله بستگی به این دارد که اطلاعات روی کاغذ ثبت شده باشد یا بطور الکترونیکی در سیستم کامپیوتری قرار گرفته باشد. در ادامه در مورد هر یک توضیح داده شده است.

اطلاعات روی کاغذ

چنانچه اطلاعات مورد نظر مهاجم بصورت فیزیکی و بر روی کاغذ قرار داشته باشد، کاغذها و اطلاعات روی آنها را در مکانهایی شبیه موارد زیر پیدا خواهد شد:

- کمدهای بایگانی
- داخل کشوی میز
- ماشین فاکس
- دستگاه چاپگر
- داخل سطل آشغال

برای آنکه مهاجم بتواند مکان های فوق را جستجو کند باید از لحاظ فیزیکی به آنها دسترسی داشته باشد. چنانچه این شخص یکی از پرسنل سازمان باشد احتمالاً به اتاقهای آن سازمان و کمدهای بایگانی دسترسی خواهد داشت البته اگر کشوی میزها قفل نباشد. ماشین فاکس و چاپگر در مکان هایی قرار دارند که بیشتر افراد سازمان بتوانند از آن استفاده کنند و بسیار اتفاق می افتد. اشغال های آن در خارج ساختمان قرار داده می شود تا پس از ساعت اداری تخلیه شوند.

ممکن است برخی اعمال احتیاطی از بین قفل کردن کمدهای بایگانی و کشوی میزها تا حد زیادی از موفقیت مهاجم کم کند، اما او به جستجوی خود در وقت نهار ادامه می دهد تا کمدهای قفل نشده را پیدا کند. علاوه بر این کمدهای بایگانی و کشوی میزها دارای قفل ساده ای هستند که براحتی قابل باز کردن می باشد. برای دستیابی به اطلاعات ثبت شده فیزیکی به دسترسی فیزیکی نیاز است.

استفاده از امنیت خوب در سایت می تواند دسترسی افراد خارجی به اطلاعات فیزیکی را محدود کند اما این روش در برابر پرسنل همان سازمان نمی تواند محافظتی انجام دهد.

اطلاعات الکترونیکی

اطلاعات الکترونیکی در مکان های زیر ذخیره می شوند:

- روی سرور
- داخل کامپیوتر
- روی فلاپی دیسک
- روی CD-ROM
- روی نوارهای بک آپ

دسترسی به برخی از موارد فوق (مانند فلاپی دسک، CD-ROM ، نوارهای بک آپ و کامپیوتر همراه) با سرقت آنها میسر است. ممکن است اینکار نسبت به دسترسی الکترونیکی در یک سازمان آسانتر باشد.

چنانچه فایل های مورد نظر مهاجم در سیستمی باشد که او هم اجازه دسترسی به آنها داشته باشد می تواند فایل ها را باز کند . چنانچه کنترل اجازه دسترسی بدرستی انجام شود، به یک فرد غیر مجاز نباید اجازه دسترسی داده شود. استفاده از سیستم درست اکانت، بسیاری جستجوهای عمدی را ناموفق خواهد کرد. در عوض فرد مهاجم هم سعی می کند اکانت خود را ارتقا دهد بطوریکه بتواند فایل را مشاهده کرده و کنترل دسترسی را کاهش دهد. سیستم هایی که اجازه می دهند این عمل بطور موفقیت آمیز انجام شود، آسیب پذیری سیستم بسیار بالا خواهد بود. با استفاده از استراق سمع، اطلاعات رد حال انتقال قابل دستیابی خواهند بود. در یک شبکه محلی مهاجم با نصب sniffer روی کامپیوتری که به شبکه محلی متصل شده است این کار را انجام می دهد. Sniffer یک کامپیوتر است و بگونه ای پیکربندی شده است که تمام ترافیک روی شبکه را دریافت کند (در حالت عادی کامپیوتری که در شبکه قرار دارد فقط ترافیکی را در یافت می کند که به آدرس خودش ارسال شده باشد.) مهاجم پس از آنکه بتواند امتیاز خود را ارتقا دهد و سیستمش را به شبکه متصل کند، sniffer را نصب خواهد کرد.

اگر چه sniffer بگونه ای قابل پیکر بندی است که بتواند تمام ترافیک شبکه را دریافت کند اما اکثر آنها فقط شناسه کاربر و کلمه عبور را از شبکه می گیرند.

در شبکه های گسترده یا WAN هم استراق سمع قابل انجام است اما این استراق سمع نیاز به تجهیزات گسترده و دانش قوی تری دارد. بهترین محل برای استراق سمع در WAN، جعبه های سیم بندی است. حتی از خطوط فیبرنوری هم استراق سمع انجام پذیر است. برای نمونه برداری از اطلاعات موجود روی خطوط فیبرنوری امکانات بسیار خاصی نیاز است و مهاجم های عادی معمولاً چنین امکاناتی در اختیار ندارند.

استفاده از روش حائل شدن برای دسترسی به اطلاعات، یکی از انتخاب های مشکل برای مهاجم است چون برای رسیدن به موفقیت مجبور است خود را بین مسیر ارتباطی گیرنده و فرستنده اطلاعات قرار دهد. برای انجام این عمل

در اینترنت، مهاجم نام خود را عوض می کند و بدین ترتیب نام کامپیوتر به یک آدرس نادرست تخصیص داده می شود. پس از آن ترافیک ارسالی بجای آنکه به سوی مقصد برود برای مهاجم ارسال می شود اگر مهاجم بتواند سیستم خود را بدرستی پیکربندی کند، کامپیوتر ارسال کننده اطلاعات به هیچ وجه نخواهد فهمید که با مقصد غیر واقعی در حال صحبت است.

علاوه بر این ممکن است مهاجم عمل حائل شدن را روی پروسه ای که از قبل در حال انجام است، پیاده کند. استفاده از این روش برای ترافیک های دو طرفه (با تعاملی) مانند telnet بهترین نوع حمله می باشد. در اینگونه موارد مهاجم در همان بخشی از شبکه قرار می گیرد که به عنوان سرور (سرویس دهنده) یا کلانیت (سرویس گیرنده) شناخته می شود. در این حالت مهاجl به کاربر مجاز فرصت می دهد کار خود را با سرور آغاز کند و پس از آن از نرم افزار خاصی استفاده می کند و از آن پس از ارتباط ایجاد شده استفاده کند. این نوع حمله باعث می شود تا امتیاز و مجوز مهاجم همانند مجوز کاربر باشد.

حمله برای دستکاری اطلاعات

در این نوع حمله، مهاجم سعی می کند اطلاعاتی را تغییر دهد که مجاز به تغییر آنها نیست. این حمله ممکن است در هر جایی که اطلاعات ثبت شده است انجام پذیرد و یا اینکه روی اطلاعات در حال انتقال انجام شود. این نوع حمله باعث می شود صحت و تمامیت اطلاعات از بین برود. انواع دستکاری هایی که روی اطلاعات انجام می شود به ترتیب زیر است:

تعویض اطلاعات

از جمله روشهای دستکاری اطلاعات، تعویض اطلاعات موجود است، همانند مهاجمی که حقوق و دستمزد پرسنل اداره را عوض کند. این اطلاعات از قبل در آن سازمان موجود بود، اما پس از حمله نادرست خواهد بود. این نوع حمله معمولاً روی اطلاعات حساس و اطلاعات عمومی انجام می شود.

داخل کردن اطلاعات

نوعی دیگری از حمله برای دستکاری، داخل کردن اطلاعات می باشد. با انجام چنین حمله ای، اطلاعاتی که از قبل در سازمان وجود نداشته است به آن اضافه می شود. این نوع حمله روی اطلاعات تاریخی و یا سوابق یا اطلاعاتی که قرار است بر مبنای آنها کاری انجام گیرد اعمال می شود. برای مثال مهاجمی را در نظر بگیرید که معامله ای صوری را به اطلاعات یک بانک اضافه می کند و بدین ترتیب از حساب یک مشتری به حساب خودش پول واریز می کند.

حذف اطلاعات

این نوع حمله برای پاک کردن اطلاعات موجود بکار می رود و مانند بخش قبل روی اطلاعات تاریخی، سوابق یا اطلاعاتی که قرار است بر مبنای آنها کاری انجام گیرد اعمال می شود. برای مثال مهاجمی را در نظر بگیرید که معامله انجام شده ای را از سیستم بانک پاک می کند و بدین ترتیب پول در حساب خودش باقی خواهد ماند.

حمله برای تغیر اطلاعات چگونه انجام می گیرد؟

براساس نوع دسترسی که مهاجم در اختیار دارد، این نوع حمله علیه اطلاعات روی کاغذ یا اطلاعات به فرم الکترونیکی انجام میگیرد که در ادامه هر یک را شرح می دهیم:

اطلاعات روی کاغذ

تغیر اطلاعات ثبت شده روی کاغذ طوریکه قابل کشف نباشد کار مشکلی است. برای امضای مجدد سندهایی که دارای امضاء هستند (مانند سندهای قرارداد) نیاز به دقت و مهارت فوق العاده ای است. برای تغییر محتوای سند طولانی که از تعداد زیادی صفحات کاغذی تشکیل شده است باید آن سند مجدداً گردآوری و تنظیم گردد.

افزودن اطلاعات یا حذف اطلاعات از یک سند دست نوشته کار بسیار سختی است چرا که به لحاظ ترتیب و توالی مطالب سند، هر گوه تغییر به زودی کشف خواهد شد. به همین دلیل برای تغییر اطلاعات سندهای دست نوشته بهترین کار جایگزین کردن کل سند با سند دیگر می باشد. البته واضح است این نوع حمله نیاز به دسترسی فیزیکی به آن سند دارد.

اطلاعات الکترونیک

انجام تغییر روی اطلاعاتی که دارای فرم الکترونیکی هستند به مراتب ساده تر از اطلاعاتی است که روی کاغذ ثبت شده است. فرض کنید مهاجم به فایلی دسترسی داشته باشد، در این صورت انجام تغییرات نیاز به مهارت کمی دارد. چنانچه مجاز به دسترسی به آن فایل نباشد سعی می کند در ابتدا میزان دسترسی خود را به سیستم افزایش دهد یا نیاز به مجوز برای باز کردن فایل را از بین ببرد. بدین ترتیب مهاجم اول میزان آسیب پذیری سیستم را بررسی می کند و پس از افزایش سطح دسترسی خود، فایل را تغیر می دهد.

برای تعویض فایل های بانک اطلاعاتی و یا معاملات تجاری دقت زیادی لازم است. در برخی موارد معاملات به ترتیب شماره خورده اند و اضافه یا حذف کردن یک فایل بدون داشتن شماره ترتیب صحیح باعث می شود تا سیستم خطایی اعلام کند. در چنین حالتی مهاجم مجبور است تغییرات کلی تری در سیستم اعمال کند تا خود را در برابر کشف تغییرات محافظت کند. ایجاد تغییر روی اطلاعاتی که در حال انتقال است کار سختی است. در این موارد بهترین راه آن است که ابتدا یک حمله از نوع حائل شدن به سیستم انجام گیرد. سپس قبل از آنکه اطلاعات به طرف مقصد اصلی ارسال شود اطلاعات تغیر داده شود.

Dos : حمله جلوگیری از سرویس دهی

حمله برای جلوگیری از سرویس دهی باعث می شود کاربر مجاز نتواند از منابع موجود در سیستم، اطلاعات یا قابلیت های آن سیستم استفاده کند. اگر چه در این حمله که به اختصار Dos گفته می شود، به مهاجم اجازه دسترسی و تغییر اطلاعات داده نمی شود، اما وی از سرویس دهی به دیگر کاربران مجاز جلوگیری می کند. انگیزه حمله Dos چیزی جز خرابکاری نیست و انواع آن بصورت زیر می باشد:

جلوگیری از دسترسی به اطلاعات

چنانچه حمله Dos روی اطلاعات سیستم انجام شود اطلاعات سیستم غیرقابل دسترسی می گردد. این نوع حمله بوسیله نابود کردن اطلاعات یا تغییر اطلاعات بفرمی که غیر قابل استفاده گردد، انجام می گرد. روش دیگر این حمله آن است که اطلاعات همچنان بدون تغییر می ماند اما در مکانی غیر قابل دسترسی قرار داده می شود.

جلوگیری از سرویس دهی به کاربردهای نرم افزاری

نوع دیگر حمله Dos آن است که کاربردهای نرم افزاری که اطلاعات را نمایش می دهند یا آنها را تغییر می دهند، هدف حمله قرار می گیرد. این حمله معمولاً به سیستم کامپیوتری انجام می گیرد که آن کاربرد را اجرا می کند. چنانچه این کاربرد غیر قابل استفاده گردد، سازمان مذکور قادر به انجام وظایف خود از طریق آن کاربرد نخواهد بود.

جلوگیری از دسترس به سیستم

یکی از انواع حمله Dos آن است که سیستم کامپیوتری از کار انداخته شود. این نوع حمله باعث خواهد شد سیستم بهمراه تمام نرم افزارهای کاربردی که روی آن اجرا می شود و اطلاعاتی که روی آن قرار داده شده است غیر قابل استفاده گردد.

جلوگیری از دسترسی به ارتباطات

حملات Dos بر روی ارتباطات سالهاست که انجام می شود. این نوع حمله می تواند به روش های مختلف انجام شود: از قطع کردن سیم و مختل نمودن ارتباط رادیویی گرفته تا از کار انداختن یک شبکه با افزایش ترافیک شبکه. در این نوع حمله هدف اصلی همان واسطه ارتباطی است. در این حالت سیستم و اطلاعات موجود در آن آسیبی نمی بیند اما مختل شدن ارتباط، دسترسی به سیستم و اطلاعات آنرا غیر ممکن می سازد.

حملات Dos چگونه انجام می شود؟

اساساً حملات Dos، حمله ای به سیستم کامپیوتری و شبکه می باشد. در اینجا نمی خواهیم بگوییم که حملات Dos بر ضد اطلاعات روی کاغذ انجام نمی گیرد، اما انجام این نوع حملات به جهان الکترونیک بسیار آسانتر است. در ادامه به بررسی هر یک از این موارد می پردازیم:

اطلاعات روی کاغذ

یکی از موارد مورد توجه در حمله فیزیکی Dos، اطلاعاتی می باشد که بصورت فیزیکی روی کاغذ ثبت شده است. برای آنکه اطلاعات غیر قابل استفاده گردند باید آنها را سرقت کرد یا در محل نابود نمود. به عنوان مثال مهاجم می تواند کاغذها را ریز ریز کند . حال اگر از این اسناد کپی وجود نداشته باشد اطلاعات نابود شده است. به عنوان مثالی دیگر، مهاجم می تواند ساختمانی که اسناد کاغذی را در آن قرار دارد را به آتش بکشد. بدین ترتیب اطلاعات از بین می رود و از دسترسی سازمان به این اطلاعات جلوگیری می شود. اینکار می تواند بطور غیر مستقیم هم انجام می شود بدین ترتیب که مهاجم با دستکاری در سیم کشی ساختمان، زمینه آتش سوزی را فراهم کند یا اسناد را بصورت نادرست در اختیار پرسنل سازمان قرار دهد و آنها هم ناخواسته اسناد را از بین ببرند.

اطلاعات الکترونیکی

روش های متفاوتی وجود دارد که اطلاعات به فرم الکترونیکی در معرض حمله Dos قرار گیرند.

این نوع اطلاعات قابل حذف کردن نمی باشد و بدین وسیله از دسترسی به آنها جلوگیری می شود. برای موفق بودن این حمله لازم است تمام پشتیبان های تهیه شده از اطلاعات حذف گردد. با ایجاد تغییر در یک فایل هم می توان اطلاعات آنرا غیرقابل استفاده نمود. برا مثال مهاجم می تواند ابتدا فایلی را رمزنگاری کند و پس از آن کلید

رمزنگاری را خراب کند. بدین ترتیب هیچ کس قادر نخواهد بود از آن فایل استفاده کند (مگر اینکه یک فایل پشتیبان از آن قبلاً تهیه شده باشد).

اطلاعات الکترونیکی هم مستعد حملات فیزیکی می باشند به عنوان مثال یک سیستم کامپیوتری بهمراه اطلاعاتش قابل سرقت است. حملات Dos کوتاه مدت را می توان با خاموش کردن کامپیوتر انجام داد. علاوه بر این خاموش کردن کامپیوتر باعث می شود از سرویس دهی به خود سیستم کامپیوتر هم جلوگیری شود (Dos نسبت به خود سیستم) . بوسیله حمله ای که مستقیماً به سیستم انجام می شود، می توان سیستم کامپیوتری را فلج کرد. چندین مهاجم از این دست موجود است (که به آسیب پذیری سیستم عمل کامپیوتر و پروتکل های بکار رفته در آن بستگی دارد)

برنامه های کاربردی با چند آسیب پذیری معروف غیرقابل استفاده می شوند. این نوع آسیب پذیری به مهاجم اجازه می دهد مجموعه ای از دستورات از پیش تعریف شده را به برنامه کاربردی ارسال کند. این دستورات به آن کاربرد می گویند که پردازش به درستی انجام نمی شود. در نتیجه برنامه کاربردی از کار می افتد. چنانچه نرم افزار کاربردی مجدداً راه اندازی گردد سرویس های آن مجدداً فعال می شود اما تا راه اندازی مجدد غیر قابل استفاده می ماند.

شاید آسانترین راه برای مختل کردن ارتباط مخابراتی بریدن سیم باشد ولی این کار نیاز به دسترسی فیزیکی به کابل های شبکه دارد و در برخی موارد به ابزار خاصی نیاز دارد. روش دیگر Dos بر ضد ارتباطات آن است که مقدار بسیار زیاد و حجم عظیمی از ترافیک دیتا به یک سایت ارسال شود. این حجم ترافیک باعث خواهد شد واسطه های ارتباطی در حجم بالایی از تبادل اطلاعات فرو رود، در نتیجه سرویس لازم به کاربران مجاز ارائه نخواهد شد. همه حمله های Dos که بر ضد اطلاعات الکترونیکی انجام می شود عمدی نمی باشد، بلکه بطور غیر عمدی اتفاق می افتد. برای مثال امکان دارد کارگری که در حال کندن زمین است بطور تصادفی کابل های مخابراتی و فیبر نوری را قطع کند. از این قبلی حوادث برای کاربران تلفن و اینترنت زیاد اتفاق می افتد. حتی بچه های هم می

توانند باعث حمله Dos گردند. بچه هایی که از مرکز دیتا بازدید می کنند با تعداد زیادی چراغ های نمایشگر و کلیدهای برق برخورد می کنند که اکثر آنها برای بچه های وسوسه انگیز است. اینکه فرضاً با خاموش کردن یک کلید چه اتفاقی می افتد، می تواند باعث از کار افتادن کل سیستم شود.

حمله تکذیبی و انکار

این حمله باعث می شود تا اطلاعات بصورت نادرست داده شود یا اینکه وقوع یک واقعه حقیقی یا معامله ای که صورت رفته است انکار می شود. انواع حمله به صورت زیر است:

ماسک زدن

در این روش مهاجم سعی می کند تا هویت شخص یا سیستم دیگری را جعل کند. این نوع حمله در ارتباطات بین دو سیستم قابل انجام است.

تکذیب یک واقعه

تکذیب یک واقعه یعنی انکار انجام فعالیتی که ثبت شده است. فرض کنید فردی با استفاده از کارت اعتباری از فروشگاه خرید می کند، اما زمانیکه شرکت صادر کننده کارت اعتباری صورتحساب خرید را برایش ارسال می کند، شدیداً منکر خرید از چنین فروشگاهی می شود.

حمله تکذیبی چگونه انجام می شود

این حمله برضد اطلاعاتی با فرم فیزیکی و یا الکترونیکی انجام می شود. میزان مشکل بودن این نوع حمله به اقدامات احتیاطی که سازمان انجام داده است بستگی دارد. در ادامه به بررسی هر یک از این موارد می پردازیم:

اطلاعات روی کاغذ

یک فرد حقیقی میتواند با استفاده ماسک زدن، از نام شخص دیگری در یک سند استفاده کند. چنانچه سند به امضا نیاز داشته باشد، مهاجم آنرا هم جعل می کند. زمانیکه مهاجم با یک سند تایپ شده رو برو است کارش به مراتب راحت تر از مانی است که بخواهد سند دست نویسی را جعل کند.

به طریق دیگر یک شخص می تواند واقعه یا انجام معامله ای را تکذیب کند و ادعا کند که وی در انجام آن نقشی نداشته است. در اینجا هم اگر امضای وی روی یک پیمان نامه یا رسید کارت اعتباری وجود داشته باشد آن شخص باید ثابت کند که امضاء به وی تعلق ندارد. البته شخصی که قصد دارد چنین حمله ای را ترتیب دهد، از همان ابتدا از امضایی شبیه به امضای خود ولی بطور اشتباه استفاده خواهد کرد.

اطلاعات الکترونیکی

اطلاعاتی که دارای فرم الکترونیکی هستند نسبت به اطلاعات به فرم فیزیکی از آسیب پذیری بیشتری در برابر حملات تکذیبی برخوردار هستند. یک سند الکترونیکی به راحتی قابل ایجاد و ارسال است چون نیاز چندانی به تعیین هویت فرد ارسال کننده ندارد. برای مثال در یک پیام پست الکترونیک، بخش آدرس ارسال کننده پیام (آدرسی که جلوی عبارت "FROM" وجود دارد قابل تعویض توسط فرد مهاجم است. اکثر افراد هنگام خواندن

پیام های پست الکترونیکی که برایشان ارسال شده است تلاش چندانی برای تعیین هویت واقعی ارسال کننده انجام نمی دهند.

این مطلب درباره اطلاعاتی که از یک سیستم کامپیوتری ارسال می شود هم صادق است صرف نظر از موارد استثنایی، هر سیستم کامپیوتری می تواند IP Address خود را به هر شماره ای که می خواهد تغییر دهد. بدین ترتیب یک کامپیوتر می تواند برای سیستم کامپیوتر دیگر ماسک بزند و هویت اصلی خود را پنهان کند.

توجه: این کار ساده است. یک سیستم می تواند IP Address سیستم دیگری را برای خود قرار دهد (البته به شرطی که هر دو در یک شبکه قرار نداشته باشند) و بدین ترتیب خود را به جای او جا بزند. انجام اینکار روی انترنت کار آسانی نیست و ممکن است تماس درست را نتیجه ندهد.

تکذیب یک واقعه در مورد اطلاعات به فرم الکترونیکی نسبت به اطلاعات فیزیکی بسیار راحت تر است. در اکثر موارد سندها از نوع دست نویس نیستند و رسید مربوط به کارتهای اعتباری دارای امضاء مشتری نمی باشد. به استثناء مواردی که از امضای دیجیتالی استفاده می شود، نمی توان ثابت کرد این سند توسط شخص مقابل مورد پذیرش قرار گرفته است. حتی در مواردی که امضای دیجیتالی استفاده شده است، فرد می تواند ادعا کند که امضای وی به طریقی به سرقت رفته است و یا کلمه عبور محافظ کلید، لو رفته است. از آنجا که اثبات این موارد سخت است، تکذیب روش بسیار آسانتری است (ضرب المثل معروف ایرانی مگوید دیوار حاشا بلند است).

تکذیب معاملاتی که توسط کارت اعتباری انجام می شود کار ساده ای در جهان الکترونیک است. روی رسید کارت اعتباری امضای وجود ندارد که با امضای صاحب کارت تطبیق داده شود. تنها دلیلی که برای اثبات وجود دارد ارسال اجناس معامله شده به آدرس صاحب کارت می باشد، حال اگر این اجناس به جای دگر فرستاده شود چه کار می توان کرد؟ و بالاخره چه دلیلی وجود دارد که خریدار همان صاحب کارت باشد؟

فصل سوم

سرویسهای امنیت اطلاعات

سرویسهای امنیت اطلاعات، سرویسهایی در سطح پایه می باشد که برای خنثی کردن حملات شرح داده شده در فصل ۲ بکار می رود. این سرویسها عبارتند از:

- محرمانه سازی
- تمامیت اطلاعات (یا امانت داری)
- فراهمی (یا در دسترس بودن)
- مجوز سنجی

هر سرویس برای مقابله با نوع خاصی از حملات شرح داده شده بکار می رود (جدول ۱-۳ را ببینید). توجه شود سرویسهای تعریف شده در اینجا با مکانیزم های امنیتی اشتباه نشود، چون مکانیزم های امنیتی حاصل پیاده سازی این سرویسها می باشد. نوع کار بردن سرویسهای امنیتی بستگی به مقدار خطر پذیری و طرح امنیتی سازمان دارد. برای درک احتیاجات اصلی امنیت سازمان، باید دید چگونه با استفاده از سرویسهای امنیتی می توان با نوع خاصی از حمله مقابله گردد.

محرمانه سازی

سرویس محرمانه سازی برای تأمین امنیت اطلاعات بکار می رود و اگر بدرستی از آن استفاده شود فقط کاربران مجاز اجازه دسترسی به اطلاعات دارند. برای اینکه این سرویس کار خود را به درستی انجام دهد، باید بهمراه مجوز سنجی کار کند تا بتواند هویت افراد را بطور صحیح تشخیص دهد. سرویس محرمانه سازی را می توان در مورد اطلاعات به فرم فیزیکی مانند فایل های کاغذی، در مورد اطلاعات به فرم الکترونیکی مانند فایل های کامپیوتری و در محل های عبور اطلاعات اعمال کرد.

محرمانه سازی فایل

راه های مختلفی برای محرمانه سازی فایل وجود دارد که به چگونگی وجود فایل بستگی دارد. در مورد فایل های کاغذی لازم است فایل های کاغذ بطور فیزیکی محافظت گردند. اصولاً فایل فیزیکی در مکان خاصی قرار داده می شود بنابراین لازم است دسترسی به آن محل کنترل گرد، بدین ترتیب که کمدهای فایل و کشوی میزها قفل گردد، اتاقهای آن سایت در برابر دسترسی افراد محدود گردد یا اینکه روی کل سایت محدودیت اعمال گردد.

نوع حمله سرویس امنیتی	محرمانه سازی	تمامیت	فراهمی	مجوزسنجی
دسترسی	×			×
دستکاری	×		×	
جلوگیری از سرویس دهی		×		
تکذیب	×		×	

جدول ۱-۳ سرویسهای امنیت اطلاعات در برابر حملات

برای فایل هایی که به فرم الکترونیکی هستند کاراکترهای مختلف وجود دارد. اول اینکه این فایل باید در چند مکان قرار داشته باشد. (نوارهای پشتیبان، چند کامپیوتر مختلف، فلاپی دیسک، CD و از این قبیل) دوم اینکه دسترسی فیزیکی به محل فایل امکانپذیر نباشد. نحوه محرمانه سازی نوارهای پشتیبان و دیسک کامپیوتری همانند امنیت فیزیکی فایل های کاغذی می باشد. نحوه محرمانه سازی نوارهای پشتیبان و دیسک دسترسی فیزیکی پیدا کند لازم است دسترسی فیزیکی تحت کنترل قرار گیرد. (که البته ممکن است شامل رمزنگاری فایل هم باشد لازمه کنترل دسترسی به کامپیوتر آن است که تعیین هویت و اعتبار سنجی بدرستی انجام گیرد (که یک سرویس مجوز

سنجی می باشد) و پیکربندی سیستم بگونه ای باشد که کاربر غیر معتبر نتواند با عبور از بخشهای تعیین هویت و اعتبار سنجی خود را به کاربری معتبر تبدیل کند. (همانند عبور از نقاط آسیب پذیر سیستم) در جدول ۲-۳ مکانیزم های و نیازهای مربوط به محرمانه سازی فایل آورده شده است.

مکانیزم های محرمانه سازی	کنترل امنیت فیزیک کنترل دسترسی به فایل های کامپیوتر رمز نمودن فایل
نیازهای محرمانه سازی	تعیین هویت و اعتبار سنجی پیکر بندی درست کامپیوتر مدیریت صحیح در صورت استفاده از رمزنگاری
جدول ۲-۳ مکانیزم های و نیازهای سرویس محرمانه سازی	

محرمانه سازی اطلاعات بهنگام ارسال و مخابره

فقط اطلاعات موجود در فایلهای ذخیره شده نیستند که به محافظت صحیح نیاز دارند چون هنگام ارسال نیز امکان حمله به آنها وجود دارد. از اینرو محرمانه سازی اطلاعات، به هنگام ارسال نیاز می باشد. اینکار از طریق رمزنگاری انجام می شود.

محافظت اطلاعات را می توان فقط روی پیام اصلی انجام داد و ای اینکه تمام ترافیک موجود در لینک را رمزنگاری کرد. رمزنگاری می تواند به تنهایی اطلاعات را در برابر استراق سمع محافظت کند اما نمی تواند

محافظت کاملی در برابر حائل شدن انجام دهد. برای آنکه در برابر حائل شدن هم محافظت انجام شود لازم است از تعیین هویت و اعتبار سنجی بصورت درست استفاده گردد تا هویت نقطه دوردست تعیین گردد.

محرمانه سازی جریان ترافیک

برخلاف دیگر سرویسهای محرمانه سازی، سرویس محرمانه سازی جریان ترافیک به اصل اطلاعات ذخیره شده و یا ارسال شده ربطی ندارد بلکه به نوع و شکل مبادله اطلاعات بن دو نقطه مربوط می شود. با استفاده از این نوع اطلاعات (توسط تحلیل گر ترافیک) می توان سازمانی که در حال ارتباط است را شناسایی کرد. مقدار اطلاعاتی که بین دو نقطه پیتزاهایی که به کاخ سفید و پنتاگون تحویل داده می شود را تحت نظر دارند. ایده آنها این است که افزایش تعداد پیزاهای تحویلی نشانگر افزایش پرسنل حاضر و در نتیجه نشانگر بروز بحران است.

یکی از روش های محرمانه سازی جریان ترافیک آن است که مقدار ترافیک روان بین دو نقطه افزایش داده شود تا مقدار اصلی ترافیک معلوم نباشد. در ارتش دو سایت با هم ارتباط مخابراتی برقرار می کنند و صرف نظر از تعداد واقعی پیام هایی که ارسال می شود، جریان ترافیک ثابتی را ارسال می کنند. مقدار این جریان از مقدار واقعی بیشتر است بطوریکه بقیه جریان ترافیک با اطلاعات بی اهمیت پر می شود. بدین ترتیب میزان ترافیک ثابت میماند و در نتیجه کسی نمی تواند تغییر تعداد پیام های ارسالی را تشخیص دهد.

حملات قابل پیشگیری توسط محرمانه سازی

با استفاده از محرمانه سازی می توان حمله دسترسی را خنثی نمود، اما محرمانه سازی به خودی خود قادر به حل کامل مشکلات نمی باشد. لازم است سرویس محرمانه سازی بهمراه سرویس مجوز سنجی کار کند تا هویت فردی که سعی دارد به اطلاعات دسترسی پیدا کند شناسایی شود. ترکیب سرویسهای محرمانه سازی و مجوز سنجی می تواند خطر دسترسی غیرمجاز را کاهش دهد.

تمامیت

سرویس تمامیت برای صحت و کامل بودن اطلاعات ایجاد شده است. چنانچه سرویس تمامیت بدرستی استفاده شود، کاربر می تواند از صحت اطلاعات اطمینان حاصل کند و مطمئن باشد توسط فرد غیر مجاز دستکاری نشده است. این سرویس هم مانند محرمانه سازی باید با سرویس مجوز سمجی کار کند تا هویت افراد بدرستی تعیین شود. سرویس تمامیت، محافظتی در برابر حملات دستکاری می باشد و اطلاعاتی که به این طریق محافظت می شود دارای فرم فیزیکی و الکترونیکی است یا در حال انتقال می باشد.

تمامیت فایل ها

اطلاعات ممکن است روی کاغذ یا داخل فایل های الکترونیک قرار داشته باشد. استفاده از سرویس تمامیت برای حفاظت فایل های کاغذی راحت تر از فایل های الکترونیک است چون تشخیص ایجاد تغییر در فایل کاغذی آسان است. ایجاد تغییر در فایل کاغذی بگونه‌ایکه هنگام بازرسی مجدد تغییرات آن کشف نگردد به مقداری مهارت نیاز دارد، در صورتیکه هر کس به یک فایل الکترونیکی دسترسی داشتهباشد می تواند آن را دستکاری کند.

راههای متفاوتی وجود دارد تا فایل های کاغذی در برابر دستکاری و تغییر محافظت گردند که از آن جمله می توان به استفاده از صفحات امضا شده، پاراف کردن هر صفحه با مشخصات فردی و سازمانی و شماره صفحه، صحافی کردن صفحات بصورت کتاب و توزیع چند کپی از فایل در مکانهای مختلف اشاره کرد. استفاده از این مکانیزم باعث می شود دستکاری اطلاعات یک فایل بدون آنکه این تغیر قابل کشف باشد کار بسیار مشکلی باشند. اگر چه افراد جعل کننده قادر به کپی امضاء می باشد اما این کار به مهارت زیادی نیاز دارد. پاراف کردن هر صفحه باعث می شود جابجا نمودن یک صفحه مشکل باشد. صحافی کردن صفحات نیز باعث می شود حذف یک صفحه

یا اضافه نمودن یک صفحه جدید به آن فایل مشکل شود. قرار دادن چند کپی از فایل در چند مکان متفاوت باعث می شود تغییر تمام اسناد بطور همزمان عملاً غیرممکن گردد. البته روش دیگری که جهت محافظت از اسناد کاغذی در برابر دستکاری بکار می رود جلوگیری کامل از دسترسی افراد غیرمجاز می باشد این کار توسط همان مکانیزمی که برای محرمانه سازی بکار می رود انجام می شود.

عموماً دستکاری فایلهای الکترونیکی آسانتر است. در اکثر موارد فایل در یک نرم افزار واژه پرداز مانند word باز می شود و اطلاعاتی از آن حذف و یا به آن اضافه می شود. پس از آن با ذخیره فایل، اطلاعات جدید جایگزین اطلاعات قدیمی می شود. روش ابتدایی که برای حفظ تمامیت حالت کنترل دسترسی به گونه ای نیست که از دسترسی به فایل کاملاً جلوگیری شود بلکه بگونه ای تنظیم می شود که امکان خواندن فایل وجود دارد ولی امکان نوشتن در فایل و تغییر آن وجود ندارد. همانند سرویس محرمانه سازی در اینجا هم تشخیص هویت فردی که فایل را مشاهده می کند بسیار مهم است. تحقق این امر با استفاده از هویت سنجی و اعتبار سنجی ممکن است.

استفاده از روش کنترل دسترسی به فایل های کامپیوتری به شرطی خوب کار می کند که فایل های فقط در یک کامپیوتر قرار داشته باشند و یا در شبکه ای باشد که تحت کنترل سازمان است. اگر فایل های به بخش ها یا سازمان های دیگر کپی شود چه اتفاقی می افتد؟ واضح است که در این حالت کنترل دسترسی به فقط یک کامپیوتر یا یک شبکه نمی تواند محافظت لازم را فراهم کند. بنابراین لازم است مکانیزمی برای تشخیص تغییرات غیرمجاز وجود داشته باشد. راه حل این مسئله، مکانیزم امضای دیجیتال است. امضای دیجیتال روی فایل قادر به تشخیص دستکاری در آن فایل می باشد. به منظور ارزش دار کردن اینکار، لازم است امضای دیجیتال توسط کاربر بخصوصی شناسایی شود به همین دلیل سرویس تمامیت باید با هویت سنجی و اعتبار سنجی کار کند.

حملات قابل پیشگیری

سرویس تمامیت قادر است از موفقیت حملات تکذیبی و دستکاری اطلاعات جلوگیری کند. همانطور که می دانیم حمله از نوع دستکاری می تواند فایل یا اطلاعات در حال انتقال را تغییر دهد، در حالیکه اگر سرویس تمامیت بدرستی کار کند تغییرات غیرمجاز ایجاد شده کشف خواهد شد. با ترکیب این سرویس هویت سنجی و اعتبار سنجی حتی تغییراتی که خارج از سازمان روی فایل های انجام می شود قابل کشف است.

محافظت در برابر حملات موفق تکذیبی بدون استفاده از سرویس تمامیت، هویت سنجی و اعتبار سنجی خوب انجام پذیر نیست. در این موارد از امضای دیجیتال جهت کشف حمله استفاده میشود.

فراهمی

سرویس فراهمی باعث می شود اطلاعات همیشه در دسترس و قابل استفاده باشد. فراهمی به کاربر اجازه می دهد به کامپیوتر، اطلاعات روی کامپیوتر و نرم افزارهای کاربردی (که عملیات خاصی روی اطلاعات انجام میدهند) دسترسی پیدا کند. علاوه بر این استفاده از سرویس فراهمی برای سیستم های ارتباطی باعث می شود اطلاعات بین مکانهای مختلف و کامپیوترها مبادله گردد. اگر چه سرویس فراهمی در مورد فایل های کاغذی هم قابل فرض است اما اغلب زمانی که از فراهمی صحبت می شود، اطلاعات و قابلیت های سیستم به فرم الکترونیکی هستند، اگر چه فراهمی فایل های کاغذی اطلاعات هم قابل فرض است. در ادامه فرمهای مختلف فراهمی معرفی می شود.

استفاده از پشتیبان

تهیه پشتیبان ساده ترین شکل سرویس فراهمی می باشد و منظور آناست که نسخه دومی از اطلاعات در مکان امنی ذخیره شده باشد. پشتیبان می تواند بصورت فایل های کاغذی (کپی اسناد مهم) یا فایل های الکترونیکی پشتیبان

کامپیوتر) باشد. استفاده از پشتیبان باعث می شود بهنگام تخریب عمدی یا اتفاقی فایل ها، در برابر از دست دادن کل آنها محافظت بعمل آید. مکان امن مورد نظر می تواند یک صندوق نسوز در همان سایت باشد و یا اینکه یک سایت دوردست باشد که دارای امنیت فیزیک مناسب باشد.

اگر چه استفاده از پشتیبان باعث می شود فراهمی اطلاعات تأمین شود، اما منظور، فراهمی از نظر زمانی نمی باشد و ممکن است بازیابی اطلاعات مدت زمانی طول بکشد، چرا که اطلاعات باید از مکان دور به سازمان برگردانده شود و حداقل اینکه از مکان امن واقع در همان سازمان دوباره به سیستم برگردانده شود.

Fail-over ، غلبه بر خطا

Fail-over روشی است که در آن اطلاعات یا قابلیت یک سیستم مجدداً تشکیل می شود. برخلاف پشتیبان، در این روش بروز خطا بطور خودکار تشخیص داده می شود و قابلیت آن سیستم (از قبیل پردازش، دسترسی به اطلاعات یا ارتباطات) مجدداً برقرار می شود. در این روش از یک پروسه خودکار سخت افزارهای یدکی استفاده می شود.

Fail-over روشی است که در آن تشکیل و راه اندازی مجدداً سیستم بطور آنی انجام می شود. سیستم یدکی که برای جایگزینی با سیستم اصلی بکار می رود می تواند در همان مکان قرار داشته باشند تا در مواقع بروز خطا از آن استفاده شود. این سیستم از بسیاری سیستم های Fail-over لحظه ای ارزانتر می باشد.

بازیابی در اثر حادثه

این روش باعث محافظت اطلاعات سیستم و قابلیت های آن در برابر حوادث ناگوار شود. بازیابی در اثر حادثه پروسه ای پیچیده و سخت است چون که امکان دارد که وسایل و امکانات سیستم یا اتاق های سازمانی از دست رفته باشد.

حملاتی که قابل پیشگیری هستند

سرویس فراهمی باعث میشود سیستم پس از حملات Dos (جلوگیری از سرویس دهی) بازیابی شود. اگر چه راهی برای پیشگیری از حملات Dos وجود ندارد، اما سرویس فراهمی باعث کاهش اثرات ناشی از آن می شود و می توان قابلیت های آن سیستم را در اسرع وقت بازیابی کرد.

مجوز سنجی

اغلب زمانی که از امنیت صحبت می شود، سرویس مجوز سنجی فراموش می شود. دلیل عمده هم این است که سرویس مجوزسنجی به خودی خود قادر به محافظت در برابر حملات نمی باشد، بلکه باید به همراه سرویسهای دیگر استفاده شود تا آن سرویسها بطور مؤثرتر کار کنند. این سرویس خودش سخت ترین بخش امنیت است چون بدون آ»که ارزشی به سیستم اضافه کند پیچیدگی آنرا می افزاید. سرویس مجوزسنجی هزینه را افزایش می دهد و قابلیت استفاده از سیستم را می کاهد. بدون سرویس مجوزسنجی، مکانیزمهای تمامیت و محرمانه سازی شکست خواهند خورد.

A & 1 : هویت سنجی و اعتبار سنجی

هویت سنجی و اعتبار سنجی (که به اختصار A & 1 گفته می شود) دو هدف را دنبال می کند. اول آنکه A & 1 وظیفه دارد هویت فردی که قصد انجام کاری را دارد تعیین کند (تعیین هویت) و دو م آنکه ثابت کند این فرد همان کسی است که خودش ادعا می کند (اعتبار سنجی) عمل اعتبار سنجی را می توان با استفاده از موارد زیر را انجام داد:

- برپایه آنچه شخص می داند (مانند کلمه عبور یا PIN)

- برپایه آنچه شخص دارد (مانند کارت هوشمند یا مهر شخصی)
- برپایه آنچه هست (مانند اثر انگشت یا اسکن نمودن شبکیه چشم)

اگرچه هر یک از موارد فوق به تنهایی قابل استفاده است اما بهتر است ترکیبی از آنها استفاده شود (مثلاً کلمه عبور و کارت هوشمند با هم استفاده شود)، اینکار به « اعتبار سنجی دو فاکتوری» معروف است. دلیل استفاده از دو فاکتور آن است که هر یک از آنها به تنهایی دارای ضعفهای می باشد. برای مثال امکان دارد کلمه عبور لو برود. کارت هوشمند قابل سرقت است. جعل کردن اعتبار سنجی بیومتریک اگر چه بسیار مشکل است اما ممکن است. برای مثال ممکن است فرد را مجبور نمایند انگشت خود را روی دستگاه اسکن اثر انگشت قرار دهد.

در جهان فیزیکی می توان اعتبار سنجی را توسط عکسی انجام داد که به نگهبان یک سازمان نشان داده می شود و در واقع می تواند اعتبار لازم برای وارد شدن یکی از کارکنان آن سازمان را فراهم نماید. از اسکنرهای اثر انگشت نیز برای اعتبارسنجی افراد استفاده می شود. به هر حال مکانیزم های اعتبارسنجی بطور مستقیم با وجود فیزیکی و هویت افراد رابطه دارد. اما در جهان الکترونیک، اعتبار سنجی نمی تواند به آن خوبی که در جهان فیزیکی عمل می کند، انجام وظیفه کند. استفاده از کلمه عبور مکانیزمی سنتی که برای اعتبار سنجی در کامپیوتر بکار می رفته است. در این سیستم هویت فرد به "ID" کاربر وابسته است که این ID توسط مدیر سیستم تعیین می شود. مدیر سیستم چنین تلقی می کند که فرد دریافت کننده ID کاربر، همان فرد شناسایی شده است. کلمه عبور یکی از عوامل اعتبار سنجی است و ذاتاً دارای ضعف می باشد. بر خلاف جهان فیزیکی در اینجا ضمانتی بر وجود فیزیکی فر نمی باشد. از اینرو توصیه می شود از اعتبار سنجی دو فاکتوری استفاده شود تا مکانیزم اعتبار سنجی قدرتمندی پیاده سازی شود. استفاده از A & 1 (هویت سنجی و اعتبار سنجی) به کنترل دسترسی در فایل های کامپیوتری کمک می کند که کنترل دسترسی هم به نوبه خود باعث محرمانه سازی و تمامیت فایل های الکترونیکی در کامپیوتر می گردد. علاوه بر این استفاده از A & 1 در رمزنگاری و امضای دیجیتالی نقش مهمی دارد. البته در این حالت A & 1 روی کاربر دوردست انجام می شود. بدنی ترتیب کاربری که در نقطه دوردست قرار گرفته است ابتدا هویت خود را

برای مکانیزم محلی ثابت می کند و مدرکی برای نقطه دور مقابل فراهم می کند. در ابتدا باید اعتبار کاربر توسط ماشین محلی که حاوی امضای دیجیتال است و توسط مکانیزمی این امضا را محافظت می کند، تأئید شود. پس از آن ماشین محلی به کاربر اجازه می دهد از مکانیزم امضا برای ارسال پیام استفاده کند. کاربر دریافت کننده پیام از امضای دیجیتال استفاده می کند تا مطمئن شود ارسال کننده پیام معتبر است.

در بسیاری موارد، از مکانیزم های A & 1 به عنوان کلیدی برای دیگر سرویسهای امنیتی سازمان استفاده می شود. در این حالت اگر مکانیزم A & 1 مرتکب اشتباه شود، ضمانتی روی سرویسهای محرمانه سازی و تمامیت نمی‌باشد.

بازرسی

بازرسی، وقایع گذشته را گزارش گیری و ثبت می کند. گزارشات بازرسی حاوی اعمالی است که فرد رد کامپیوتر و یا در جهان فیزیکی انجام داده است. بدون استفاده از A & 1 مناسب، گزارشات بازرسی قابل استفاده نخواهدبود، زیرا کسی نمی تواند ضمانت کند این گزارشات آنطور که بوده است ثبت شده است. بازرسی هایی که در جهان فیزیکی رخ می دهد شامل ورود و خروج افراد، صفحات امضا شده و حتی فیلمهای ویدیویی ضبط شده می باشد. منظور از این گزارشات فیزیکی، ثبت کارهای انجام شده است. علاوه بر این لازم است سرویس تمامیت، صحت گزارشات و عدم دستکاری در آنها را ضمانت کند. در غیر اینصورت گزارشات بازرسی مورد تردید قرار می گیرد. اما در جهان الکترونیک کامپیوتر گزارشاتی تهیه می کند که در آن اعمال انجام شده توسط کاربران صاحب ID ثبت می شود. اگر وظیفه A & 1 بدرستی انجام شود می توان این وقایع را به افراد نسبت داد. در اینجا نیز همانند گزارشات کاغذی، لازم است گزارشات بازرسی روی سیستم کامپیوتر از دستکاری توسط افراد غیرمجاز محافظت گردد. بنابراین تمام گزارشات بازرسی صرف نظر از نوع آن باید از هرگونه دستکاری محافظت گردند.

حملات قابل پیشگیری

سرویس مجوزسنجی هیچ حمله ای را پیشگیری نمی کند. در واقع این سرویس باید همراه سرویسهای دیگر و بخصوص محرمانه سازی و تمامیت کار کند. بدین ترتیب میتواند افرادی که قصد انجام عملیاتی را دارند، شناسایی و اعتبار آنها را تأئید کند. علاوه بر این سرویس مجوز سنجی گزارشاتی از آنه توسط کاربران معتبر انجام شده است را ثبت می کند تا بدین وسیله وقایع انجام شده قابل بازسازی باشد.

فصل چهارم

سیـــاست گـــذاری

شاید بتوان گفت در بحث حرفه ای امنیت اطلاعات کمتر به مسئله سیاست گاری پرداخته شده است. از اینرو در پاسخ افراد حرفه ای که دوست دارند نحوه کار سیستم ها را بهتر و بیشتر بفهمند دانش فنی کمی وجود دارد. از طرفی چون سازمان همیشه به نتیجه کار توجه می کند لذا نسبت به این کار و افرادی که این شغل را دارند ناسپاسی میشود. لازم به ذکر است سیاست مورد نظر در اینجا با سیاست و روابط دیپلماتیک بین کشورها فرق دارد. در اینجا سیاست، روش کار و مجموعهای از بایدها و نبایدها است.

سیاست گذاری نقش اجرا را ایفا می کند و افراد را به انجام کارهایی وا میدارد که نمی خواهند انجام دهند. سیاست سازمان بسیار اهمیت دارد و شاید در بخش امنیت اطلاعات سازمان مهم ترین شغل باشد.

سیاست گذاری مهم است

سیاست گذاری چگونگی پیکره بندی سیستم را تعیین می کند و معین می کند پرسنل سازمان در شرایط عادی چگونه عمل می کنند و در شرایط غیرعادی چه عکس العملی از خود نشان دهند. بدین ترتیب سیاست گذاری دو وظیفه اصلی زیر را انجام میدهد:

- چگونگی امنیت را در سازمان تعیین می کند.
- به هر کس می گوید از او چه انتظاری وجود دارد.

وظیفه اول- تعیین چگونگی امنیت

سیاست، نحوه پیاده سازی امنیت را تعیین می کند. این مسئله شامل پیکره بندی مناسب کامپیوتر و شبکه می شود. علاوه بر این سیاست گذاری، مکانیزم های مناسبی را برای محافظت اطلاعات و سیستمها تعیین می کند.

اما سیاست فقط به جنبه های فنی امنیت نمی پردازد بلکه وظایف مرتبط با امنیت را نیز برای پرسنل تعیین می کند. (از جمله این وظایف می توان به مدیریت کاربران اشاره کرد). علاوه بر این نحوه رفتار پرسنل به هنگام استفاده کامپیوتر توسط سیاست سازمان تعیین می شود.

بالاخره سیاست گذاری عکس العمل سازمان را به هنگامیکه کارها مطابق انتظار انجام نمی شود تعیین می کند. به هنگامیکه حادثه امنیتی رخ می دهد یا سیستم خطا می کند، این سیاست سازمان است که می گوید چه کار باید کرد و هدف سازمان در طول حادثه چه خواهد بود.

وظیفه دوم- نقش و وظیفه افراد

از جمله بخش های مورد نیاز در اجرای برنامه های امنیتی سازمان، وظیفه و نقش افراد است. سیاست گذاری چارچوبی فراهم می کند تا پرسنل یک سازمان برای رسیدن به امنیت با یکدیگر همکاری کنند. سیاست سازمان و پروسه ای که در پیش گرفته می شود تعیین کننده اهداف برنامه امنیتی می باشد. وقتی این اهداف به پرسنل سازمان ابلاغ گردید، پایه های یک کار تیمی موفق فراهم شده است.

انواع سیاست

سیاستها و پروسه های کاری زیادی وجود دارد که تعیین کننده چگونگی پیاده سازی امنیت سازمان است. توجه شود مفاهیمی که در این بخش ها آمده است را می توان با هم ترکیب کرده یا حتی به بخش های مختلف تفکیک کرد بطوریکه برای یک سازمان خاص بهترین و مناسب ترین راه بدست آید.

برای هر یک از انواع سیاست گذاری، اهم مطالب توضیح داده شده است. اما در تمام این سیاست گذاری ها، سه بخش مشترک وجود دارد که عبارتند از:

۱. هدف : هر روش و سیاست گذاری نیاز به هدفی دارد که به درستی تعیین شده باشد. در بخش هدف سند سیاستگذاری باید به وضوح گفته شود چرا سیاست گذاری ایجاد شده است و سازمان مربوطه به چه منافعی خواهد رسید.

۲. حوزه عمل: لازم است هر سیاست گذاری شامل بخشی باشد که قابلیت اجرای آنرا تعیین کند. برای مثال ممکن است سیاست گذاری امنیتی به تمام سیستمهای کامپیوتری و شبکه های اعمال شود در حالیکه سیاست گذاری اطلاعاتی به تمام پرسنل یک سازمان اعمال می شود.

۳. مسئولیت: در این بخش تعیین می شود برای اجرای درست و کامل یک پروسه چه کسی مسئول است. مسئولیت به هر کسی سپرده شود لازم است به درستی آموزش داده شود و از نیازهای آن سیاست گذاری مطلع گردد.

سیاست اطلاعاتی

سیاست اطلاعاتی ، تعیین کننده اطلاعات حساس سازمان است و می گوید چگونه باید از آنها محافظت شود. این سیاست باید بگونه ای ایجاد شود که تمام اطلاعات سازمان را پوشش دهد. بر طبق این سیاست گذاری هر یک از پرسنل سازمان در قبال حفاظت از اطلاعات حساسی که در اختیارش قرار می گیرد پاسخگو خواهد بود. بخشهای مختلف سیاست اطلاعاتی عبارتند از:

شناسایی اطلاعات حساس

نوع اطلاعاتی که در یک سازمان حساس فرض می شوند عبارتند از لیست حقوق افراد، آدرس و شماره تلفن منازل پرسنل، اطلاعات بیمه درمانی و هر نوع اطلاعات مالی که جنبه عمومی ندارد. لازم است این مسئله را بخاطر داشته

باشید که اطلاعات موجود در سازمان برای همیشه و همه اوقات حساس نیستند. انتخاب اطلاعات حساس بوسیله سیاست گذاری انجام می گیرد و لازم است به پرسنل اطلاع داده شود.

طبقه بندی

برای بیشتر سازمانها استفاده از دو یا سه سطح طبقه بندی کفایت می کند. پایین ترین سطح طبقه بندی اطلاعات، طبقه بندی عمومی می باشد، به عبارت دیگر اطلاعاتی که از قبل شناخته شده است و می توان در اختیار عموم قرار داد.

بعد از سطح فوق اطلاعاتی قرار دارد که نمی توان در اختیار عموم قرار داد. برای این نوع اطلاعات اسامی متفاوتی وجود دارد که از آن جمله می توان به اختصاصی، محرمانه شرکتی یا حساس شرکتی اشاره کرد. این اطلاعات صرفاً در اختیار پرسنل همان سازمان و یا سازمانهای غیر رقیب و دوست قرار داده می شود. چنانچه این اطلاعات در اختیار عموم یا رقبا قرار گیرد سازمان زیان خواهد دید.

سومین سطح طبقه بندی اطلاعات حساس، طبقه بندی انحصاری یا حفاظت شده است. اطلاعاتی که در این سطح قرار می گیرد و در حالت عادی در انحصار تعداد محدودی از پرسنل سازمان قرار دارد. این اطلاعات در اختیار تمام پرسنل قرار نمی گیرد و افرادی که خارج از سازمان قرار دارند کاملاً از این اطلاعات بی بهره اند.

توجه: طبقه بندی اطلاعات بصورت محرمانه، سری و خیلی سری کار خوبی نیست، چون این نوع طبقه بندی برای اطلاعات حکومتی استفاده می شود.

علامت گذاری اطلاعات حساس

برای هر سطح از اطلاعات حساس (که بالاتر از اطلاعات عمومی قرار می گیرد) لازم است سیاست گذاری نحوه علامتگذاری اطلاعات توسط سیاست اطلاعات تعیین شود. چنانچه اطلاعات روی کاغذ ثبت شده باشد، بالا و پایین هر صفحه باید علامتگذاری شود. اگر از برنامه word استفاده کرده اید می توانید با استفاده از headers and footers اینکار را انجام دهید.

ذخیره نمودن اطلاعات حساس

لازم است اطلاعات روی کاغذ و داخل کامپیوترها توسط سیاست گذاری آدرس دهی شود. هیچ وقت نباید اطلاعات روی میز رها شود، بهتر است اطلاعات داخل کمد فایلی و یا کشوی میز قرار داده شود.

چنانچه اطلاعات روی کامپیوتر ذخیره شده است لازم است سیاست گذاری سطح مناسبی از محافظت را مشخص کند. اینکار شامل کنترل دسترسی به فایلها و قرار دادن کلمه عبور برای انواع خاص اسناد می باشد. در موارد فوق العاده از رمز نگاری هم استفاده می شود. به خاطر داشته باشید مدیریت سیستم باید قادر به مشاهده تمام اسناد موجود در کامپیوترها باشد.

انتقال اطلاعات حساس

در سیاست اطلاعاتی نحوه انتقال اطلاعات تعیین می شود. اطلاعات به طرق مختلفی (مانند پست الکترونیک، پست عادی، فکس و غیره) انتقال داده می شوند و هر یک از این روش های باید در سیاست گذاری تعیین شده باشد.

چنانچه برای انتقال اطلاعات از پست الکترونیک استفاده شود، لازم است رمزنگاری فایل های ضمیمه و بدنه پیام توسط سیاست اطلاعاتی مشخص شده باشد. چنانچه ارسال اطلاعات بصورت ارسال نسخه های چاپی انجام گیرد

باید از روشی استفاده گردد که از دریافت آن توسط گیرنده اطمینان حاصل شود. از جمله این روش ها میتوان به پست سفارش اشاره کرد. چنانچه سندی از طریق فاکس ارسال می شود بهتر است ابتدا به گیرنده سند تلفن بزنید و او را از ارسال سند مطلع کنید تا منتظر دریافت آن بماند. با این کار از ماندن سند مذکور به مدت طولانی روی دستگاه فاکس گیرنده جلوگیری می کنید و بدین ترتیب امکان سوء استفاده یا به سرقت رفتن آن از بین خواهد رفت.

انهدام اطلاعات حساس

چنانچه اطلاعات حساس در سطل آشغال ریخته شود قابل استفاده برای افراد غیرمجاز خواهد شد، از اینرو اطلاعات حساسی که روی کاغذ است باید قبل از دور ریختن از بین برود و ریز ریز شود. امروزه دستگاه های خردکنی وجود دارد که کاغذ را در دو جهت افقی و عمودی خرد می کند بطوریکه بازسازی صفحه کاغذ تقریباً غیرممکن می شود. بدین ترتیب سطح بالایی از محافظت پیاده سازی می شود.

اگر حذف اطلاعات از روی کامپیوتر بدرستی انجام نشود افراد غیر مجاز به بازیابی فایل های حذف شده خواهند بود. هم اکنون چندین برنامه نرم افزاری تجاری وجود دارد که با استفاده از آن می توانید عمل پاک کردن اطلاعات از روی کامپیوتر را با امنیت بالا انجام دهید.

توجه: این امکان وجود دارد که اطلاعات الکترونیک حذف شده را حتی بعد از آنکه اطلاعات جدیدی روی هارد یا فلاپی نوشته شد بازیابی کرد. البته وسیله ای که بتواند اینکار را انجام دهد بسیار گران قیمت است و جنبه تجاری ندارد. از اینرو معمولاً تخریب فیزیکی هارد یا فلاپی لازم نیست.

سیاست امنیتی

سیاست امنیتی تعیین کننده نیازهای فنی برای برقراری امنیت در کامپیوترهای و تجهیزات شبکه است. سیاست امنیتی تعیین می کند مدیریت شبکه یا سیستم از چه پیکره بندی استفاده کند تا امنیت مورد نظر بدست آید. این پیکره بندی تأثیر خود را روی کاربران و نیازمندیهایی که در بخش سیاست گذاری به آنها اشاره شد اعمال خواهد کرد. اولین کسی که در قبال اجرای این سیاست مسئول است مدیریت شبکه و سیستم کامپیوتری است.

سیاست امنیتی باید نیازهایی که در اجرای هر سیستمی احتیاج است را تعیین کند. البته این سیستم به خودی خود نباید پیکره بندی خاصی را در سیستم عامل های مختلف تعیین کند و لازم است اینکار به پروسه خاص پیکره بندی سیستم عامل موکول شود. این پروسه به صورت ضمیمه در آخر سیاست گذاری ارائه می شود و نه در خود سیاست گذاری.

بخشهای مختلف سیاست اطلاعاتی عبارتند از:

هویت سنجی و اعتبار سنجی

نحوه تعیین هویت کاربران از جمله مواردی است که باید توسط سیاست امنیتی تعیین شود. به عبارت دیگر لازم است سیاست امنیتی استانداردهایی را برای هویت کاربران تعیین کند.

از این مهمتر لازم است سیاست امنیتی مکانیزم اعتبار سنجی را برای کاربران و مدیران سیستم تدوین کند. اگر این مکانیزم استفاده از کلمه عبور باشد در اینصورت لازم است سیاست گذاری مذکور کلمه عبوری با طول حداقل تعیین کند و حداقل و حداکثر طول کلمه عبور و نیازمندیهای مشتمل بر کلمه عبور را هم تعیین کند.

هر سازمانی به هنگام ایجاد سیاست امنیتی خود باید در مورد محورهای مدیریتی تصمیم بگیرد بطوریکه تعیین شود از یک مکانیزم اعتبارسنجی برای مجوزهای مختلف استفاده شود یا اینکه از مکانیزمهای قوی تری استفاده شود. اگر نیاز به مکانیزم قوی تر احساس شود، لازم است در این قسمت از سیاست گذاری، نیازهای امنیتی تعیین شود.

در مواردی که به دسترسی از راه دور نیاز است (همانند VPN یا دسترسی dail-in) استفاده از مکانیزمهای قوی تر مناسب می باشد.

کنترل دسترسی

از جمله مواردی که در سیاست امنیتی تعیین می شود استانداردهایی است که برای کنترل دسترسی به فایلهای الکترونیکی مورد نیاز است. دو نیاز عمده که باید تعیین شود عبارتند از:

۱. مکانیزم مورد نیاز

۲. تنظیمات پیش فرض در فایل های جدید

مکانیزمی که به آن اشاره شد می تواند نوعی کنترل دسترسی باشد که بر حسب نوع کاربر استفاده کننده از فایل تعیین میشود. لازم است این مکانیزم بهمراه مکانیزم اعتبار سنجی کار کند تا فقط کاربران مجاز قادر به دسترسی به فایل ها باشند. چنین مکانیزمی باید تعیین کند کدام کاربر اجازه خواندن، نوشتن یا اجرای یک فایل را دارد.

تنظیمات پیش فرضی که برای فایلهای جدید در نظر گرفته می شود باید بتواند چگونگی اجازه دسترسی به هر فایل جدید را تعیین کند. این بخش از سیاست گذاری مجوز خواندن، نوشتن و اجرای هر فایل را برای مالک آن فایل و دیگر کاربران سیستم تعیین می کند.

گزارش گیری

از جمله بخش های سیاست امنیتی، گزارش گیری از تمام وقایع سیستم است. در حالت عادی سیاست امنیتی نیاز به گزارش گیری از وقایع زیر را دارد:

- ورود یا login (موفق و غیر موفق)

- خروج یا logout
- دسترسی نادرست به فایل یا سیستم
- فعالیت های صدور مجوز
- وقایع سیستم (مانند خاموش کردن یا بوت نمودن که توسط مدیران انجام می شود)

لازم است رد واقعه حاوی اطلاعات زیر باشد:

- ID کاربر
- تاریخ و زمان
- ID پردازشی
- فعالیت انجام شده
- موفقیت یا عدم موفقیت واقعه

سیاست امنیتی طول رکوردهایی که باید ذخیره کند را تعیین میکند. حتی اگر ممکن باشد نحوه مرور و آزمایش رکوردهای گزارش گیری باید توسط سیاست گذاری تعیین شود.

اتصال شبکه ای

برای هر نوع اتصال به شبکه سازمان لازم است قوانین مربوط به این اتصال و مکانیزم های محافظتی توسط سیاست امنیتی تعیین گردد. برای ارتباط تلفنی، استفاده از تکنیک های مناسب اعتبار سنجی لازم می باشد. اگر اتصال شبکه ای از نوع دائم است استفاده از دیوار آتش مناسب است.

دسترسی از راه دور به سیستم داخلی

اغلب سازمانها به پرسنل خود اجازه میدهند از راه دور به سیستم داخلی آن سازمان دسترسی داشته باشند. لذا لازم است سیاست امنیتی برای مواقعی که این نوع دسترسی اعطاء می شود مکانیزم مناسبی تعیین کند. مناسب است تمام ارتباطات با استفاده از رمزنگاری محافظت گردند و روی نوع رمزنگاری که باید استفاده شود تأکید گردد. علاوه بر این از آنجا که ورود به سیستم از خارج صورت می گیرد، استفاده از مکانیزمهای اعتبار سنجی قوی تر لازم است.

کد خرابکاری

از جمله وظایف سیاست امنیتی تعیین محل نرم افزار امنیتی است که کدهای خرابکاری (مانند ویروس ها و برنامه های اسب تروجان) را جستجو می کند. محل های مناسب عبارتند از سرور فایل، روی سیستم DESKTOP و روی سرور پست الکترونیک.

تنظیمات نرم افزار امنیتی در سیاست امنیتی تعیین می شود. این تنظیمات شامل مواردی است که برای بررسی فایلها به هنگام بازکردن بکار می رود.

از جمله موارد دیگری که توسط سیاست امنیتی تعیین می شود به روز کردن امضاء برای برنامه های امنیتی است. این کار بصورت دوره ای باید انجام شود برای مثال لازم است امضاء بطور ماهانه به روز گردد.

رمز نگاری

از جمله مواردی که لازم است در سیاست امنیتی تعیین شود الگوریتم های قابل قبول رمزنگاری برای استفاده در سازمان است بطوریکه این رمزنگاری به همان سیاست اطلاعاتی بر می گردد. بدین ترتیب الگوریتم یا الگوریتمهای

مناسبی برای حفظ اطلاعات حساس بکار می رود. علاوه بر این لازم است پروسه مدیریت کلید توسط این سیاست تعیین گردد.

بازبینی استثنائات

حتی اگر بهترین تصمیم گیری توسط مجری امنیتی و مدیریت سیستم اتخاذ شده باشد، باز هم زمانهایی وجود دارد که سیستم در موقعیتی جدید قرار می گیرد بطوریکه این موفقیت در سیاست گذاری امنیتی دیده نشده است. برای مثال نیاز می شود سیستم برخی نیازهای تجاری را برآورده کند و برآورده کردن این احتیاجات مهمتر از آن است که سیاست امنیتی سیستم اجرا شود. با بروز چنین اتفاقی باید مکانیزمی توسط سیاست گذاری امنیتی فراهم شود و ضمن آنکه ریسک معینی توسط سازمان پذیرفته می شود نیازهای موقت سازمان نیز برطرف شود.

ضمائم

جزئیات مربوط به پیکره بندی امنیتی سیستم عامل های مختلف در بخش ضمائم یا در پروسه پیکره بندی جداگانه ای قرار داده می شود. این مطلب باعث می شود در صورت نیاز اسناد مربوط به این جزئیات بدون تغییر در سیاست امنیتی سازمان تصحیح و دستکاری شود.

سیاست استفاده از کامپیوتر

سیاست استفاده از کامپیوتر درباره اینکه چه کسی از سیستم کامپیوتری استفاده می کند و چگونگی بکار بردن آن صحبت می کند. به نظر می رسد بیشتر اطلاعات موجود در این سیاست گذاری عمومی و معمولی باشد، اما در

صورتیکه سازمان سیاست خاصی درباره مالک کامپیوتر و استفاده از آن وضع نکند راه را برای اقامه دعوی از طرف پرسنل باز گذاشته است.

مالک کامپیوتر

سیاست استفاده از کامپیوتر باید به وضوح تعیین کند تمام کامپیوترها به سازمان تعلق دارد و کامپیوترهایی که برای استفاده در اختیار قرار داده شده است با شغلشان مطابقت دارد. علاوه بر این بر این بر طبق این سیاست، استفاده از کامپیوتر های غیر سازمانی برای امور تجاری سازمان ممنوع است. برای مثال اگر کارمندی کارهای سازمان را در خانه اش انجام می دهد لازم است سازمان کامپیوتر مناسبی برای او فراهم کند. شاید بیان این نکته در اینجا مناسب باشد که فقط کامپیوترهای ارائه شده از طرف سازمان باید بتوانند از طریق سیستم دسترسی از راه دور به کامپیوتر داخلی سازمان وصل شوند.

مالک اطلاعات

بر طبق سیاست استفاده از کامپیوتر، تمام اطلاعاتی که روی کامپیوترهای سازمان ذخیره و یا استفاده می شود به سازمان تعلق دارد. امکان دارد برخی از پرسنل، کامپیوترهای سازمان را برای ذخیره اطلاعات شخصی بکار گیرند. اگر این سیاست بدرستی بیان نشود ممکن است این انتظار بوجود آید که اطلاعات شخصی پرسنل- در صورت ذخیره شدن در دایرکتوری اختصاصی- باقی خواهد ماند و از بین رفتن اطلاعات باعث ارائه دعوی از طرف پرسنل گردد.

استفاده قابل قبول از کامپیوتر

اکثر سازمانها از پرسنل خود انتظار دارند از کامپیوترهای سازمان فقط برای مقاصد کاری استفاده شود. این مسئله معمولاً فرضیه خوبی نیست و بنابراین لازم است در سیاست گذاری تبیین شود. شاد مناسبتر این باشد که گفته شود «کامپیوترهای سازمانی فقط برای مقاصد تجاری برده شود» و مقاصد تجاری بصورت جزئی توضیح داده شود.

گاه و بیگاه سازمان ها به پرسنل خود اجازه می دهند برای مقاصد دیگر هم از کامپیوتر سازمان استفاده نمایند. برای مثال ممکن است سازمانی به کارمندانش اجازه دهد از طریق شبکه داخلی سازمان بازی کامپیوتری انجام دهند. در صورت مجاز بودن اینکار لازم است به وضوح در سیاست سازمان بیان شود.

در استفاده از کامپیوترهای سازمان به این مطلب هم بر می خوریم که چه نرم افزارهایی قابل نصب روی کامپیوتر است. مناسب است سازمان خاطر نشان شود نرم افزار غیر مجاز نباید روی کامپیوترها نصب گردد. تعیین اینکه چه نرم افزارهایی مجاز است و چه کسی می تواند نرم افزارهای مجاز را نصب کند بر عهده سیاست استفاده از کامپیوتر است.

عدم پنهان کاری

شاید مهم ترین بخش سیاست استفاده از کامپیوتر ذکر این نکته باشد که پرسنل درباره اطلاعاتی که ذخیره، ارسال و یا دریافت می نمایند نباید توقع هیچ گونه پنهان کاری و شخصی گرایی داشته باشند. دانستن این مطلب از طرف پرسنل بسیار حائز اهمیت است که تمام اطلاعات توسط مدیریت بررسی و مشاهده می شود. این اطلاعات شامل پست الکترونیک هم می شود. علاوه بر این لازم است پرسنل این مطلب را درک کنند که تمام فعالیت های مرتبط با کامپیوتر توسط مدیریت و مسئول امنیتی قابل مشاهده و کنترل است.

سیاست استفاده از اینترنت

معمولاً سیاست استفاده از اینترنت در سیاست استفاده از کامپیوتر گنجانده می شود، اما بعضی مواقع بدلیل طبیعت استفاده از کامپیوتر در سیاست جداگانه ای تفکیک می شود. امکان اتصال به اینترنت توسط سازمان فراهم می شود بطوریکه پرسنل بتوانند وظایف شغلی را بطور کاراتری انجام دهند و در نتیجه سود بیشتری به سازمان برسد. متأسفانه اینترنت برای پرسنل مکانیزمی را ارائه می دهد که از منابع کامپیوتر سوءاستفاده شود.

سیاست استفاده از اینترنت کاربردهای مناسب اینترنت را تعیین می کند ،از قبیل تحقیقات مرتبط با امور تجاری ، خرید و فروش و یا ارتباطاتی که با استفاده از پست الکترونیک انجام می شود)، در این سیاست استفاده های نادرست از اینترنت هم تعیین می شود. (از قبیل مشاهده وب سایتهای نامربوط با امور تجاری، دان لود کردن نرم افزارهائی که دارای حق کپی رایت هستند و گرفتن فایل های موزیک و ارسال نامه های متوالی) در صورتیکه سیاست استفاده از اینترنت از سیاست استفاده از کامپیوتر تفکیک شده باشد، باید خاطر نشان شود سازمان قادر است استفاده پرسنل از اینترنت را کنترل و مشاهده کند و پرسنلی که از اینترنت استفاده می کنند نباید توقع مخفی کاری و شخصی گرایی داشته باشند.

سیاست پست الکترونیک

امکان دارد برخی سازمانها بخواهند سیاست بخصوصی درباره استفاده از پست الکترونیک اعمال نمایند (امکان دارد این سیاست در سیاست استفاده از کامپیوتر لحاظ شده باشد). بیشتر سازمانها برای ارتباط تجاری خود از پست الکترونیک استفاده می کند. اگر سازمانی قصد داشته باشد سیاست جداگانه ای درباره پست الکترونیک وضع کند باید آنرا به د بخش داخلی و خارجی تقسیم کرد.

در پست الکترونیک داخلی، پرسنل مجاز به ارسال لطیفه های ناجور برای همکاران خود نیستند. علاوه بر این لازم است خاطر نشان شود پرسنل توقع هیچ نوعی مخفی کاری و شخصی گرای در پست الکترونیک نداشته باشند چون ممکن است پیامهایشان مشاهده و کنترل شود.

در مورد پست الکترونیک خارجی، نامه های الکترونیکی که از سازمان خارج می شود نباید حاوی اطلاعات حساس باشد. قرار دادن امضاء در انتهای نامه الکترونیکی خروجی عمل مناسبی برای سازمان است تا بدین وسیله خاطر نشان شود اطلاعات مذکور باید محافظت شود.

لازم است ملاحظات مربوط به نامه های الکترونیکی ورودی توسط سیاست پست الکترونیک تعیین گردد. برای مثال بسیاری از سازمانها فایل های ضمیمه شده ورودی را از نظر ویروس کنترل می نمایند. بنابراین سیاست مذکور باید با رجوع به سیاست امنیتی سازمان، پیکره بندی مناسبی درباره مقابله با ورود ویروس ایجاد نماید.

پروسه مدیریت کاربر

پروسه مدیریت کاربر یک پروسه امنیتی است که اغلب سازمانها از آن چشم پوشی می کنند و در عین حال پتانسیل ایجاد بزرگترین خطر را دارد. اگر چه مکانیزمهایی که سیستم ها را در برابر افراد غریبه محافظت می کنند بسیار جالب و شگرف هستند، اما در صورتیکه کاربران کامپیوتر بدرستی مدیریت نشوند آن مکانیزم ها کارآیی نخواهند داشت.

پروسه پرسنل جدید

برای آنکه پرسنل جدید به منابع کامپیوتری دسترسی صحیح پیدا کنند انجام این پروسه لازم است. در این پروسه لازم است بخش امنیت با دایره منابع انسانی و مدیریت سیستم همکاری دو جانبه داشته باشد. بطور ایده آل در

خواست برای منابع کامپیوتری بیشتر توسط سرپرست پرسنل جدید صورت می پذیرد و توسط این فرد امضاء و تأئید می شود. بسته به دایره مذکور کارمندان جدید درخواست خود را به سرپرستان داده و سرپرست درخواست دسترسی به منابع را صادر می کند. پس از آن مدیریت سیستم دسترسی صحیح به فایل ها و سیستم ها را فراهم می کند. این پروسه در مورد کارمندان موقت و مشاورانی که برای یک دوره زمانی با سازمان همکاری می کنند هم لازم است بطوریکه اکانت با تمام شدن زمان همکاری باطل گردد.

پروسه پرسنل انتقالی

هر سازمانی باید پروسه ای برای بررسی دسترسی کامپیوتری پرسنل داشته باشد تا به هنگام انتقال کارمندان توسط سازمان از آن استفاده شو. این پروسه بدون همکاری بخش منابع انسانی و مدیریت سیستم کامل نخواهد شد. در حالت ایده آل سرپرست قدمی تشخیص می دهد که کارمند انتقال یافته دیگر نیاز به دسترسی به این بخش ندارد و برای کارمند جدید درخواست دسترسی می کند. پس از آن مدیریت سیستم این تغییرات را اعمال خواهد کرد.

پروسه خاتمه استخدام

شاید مهم ترین بخش پروسه مدیریت کاربر، حذف کاربری است که دیگر برای سازمان کار نمی کند. این پروسه باید با همکاری دایره منابع انسانی و مدیریت سیستم صورت پذیرد. وقتی منابع انسانی تشخیص داد کارمندی در حال ترک سازمان است، مدیریت سیستم باید قبل از زمان مقرر خبردار شود تا بدین وسیله در آخرین روز استخدام آن کارمند، اکانت وی غیر فعال گردد. ممکن است در بعضی از موارد لازم شود قبل از خبردار شدن کارمند از اخراج، اکانتش غیر فعال گردد. این حالت هم باید در پروسه اتمام استخدام لحاظ شود. پروسه خاتمه استخدام باید پرسنل موقت و مشاورانی که اکانت دارند را هم شامل شود. ممکن است این افراد در بخش منابع انسانی شناخته

شده نباشد. وظیفه سازمان است که تشخیص دهد چه کسی در مورد این قبیل اطلاع کافی دارد و آنها را بطور مناسب در پروسه فوق قرار دهد.

پروسه مدیریت سیستم

در پروسه مدیریت سیستم، چگونگی همکاری مدیریت سیستم و بخش امنیت در جهت امن کردن سیستمهای سازمان تعیین میشود. اسناد طی چند پروسه خاص ساخته می شود و این پروسه ها هستند که تعیین می کنند وظایف مدیریت سیستم که با امنیت ارتباط دارد چگونه تکمیل گردد.

ارتقاء نرم افزار

در این پروسه تعیین می شود مدیریت سیستم هر چند وقت یکبار وجود مکملهای نرم افزاری یا مکمل های جدید آنرا از فروشنده اولیه کنترل کند. انتظار می رود به محض ظهور وصله های جدید نرم افزاری مدیریت سیستم آنها را نصب نکند بلکه بر طبق این پروسه ابتدا کارآیی آنها آزمایش شود و پس از آن نصب گردد. بر طبق این پروسه هر نوع ارتقاء نرم افزاری در صورت انجام باید مستند گردد.

بررسی آسیب پذیری و راه های نفوذ

هر سازمانی باید پروسه ای برای شناسایی راه های نفوذ و آسیب پذیرهای کامپیوتر داشته باشد. در حالت عادی بررسی راه های نفوذ بوسیله سیاست امنیتی هدایت می شود و توسط مدیریت سیستم تثبیت می شود. تعدادی ابزار تجاری برای بررسی آسیب پذیری ها وجود دارد ضمن اینکه ابزارهای رایگان هم قابل استفاده است.

لازم است پروسه مذکور تعیین کند سیستم هر چند وقت یکبار تحت بررسی قرار گیرد. پس از آنکه بررسی انجام شد نتیجه آن به اطلاع مدیریت سیستم رسانده می شود تا تصحیح لازم اتخاذ شود (امکان دارد به دلیل نرم افزار خاص بکار برده شده رد سیستم آسیب پذیر های آن قابل تصحیح نباشد). پس از آن مدیریت سیستم برنامه زمانبندی بعدی بررسی را جهت تثبیت آسیب پذیری ها دارد.

بازبینی سیاست گذاری

در هر سیستمی نیازهای امنیتی توسط سیاست امنیتی سازمان تعیین می شود . لازم است با استفاده از بازرسی های داخلی و خارجی که بصورت دوره ای انجام می شود از برآورده شدن این سیاست اطمینان حاصل شود. لازم است در بازرسی های اصلی، سیاست امنیتی با مدیریت سیستم همکاری کند. انجام این کار با استفاده از ابزارهای خودکار یا بصورت دستی قابل انجام است.

در پروسه بازبینی سیاست لازم است تعیین شود هر چند وقت یکبار این بازبینی انجام پذیرد. علاوه بر این لازم است تعیین شود نتایج بازبینی را چه کسی می گیرد و در برابر مواردی که برآورده نشده است چه رفتاری انجام خواهد شد.

بازبینی گزارشات

گزارشات حاصل از سیستم های مختلف باید بطور مرتب بازبینی گردد. بطور ایده آل این کار بطور خودکار توسط مسئول امنیتی انجام می گیرد بطوریکه وی به جا بررسی کل گزارشات فقط گزارشاتی را بررسی می کند که توسط ابزار خودکار علامتگذاری شده است.

در صورت استفاده از ابزار خودکار لازم است پیکره بندی ابزار مذکور و چگونگی رفتار با استثنائات توسط پروسه بازبینی گزارشات تعیین شود. در صورت استفاده از پروسه دستی، لازم است در پروسه تعیین شود بررسی فایل های گزارش- یا لاک کردن فایل ها- هر چند وقت یکبار انجام شود و چه نوع وقایعی برای ارزیابی بیشتر علامتگذاری شود.

مانیتورینگ منظم

هر سازمان باید پروسه ای داشته باشد که کنترل و مانیتورینگ ترافیک شبکه را مستند نماید. برخی از سازمانها این نوع کنترل را بصورت پیوسته انجام می دهند. برخی دیگر عمل مانیتورینگ را بطور تصادفی انجام می دهند. بهر حال سازمان شما هر یک از این دو روش را که انتخاب نماید لازم است آن را مستند و مکتوب نماید.

پروسه واکنش به حادثه

در پروسه واکنش در برابر حادثه که به اختصار IRP گفته می شود چگونگی واکنش سازمان به هنگام وقوع حادثه امنیتی تعیین می شود. با توجه به اینکه حوادثی از این دست باهم تفاوت خواهند داشت لازم است IRP تعیین کند چه کسی اجازه این کار را دارد و چه کاری در این زمینه نیاز است. البته لزوماً کارهایی که باید انجام شود تعیین نمی شود و اینکار به افرادی که روی حادثه کار می کنند موکول می شود.

اهداف رسیدگی به حادثه

اهداف سازمان به هنگام رسیدگی به یک حادثه باید توسط IRP تعیین شود. نمونه هایی از اهداف IRP به قرار زیر است:

- حفاظت سیستم های سازمان
- حفاظت از اطلاعات سازمان
- عملیات تعمیر و بازیابی
- پیگیری نمودن متخلف
- کاهش تبلیغات بد

این اهداف باهم در تعارض نیستند و داشتن چند هدف باعث بروز خطا نمی شود. کلید این بخش از پروسه آن است که اهداف سازمان قبل از آنکه حادثه ای رخ دهد شناخته شود.

تشخیص حادثه

شاید بتوان گفت تشخیص حادثه مشکل ترین قسمت پروسه واکنش به حادثه می باشد. برخی حوادث واضح هستند (برای مثال از شکل انداختن وب سایت شما). در حالیکه حوادث دیگر بصورت ورود بدون اجازه یا اشتباه کاربر است (برای مثال از دست دادن برخی فایل های دیتا). قبل از آنکه وقوع حادثه اعلام گردد لازم است تحقیقاتی توسط مدیریت سیستم انجام پذیرد تا معلوم گردد این موارد واقعاً حادثه هستند و علاوه بر این مراحلی که بری تشخیص حادثه باید توسط مدیر طی شود تا وقایعی که بطور واضح یک حادثه نیستند را تعیین کند.

پیشرفت قدم به قدم

لازم است همچنانکه اطلاعات بیشتری درباره واقعه بدست می آید IRP یک پروسه پیشرفت تدریجی هم تعیین کند. برای اغلب سازمانها این پروسه تیم واکنش به حادثه را فعال می کند. این امکان

وجود دارد که در مؤسسات مالی پروسه پیشرفت قدم به قدم دو سطح متفاوت داشته که این مسئله بستگی به وجود سرمایه در وقایع دارد.

هر سازمان اعضای تیم واکنش به حادثه را تعیین می کند. اعضای این تیم باید از بین بخش های زیر انتخاب شوند، اعضای دیگر بر حسب نیاز اضافه می شوند:

- امنیتی
- مدیریت سیستم
- حقوقی
- منابع انسانی
- روابط عمومی
- کنترل اطلاعات

با آشکار شدن حادثه، سازمان باید برای کنترل اطلاعاتی که منتشر شده است تلاش کند. مقدار اطلاعاتی که رها شده است بستگی به تأثیری دارد که حادثه مذکور روی سازمان داشته است. اطلاعات باید به طریقی رها شده باشد که قابل برگرداندن قطعی به سازمان باشد.

توجه: به غیر از پرسنل روابط عمومی و حقوقی، پرسنل دیگر سازمان نباید هیچ توضیحی در مورد حادثه به مطبوعات بدهند.

واکنش

واکنشی که سازمان در برابر حادثه انجام می دهد بطور مستقیم به اهداف IRP ارتباط دارد. برای مثال چنانچه حفاظت از اطلاعات و سیستم مورد نظر باشد، مناسب است سیستم ها از روی شبکه برداشته شوند و نیازها از نو

بازسازی و اصلاح گردد. در بعضی موارد لازم است سیستم بصورت زنده باقی بماند و سرویس ها فعال باقی بماند بطوریکه به مزاحم اجازه بازگشت به سیستم داده شود تا با استفاده از تله مناسب بتوان او را دنبال و دستگیر کرد. در هر صورت لازم است قبل از بروز هر نوع حادثه، نوع واکنشی که سازمان بکار می برد کاملاً تشریح و تمرین شود.

توجه: تلافی کردن به هیچ وجه ایده خوبی نیست. ممکن است اینکار غیر مجاز باشد، بنابراین و در هیچ شرایطی توصیه نمی شود.

اعتبار

از جمله قسمت های مهم در پروسه IRP تعیین شخصی از سازمان یا تیم واکنش به حادثه است که موقع حاده اختیار فعالیت داشته باشد. این بخش از پروسه باید تعیین کند چه کسی اجازه دارد سیستم را از سرویس خارج کند و با مشتریان، مطبوعات و نیروهای قانونی تماس برقرار کند. مناسب است برای انجام این تصمیمات یکی از متصدیان سازمان برگزیده شود. ممکن است این فرد یکی از اعضای تیم واکنش به حادثه باشد. به هر حال متصدی مذکور باید به هنگام تبیین پروسه IRP مشخص شود نه در زمان وقوع حادثه.

مستند سازی

پروسه IRP معین می کند تیم واکنش به حادثه چگونه فعالیت های خود را مستند و مکتوب نماید. این مسئله به دو دلیل اهمیت دارد، اول اینکه پس از اتمام حادثه می توان آنچه را اتفاق افتاده است مشاهده کرد و دیگر اینکه در صورت کمک گرفتن از نیروهای قانونی به روند پیگرد کمک میکند. بهتر است تیم واکنش به حادثه تعدادی دفترچه یادداشت برای استفاده در هنگام بروز حادثه آماده کند.

آزمایش پروسه

واکنش به حادثه به تمرین نیاز دارد. انتظار نداشته باشید اولین بار که از IRP استفاده می شود همه چیز بی عیب از آب در آید. به همین دلیل هنگامیکه IRP برای بار اول نوشته می شود توسط تیمی که در اتاق کنفرانس نشسته است مورد بررسی قرار می گیرد. در این حالت یک وضعیت خاص به تیم ارائه می شود و تیم دوباره عملیاتی که در قبال آن باید انجام دهد تصمیم می گیرد. هر یک از اعضای تیم باید این پروسه را دنبال کند. این کار کمک می کند نقص ها موجود در پروسه تشخیص داده شود و نسبت به تصحیح آن اقدام شود.

علاوه بر این لازم است IRP در عمل هم آزمایش شود. یکی از اعضای تیم امنیتی حمله ای را علیه سیستم کامپیوتری سازمان شبیه سازی می کند و تیم واکنش در برابر حادثه را مجبور به پاسخ می کند. ممکن است این آزمایش بدون اعلام قبلی انجام شود.

پروسه مدیریت پیکره بندی

در پروسه مدیریت پیکره بندی مراحلی که باید طی شود تا وضعیت سیستم های کامپیوتری سازمان بهبود یابد تعیین می شود. هدف از انجام این پروسه شناسایی تغییرات مناسب است. از دید امنیتی این تغییرات به عنوان حادثه شناخته نمی شود اما لازم است پیکره بندی جدید آزمایش شود.

حالت اولیه سیستم

زمانیکه سیستم جدیدی تولید می شود لازم است حالت اولیه آن مستند گردد. این مستند سازی باید حداقل موارد زیر را در بر گیرد:

- سیستم عامل و نسخه آن

- میزان وصله کاری
- نرم افزارهای در حال اجرا روی آن و نسخه هر یک

علاوه بر این ایجاد CRYPTOGRADHIC CHECKSUMS برای تمام سیستم های باینری و دیگر فایل هایی که در حین تولید سیستم نباید تغییر کند مناسب می باشد.

پروسه کنترل تغییر

با انجام هر تغییری روی سیستم لازم است پروسه کنترل پیکره بندی اجرا شود. بدین ترتیب قبل از انجام تغییرات پیشنهادی لازم است آنها بررسی و کنترل شوند. علاوه بر این لازم است هر گونه درخواست تغییر مکتوب گردد. بعد از آنکه تغییرات اعمال شد پیکره بندی سیستم به روز می شود تا سیستم حالت جدید سیستم را به خود بگیرد.

اصول طراحی

هر سازمانی که برای ایجاد سیستم جدید یا قابلیت های جدید پروژه ای در دست انجام دارد، باید اصول طراحی هم داشته باشد. این اصول تعیین کننده مراحلی است که سازمان برای به بهره برداری رساندن پروژه خود باید دنبال کند. اصول طراحی مراحل زیادی را شامل می شود که ارتباطی با بحث امنیت ندارد بنابراین در اینجا تشریح نمی شود. اما چنانچه امنیت ابتدایی در پروژه جدید اعمال شود احتمال آنکه امنیت کاملی در سیستم های نهایی برقرار شود بیشتر خواهد بود. برای هر یک از فازهای طراح که در ادامه آورده شده است ملاحظات تشریح خواهد شد.

فاز ۱ شناسایی نیازمندیها

آن دسته از نیازهای امنیتی که در فاز تشخیص هر پروژه وجود دارد باید توسط اصول طراحی تعیین شود. در اصول طراحی در مورد بعضی از نیازها به سیاست اطلاعاتی و امنیتی سازمان اشاره شود. علاوه بر این در سند نیازمندیها ، باید اطلاعات حساس و نیازهای کلیدی امنیت پروژه تعیین گردد.

فاز ۲ طراحی

اصول طراحی، آن دسته از مسائل امنیتی را که باید در طول فاز طراحی پروژه ارائه شود تا از امن بودن پروژه اطمینان حاصل شود تعیین می کند. متصدی امنیتی می تواند به عنوان یکی از اعضای تیم طراحی یا تیم بازرسی به کار بپردازد. هر کدام از نیازهای امنیتی که نتوان د رطراحی برآورده کرد باید مشخص گردد و در صورت ناز پروسه استثنائات شروع شود.

لازم است با شروع کدنویسی یک سیستم، به نویسنده آن سیستم درباره مشکلات احتمالی کدنویسی مانند سرریز شدن بافر آگاهی داده شود تا از مشکلات احتمالی در آینده پیشگیری شود.

فاز ۳ آزمایش با رفتن پروژه به سمت آزمایش باید نیازهای امنیتی به دقت بررسی و امتحان شود. خوب است متصدی امنیتی در نوشتن طرح آزمایش همکاری نماید. به خاطر داشته باشید امکان دارد آزمایش نازهای امنیتی مشکل باشد. (اثبات اینکه مزاحمی قادر به دیدن اطلاعات حساس نیست سخت است)

فاز ٤ اجرا

فاز اجرایی پروژه، نیازهای امنیتی خاص خود دارد. در طی این پروسه، تیم اجرا باید پروسه مدیریت پیکره بندی صحیحی را بکار ببرد. علاوه بر این قبل از آنکه سیستم جدیدی به بهره برداری برسد لازم است متصدی امنیتی سیستم را از لحاظ وجود راه های نفوذ و برآورده شدن صحیح سیاست امنیتی مورد بررسی قرار دهد.

تدابیر جبران حادثه

هر سازمانی باید طرحی برای جبران حادثه که به اختصار DRP گفته می شود داشته باشد. اما بسیاری از سازمانها هیچ طرحی در این زمینه ندارند، چون فراهم کردن آنرا بسیار پرهزینه می دانند و نیازی به فراهم کردن hot stie نمی بینند (منظور از hot stie مجموعه کاملی از ادوات و سیستم های آماده بکار در مکان دیگر است که در هنگام بورز حادثه بلافاصله جایگزین سیستم اصلی می شود و از قطع سرویس دهی جلوگیری می کند).

DRP لزوماً به hot stie نیاز ندارد بلکه DRP طرحی است که سازمان به هنگام بروز بدترین شرایط دنبال می کند. شاید این طرح سند بسیار ساده ای باشد که به متصدی اصلی می گوید به هنگام بروز آتش سوزی ساختمان، به رستوران محلی برود. اسناد دیگر می تواند پیچیده تر باشد و تعیین کند در صورت از کار افتادن یک یا همه سیستمهای کامپیوتری سازمان چگونه به عملکرد خود ادامه دهد.

اگر DRP به درستی تنظیم شود سطوح مختلفی از خرابی بصورت خرابی تک سیستم، خرابی مرکز دیتا و خرابی کل سایت خواهد داشت.

خرابی تک سیستم

بروز خرابی سیستم بسیار محتمل است. این نوع خرابی می تواند در مادربورد ، کارت واسطه شبکه دیسک حافظه خوان و اجزای دیگر بوجود ید. به عنوان بخشی از روند DRP لازم است محیط سازمان از نظر خرابیکه روی هر

یک از ادوات یا سیستم های تکی ایجاد می کند مورد بررسی قرار گیرد و برای هر خرابی طرحی وجود داشته باشد تا بر اساس آن عملکرد کلی برای زمان معقولی قابل ادامه باشد. این مدت به حساسیت سیستم مورد نظر بستگی دارد. به عنوان مثال سایت کارخانه ای را در نظر بگیرید که فقط با یک سستم ایجاد شده است و برنامه زمانبندی تولیدات، تدارکات و سفارشات بر عهده آن است. در این صورت لازم است این سیستم همیشه در حال کار باشد، در غیر اینصورت تولید کارخانه متوقف خواهد شد. این نوع خرابی را می توان با داشتن یک سیستم یدکی آماده به کار حل کرد و یا اینکه مجموعهای از سیستم ها در سایت کارخانه استفاده شود بطوریکه وظایف بین آنها تقسیم شود. انتخاب هر یک از این دو راه حل بستگی به هزینه هر یک دارد.

صرف نظر از اینکه چه راه حلی برگزیده شود، DRP می گوید چه کارهایی انجام شود تا بدون از کار افتادن سیستم، عملکرد کلی ادامه پیدا کند. لازم است DRP با همکاری و اطلاع بخش عملیاتی سازمان نوشته شود تا آنها هم بدانند به هنگام بروز خرابی برای ادامه دادن عملکرد کلی، چه مراحلی را دنبال نمایند.

پیشامدهای مرکز دیتا

DRP باید برای پیشامدهای مهمی که احتمالاً در مرکز دیتا اتفاق می افتاد پروسه هایی را تعیین کند. برای مثال در صورت بروز آتش سوزی و بلا استفاده شدن مرکز دیتا، چه مراحلی برای احیای مجدد قابلیت های سیستم انجام گیرد. یکی از ملاحظاتی که باید مد نظر قرر گرد، امکان از دست دادن تجهیزات است لذا در طرح مذکور باید ذخیره کردن تعدادی تجهیزات یدکی لحاظ شود.

در صورتیکه مرکز دیتا غیرقابل استفاده شود اما بقیه امکانات موجود باشد، مکانی که باید تجهیزات جدید به آنجا برده شود و خطوط ارتباطی که باید برپا شود توسط DRP تعیین می شود. استفاده از hot stie هم یک گزینه برای

این نوع پیشامد می باشد اما هزینه بر است. اگر hot stie جزء طرح نباشد لازم است سازمان مکانهای مناسب دیگری را برای تجهیزات مورد بررسی قرار دهد تا در صورت لوم سیستم های کامپیوتری بازسازی گردد.

همانند آنچه درباره خرابی سیستم تکی گفته شد در اینجا هم DRP باید تعیین کند در طول بازسازی سیستم سازمان چگونه عملکرد خود را ادامه دهد.

پیشامدهای سایت

پیشامدهایی که باعث نابود شدن سایت می شود نوعی از وقایع است که به هنگام صحبت درباره DRP بیشتر به آن پرداخته می شود. اگر چه احتمال وقوع این نوع وقایع حداقل است اما بیشترین ضرر و صدمه را به سازمان وارد می کند. در طرح ریزی DRP برای اینگونه وقایع لازم است هر بخش از سازمان در ایجاد آن سهیم باشد (قادر به ایجاد قسمت خودش باشد). اولین قدم سازمان تشخیص آن دست از قابلیت های حیایت است که به منظور باقی ماندن سازمان باید مجدداً برپا شود. اگر سازمان یک سایت E-commerce باشد، شبکه و سیستم های کامپیوتری بحرانی ترین بخش آن می باشد. از طرف دیگر در صورتیکه سازمان نوعی کارخانه تولیدی باشند، عملکرد کارخانه به مراتب مهم تر از سیستم های کامپیوتری می باشد.

آزمایش DRP سندی بسیار پیچیده است و احتمال اینکه در اولین مرتبه از نوشتن به موفقت منجر شود کم است. از اینرو لازم است DRP مورد آزمایش قرار گیرد. آزمایش DRP نه تنها از صحیح بودن DRP در زمان حال اطمینان حاصل می کند، بلکه باقی ماندن به همین حالت را هم مورد آزمایش قرار می دهد.

آزمایشات DRP برای سازمان بسیار پر خرج و از هم گسیخته است. بنابراین مناسب است سازمان پرسنل کلید را شناسایی کند و آزمایش را بطور دوره ای روی آنها انجام دهد و آزمایشات تمام عیار و همه جانبه ای را بطور سالانه اجرا کند.

ایجاد سیاست مناسب

بعد از آنکه تمام سیاست هایی که یک سازمان ممکن است داشته باشد را تشریح کردیم بیایید از ایجاد سیاستی صحبت کنیم که برای سازمانتان مناسب خواهد بود. سازمانها با هم تفاوت دارند پس هر سازمانی سیاست متفاوتی خواهد داشت. البته این بدان معنا نیست که الگوی کلی سیاست ها قابل استفاده نمی باشد، بلکه استفاده از الگو برای هر سازمانی بسیار آموزنده است، اما کپی کردن سیاست سازمان دیگر بصورت کلمه به کلمه نمی تواند بهترین روش در ایجاد سیاست شما باشد.

شناسایی آنچه اهمیت دارد

اولین قدم در ایجاد سیاست سازمان، تشخیص سیاست هایی است که برای شما مهم می باشد. لزوماً هر سیاستی برای هر سازمانی نیاز نمی باشد. علاوه بر این براساس موقعیتی که سازمان شما در آن قرار دارد بعضی سیاست گذاری ها از بقیه مهم تر می باشد. برای مثال سازمانی که روی اینترنت اطلاعات ارسال می کند بیش از آنکه به سیاست استفاده از کامپیوتر نیاز داشته باشد، به طرح جبران حادثه نیاز دارد.

متصدی امنیتی سازمان باید قادر به تشخیص این مسئله باشد که کدام سیاست بیشترین اهمیت را دارد. در غیر اینصورت لازم است برآوردی از خطر در این حوزه ارائه گردد. علاوه بر این لازم است متصدی امنیتی به دنبال دستیار از مدیریت سیستم، منابع انسانی و اداره نماینده عمومی باشد تا مهم ترین و با اهمیت ترین سیاست ها را بدست آورد.

تعیین رفتار قابل قبول

بعضی از رفتارهای پرسنلی قابل قبول و بعضی دگر غیر قابل قبول هستند، قابل قبول بودن رفتار به فرهنگ حاکم در سازمان بستگی دارد. به عنوان مثال ممکن است سازمانی به پرسنل خود اجازه دهد بدو ن هیچ محدودیتی در اینترنت سیر کنند. به این ترتیب فرهنگ این سازمان بر پایه پرسنل و مدیران آنها شکل می گیرد بطوریکه آنچه اهمیت دارد تکمیل کار است. بعضی دیگر از سازمانها روی دسترسی بعضی از پرسنل به اینترنت محدودیت قرار می دهند و حتی با نصب بعضی نرم افزارهای خاص، دسترسی افراد به وب سایتهای غیر قابل قبول را محدود می نمایند.

سیاست هر سازمان بصورت قابل توجهی با دیگری تفاوت دارد. در واقع امکان دارد سازمان اول تصمیم بگیرد سیاست استفاده از اینترنت را به هیچ وجه بکار نبرد. به خاطر داشتن این نکته در حرفه امنیتی مهم است که هر سیاست گذاری با هر سازمانی مطابقت ندارد. بنابراین قبل از اعمال هر سیاستی لازم است وقت صرف شود تا فرهنگ حاکم بر سازمان و انتظاری که سازمان از پرسنل خود دارد، فرا گرفته است.

شناسایی بخش های تأثیر گذار

سیاستی که در یک فضای بسته ایجاد شود بندرت به موفقیت دست پیدا می کند. با توجه به این نکته لازم است متصدی امنیتی در تبیین سیاست گذار از دیگر اعضای سازمان کمک بگیرد. مسائل امنیتی باید با مشورت نماینده عمومی سازمان و بخش منابع انسانی توسعه و بسط داده شود. از وجود گروه های دیگر هم می توان استفاده کرد. این گروه های عبارتند از مدیریت سیستم، کاربران سیستم کامپیوتری و بخش امنیت فیزیک. خلاصه کلام اینکه همه کسانی که از سیاست اعمالی متأثر می شوند باید در پروسه ایجاد و بسط آن سهم باشند. بدین ترتیب درباره آنچه از آنها انتظار خواهد رفت در ک درستی پیدا می کنند.

تعیین رئوس مطالب

توسعه سیاست گذاری با طرح ریزی خوب شروع می شود. برای مثال RFC 2196 با نام سایت هندبوک امنیتی تعداد از رئوس مطالب را برای سیاست گذار های مختلف ارائه می کند.

ایجاد سیاست

بخش امنیت سیاست های امنیت را به عهده بگیرد. منظور از این عبارت این نیست که بخش امنیت این کار را بدون گرفتن اطلاعات از دیگر بخش ها انجام دهد بلکه منظور این است که بخش امنیت مالکیت پروژه را به عهده دارد و آنچه را اتفاق می افتد تحت نظر دارد.

پروسه را با رئوس مطالبی که آماده کرده اید و پیش نویسی از هر یک از بخش های سیاست گذاری شروع کنید. همزمان با افرادی که از سیاست متأثر می شوند تماس گرفته و پروژه را با آنها در میان بگذارید. از آنها دعوت کنید که بخشی از پروژه باشند. به کسانی که به این دعوت پاسخ مثبت می دهند پیش نویسی از سیاست گذاری تحویل دهید و با برگزاری یک جلسه، پیش نویس مذکور را برایشان تشریح نمایید. با توجه به اندازه سازمان و نوع سیاستی که بکار می رود ممکن است به بیش از یک جلسه نیاز داشته باشید.

در هر جلسه بخش امنیت باید به عنوان رئیس جلسه عمل کند. سیاست را بخش به بخش تشریح کند، تعبیر تمام افراد را گوش کند و هر یک را توضیح دهد. البته به خاطر داشته باشید که ممکن است تعابیر نادرستی از آن سیاست وجود داشته باشد. در این حالت بخش امنیتی باید دلیل بروز هر خطر و افزایش آنرا ارائه دهد بطوریکه تمام حضار دلیل انتخاب های انجام شده در سیاست گذار را کاملاً درک نمایند.

خوب است همین پروسه را در پیش نویس نهایی تکرار نمایید. وقتی پیش نویس تکمیل گردید آنرا برای تأئید و اجرا به مدیریت تحویل دهید.

اعمال سیاست

ایجاد سیاست کار آسانی است بطوریکه برای ایجاد آن افراد کمی نیاز است. اما برای اعمال موثر سیاست باید با کل سازمان کار کنید.

سهیم کردن

هر بخش از سازمان که از سیاست اعمالی متأثر میشود باید در مفهوم واقعی سیاست شریک باشد. به این ترتیب کارها آسانتر می شو، چون تمام افرادی که تحت این سایت قرار می گیرند در ایجاد آن نقش پیدا می کنند. میتوانید به مدیریت آن بخش نشان دهید که یکی از افراد آن بخش در ایجاد سیاست گذاری شریک شده است و به این ترتیب اعلام کنید به آنها اهمیت داده اید.

از جمله مواردیکه میتواند کمک کند بیان مطلب از طرف مدیریت بالاتر است چون باعث میباشد در اجرای آن سیاست راه شما آسانتر شود و در شریک کردن بخشهای مختلف سازمان کمک خواهد کرد.

آموزش لازم است پرسنلی که تحت تأثیر سیاست جدید قرار می گیرند بر اساس میزان مسئولیت آنها آموزش داده شوند. منظور از این مسئولت میزان پاسخگویی امنیتی است. اگر چه بخش های آموزش و منابع انسانی می توانند به این امر کمک کنند، اما آموزش پرسنل به عهده بخش امنیتی است. این مسئله بخصوص زمانیکه تغییرات اعمالی مستقیماً روی تمام کاربران تأثیر می گذارد اهمت دارد. به عنوان مثال، تغییر در سیاست کلمه عبور را در نظر بگیرید. صبح شنبه باید کلمات عبور کاربران طولی برابر هشت کاراتر داشته باشند، بطوریکه ترکیبی از حرف و شماره باشد و برای ۳۰ روز اعتبار داشته باشد. زمانیکه این تغییر را در ویندوز انجام می دهید، بلافاصله کار تمام می شود. این مسئله هر کاربر را مجبور می کند تا صبح شنبه کلمه عبورش را عوض کند. عدم آموزش کاربران باعث می شود کاربران کلمات عبور را درست انتخاب نکنند یا با بخش پشتیبانی تماس بگیرند. به همین ترتیب اگر

کاربران نتوانند کلمه عبور انتخاب خود را به خاطر بیاورند، هر روز با بخش پشتیبانی تماس می گیرند و عملاً کلمه عبور از کار می افتد. هیچ یک از این دو حالت برای سازمان خوب نیست.

راه بهتر این است که با مشاور آموزش امنیتی تماس بگیرید. در آنجا تغییرات اعمالی به پرسنل گفته می شود و آنها آموزش داده می شود چگونه کلمه عبور قدرتمندی را انتخاب کنند بطوریکه به خاطر آوردن آنهم آسان باشد. همزمان باید تغییرات اعمالی به بخش پشتیبانی اطلاع داده شود تا آنها هم در جریان قرار بگیرند. بخش امنیتی می تواند با همکاری مدیریت سیستم راهی پیدا کند تا تمام پرسنل مجبور نباشند تغییرات را در یک روز انجام دهند و تغییرات بعضی از کاربران به تعویق انداخته شود. این راه باعث می شود تحولات بصورت آهسته انجام شود.

اجرا

چنانچه در مثال بالا بخش قبل نشان داده شد اعمال تغییرات بنیادی برای سازمان ضرر دارد. در عوض تغییرات تدریجی که به خوبی طرح ریزی شده باشد بسیار بهتر است. به این ترتیب بخش امنیتی باید از همکاری مدیریت سیستم و دیگر بخش های تحت تأثیر بهره مند شود تا تغییرات را به آسانی انجام دهد. به خاطر داشته باشید عموماً به مقوله امنیت به عنوان مانعی برای انجام کار نگریسته می شود پس دلیلی ندارد این ایده را به اثبات برسانیم.

استفاده موثر از سیاست

اگر چه می توان از سیاست سازمان به عنوان اهرم فشار استفاده کرد اما اینکار به ندرت موثر خواهد بود. در عوض استفاده از آن بعنوان ابزاری آموزشی بسیار موثرتر می باشد. به خاطر داشته باشید اکثر پرسنل به سازمان خود علاقه و توجه دارند و سعی دارند وظیفه خود را به بهترین نحوی که بتوانند انجام دهند.

پروژه و سیستم های جدید

وقتی پروژه یا سیستم جدیدی راه اندازی می شود باید سیاست امنیتی و پروسه طراحی جاری دنبال شود. این مسئله به بخش امنیتی امکان می دهد بخشی از فاز طراحی پروژه باشد و بتواند در ابتدای پروسه نیازهای امنیتی را شناسایی کند.

اگر سیستم جدید قادر به معرفی نیازهای امنیتی نباشد به سازمان فرصتی داده می شود تا خطر اضافه شده از این طریق را بفهمد و مکانیزم های دیگری را برای مدیریت خطر افزوده شده فراهم کند.

پروژه و سیستم های موجود

همچنانکه سیاست های جدید ایجاد می شود لازم است سیستم های موجود هم تحت بررسی و آزمایش قرار گیرد تا معین گردد آیا می تواند مورد تصویب این سیاست قرار گیرد. بخش امنیتی باید برای اعمال تغییرات مناسب با مدیریت سیستم و بخش هایی که از سیستم ها استفاده می کنند همکاری کند. شاید این کار مستلزم فراهم آوردن برخی تغییرات توسعه ای باشد که فوراً قابل اجرا نباشد. بخش امنیت باید احتمال وقوع برخی تأخیرات را درک کند و برای آنکه از انجام به موقع تغییرات مطابق با برنامه و طراحی سستم اطمینان حاصل شود با مدیریت همکاری کند.

بازرسی

بسیار از سازمان ها دارای بخشی بازرسی داخلی هستند که سیستم ها را از نظر مطابقت با سیاست بطور دوره ای بازرسی می نمایند. بخش امنیتی باید درباره سیاست جدید به بخش بازرسی نزدیکی شود و با آنها همکاری کند، بطوریکه بازرسان قبل از آنکه گزارشی بر خلاف سیاست تهیه کنند سیاست گذاری را در ک کرده باشند. این تبادل باید بصورت دو طرفه انجام گیرد. بخش امنیتی باید چگونگی ایجاد سیاست و انتظاراتی را که از سیاست دارد

برای بازرسی توضیح دهد. متقابلاً بازرسی باید چگونگی بازرسی ها و آنچه که دنبال آن می باشد را برای بخش امنیتی تشریح نماید. علاوه بر آن لازم است توافقاتی درباره سیستم هایی که برای بخش های مختلف سیاست در نظر گرفته شده است انجام گیرد.

بازبینی سیاست

حتی یک سیاست خوب نمی تواند همیشگی باشد. هر سیاستی باید بطور منظم مورد بازبینی قرار گیرد تا از مناسب بودن آن برای سازمان اطمینان حاصل گردد. انجام اینکار بصورت سالی یکبار برای اکثر سازمان ها مناسب است. بعضی از پروسه ها از بیل پروسه واکنش به حادثه یا طرح جبران احتمالاً به بازبینی سریعتر نیاز خواهد داشت.

فصل پنجم

روند بهینه در امنیت اطلاعات

«روند بهینه» به مجموعه توصیه هایی اشاره دارد که عموماً سطح امنیت مناسبی فراهم می کند. روند بهینه حاصل ترکیب روش هایی است که در سازمان های متفاوت بیشترین تأثیر را دارد. این روش ها برای هر سازمانی کفایت نمی کند بطوریکه برخی سازمانها برای رسیدن به مدیریت مناسبی از خطرپذیری نیاز به سیاست، پروسه، آموزش و کنترل های فنی امنیتی بیشتری خواهند داشت.

روندی که در این فصل تشریح می گردد نقطه شروعی برای سازمان شما است. این روند و فعالیت ها همراه با ارزیابی خطرات بکار برده می شود تا معیارها و سنجشهایی که باید در محل قرار داده می شد، اما قرار داده نشده است و همینطور معیارها و سنجشهایی که در محل قرار داده شده است اما بی تأثیرند شناسایی گردد.

امنیت مدیریتی

مواردی که در حوزه های سیاست و پروسه ها، منابع ، مسئولیت پذیری، آموزش و طرح های احتمالی قرار می گیرد جزو فعالیت های امنیت مدیریتی قرار دارد. این اقدامات سعی دارند اهمیت اطلاعات سیستم های اطلاعاتی شرکت را شناسایی کنند و آنرا برای پرسنل تشریح نمایند. علاوه بر این روند امنیت مدیریتی ، منابع مورد نیاز برای مدیریت خطر پذیری را شناسایی می کند و فردی که باید در قبال مخاطرات متوجه سازمان جوابگو باشد تعیین می‌شود.

سیاست ها و پروسه ها

سیاست امنیتی سازمان، روش امنیتی در نظر گرفته شده برای سازمان را تعیین می کند. پس از تبیین سیاست انتظار می رود اکثر پرسنل از آن تبعیت کنند. چنانچه قبلاً هم گفته شد باید این نکته را در نظر داشته باشید که برآورده

شدن کامل سیاست اتفاق نخواهد افتاد. در برخی موارد بدلیل نیازهای تجاری از سیاست تبعیت نمی شود. در موارد دیگر بدلیل آنکه دنبال کردن سیاست سختیهایی در پی دارد از آن صرف نظر می شود.

حتی با وجود این حقیقت که همیشه از سیاست پیروی نمی شود، ترکیبی کلیدی از برنامه قدرتمند امنیتی توسط سیاست شکل می گیرد. از اینرو لازم است مجموعه ای از فعالیت ها و روندهای توصیه شده در آن لحاظ شود. بدون وجود سیاست پرسنل نمی دانند سازمان برای حفاظت از اطلاعات و سیستم ها چه انتظاری از آنها دارد.

در حداقل موارد، سیاست های زیر بعنوان روند بهینه توصیه می شود:

- سیاست اطلاعاتی: میزان حساسیت اطلاعات سازمان را تعیین می کند و نحوه صحیح ذخیره، انتقال، علامتگذاری و نیازهای مصرفی آن اطلاعات را تعیین می کند.
- سیاست امنیتی : کنترل های فنی و پیکره بندی امنیتی مورد نیاز کاربران و مدیریت ها را برای پیاده سازی روی تمام کامپیوترها تعیین می کند.
- سیاست استفاده: استفاده های مجاز از سیستم های کامپیوتری سازمان و جریمه استفاده نادرست از این سیستم ها را تعیین می کند. این سیاست روش مورد قبول برای نصب نرم افزار روی سیستم کامپیوتری را هم تعیین می کند.
- سیاست بک آپ: دوره زمانی مورد نیاز برای تهیه بک آپ (پشتیبان) از اطلاعات و نیازهای انتقال این اطلاعات به محل دیگر را تعیین می کند. در سیاست بک آپ می توان طول زمانی که اطلاعات باید قبل از استفاده مجدد به حالت ذخیره باقی بماند را تعیین نمود.

سیاست ها نمی توانند به تنهایی راهنمای سازمان در برنامه امنیتی باشند. از اینرو لازم است پروسه هایی هم تعیین گردد تا راهنمای پرسنل به هنگام تنظیم سند خاص و تعیین مراحل مورد نیاز در وضعیت های مختلف امنیتی گردد.

پروسه هایی که باید برای سازمان تبیین گردد عبارتند از:

- **پروسه مدیریت کاربر**

این پروسه اطلاعاتی از قبیل اینکه چه کسی به کدام یک از کامپیوترهای سازمان اجازه دسترسی دارد را شامل می شود و تعیین می کند برای آنکه مدیریت سیستم بتواند هویت کاربران را شناسایی کند به چه اطلاعاتی نیاز دارد. در پروسه مدیریت کاربر تعیین می شود هنگامیکه مجوز یکی از پرسنل باید لغو شود چه کسی مسئول خبر دادن به مدیریت سیستم خواهد بود؟ ابطال مجوز دسترسی از این جهت اهمیت دارد که فقط افرادی با نیاز تجاری واقعی قادر به دسترسی به سیستم ها و شبکه های سازمان باشند.

- **پروسه مدیریت پیکره بندی**

این پروسه مراحل لازم برای ایجاد تغییر در سیستمهای تولیدی را تعیین می کند. این تغییرات شامل ارتقای نرم افزاری و سخت افزاری ، روی خط آوردن سیستم های جدید و حذف سیستم های غیر ضروری می باشد.

منابع

پیاده سازی صحیح روند امنیتی به تخصیص منابع نیازدارد. متأسفانه برای تعیین میزان منابعی که برنامه امنیتی نیازدارد (بر حسب پول یا پرسنل) فرمولی وجود ندارد تا مثلاً بر حسب اندازه سازمان آنرا تعیین کرد. این مسئله به متغیرهای زیادی بستگی دارد. منابع مورد نیاز به عواملی از قبیل اندازه سازمان، تجارت سازمان و میزان مخاطره ای که متوجه سازمان است بستگی دارد.

می توان با کلی گویی گفت میزان منابع براساس ارزیابی کامل و صحیحی از خطر پذیری سازمان و طرحی است که برای خطرپذیری ریخته می شود. برای تعیین صحیح منابع مورد نیاز لازم است برنامه مدیریت پروژه را اعمال

نمایید. اگر با برنامه امنیتی به عنوان یک پروژه رفتار شود، سازمان باید برای ایجاد توازن در مثلث، برای افزایش زمان یا کاهش وسعت پروژه منابع کافی صرف کند.

متصدی

صرف نظر از اینکه سازمان بزرگ و یا کوچک باشد لازم است به منظور مدیریت خطرپذیری در امنیت اطلاعات، به برخی پرسنل وظایف ۰خاص واگذار شود. در یک سازمان کوچک این وظایف به یکی از اعضای متصدی فنی اطلاعاتی واگذر می شود حال آنکه سازمان بزرگتر دارای بخشی است که به امنیت اختصاص داده شده است. روند بهینه اندازه متصدی را تعیین نمی کند اما شدیداً پیشنهاد متصدیان بخش امنیت باید مهارتهای زیر را داشته باشند:

- مدیریت امنیتی : فهمیدن روز به روز ادوات اداری
- ایجاد سیاست : تجربه ایجاد و نگهداری سیاست ها، پروسه ها و طرح های امنیتی
- معماری : فهمیدن معماری شبکه، سیستم و پیاده سازی سیستم های جدید
- تحقیق: آزمودن تکنولوژی جدید امنیتی و دیدن چگونگی اثر خطرات روی سازمان
- ارزیابی: تجربه ارزیابی خطرپذیری سازمان، مهارت ارزیابی شامل تست نفوذ امنیتی
- بازرسی: تجربه اداره بازرسی های سیستم و پروسه ها

اگر چه تمام این مهارت ها برای سازمان مفید است اما سازمان کوچک نمی تواند تمام این مهارتها را به متصدی تحمیل کند. در این مرد مقرون به صرف ترین کار این است که متصدی مهارت های مدیریت امنیتی و ایجاد سیاست را داشته باشد و برای مهارت های دیگر از شرکتهای خارجی کمک گرفته شود.

بودجه

بودجه امنیتی یک سازمان به وسعت پروژه امنیتی آن سازمان بستگی دارد تا اینکه متأثر از اندازه سازمان باشد. امکان دارد سازمانی که دارای برنامه های امنیتی قویتری است از سازمان کوچکتری که برای ساخت یک برنامه امنیتی شروع بکار کرده است بودجه کمتری داشته باشد.

یکی از مهم ترین مسائل بودجه امنیتی رعایت توازن در آن است بطوریکه بودجه امنیتی باید بین هزینه های توسعه، عملکردهای جاری و آموزش تقسیم شود. بسیاری از سازمانها این اشتباه را مرتکب می شوند که ابزارهای امنیتی را خریداری می کنند اما پول کافی برای آموزش آن ابزارهای در بودجه نمی گنجانند. از طرف دیگر سازمان ابزارهایی خریداری می کند به امید اینکه بتواند از تعداد پرسنل و متصدیان بکاهد یا حداقل اینکه تعداد آنها را در سطح جاری نگه دارد. در اغلب موارد ابزارهای جدید امنیتی باعث کاهش تعداد پرسنل نمی شود.

بودجه ای که با روند بهینه تطبیق داشته باشد باید مطابق با طرح های پروژه امنیتی باشد (که به نوبه خود مطابق با مخاطراتی است که متوجه سازمان است). برای تکمیل طرح های پروژه امنیتی لازم است پول کافی در بودجه صرف شود.

مسئولیت و پاسخگویی

به منظور مدیریت خطر پذیری در امنیت اطلاعات لازم است به برخی موقعیت های سازمان مسئولیت واگذر شود. اخیراً در سازمانهای بزرگ رسم شده است این مسئولیت به موقعیتی با سطح اجرایی خاص به نام رئیس امنیت اطلاعات یا CISO واگذر شود. طرف نر از میزان بزرگی سازمان، موقعیتی با سطح اجرایی باید این مسئولیت را داشته باشد. در برخی سازمانها از رییس بخش مالی برای وظایف امنیتی استفاده می شود در حالیکه در برخی دیگر، از رئیس بخش اطلاعات یا رئیس بخش فنی بدین منظور استفاده ld شود.

صرف نظر از اینکه از کدام موقعیت با سطح اجرایی استفاده می شود لازم است به آن فرد فهمیده شود امنیت بخش مهمی از وظیفه و شغل او می باشد. موقعیت اجرایی باید اجازه تعیین سیاست سازمان را داشته باشد و بتواند در تمام سیاستهای مرتبط با امنیت دخالت کند. این موقعیت باید قادر به اعمال سیاست روی مدیریت های سیستمی و کسانی که عهده دار امنیت فیزیکی سازمان هستند باشد.

از بخش اجرایی انتظار نمی رود وظایف و مدیریت های امنیتی را روز به روز اجرا کند. این وظایف را می توان به متصدی امنیتی محول کرد. رئیس امنیت سازمان باید معیار و استانداردی تعیین کند تا براساس آن نیل به اهداف امنیتی قابل سنجش و ارزیابی باشد. مواردی از قبیل تعداد آسیب پذیری سیستم ، جریانهایی که علیه پروژه امنیتی وجود دارد، و فرآیندی در جهت روند بهینه می تواند این معیارها را تشکیل دهد.

آموزش

یکی از مهم ترین بخش های مدیریت خطرپذیری در امنیت اطلاعات، مبحث آموزش پرسنل است. اگر پرسنل دانش و تعهد لازم را نداشته باشند هر تلاشی برای مدیریت خطرپذیری بیهوده خواهد بود. در روند بهینه پیشنهاد می شود آموزش دارای سه شکل باشد:

- اقدامات پیشگیرانه
- اقدامات تنبیهی
- اقدامات تشویقی

اقدامات پیشگیرانه

به پرسنل جزئیات مربوط به اقداماتی که با محافظت از منابع اطلاعاتی سازمان مرتبط است ارائه می شود. به پرسنل گفته می شود چرا سازمان از منابع اطلاعاتی خود حفاظت می کند، و چگونه اتخاذ این اقدامات پیشگیرانه باعث می شود پرسنل بهتر بتوانند سیاست های سامان را برآورده کنند. اگر دلایل امنیتی برای پرسنل تشریح نشود امکان دارد انها بدنبال راههایی بگردند که از سیاست ها و پروسه های اتخاذ شده شانه خالی نمایند.

اقدامات پیشگیرانه قوی دارای شکل های زیادی است. برنامه های اطلاع رسانی که شامل تبلیغات و آموزش پرسنل است و مقاله های خبری و پوستر و همینطور پیام های پست الکترنیک که مسئولت پرسنل را به آنها یادآوری کند نمونه هایی از این اقدامات می باشد. در این تبلیغات عنوانهای اصلی باید بصورت زیر باشد:

- اشتباهات عمومی پرسنل از قبیل نوشتن و به اشتراک گذاشتن کلمه عبور
- فراموش کاریهای عمومی از قبیل دادن اطلاعات اضافی به تماس گیرنده
- اطلاعات مهم امنیتی
- عناوین رایج امنیتی از قبیل ضد ویروس و امنیت دسترسی از راه دور
- عناوینی که به پرسنل کمک میکند، مثل اینکه در سفر چگونه از کامپیوتر محافظت شود.

لازم است در تمام ملاقاتها و گردهمایی ها سازمان، اطلاع رسانی امنیتی به پرسنل مدنظر قرار گیرد. پرسنل جدید باید در کلاسهای کوتاه تحت آموزش قرار گیرند و پرسنل دیگر همان کلاسها را هر دو سال یکبار بگذرانند. این کلاسها باید اطلاعات زیر را پوشش دهند:

- چرا امنیت برای سازمان اهمیت دارد؟
- مسئولت پرسنل در قبال مسئله امنیت کدام است؟
- اطلاعات مفصل درباره سیاست های سازمان در حفاظت از اطلاعات
- اطلاعات مفصل درباره سیاست استفاده در سازمان

- روش های انتخاب کلمه عبور قدرتمند
- رو شهای پرهیز از بروز حملات مهندسی اجتماعی

مدیریت ها باید ضمن اینکه از آموزش های ابتدایی پرسنل بهره مند می شوند باید آموزش های دیگری درباره مسئولیت خاص خود بگذرانند. آموزش های اضافی مذکور باید کوتاهتر بوده (حدوداً نیم ساعت) و عناوین زیر را در بر گیرد.

- آخرین روش هکرها
- تهدیدات رایج امنیتی
- آسیب پذیری های رایج امنیتی و نرم افزارهای مکمل (patch)

تولید کننده های نرم افزار باید آموزش پایه ای اطلاع رسانی پرسنل را بگذرانند. این کلاسها باید عناوین دیگری درباره مسئولیت این افراد در قبال امنیت در پروسه تولید نرم افزار را هم در بربگیرد. تمرکز این کلاسها باید روی روش تولید نرم افزار و پروسه های مدیریت پیکره بندی قرار داشته باشد.

از دیگر کارها می توان به برگزاری سمینارهای دوره ای برای ارائه وضعیت به تیم مدیریتی سازمان اشاره کرد که در جریان آن اطلاعات مفصل حاصل از ارزیابی خطر پذیری و طرح های موجود برای کاهش مخاطرات ارائه می شود. این سمینارها باید توضیح درباره معیارها و سنجش برنامه امنیتی توسط این معیارها را در بر بگیرد.

در برنامه آموزشی، متصدی امنیتی را فراموش نکنید. اگر چه فرض می شود متصدی امنیتی مسئولیت هایش را همانند پرسنل درک کرده است با این حال باید ضمن آموزش با آخرین ابزارهای امنیتی و روش هکرها آشنا شود.

اقدامات تنبیهی

اکثر پرسنل به اقدامات پیشگیرانه جواب می دهند و سعی در دنبال کردن سیاست های سازمان دارند. با اینحال تعدادی از پرسنل قصور می کنند و باعث آزار سازمان می شوند. تعدادی از پرسنل خودسرانه از سیاست سازمان

سرپیچی می کنند. ازاینرو سازمان تصمیم می گیرد از دست این پرسنل خلاص شود. برای این منظور ابتدا سازمان باید ثابت کند این پرسنل در جریان اموزش های امنیتی قرار گرفته اند. به همین دلیل در جریان دوره های آموزش و پس از طی دوره از پرسنل خواسته می شود با امضای فرمهای خاص تعهد نمایند سیاست سازمان را دنبال خواهند کرد.

اقدامات تشویقی

با توجه به طبیعت خاص موضوعات امنیتی، پرسنل سازمان از اینکه آسیب پذیریها را به بخش امنیتی گزارش دهند اکراه دارند. از طرف دیگر چون پرسنل امنیتی قادر نیستند همه جا باشند و همه چیز را مشاهده کنند، لذا بهترین افرادی که سیستم هشدار دهنده امنیتی را ایجاد می کنند همان پرسنل سازمان می باشند.

یکی از روش هایی که گزارشات امنیتی را افزایش می دهد داشتن برنامه تشویقی است. لازم نیست این تشویق خیلی بزرگ باشد و مقدار کمی پول برای آن کافی است. پرسنل باید مطمئن شوند ارائه این گونه گزارشات کار خوبی است و به خاطر وجود خطا یا اشکال امنیتی مجازات نخواهند شد. علاوه بر این می توان با ارائه کارهای تشویقی پرسنل را تحریک کرد تا در جهت افزایش سطح امنیتی سازمان پیشنهادات سازنده ارائه دهند.

طرح های احتمالی و آتی

حتی تحت بهترین شرایط، نمی توان مخاطراتی که متوجه منابع اطلاعاتی سازمان است را کاملاً از بین برد به منظور اینکه عمل جبران و بازیابی به سریعترین وجه ممکن انجام شود و کمترین تأثیر را روی مسائل تجاری بگذارد باید طرح های احتمالی را تنظیم کرد.

واکنش در برابر حوادث

هر سازمانی باید برای واکنش در برابر حوادث پروسه ای داشته باشد که براساس آن مراحل لازم به هنگام تخریب یا نفوذ بیگانه تعیین می شود. بدون این پروسه، به هنگام مواجه شدن با حوادث زمان زیادی هدر خواهد رفت بطوریکه باعث تبلیغات بد علیه سازمان، ضرر تجاری و یا نفوذ اطلاعاتی می گردد.

در این پروسه تعیین می شود چه کسی برای واکنش در برابر حوادث به سازمان پاسخگو است. بدون داشتن دستورالعمل های واضح در این زمینه، زمان زیادی صرف خواهد شد تا در بین پرسنل آخرین فرد مسئول در برابر از کار افتادن یک سیستم پیدا شود و یا با نیروهای قانونی تماس گرفته شود.

در روند بهینه پیشنهاد می شود بطور دوره ای پروسه واکنش در برابر حادثه آزمایش نفوذ شود. تست های اولیه فقط جنبه اخطار دارد و ممکن است شامل جمع شدن پرسنل دور میز کنفرانس و صحبت درباره نحوه واکنش هر کس باشد. آزمایش های واقعی تر باید جایی طراحی شود که وقایع اخطاری مزاحمت های واقعی را شبیه سازی کند.

بک آپ و بایگانی دیتا

پروسه بک آپ (پشتیبان) براساس سیاست بک آپ انجام می گیرد. در این پروسه مان بک آپ گیری و مراحل لازم برای انجام عمل بک آپ و ذخیره آنها بصورت مطمئن تعیین می شود. در پروسه بایگانی دیتا تعیین می شود واسطه بک آپ هر چند وقت یکبار استفاده مجدد می گردد.

وقتی زمان پس گرفتن واسطه بک آپ (واسطه بک آپ می تواند فلاپی دیسک، سی دی و یا دیگر وسایل ذخیره دیتا باشد) از محل نگهداری آن فرا برسد، باید نحوه درخواست واسطه بک آپ ، نحوه ذخیره مجدد اطلاعات و چگونگی بازگرداندن واسطه بک آپ به محل نگهداری آن در پروسه تعیین شده باشد.

اگر سازمان چنین پروسه ای را بطور واضح تعیین نکرده باشد با این خطر روبرو خواهد بود که هر یک از پرسنل تفسیر متفاوتی از سیاست بک آپ داشته باشند، در نتیجه باعث می شود واسطه بک آپ به موقع به خارج انتقال داده نشود و عمل ذخیره اطلاعات بدرستی انجام نگیرد.

جبران حادثه

طرح های جبران حادثه به منظور برآورده کردن احتیاجات و لوازم مورد نیاز در هنگام بروز حادثه در محل امکانات سازمان قرار می گیرد. در این طرحها منابع کامپیوتری که از اهمیت بیشتری برای سازمان برخوردار است تعیین می شود و موارد لازم برای بازگرداندن منابع برای استفاده مجدد دقیقاً آماده می شود.

این طرح ها بگونه ای در محل پیاده سازی می شود که انواع حوادث، خواه از دست دادن فقط یک سیستم تا کل امکانات را تحت پوشش قرار دهد. علاوه بر این اجزاء زیر ساختی مهم و کلیدی همانند خطوط مخابراتی در این سناریو لحاظ می شود.

در طرح های جبران حادثه لزوماً از یک hot site استفاده نمی شود. hot site در واقع مجموعه کاملی از امکانات است که می تواند به هنگام بروز حادثه و از دست رفتن تجهیزات اصلی، جایگزین شود. با این حال طرح مذکور باید بگونه ای باشد که هزینه صرف شده برای آن با احتمال بروز خرابی در سازمان تناسب داشته باشد.

هر طرحی که برای جبران حادثه در نظر گرفته شده باشد باید بصورت دوره ای آزمایش شود بطوریکه حداقل سالی یکبار این آزمایش صورت گیرد. در این آزمایش پرسنل و متصدیان به سایت جایگزین نقل مکان می کنند.

طرح های پروژه امنیتی

از آنجا که امنیت فرآیندی پیوسته و مداوم است لذا باید با امنیت اطلاعات به عنوان پروژه ای پیوسته رفتار شود. با تقسیم بندی کل پروژه رفتار شود. با تقسیم بندی کل پروژه به پروژه های کوچکتر، کل طرح از انجام پروژه های کوچک تکمیل می گردد. در روند بهینه پیشنهاد می شود بخش امنیتی طرح های زیر را ایجاد کند.

- اصلاحی
- ارزیابی مخاطرات
- ارزیابی آسیب پذیر
- بازرسی
- آموزشی
- بازبینی سیاست

طرح های اصلاحی

طرح های اصلاحی به دنبال ارزیابی می آیند. اگر پس از ارزیابی معلوم شد ناحیه ای خطرپذیر وجود دارد ایجاد طرح های اصلاحی لازم می شود ت ابا انجام اصلاحات و تغییرات مناسب نواحی خطر پذیر از بین برود. طرح های اصلاحی می تواند شامل طرح هایی از قبیل ایجاد سیاست، ابزارهای اجرایی یا تغییرات سیستمی ، برگزاری برنامه های آموزشی باشد. هر بار که در سازمان ارزیابی انجام گیرد باید یک طرح اصلاحی پایه گذاری شود.

طرح های ارزیابی مخاطرات

در هر سازمان طرح های سالانه ای توسط بخش امنیتی ایجاد می شود که به ارزیابی مخاطرات متوجه سازمان می پردازد. در سازمانهای کوچک و متوسط این طرح های بصورت طرح همه جانبه و سالی یکبار اجرا می شود. در سازمانهای بزرگ این طرح روی هر بخش بصورت ارزیابی همه جانبه و با دوره های زمانی کوتاهتر اجرا می شود.

توجه: شاید بنظر برسد در مورد سازمانهای بزرگ، پیشنهاد ارزیابی بصورت سالی یکبار رعایت نشده است. در عمل انجام ارزیابی نیاز به زمانهایی برای ایجاد، اجرا و تحلیل دارد بطوریکه در سازمانهای بزرگ هر کدام از این کارها چند ماه وقت لازم دارد. لذا اگر ارزیابی بصورت همه جانبه و هر بار روی کل سازمان انجام گیرد قبل از آنکه تحلیل و تغییر مناسبی انجام گیرد نوبت ارزیابی بعدی فرا می رسد. لذا بهتر است ارزیابی های کوچکتر و پاره ای و با دوره زمانی کوتاهتر انجام گیرد.

طرح های ارزیابی آسیب پذیری

بخش امنیتی باید بطور منظم به ارزیابی آسیب پذیریهای سیستم بپردازد. این بخش تمام کامپیوترهای سازمان را بصورت ماهیانه بررسی و ارزیابی می کند. اگر تعداد کامپیوترهای خیلی زیاد باشد باید آنها را گروه بندی کرد و هر بخش را در یک هفته ارزیابی نمود. به منظور اطمینان از انجام فعالیتها لازم است طرح های مذکور به اطلاع مدیریت سیستم ها رسانده شود.

طرح های بازرسی

بخش امنیتی باید بازرسی هایی داشته باشد که براساس آن از برآورده شدن سایت سازمان اطمینان حاصل شود. این بازرسی ها روی مواردی از قبیل پیکره بندی کامپیوتر، سیاست بک آپ و یا حفاظت اطلاعات به فرم فیزیکی

تمرکز می کند. از آنجا که بازرسی نیاز به نیروی انسانی زیادی دارد لذا در هر بازرسی فقط بخشی از سازمان هدف قرار می گیرد، اگر در ان بخش معضلات قابل توجهی پیدا شد بازرسی بصورت گسترده تر و کامل انجام خواهد گرفت.

طرح های آموزشی

طرح های لازم برای آموزش های اطلاع رسانی توسط بخش منابع انسانی ایجاد و اجرا می شود. این طرحها شامل کلاسهای آموزش و اطلاع رسانی و طرح های تبلیغاتی نیز می شود. برنامه کلاسها بگونه ای طرح میشود که هر یک از پرسنل هر دو سال یکبار کلاس اطلاع رسانی را بگذراند.

طرح های بازبینی سیاست

بخش امنیتی با ایجاد طرح های لازم، سیاست های اتخاذ شده را مورد بازبینی قرار می دهد. عموماً لازم می شود هر سال حداقل دو سیاست بازبینی شود.

امنیت فنی

امنیت فنی روی کامپیوتر و شبکه، کنترل امنیتی اعمال می کند. این کنترل ها باعث آشکار سازی سیاست ها و پروسه های سازمان می گردد.

اتصال شبکه

انتقال اطلاعات بین سازمانهای مختلف در نتیجه رشد اتصالات بین شبکه های مختلف امکانپذیر شده است. از آنجا که سازمانها بدنبال استفاده از شبکه برای مقاصدی همچون ارتباطات، بازاریابی، تحقیقات و افزایش تجارت هستند لذا اتصال به اینترنت هم در حال گسترش و افزایش است. به منظور جلوگیری از ورود غیرمجاز به سازمان، روند بهینه موارد زیر را پیشنهاد می کند:

اتصال دائم

اتصالات دائم شبکه ای که به سازمانهای دیگر یا به اینترنت برقرار شده است توسط فایروال محافظت می شود. وظیفه فایروال این است که شبکه سازمان را از اینترنت یا شبکه سازمانهای دیگر تفکیک کند تا آسیب ایجاد شده در یک شبکه به شبکه دیگر سرایت نکند. فایروال بر حسب نیاز سازمان به یکی از صورت های روتر فیلتری، فایروال فیلتر بسته ای یا فایروال لایه کاربردی می باشد.

اتصال تلفنی

از آنجا که افراد غیر مجاز می توانند از طریق اتصال تلفنی به سازمان دسترسی پیدا کنند لذا محافظت از آن لازم است، و از آنجا که اتصال تلفنی همانند اتصال دائم امکان دسترسی به شبکه داخلی سازمان را می دهد بنابراین باید از اعتبار سنجی دو فاکتوری استفاده شود. مکانیزم های اعتبار سنجی دو فاکتوری مناسب به ترتیب زیر می باشد:

- مودم Dial- Back استفاده از این نوع مودم بهمراه مکانیزم اعتبار سنجی کفایت می کند. در این صورت مودم Dial- Back بگونه ای تنظیم می شود تا قبل از برقراری اتصال تلفنی، شماره را بگیرد. کاربری که سعی در برقراری تماس دارد نباید قادر به تغییر این شماره باشد. مودم Dial- Back برای کاربران متحرک (یا موبایل) مناسب نیست.

- کلمه عبور دینامیک یا پویا :اگر از کلمه عبور پویا با چیزهایی که کاربر می داند استفاده شود مکانیزم اعتبار سنجی مناسبی فراهم می شود.
- تجهیزات رمزنگاری: اگر از تجهیزات رمز نگاری قابل حمل با چیزهایی که کاربر می داند استفاده شود مکانیزم اعتبارسنجی خوبی ایجاد می شود. وسیله رمزنگاری با کلید رمزنگاری مناسبی از قبل بارگذاری می شود بطوریکه با چیزهایی که کاربر دارد ترکیب شده است.

هر یک از این مکانیزم ها برای اعتبار سنجی کاربرانی که قصد ارتباط از طریق خطوط تلفنی دارند مناسب است. این مکانیزم ها را می توان برای اتصالات VPN هم بکار برد.

حفاظت در برابر ویروس

یکی از شایع ترین تهدیداتی که متوجه اطلاعات سازمان است ویروسهای کامپیوتری است. از آنجا که تعداد و پیچیدگی ویروس ها بطور دائم در حال افزایش است لذا باید احتمال وجود ویروس و سوءاستفاده از نرم افزارهای کاربردی را همیشه در نظر داشته باشید. ویروس از سه روش عمده وارد سازمان می شود:

- فایل هایی که بین کامپیوتر خانگی و کامپیوتر کاری به اشتراک گذاشته شده است.
- فایل هایی که از اینترنت دان لود می شوند.
- فایل هایی که با ضمیمه شدن به پیام های پست الکترونیک به سازمان وارد می شود.

به منظور مدیریت این خطر، روند بهینه پیشنهاد می کند برنامه ضد ویروس قدرتمندی برای سازمان ایجاد و نصب گردد. چنین برنامه ای ویروس را در سه نقطه زیر کنترل می کند:

- سرور: نرم افزار ضد ویروس روی تمام سرورهای فایل نصب می شود و بگونه ای تنظیم می شود تا بصورت دوره ای تمام فایل های را از لحاظ وجود ویروس کنترل کند.

- کامپیوترهای رومیزی (descktop): نرم افزار ضد ویروس روی تمام کامپیوترهای رومیزی نصب می شود و بصورت دوره ای تمام فایل ها را از نظر وجود ویروس کنترل می کند. علاوه بر این نرم افزار ضد ویروس بگونه ای تنظیم می شود تا هر فایلی که باز میشود را کنترل کند.
- سیستم های پست الکترونیک: نرم افزار ضد ویروس روی سرور اصلی پست الکترونیک یا در مسیر ورود پیامهای پست الکترونیک به سازمان قرار داده میشود. نرم افزار بگونه ای تنظیم می شود که قبل از تحویل فایل به کاربر آنرا کنترل می کندو

نصب، پیکره بندی و تنظیم نرم افزار ضد ویروس فقط نیمی از راه حل مقابله با مشکل ویروس است. به منظور تکمیل اینکار لازم است نرم افزار مرتباً به روز شود. به روز کردن نرم افزار ضد ویروس براساس توصیه سازنده آن انجام می گیرد اما حداقل ماهی یکبار باید انجام شود.

اعتبار سنجی

اعتبار سنجی کاربران مجاز باعث می شود از ورود کاربران غیرمجاز و دستیابی به سیستم های اطلاعاتی جلوگیری شود. علاوه بر این مکانیزمهای اعتبار سنجی، کاربران مجاز را از مشاهده اطلاعاتی که برای آنها مجاز شمرده نشده است باز می دارد. در حال حاضر مکانیزم اصلی اعتبار سنجی جهت دسترسی به سیستم داخلی، استفاده از کلمه عبور است. در صورت استفاده از کلمه عبور، توصیه های زیر در روند بهینه وجود دارد:

- طول کلمه عبور: حداقل باید هشت کاراکتر باشد.
- تغییر کلمه عبور بصورت متناوب: کلمه عبور نباید بیش از ۶۰ روز اعتبار داشته باشد.
- تاریخچه کلمه عبور: از ده کلمه عبور اخیراً استفاده شده، نباید دو باره استفاده کرد.
- محتوایی کلمه عبور: ساخت کلمه عبور از یک حرف یکسان کار درستی نیست. کلمه عبور باید از حروف، اعداد و کاراکترهای خاص نشانه گذاری ساخته شود. به هنگام تغییر کلمه عبور باید از حروف،

اعداد و کاراکترهای خاص نشانه گذاری ساخته شود. به هنگام تغییر کلمه عبور لازم است محدودیت های فوق توسط سیستم اعمال شود.

کلمه عبور بصورت رمز شده ذخیره می شود و از دسترس کاربران عادی دور نگهداشته می شود. در مورد اطلاعات و سیستم های خیلی حساس، کلمه عبور به تنهایی حفاظت کافی ایجاد نمی کند. در این حالت از کلمه عبور دینامیک یا اعتبار سنجی های دو فاکتوری باید استفاده شود.

بازرسی

ثبت اتفاقات رخ داده در سیستم کامپیوتری مکانیزمی است که بازرسی یا گزارش گیری نامیده می شود. فایلهای گزارش گیری که به Audit log و Audit file معروف است حاوی اطلاعاتی از قبیل اتفاقات رخ داده (ورود، خروج، دسترسی به فایل و ...) ،کسی که آنرا انجام داده، زمان انجام و موفقیت یا عدم موفقیت آن می باشد. فایل های حاصل از بازرسی، منبع رسیدگی به حقایق پس از وقوع آن می باشد. بطوریکه می توان از اطلاعات آن به نحوه نفوذ به کامپیوتر و اطلاعاتی که مورد تهاجم قرار گرفته است و احتمالاً تغییر داده شده است، پی برد. در یک فایل گزارش موارد زیر باید ثبت شده باشد:

- ورود / خروج ها
- تلاشها ناموفق برای ورود
- تلاش برای برقراری اتصال شبکه ای
- تلاش برای برقراری اتصال تلفنی
- ورود مدیریت بصورت ناظر ارشد (یا root)
- وظایف اعطا شده به ناظر ارشد (یا root)
- دسترسی به فایل های حساس

در حالت ایده آل وقایع مذکور در فایلی ثبت می گردد که در سیستم امنی واقع شده است. در این صورت مهاجم قادر به پاک کردن فایل مذکور و سابقه فعالیتهایش نخواهد بود.

فایل های گزارش گیری بطور منظم باید بازبینی شوند. متأسفانه انجام این کار بصورت دستی کاری خسته کننده و ملال آور است. ضمن اینکه باید وقایع زیادی بررسی شود تا شاید چند مورد جالب توجه در آن پیدا شود. به همین دلیل لازم است سازمان با استفاده از ابزارهای مناسب عمل بازبینی را بصورت خودکار انجام دهد. پیشنهاد می شود عمل بازبینی Audit log بصورت هفته ای انجام گیرد.

رمز نگاری ارسال اطلاعات حساس از طریق واسطه نامطمئنی مانند اینترنت و خطوط تلفن آنها را در معرض خطر قرار می دهد. به طریق مشابه ذخیره کردن این اطلاعات روی کامپیوتر قابل حمل و محافظت نشده خطرناک است. رمزنگاری باعث محافظت از اطلاعات می شود.

اگر اطلاعات مورد نظر حساس است باید هنگام ارسال روی خطوط ناامن یا از طریق پست الکترونیک رمزنگاری گردد. الگوریتم بکار رفته برای رمز نگاری باید با میزان حساسیت اطلاعات تطبیق داشته باشد بطوریکه حفاظت آن را ضمانت کند. به طریق مشابه برای خطوط ارتباطی موجود بین مکانهای مختلف سازمان باید از رمزنگاری استفاده شود. در صورت استفاده از VPN لازم است شکل قدرتمندی از رمزنگاری برای ارسال اطلاعات بین دو سایت استفاده شود.

در صورت استفاده از پست الکترونیک برای ارسال اطلاعات در داخل سازمان به رمزنگاری نیاز نیست. اما اگر برای ارسال اطلاعات حساس به خارج از سازمان از پست الکترونیک استفاده می شود پیام ارسالی باید رمز شود.

اطلاعات حساسی که روی کامپیوتر همراه نگه داشته می شود به رمزنگاری نیاز دارد. الگوریتم بکار رفته برای رمزنگاری باید با میزان حساسیت اطلاعات تطابق داشته باشد. کامپیوتر همراه باید بگونه ای باشد که کاربر بتواند اجازه دستیابی به اطلاعات را برای خود ایاد کند. اگر کاربری موجود نباشد سیستم مورد استفاده اجازه دسترسی به

اطلاعات را به سازمان می دهد. الگوریتمی که برای رمز نگاری استفاده می شود باید شناخته شده باشد و به خوبی تحت آزمایش قرار گرفته باشد.

بک آپ و بازیابی

بک آپ و بازیابی از بخش های مهم سازمان است و به هنگام بروز خرابی سازمان را قادر به بازیابی عملکردهایش می کند. هر چه عمل بک آپ رایجتر باشد ، بازیابی عملکرد های سازمان پس از بروز خطا و خرابی راحت تر خواهد بود. از اطلاعات موجود در روی سرور هر روز باید بک آپ گرفته شود. بک آپ کامل باید هفته ای یکبار انجام شود و شش روز دیگر بک آپ افزایشی گرفته می شود. بک آپ های تهیه شده بصورت دوره ای بررسی می شود تا از صحت کپی اطلاعات مهم اطمینان حاصل گردد. بک آپ گرفتن از کامپیوتر همراه و رومیزی برای اکثر سازمانها مشکل ساز است . مشکل اول این است که این کامپیوتر ها حجم زیادی از اطلاعات مستقل را دارا هستند . مشکل دوم لزوم انجام بک آپ از طریق شبکه است . عموماً زمانی باید از اطلاعات کامپیوتر های همراه و رومیزی بک آپ تهیه شود که حاوی اطلاعات حساس برای ذخیره روی سرور فایل شبکه باشد. در این صورت سیستم بک آپ با کامپیوتر در یک مکان قرار می گیرد.

بعد از آنکه عمل بک آپ انجام گرفت مسئله ذخیره کردن فایل های پشتیبان تهیه شده پیش می آید. عمل بک آپ بدین منظور انجام می شود که در صورت بروز خطا یا اشکال، سازمان بتواند اطلاعات را بازیابی کند. خطای مذکور انواع مختلفی دارد بطوریکه می تواند از حذف اشتباهی یک فایل مهم توسط کاربر یا حوادثی که باعث صدمه دیدن سایت می شود ناشی شده باشد . این دو نوع خطا باعث ایجاد تضاد می شود. از طرفی برای ذخیره مجدد اطلاعات مهم توسط کاربر لازم است فایل های بک آپ دم دست باشند و از طرف دیگر به منظور حفاظت از آنها لازم است از سایت اصلی دور نگهداشته شوند.

روند بهینه توصیه می کند بک آپ های تهیه شده ، در خارج ا ز محل اصلی و با حداکثر حفاظت ذخیره گردند. به منظور آنکه فایل های بک آپ هنگام نیاز سر وقت به سایت اصلی عودت داده شود. لازم است بصورت مرتب دسته بندی گردد و در عرض ۲۴ ساعت پس ا ز ساخت ، به خارج سایت فرستاده شود.

امنیت فیزیکی

به منظور داشتن حفاظتی کامل باید از امنیت فیزیکی همراه با امنیت فنی و مدیریتی استفاده شود. اگر دسترسی فیزیکی به سرورهای کامپیوتری کنترل نشود ، امنیت فنی هر چه هم شدید باشد نمی تواند اطلاعات حساس را محافظت کند. به طریق مشابه شرایط محیطی و برق قادر است روی موجودیت و فرا همی (در دسترس بودن) سیستم های اطلاعاتی تأثیر بگذارد. روند بهینه توصیه می کند برای محافظت از موجودیت و فرا همی سیستم های اطلاعاتی ، در چهار حوزه زیر از امنیت فیزیکی استفاده شود.

- دسترسی فیزیکی
- شرایط محیطی
- اتفای حریق
- برق

دسترسی فیزیکی

تمام سیستم های حساس کامپیوتری در برا بر دسترسی غیر مجاز محافظت می شوند. این کار در مرکز دیتا تمرکز می یابد . دسترسی به مرکز دیتا توسط لیست دسترسی کنترل می شود. دیوارها و سقف مرکز دیتا باید بصورتی باشد که کسی نتواند از طریق سقف کاذب یا دریچه های تأسیساتی وارد آن شود.

شرایط محیطی

کامپیوترها نسبت به دمای بالا حساس هستند. علاوه بر این خود کامپیوتر گرمای قابل توجهی تولید می کند . بدین منظور لازم است با استفاده از لوازم مناسب دمای محیط ثابت نگه داشته شود و رطوبت محیط در سطح معین و مناسبی تنظیم شود. دستگاههای تهویه باید قادر باشند در صورت بالا رفتن دما از حد مجاز به مدیریت هشدار دهند.

اتفای حریق

استفاده از سیستم های اتفای حریق آبی برای مرکز دیتا مناسب نیست چون در صورت فعالیت به کامپیوترها آسیب می رساند. به همین دلیل باید از سیستم های اتفای حریق غیر آبی استفاده شود .

برق

کامپیوترها برای کار به برق نیاز دارند. در خیلی جاها اضافه ولتاژ و قطعی کوتاه برق رخ می دهد این قبیل وقفه ها باعث خراب شدن کامپیوتر و از دست رفتن دیتا می شود. به همین دلیل لازم است کامپیوترهای حساس در برا بر قطعی برق محافظت شوند.

استفاده از باطری بک آپ و UPS به خوبی این کار را انجام می دهد و باید اندازه آن بگونه ای تنظیم شود که بتوان کامپیوتر را بصورت صحیح خاموش کرد. برای قطعی برقی های طولانی تر باید از ژنراتور استفاده شود. به هر حال سیستم برق باید بگونه ای باشد که در صورت بروز قطعی، به مدیریت خبر داده شود.

نتیجه گیری

در اولین روزهای استفاده از رایانه ها در سیستمهای به اشتراک گذاشته شده تنها از نام کاربری برای شناسایی افراد استفاده می شد و نیازی به وارد کردن رمز عبور نبود. بعد از آنکه کاربران بدخواه آغاز به سوء استفاده از این سیستم کردند رمزهای عبور نیز به آن سیستمها اضافه شدند. امروزه راهبران بیش از هر زمان دیگر باید به امنیت شبکه و رایانه ها بیاندیشند. مهمترین دلایل این مسئله عبارتند از:

- ارزش سرمایه گذاری روی تجهیزات سخت افزاری و برنامه های نرم افزاری –نکته قابل توجه این است که رایانه ها و بسته های نرم افزاری بسیار گران قیمت هستند و جایگزینی آنها پر هزینه و دشوار است. حتی اگر در یک رخداد امنیتی نرم افزارهای و سخت افزارها کاملاً از بین نروند ممکن است مشکلات امنیتی ما را وادار به نصب مجدد همه نرم افزارها کنند و متعاقباً لازم شود کلیه نیازهای اساسی مجدداً تعریف گردند. این ا مر مستلزم صرف زمان بسیار زیادی است، خصوصاً اگر فرد مسئول، اطلاعات فنی کافی در این زمینه نداشته باشد.
- ارزش داده های سازمانی – این داده ها ممکن است شامل لیست مشتری ها، پروژه های مالی و یا برنامه های تجاری باشند که توسط کاربر نوشته شده اند.
- ارزش داده های فردی– ممکن است داده های 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 رایانه ای– همگام با پیشرفتهای فناوری، گروهی از خرابکاران که از دزدی داده های رایانه ای سود می برند نیز بوجود آمده اند. در مواردی اینکار صرفاً برای لذت و سرگرمی صورت میگیرد و برخی افراد نیز تنها بخاطر خودنمایی در برابر دوستان خود دست به چنین کارهایی می زنند، اما در بعضی موارد اینکار برای دستیابی به منافع شخصی و سازمانی انجام می گیرد (دزدی اطلاعات کارت اعتباری یا ورود به معاملات فریبکارانه) . در تمامی موارد مذکور این اشخاص باعث ایجاد خسارت و گسترش بی اعتمادی می شوند و در حد گسترده تر مشکلات بحرانی بوجود می آورند که به اشخاص و

موقعیتهای شغلی صدمه وارد می کند. باید گفت از زمانی که اینترنت در مقیاس جهانی در اختیار کاربران قرار گرفته، تعقیب و متوقف کردن مهاجمین هر چند همچنان امکانپذیر می باشد ولی بسیار پیچیده شده است.

بخش دوم

امنیت فناوری اطلاعات و کاربران

منفرد

مقدمه

تاکید بخش دو م بیشتر بر تامین امنیت کاربران منفرد رایانه است- از مبتدیان گرفته تا کارشناسان ، و اولین مسئله ای که در این زمینه باشد شرح داده شود چگونگی حفاظت از رایانه های شخصی است.

می توان از رایانه بصورت ایمن استفاده کرد، ولی این کار به اطلاعات، زیرکی و مراقبت شدید نیاز دارد. زبان بکار رفته در این بحث بعضاً حاوی مفاهیم نامأنوسی می باشد . بعضی از اصطلاحات و تعاریف در پیوست آمده اند.

فصل اول

امنیت رایانه و داده ها

امنیت فیزیکی

اولین مرحله این است که اطمینان حاصل کنید رایانه شما از لحاظ فیزیکی ایمن است. این مرحله ممکن است بسته به اینکه رایانه خود را در کجا قرار داده اید یا اینکه رایانه و داده ها از چه حساسیتی برخوردار هستند یک قسمت جزئی یا یک قسمت بسیار مهم محسوب شود.

سرقت رایانه

سرقت رایانه ها مشکلی رو به رشد است. رایانه ها و خصوصاً رایانه های کیفی به سادگی دزدیده می شوند و بسیار سخت پیدا می شوند. چنانچه سارق مایل به استفاده شخصی از رایانه نباشد مراکز بسیار زیادی وجود دارند که رایانه های دزدی و دست و دم را خریداری می کنند. برخی از سارقان، رایانه و نمایشگر آنرا بطور کامل به سرقت نمی برند بلکه قسمتهای مهم آن مانند حافظه و پردازشگر را می دزدند. باید گفت که هر دو مورد بازار خوبی دارند و حمل و نقلشان نیز آسان است، اما پیدا کردنشان اگر چه غیرممکن نیست ولی بسیار دشوار می باشد.

قانون اول:

قبل از وقوع سرقت، به آن رایانه فکر کنید.

به سرقت رفتن رایانه بسیار آزار دهنده است و چنانچه بیمه نباشید هزینه گزافی را بر شما تحمیل خواهد کرد. در بعضی مواقع سرقت اطلاعات باعث افشای امور شغلی و یا اسرار محرمانه اشخاص می گردد و در شرایط بدتر، سرقت رایانه باعث از دست دادن شغل می شود. با اینحال چنانچه در این خصوص چند روش ساده و ارزان قیمت بکار گرفته شود میتوان از سرقت رایانه های رومیزی و کیفی جلوگیری کرد یا حداقل احتمال آنرا به میزان قابل توجهی کاهش داد.

دو راهکار برای پیشگیری از دزدی رایانه وجود دارد: کاری کنید که سرقت رایانه دشوار شود، و یا کاری کنید که میل به دزدیدن رایانه کاهش یابد. کاری کنید که سرقت رایانه دشوار شود

چند راه بری دشوار کردن سرقت رایانه وجود دارد:

- اطمینان حاصل کنید که محل نگهداری رایانه امن است. برای نگهداری از رایانه باید از آن در یک اتاق قفلدار نگهداری نمایید و یا اگر در محل کار خود با همکاران دیگری کار می کنید رایانه را در معرض دید آنان قرار دهید. رایانه خود را در محافل عمومی مانند فرودگاه ها بدون مراقبت رها نکنید.
- اگر تصور می کنید که در زمان عدم حضور شما در محل کارتان ممکن است شخصی شبانه وارد اتاق شده و رایانه را به سرقت ببرد از سیستم آژیر خطر استفاده کنید.
- جهت ایجاد ایمنی ، رایانه خود را وسیله کابل سیمی و یا زنجیر به میله، لوله یا اشیایی که قابلیت جابجایی ندارند متصل کنید. از این روش در محافل نسبتاً عمومیم مثل مدارس و یا کتابخانه ها استفاده می شود. اکثر رایانه ها دارای محلی مخصوص اتصال می باشند. رایانه های کیفی نیز برای اینکار معمولاً دارای کابلها و قفلهای بخصوصی هستند.
- چنانچه رایانه دارای قفلی می باشد که از باز شدن بدنه جلوگیری می کند از آن استفاده نمایید. می توان از پیچهای مخصوص که براحتی قابل باز کردن نیستند نیز برای این منظور استفاده کرد.
- چنانچه اطلاعات ارزشمندی (مثل داده های کاری یا اطلاعات شخصی) در رایانه شما وجود دارد، لازم است زمانی که آنرا بدون مراقبت قرار داده و یا از آن دور هستید (مثلاً اگر از هتل خارج می شوید و رایانه در اتاق است) امکان دسترسی منطقی به آنرا تا حد ممکن کاهش دهید. دسترسی منطقی به معنای استفاده واقعی از رایانه در زمانی است که امکان دسترسی فیزیکی به آن وجود دارد. استفاده از رمزهای عبور مستحکم و محافظهای صفحه نمایش مجهز به رمز های عبور گزینه های مناسبی برای شروع این نوع از حفاظت هستند.

- رایانه های کیفی و PDAها کوچک می باشند و به همین دلیل دزدیدن آنها آسان است. چنانچه از آنها استفاده زیادی نیم کنید حتماً آنها را از محیط کار خارج نمایید.
- کاری کنید که میل به دزدیدن رایانه کاهش یابد
- افرادی که مایل به خرید رایانه های دست دوم باشند بسیار اندک هستند، خصوصاً اگر مشخص باشد که رایانه دزدی است. بهترین و ارزانترین روش برای آنکه سارقان تمایلی به دزدیدن رایانه نداشته باشند این است که مشخصات خود را با علائم ثابت

رایانه های کیف و PDA ها کوچک مس باشند و به همین دلیل دزدیدن آنها آسان است. چنانچه از آنها استفاده زیادی نمی کنید حتماً آنها را از محیط کار خارج نمایید.

کاری کنید که میل به دزدی رایانه کاهش یابد

افرادی که مایل به خرید رایانه های دست دوم باشند بسیار اندک هستند، خصوصاً اگر مشخص باشد که رایانه دزدی است. بهترین و ارزانترین روش برای اینکه سارقان تمایلی به دزدیدن رایانه نداشته باشند این است که مشخصات خود را با علایم ثابت و ماندگار که نمی توان آنها را از بین برد بر بدنه رایانه حک و یا نقاشی کنید. این اطلاعات می تواند شامل اسم یا مشخصات دیگر باشد. دقت داشته باشید که از این نوع علامتها در قسمت شکاف تهویه یا شکافهای دیگر استفاده ننمایید. همچنین آگاه باشید که گاهی اوقات علامتگذاری روی بدنه می تواند باعث ابطال ضمانتنامه گردد.

رایانه ها آسیب پذیرند

رایانه ها نسبت به گرد و خاک و سطوح ناهموار حساس هستند. چنانچه کارکردن با رایانه در محلی صورت بگیرد که گرد و خاک در انجا وجود دارد مرتباً باید با دقت زیاد آنرا تمیز کرد تا شکاف تهویه مسدود نشود. برخی رایانه ا همچنین نسبت به فرورفتگی ها و برآمدگی های سطحی که روی آن قرار دارند نیز حساس می باشند.

جنبه های دیگر امنیت فیزیکی

چنانچه شما برای نصب یک قطعه سخت افزاری بدنه رایانه خود را باز کرده اید باید به اخطارهایی که درباره شوکهای الکترواستاتیک داده شده توجه کنید (شوک الکترواستاتیک باعث صدمه دید ن سخت افزار می شود و باید از وقوع آ»جلوگیری کرد). ضمناً توجه کنید که برای جلوگیری از برق گرفتگی لازم است بدن شما با زمین در تماس دائم باشد.

برای محافظت از داده های خود نسخه های پشتیبان تهیه نمایید

در قسمت قبل مطالبی در مورد ایجاد امنیت فیزیکی آمد. در این قسمت مواردی شرح داده خواهند شد که بوسیله آنها می توان اطمینان حاصل کرد که داده ها و برنامه ها از حفاظت کامل برخوردارند . شما چگونه از داده ها و برنامه های رایانه خود محافظت می کنید؟

به چند دلیل ممکن است داده ها از بین بروند که برخی از آنها در زیر آمده است:

- پاک شدن اتفاقی فایل
- دزدیده شدن رایانه
- ذخیره ناخواسته یک فایل بر روی فایل دیگر
- روند نادرست به اجرا در آمدن یک برنامه بگونه ای که باعث تغییر ریا پاک شدن داده ها شود
- وجود یک برنامه مخرب (مثل ویروس) که باعث تغییر، بازنویسی و یا حذف داده ها شود
- بروز مشکل در سخت افزار (مثل مشکلات دیسک سخت، دیسک گردان، پردازشگر و یا منبع تغذیه) بگونه ای که باعث از بین رفتن داده ها گردد

- آتش سوزی و استفاده از آب برای خاموش کردن رایانه سوخته، که باعث غیرقانونی بازیابی شدن داده ها می شود
- و...

یکی از راه حلها برای مقابله با این تهدیدات، تهیه نسخه های پشتیبان می باشد. نسخه پشتیبان به خودی خود یک کپی از فایل یا مجموعه ای از فایلها است که با انتقال به یک دیسک فلاپی و یا دیسک فشره از آن نگهداری می شود. چنانچه فایل اصلی به هر دلیلی از بین برود یا پاک شود می توان از نسخه پشتیبان استفاده کرد و آنرا جایگزین فایل قبلی نمود.

قانون دوم:

مرتباً پشتیبان تهیه کنید و اگر رایانه در معرض تهدید قرار دارد نکات حفاظتی را بکاربرید.

نسخه های پشتیبان می تواند بسیار ساده و یا بسیار پیچیده باشند (از ساده ترین انواع پشتیبان می توان به یک دیسک فلاپی که از آن در کشوی میز کار خود نگهداری می کنید اشاره کرد.) اکثر بسته های نرم افزاری پشتیبان گیر به شما اجازه می دهند فایلی را که در رایانه خود داری به روی نوارهای مغناطیسی و یا مجموعهای از دیسکهای فشرده کپی کنید. چنانچه رایانه شما دزدیده شود، با خرید یک رایانه جدید با ساختاری مشابه رایانه قدیم و با استفاده از نسخه های پشتیبان قادر خواهید بود فالهای از دست رفته را مجدداً بکار گیرید.

نقایص، تصادفات، بلایای طبیعی و حملات مهاجمین قابل پیش بینی نیستند. معمولاً علیرغم تلاشهای زیاد برای برقراری امنیت نمی توان از بورز بعضی از مشکلات جلوگیری نمود، ولی ارگ پشتیبان مناسب تهیه کرده باشید حداقل داده های خود را از دست نیم دهید و در اکثر مواقع می توانید سیستم خود را بازیابی کرده و به یک حالت متعادل و ماندگار برسانید. حتی در صورتیکه داده های رایانه تماماً از دست رفته باشد، چنانچه یک مجموعه کامل از نسخه های پشتیبان در اختیار داشته باشید قادر خواهید بود همه اطلاعات را روی رایانه جدید بازیابی کنید و

مجدداً به آنها دسترسی داشته باشید البته این مسئله صرفا زمانی کارامد است که نسخه های پشتیبان در جایی غیر از رایانه قربانی ذخیره شده باشند.

دلایل گوناگونی وجود دارند که باعث می شوند نسخه های پشتیبان اجرای کلیدی و مهمی در امنیت رایانه های محسوب شوند:

خطای کاربر

بعضی از افراد برخی مواقع بطور ناخواسته فایلهای خود را پاک می کنند. در استفاده از واسطهای گرافیکی کاربر این امکان وجود دارد که یک فایل یا شاخه بطور ناخواسته به مکانی نادرست منتقل شود. اما چنانچه مرتباً از فایلها پشتیبان تهیه شده باشد امکان بازیابی فایلهایی که بطور اتفاقی پاک شده اند وجود خواهد داشت. انجام اینکار در مقابله با اشتباهات کوچک نیز می تواند راهکار پیشگیرانه خوبی باشد.

نقص در سخت افزار

سخت افزار مورد استفاده در هر زمانی ممکن است دچار خرابی شود و باعث از بین رفتن داده ها در طول یک فرایند گردد. صدمه هایی که به دیسک وارد می شود نیز می تواند منجر به تخریب کامل دیسک شود. ولی چنانچه از فایلها پشتیبان تهیه شده باشد می توان داده ها را مجدداً روی دیسک گردان و یا سیستم جدید بازیابی نمود.

نقص در نرم افزار

اکثر برنامه های کاربردی مثل MICROSOFT WORD و EXCELو ACCESS می توانند باعث از بین رفتن ناخواسته فایلهای داده شوند. اگر نسخه پشتیبان داشته باشید و برنامه کاربردی شما ناگهان نیمی از اطلاعات حیاتی فایل کاری شما را پاک کند، باز هم قادر خواهید بود داده های خود را بازیابی نمایید.

نفوذها و تخریبهای الکترونیک

مهاجمین و ویروسها ی مخرب مرتباً باعث تغییر و یا پاک شدن داده ها می شوند. وجود نسخه های پشتیبان در این زمینه نیز به کاربران کمک شایانی می کند.

اطلاعات بایگانی

نسخه های پشتیبان بعنوان اطلاعات بایگانی شده تلقی می شوند که امکان مقایسه نرم افزارها و داده های رایج با نرم افزار ها و داده های قدیمی را بوجود می آورند . این قابلیت باعث می شود بتوانید مشخص کنید که ه چیزهایی عمداً یا سهواً دچار تغییر شده اند. برای این منظور اگر نخواهید به عقب برگشته و تاریخچه یک پروژه را بازسازی کنید نسخه های پشتیبان منابع ارزشمندی بشمار می آیند.

سرقت سرقت

رایانه ها و فروش آنها کار بسیار آسانی است. با توجه به این مسئله، تهیه نسخه های پشتیبان و ذخیره آنها در محلی خارج از رایانه و در مکانی امن کمک شایانی خواهد بود، چرا که موارد بسیاری وجود داشته که پشتیبانها نیز به همراه رایانه به سرقت برده شده اند.

بلایای طبیعی

وقوع اتفاقاتی نظیر سیل، زلزله و آتش سوزی اهمیت حفاظت از رایانه را بیشتر روشن می کنند. در این زمینه نگهداری پشتیبانها رد محلهای دیگر بسیار مفید خواهد بود.

بلایای دیگر

بعضی مواقع نشت لوله های گاز و متعاقباً آتش سوزی ناشی از آن یا ریخته شدن مواد مایع روی دستگاه تهویه باعث بروز مشکل می گردد. در این موارد نیز وجود نسخه های پشتیبان بسیار حیاتی است.

با توجه به نقش مؤثری که پشتیبانها می توانند داشته باشند وجود اشکال گوناگون آنها چندان عجیب نیست. نکته قابل توجه این است که پشتیبان بکار رفته در هر کدام از شرایط فوق ممکن است برای شرایط دیگر کاربردی نداشته باشد. به خاطر داشته باشید که استفاده از حفاظت چند لایه و بکارگیر سیستمهای گوناگون تهیه پشتیبان جهت ایجاد ایمنی در برابر خطراتی که در اداره و یا منزل با آن مواجه هستید، مؤثرترین راه است.

ذیلاً چند مورد از شیوه های تهیه پشتیبان آمده است:

- فایلهای حساس خود را روی دیسک فلاپی، دیسکهای نوری، و یا دیسکهای مغناطیسی با ظرفیت بالا که قابلیت پاک کردن نیز در آنها وجود دارد کپی کنید.
- محتویات دیسک را روی یک دیسک انعکاسی یا اگر فضای کافی موجود است روی یک شاخه در همان دیسک مادر کپی کنید. البته اینکار در خرابیهای اساسی کمک چندانی نمی کند و صرفاً اگر تعدادی از فایلها بطور ناخواسته پاک شوند بکار می آید.
- هر از چند گاه آرشیو فشرده سازی شده ای از فایلهای مهم خود ایجاد کنید. البته می توان پشتیبانهای مربوطه را روی همان سیستم اولیه و یا روی رایانه های دیگر و در مکانهای فیزیکی متفاوت کپی نمود.
- از فایلهای خود پشتیبان تهیه کرده و از طریق شبکه یا اینترنت آنرا به رایانه دیگری منتقل کنید.
- اگر در نظر دارید که در مقابل خرابی دیسکهای سخت از ایمنی زیادی برخوردار باشید در رایانه خود از دو دیسک سخت و از نرم افزار یا سخت افزاری که از هر فایل یک پشتیبان تهیه می کند استفاده نمایید.

البته لازم به ذکر است که با رعایت تمامی این موارد باز هم تهیه مداوم پشتیبان جهت حفاظت در برابر مشکلات دیگر ضروری می باشد.

از چه چیزهایی باید پشتیبان تهیه کرد؟

دو دیدگاه در این زمینه وجود دارد:

۱. از تمام فایلهایی که اختصاصی رایانه شما است- البته غیر از برنامه های کاربردی- پشتیبان تهیه کنید. این امر در قدم اول شامل فایلهای داده ای می شود ولی دقت داشته باشید که باید از تمام فایلهایی که سازگاری سیستم عامل و برنامه های کاربردی را بر عهده دارند (مثل انواع فایلهای تنظیمات و پیکربندی) پشتیبان تهیه گردد. تعیین محل نگهداری این فایلها و همچنین اطمینان از صحت آنها برای بازیابی بدون اشکال در آینده کار بسیار دشواری است، اما می توانید تمام فایلهای داده ای خود را در چند شاخه اصلی نگهداری کنید و پشتیبانها را بگونه ای تهیه نمایید که تنها اطلاعات یکتا و اختصاصی شما را پوشش دهند.

۲. از همه چیز پشتیبان تهیه کنید. با تهیه پشتیبان از تمام سیستم- بسته به نوع استفاده ای که از آن می شود- می توان کل سیستم را رد صورت لزوم بازیابی کرد. همچنین قادر خواهید بود فایلها و یا شاخه های خاص را بازیابی نمایید.

ما استفاده از هر دو روش را بصورت همزمان توصیه می کنیم:

۱. به محض تکمیل نصب سیستم خود از تمام فایلها و مشخصات رایانه بصورت متناوب- مثلاً هر چند ماه یکبار - پشتیبان تهیه نمایید.

۲. از داده های شخصی خود طبق یک زمانبندی با دوره های کوتاهتر پشتیبان تهیه کنید. بسته به نوع کاربرد، برای پشتیبان گیری روشهای گوناگونی وجود دارد:

- از تمام داده های شخصی خود پشتیبان تهیه نمایید (هر چند ماه یکبار) مگر اینکه حجم وسیعی داشته باشند و امکان اینکار وجود نداشته باشد.
- چنانچه داده های شخصی شما زیاد است متناوباً از آن پشتیبان تهیه نمایید، ولی رد فاصله های کوتاه فقط از فایلهایی پشتیبان گیری کنید که دچار تغییر شده اند . به این نوع پشتیبان گیری

پشتیبان گیری افزایشی می گویند. توجه داشته باشید که برای بازیابی فایلها در این نوع پشتیبان گیری، هم به آخرین نسخه پشتیبان کامل و هم به آخرین نسخه پشتیبان افزایشی نیاز خواهید داشت.

گونه های دیگری از پشتیبان گیری نیز وجود دارد. معمولاً برنامه های پشتیبان گیر در مورد چگونگی تهیه پشتیبان پیشنهاداتی به کاربر ارائه می کنند.

نسخه های پشتیبان باید در کجا نگهداری شوند؟

پاسخ این سؤال وابسته به دلیل شما برای استفاده از پشتیبانها است. اگر پشتیبان گیری برای حفاظت از داده ها در مقابل سرقت و یا آتش سوزی است محل ذخیره سازی نباید نزدیک سیستم رایانه باشد، بلکه باید جایی باشد که در مقابل این مشکلات از حفاظت کامل برخوردار باشد. ولی اگر تهیه پشتیبان فقط برای بازیابی داده های پاک شده یا تغییر کرده صورت می پذیرد، باید محل آن طوری انتخاب شود که دسترسی به آن آسان باشد.

یک راه حل این است که پشتیبانهای کامل را در یک محل امن و پشتیبانهای افزایشی را در محلی نزدیک قرار دهید. راه دیگر این است که جدیدترین پشتیبان تهیه شده از داده ها را در دسترس و نسخه های قدیمی تر را رد محلهای امن تر بگذارید. بعضی افراد از پشتیبانها دو نسخه تهیه می کنند و یک نسخه را در دسترس و دیگری را دو راز دسترس قرار می دهند.

اگر در رایانه خود داده هایی دارید که سارقان قصد سرقت آنها را دارند باید همیشه به یاد داشته باشید که آنها را با سرقت نسخه پشتیبان نیز قادر خواهندبود همان داده ها را بدست آورند و به همین دلیل ضروری است که از پشتیبانها نیز مانند خود رایانه حفاظت فیزیکی لازم را بعمل آورید.

آیا پشتیبانها قابل استفاده هستند؟

به چند دلیل ممکن است هنگام نیاز نتوانید از پشتیبانهای تهیه شده استفاده کنید:

- نسخه مربوطه بسیار کهنه و یا از لحاظ فیزیک صدمه دیده باشد. بروز این مشکل در دیسکهای فلاپی و رسانه های مغناطیسی بیش از همه به چشم می خورد.
- دستگاهی که پشتیبان بوسیله آن نوشته شده دارای اشکال بوده و به همین دلیل داده نوشته شده در پشتیبان قابل خواندن نباشد. در این موارد امکان دارد بتوان با یک دستگاه مشابه دیگر، پشتیبان مورد نظر را خواند.
- رسانه ای که پشتیبان روی آن قرار داده شد دچار نقص شده باشد. این نقص رسانه در دیسکهای فلاپی اشکال بسیار رایجی بود بطوریکه اگر یک دیسک تنها چند روز بعد از تهیه شدن غیر قابل خواندن می شد چندان تعجب کسی را بر نمی انگیخت. دیسکهای فشرده بعنوان رسانه های بسیار ماندگارتر شهرت داشتند، اما یک مطالعه در سالهای اخیر نشان داد دیسکهای فشرده ای که کیفیت چندان مطلوبی ندارند ممکن است بعد از گذشت حدود دو سال از زمان نوشته شدن اطلاعات روی آنها غیر قابل خواندن شوند.

خواندن نسخه های پشتیبان با دستگاهی غیر از آن که نسخه پشتیبان با آن تهیه شده کنترل مناسبی برای کسب اطمینان از صحت رسانه جای نسخه پشتیبان است. دقت داشته باشید که برای نوشتن پشتیبان از دیسکهای مغناطیسی با قابلیت پاک کردن استفاده می کنید. (مثل دیسکهای zip و فلاپی)، از دیسکهای نو و تمیز استفاده نمایید.

بعضی اشخاص پشتیبانها را برای مدت بسیار طولانی نگه می دارند، اما سؤال این است که قرار است چه زمانی از نسخه هایی که چند سال قبل از اسناد تصاویر و برنامه ها تهیه شده استفاده کنند؟ اگر در نظر دارید برای زمان طولانی پشتیبانها را نگهداری کنید باید احتمال از رده خارج شدن رسانه را نیز مد نظر قرار دهید. برای مثال اگر داده ای در یک فلاپی پنج اینچی که رد سال ۱۹۸۰ رایجبود ذخیره شده باشد آیا امروز می توان رایانه ای با دیسک گردان پنج اینچی برای بازیابی آن پیدا کرد؟

چند نسخه پشتیبان باید نگهداری شود؟

اگر شما هفته ای یکبار از آنچه دارید پشتیبان تهیه کنید در صورت مواجهه با یک فاجعه مصیبت بار، حداکثر اطلاعات یک هفته را از دست خواهید داد. انجام اینکار از دیدگاه امنیتی قابل توجیه است ولی رد طول زمان فضای اشغال شده بوسیله پشتیبانها بیشتر و بیشتر می شود. چه تعداد از این پشتیبانها را باد نگه داشت؟ اگر از دیسکهای مغناطیسی و یا دیسکهای فشرده استفاده می کنید دلیلی ندارد که بخواهید آنها را سریع دور بیاندازید، چون حجم کمی دارند قابلیت استفاده مجدد هم ندارند، اما همواره باید چند نسخه از پشتیبان را نگهداری . در تمام مثالهای بالا می توان از چهار نسخه آخر نگهداری کرد.

چرا بهتر است اینگونه عمل شود؟ چرا باید نسخه مربوط به ماه قبل را در شرایطی که نسخه جدیدتری وجود دارد نگهداری کرد؟ دلیل آن ساده است: ممکن است نسخه آخری که ایجاد کرده اید قابل خواندن نباشد، گم شود، و یا به سرقت رود. در اینصورت واضح است که اگر چه نسخه های ماههای قبلی کاملاً به روز نیستند، ولی بودنشان بهتر از نبودشان است. اینمورد یک مثال دیگر از این نکته است که ایمنی سطح بالا از معیارهای چند گانه و تا حدودی تکرار شده تشکیل می شود.

از نرم افزار خریداری شده پشتیبان تهیه کنید.

اگر گواهی نرم افزارهایی که خریداری کرده اید این اجازه را می دهد، همیشه از دیسکهای فشرده نرم افزارها یک نسخه ثانویه تهیه کرده و از آن برای عملیات نصب و پشتیبانی استفاده نمایید.

مهمترین نکته در مورد نسخه های پشتیبان

مهمترین نکته در مورد نسخه های پشتیبان این است که تهیه پشتیبان باید در فواصل زمانی منظم صورت بگیرد. بعضی اشخاص زحمت تهیه پشتیبان را به خود نمی دهند و ممکن است به عواقب اینکار خود گرفتار شوند. این

افراد عموماً وقتی هم که با مشکلی روبرو می شوند تصور می کنند مشکل دیگر تکرار نخواهد شد. همچنان توصیه ما این است که از مخاطره احتمالی پیشگیری کنید و نسخه پشتیبان تهیه نمایید.

تصدیق هویت

تصدیق هویت این امکان را فراهم می کند که رایانه بداند شما چه کسی هستید. این دانایی باعث می شود که بتوان از تقلب جلوگیری کرد. معمولاً شما با یک نام کاربری و رمز عبور شناسایی می شوید، هر چند گونه های مختلفی از این سیستمهای شناسایی وجود دارد. نکته قابل توجه این است که باید کلماتی بعنوان رمز عبور بکار گرفته شوند که نتوان را براحتی حدس زد تا مهاجمان نتوانند آنها را پیدا کنند. در عین حال باید یادآوری ان کلمات در حافظه نیز امکانپذیر باشد و شخص آنها را فراموش نکند. اگر شما مرتباً با رایانه و پایگاه وب در تماس باشید قاعدتاً تاکنون نامهای کاربری رمزهای عبور زیادی به خاطر سپرده اید، اگر آنها را بر روی یک کاغذ نزدیک رایانه نوشته این باید بدانید که از امنیت زیادی برخوردار نیستند.

شناسایی کاربر

اکثر سیستمهای برای شناسایی افراد از آنها می خواهند که بگونه ای هویت خود را احراز کنند. این مسئله میتواند با دریافت اطلاعات مختلفی انجام شود: نام کاربری ، شماره عضویت، اسم عضو و ... که رد این مباحث عموماً از نام کاربری استفاده می شود. در بعضی سیستمها بجای نام کاربری از آدرس پست الکترونیکی استفاده می شود. در حقیقت در این سیستمها آدرس پست الکترونیکی بعنوان نمادی خاص از نام کاربری تلقی می گردد. در خصوص نام کاربری قوانین مختلفی می تواند وجود داشته باشد:

- بعضی از سیستم ها طول اسم را محدود می کنند ولی بعضی دیگر برای آن محدودیتی قایل نمی شوند.

- در بعضی سیستمها حروف بزرگ و کوچک را یکسان در نظر می گیرند ولی بعضی دیگر با آنها به منزله د و حرف متفاوت برخورد می کنند.

اگر سیستم به شما امکان انتخاب ندهد، نام کاربری شما همانی خواهد بود که بوسیله سیستم تعیین شده است. اما اگر لازم باشد خودتان نام کاربر را تعیین کنید چه نکاتی را باید مد نظر قرار دهید؟ بعضی موارد در زیر آمد است:

- آیا در نظر دارید نام کاربری نشانده نده هویت واقعی شما باشد؟ آیا قرار است این اسم کمک کند که دوستان و همکارانتان شما را بشناسند؟ یک آدرس پست الکترونیکی معمولاً بعنوان یک چنین نمادی از کاربر تلقی می شود.
- آیا میخواهید با انتخاب نام مورد نظر هویت واقعی خود را پنهان نگه داری؟ اگر بوسیله این کاربری در یک فعالیت گروهی شرکت می کنید (مثلاً یک بازی اینترنتی) شاید نخواهید دیگران هویت واقعی شما را بدانند.
- آیا می خواهید نامی انتخاب کنید که یادآوری آن آسان باشد؟ چنانچه از یک خدمت برخط استفاده کنید که به ندرت آنرا بکار می گیرید ممکن است مایل باشید از اسمی استفاده کنید که براحتی بماند بعضی افراد برای خدمات مختلف از یک نام کاربری استفاده می کنند، خصوصاً اگر آن خدمات با نکته مهم و حساسی در ارتباط نباشند.
- آیا می خواهید حدس زدن نامی که بکار می برید برای دیگران مشکل باشد؟ نام کاربری حساب بانکی شما باید بگونه ای تعیین شود که دیگران نتوانند به راحتی آنرا حدس بزنند (جهت تأمین امنیت لازم باید از پشتیبانی چند لایه استفاده کرد. اگر از آدرس پست الکترونیک عمومی خود برای ورود به سیستم بانکی استفاده کنید، حدس زدن آن برای سارقان ساده تر خواهد بود.)

رمز عبور

در بعضی سیستمها نام کاربری از سوی سیستم تعیین می شود، ولی رمز عبور کلمه ای است که در هر صورت توسط کاربر تعیین می گردد و شکل آن نیز باید بگونه ای باشد که حدس زدنش توسط اشخاص دیگر دشوار باشد. زمانیکه رمزهای عبور در سیستم میزبان ذخیره می شوند معمولاً رمزگذاری می شوند تا اگر کسی به دیسک دسترسی پیدا کرد قادر به مشاهده رمزهای عبور نباشد. در بعضی موارد این رمز گذاری بگونه ای است که امکان رمزگشایی رمزهای عبور وجود ندارد که به آن رمز گذاری یکسویه می گویند. در این سیستمها وقتی برای ورود به سیستم رمز عبور را وارد می کنید، ابتدا رمزگذاری می شود و سپس با نسخه ذخیره شده در دیسک مقایسه می گردد.

قانون سوم:

از رمز عبوری استفاده کنید که بتوان آنرا براحتی به خاطر آورد، ولی حدس زدن آن برای دیگران مشکل باشد.

به علت فقدان امنیت لازم در بعضی سیستمهای میزبان گاهی اوقات این امکان وجود دارد که مهاجمان به رمز عبور تمامی کاربران دست یابند و رمزهای عبور رمزگذاری شده را بیابند. حتی اگر برای تمام رمزهای عبور از رمزگذاری یکسویه استفاده شده باشد باز هم ممکن است مهاجم بتواند رمز عبور شما را کشف کند، چون الگوریتمهای رمزگذاری این رمزهای عبور شناخته شده هستند و لذا مهاجم می تواند از آن الگوریتمها برای رمزگذاری همه کلمات درون فرهنگ لغات و سایر رمزهای عبور متداول استفاده کند. لذا مثلاً اگر شما از کلمه birthday بعنوان رمز عبور استفاده کرده باشید مهاجم هنگام رمزگذاری کلمه birthday متوجه می شود نسخه رمز گذاری شده آن با آنچه که روی دیسک است مطابقت دارد و لذا از آن پس رمز عبور شما را خواهد دانست.

از آنجا که کل ایده استفاده از رمزهای عبور برای صدور اجازه ورود شما به سیستم در زمان دلخواه و دشوار کردن حدس آن توسط افراد دیگر است، می توان چند مشخصه برای رمزهای عبور مستحکم بر شمرد. مشابه نامهای کاربری، اینجا نیز سیستمهای مختلف قوانین متفاوتی را برای رمز عبور در نظر گرفته اند (حداقل و حداکثر طول، حروف مجاز برای استفاده و سایر موارد).

- هرگز از یک کلمه منفرد در زبان مادری خود بعنوان رمز عبور استفاده نکنید. انتخاب یک عبارت، یک جمله، و یا قطعاتی از کلمات برای این منظور مناسب تر است.
- چنانچه سیستم هر حروف بزرگ و هم حروف کوچک را در رمزهای عبور بعنوان حروف مجاز قلمداد می کند، از هر دوی آنها استفاده کنید–ولی مه در جای صحیح و قابل پیش بینی خود.
- در صورت امکان از اعداد ترکیبی ، علامتهای مجاز و همچنین فضاهای خالی استفاده کنید.
- اگر سیستم اجازه می دهد که از فضای خالی استفاده کنید یا رمز عبور خود بعضی از فاصله ها را حذف کنید(یعنی رمز متشکل از لغاتی باشد که به یکدیگر چسبیده اند).
- برای اینکه رمز عبور خود را به آسانی به خاطر بسپارید می توانید از همین رمز عبور در چندین سیستم استفاده کنید. البته اگر این کار را انجام دهید و فردی رمز عبور شما را در یکی از این سیستمها کشف کند، امنیت سیستمهای دیگر که در آنها از رمز عبور مشابه استفاده می کردید نیز به خطر خواهد افتاد . بنابراین چنین رمز عبوری را برای سیستمهایی انتخاب کنید که نیز به حفاظت خاصی ندارند. بعنوان مثال برای استفاده از مطالب روزنامه ها و دیگر مطالب، نیازی به پرداخت پول یا ارائه اطلاعات محرمانه نیست، اما برای خواندن مقالات بعضی از روزنامه ها در پایگاه وب مربوطه باید یک نام کاربری و رمز عبور وارد کنید. در واقع آنها فقط می خواهند شما به سیستم آنها وارد شوید، بنابراین می توانید برای خواندن مطالب روزنامه های مختلف از یک رمز عبور مشابه استفاده نمایید.

- بعضی افراد حروف را با علائم یا ارقام مشابه عوض می کنند، مثلاً از رقم ۱ بجای ۱ یا L از شماره ۳ یا علامت # بجای حرف E ، از رقم ۰ بجای حرف O ، از علامت @ بجای حرف A، و از رقم ۵ بجای حرف S استفاده می نمایند اینکار ترفند خوبی است ، اما به یاد داشته باشید که یک مهاجم حرفه ای با این حقه ها کاملاً آشناست . این حقه ها کار وی را کمی سخت می کند، اما غیر ممکن نمی سازد.
- حرف I به جای EYE (چشم) یا AYE یا هر کلمه معنادار در زبان خودتان عوض کنید. اینکار بخصوص برای لغاتی مثل ICON که پس از این تغییر به EYECON تبدیل می شود مفید است.
- از سرنام ها (حروف اول لغتهای سازنده یک عبارت) استفاده نمایید. بعنوان مثال TGBWC سرنامی برای شعار معروف کوکاکولا (THINGS GO BETTER COKE) می باشد.
- هجی کردن لغات بصورت بر عکس آنها را کمی مبهم می کند، اما شناسایی شان را سخت نمی نمایند.
- هرگز از موارد زیر بعنوان رمز عبور خود استفاده نکنید:
- یک نام یا مشتقات آن
- نام کاربری یا اسم مستعار خودتان
- نام همسر، یا اسامی فرزندان والدین
- اسامی دوستان، رؤسا و یا همکاران
- اسامی حیوانات خانگی
- روز تولد خود یا هر یک از دوستان و خویشاوندان
- شماره تلفن ، شماره گواهینامه یا مدرک مشابه
- رنگ مورد علاقه

- مقام یا عنوان شغلی
- نام سازمانی که رد آن کار می کنید
- هر چیز دیگری که با آن شناخته می شوید
- رمزهای عبور کلاسیک مثل XYZZY یا PLOVER (رمزهای عبور مور استفاده در بسیاری از بازی های رایانه ای)،و OPEN SESAME
- لغاتی که در فیلمهای محبوب و معروف، اخبار، داستانها و یا ادبیات از آنها استفاده می شود، مثل LORD OF THE RINGS, HARRY POTTER , GONE WITH THE WIND
- حروف روی صفحه کلید که رد کنار هم قرار گرفته اند مانند SDFGHJ
- مثلهای قبل به اضافه یک رقم قبل و بعد از آنها
- تکرار حروف یا ارقام در کنار هم یا بصورت ترتیبی مثل ۱۲۳۴۵۶، aaaa9999 یا ABCDE
- رد بعضی سیستمها تعداد حرف رمز عبور باید از مقدار معینی بیشتر باشد و یا تعداد مشخصی از حروف و ارقام به اتفاق هم را رد بر گیرد. اگر در تایپ کردن حروف ضعیف باشید و فردی از پشت سر به شما و صفحه کلید نگاه کند، خواهد توانست رمز عبور شما را بفهمد.
- رمز عبور هر چه باشد باید بدون نوشتن آنرا بخاطر بسپارید. هرگز رمز عبور را جایی ننویسید و آنرا در محل کار یا روی برچسبهای عناوین قرار ندهید.
- هرگز فهرست رمزگذاری نشده رمزهای عبور را رد فایلهای رایانه ای ذخیره نکنید.

بهترین رمز عبور، رشته ای تصادفی از حروف و ارقام است، اما برای اکثر ما بخاطر سپردن این رمزهای عبور بسیار سخت می باشد. اصلاً جالب نیست که رمز عبور در یک دفتر یادداشت یا زیر صفحه کلید نوشته شده باشد. مثالهایی از رمزهای عبور مناسب برای سیستمهایی که حروف، شماره ها، نشانه های خاص و جاهای خالی را می

پذیرند و میان حروف کوچک و بزرگ تفاوت قایل می شوند ذیلاً ارائه شده اند. این رمزها بسادگی به خاطر سپرده می شوند، ذیلاً ارائه شده اند. این رمزها بسادگی به خاطر سپرده می شوند، اما یافتن آنها در فرهنگهای لغات و یا حدس زدنشان بسیار دشوار می باشد.

رمز عبور	توضیحات
Computers are useful	عبارتی که بسیاری از کاربران رایانه با آن موافق هستند
Computers aReuseFul	قرار دادن یک جای خالی مناسب و استفاده طنزآمیز از حروف بزرگ
C0mputer5@reus#fv1	رقم 0 بجای حرف O، 5 بجای S، @ بجای a، # بجای E، V بجای U، و 1 بجای حرف L، در این مثال جای خالی وجود ندارد.
Comp9uter8sa re7usef6ul	عبارت اولیه بدون جای خالی و قرار دادن شماره هایی بین هر ۴ حرف.
Comutrsa reusful	عبارت اولیه با چند حرف جا افتاده
Onupatithwa	در بسیاری از کشورهایی که سنت قصه گویی وجود دارد اشکال استانداردی برای آغاز داستان وجود دارد. در زبان انگلیسی داستانهای کودکان معمولاً با عبارت ONCE UPON A TIME, THERE WAS شروع می شوند. در این مثال از ابتدای هر لغت دو حرف گرفته شده تا طول کلمه عبور محدود شود و در عین حال قابل شناسایی نباشد.
oNup@ T-1thuua	همان عبارت قبلی که در آن جایگزینی ها و علامتهای گفته شده بکار رفته است.

رمز عبور خود را تغییر دهید

رمز های عبور باید بصورت متناوب تغیر کنند، اما تناوب این تغییر همچنان مورد بحث است. برخی از متخصصان امنیتی توصیه کرده اند که رمز عبور خود را در فواصل زمانی کوتاه تغییر دهید، اما عده ای معتقدند که اینکار باعث می شود رمزهای عبور ساده انتخاب شوند و یا برای جلوگیری از فراموش شدن رد جایی نوشته شوند. برای کاربردهای معمولی نکات زیر توصیه می شوند:

- اگر فکر می کنید رمز عبورتان در معرض سرقت بوده سریعاً آنرا عوض کنید.
- اگر رمز عبورتان را به هر دلیلی به شخص دیگری داده اید بسرعت آنرا تغییر دهید. به اشتراک گذاشتن رمزهای عبور کار صحیحی نیست و باید از آن اجتناب کرد، مگر اینکه واقعاً چاره ای جز آن وجود نداشته باشد.
- رمزهای عبور را بصورت متناوب عوض کنید. معنی کلمه متناوب از دیدگاه ارقام مختلف، متفاوت است. شاید دوره هایی بین ۶ ماه تا یکسال به نظر مناسب باشند.
- اگر سیاست سازمانی شما در این مورد دقیقتر است از آن پیروی کنید.

امتیازات را محدود کنید

اکثر سیستمها به کاربران امتیازات محدودی ارائه می دهند که از امتیازات راهبر سیستم کمتر است. هنگامیکه راهبر و کاربر رایانه یکی باشند (نظیر بسیاری از رایانه های شخصی) کاربر کلیه کارهای خود را با استفاده از امتیاز دسترسی کامل (امتیازات ریشه یا امتیازات راهبر) انجام می دهد، در حالیکه بهتر است برای فعالیتهای غیر راهبری از یک نام کاربری مجزا استفاده کند. اینکار احتمال خراب شدن ناخواسته سیستم را کاهش می دهد و در صورت نفوذ مهاجم نیز از آسیب وارده به سیستم تا حد قابل توجهی می کاهد.

فصل دوم

امنیت سیستم عامل و نرم افزارهای کاربردی

نرم افزار های تجاری

یک نرم افزار تجاری معمولا چگونه کار می کند؟

چند سال قبل هنگامی که یک نرم افزار را می خریدید ، تا زمان عرضه ی نسخه جدید آن به بازار هیچ به روز رسانی در آن اعمال نمی شد . امروزه به دلایل مختلف – بیشتر نرم افزارها به صورت منظم به روز رسانی می شوند . برای برخی از نرم افزارها مثل سیستم عاملها ، به روز رسانی منظم به معنی انجام این کار به صورت روزانه است . به روز رسانی اغلب محصولات معمولا برای کاربران هزینه ای در بر ندارد .

بسیاری از شرکتهایی که نرم افزار تجاری ارائه می دهند برای رفع اشکالات و آسیب پذیریهای امنیتی نرم افزار، به روز رسانی آن را نیز ارائه می کنند . برای دریافت خدمات به روز رسانی فروشندگان بزرگ معمولا می‌توانید به پایگاه وب آنها مراجعه کنید و از قسمت support یا download اصلاحات ارائه شده برای محصولات را بیابید .

وقتی به پایگاه وب فروشنده ی نرم افزار مراجعه می کنید بسته های نرم افزاری و نسخه های مورد استفاده خود را تعیین می نمایید و سپس پایگاه وب فهرستی از به روز رسانی های قابل دریافت را ارائه خواهد کرد . در برخی از موارد کاملا مشخص است که به روز رسانی های ارائه شده برای رایانه شما قابل استفاده هستند ، اما در بعضی موارد دیگر این مسئله وضوح کمتری دارد . وقتی شما به روز رسانی های مورد نظرتان را انتخاب کردید ، آنها را download می کنید و در مرحله بعد آنها را نصب می نمایید . با توجه به نوع نرم افزار امکان دارد برنامه ای که download کرده اید به سادگی و در یک مرحله اجرا شود و یا اینکه برای نصب شدن نیازمند اجرای دستورالعملهای خاصی باشد . در برخی موارد بسته ی نرم افزاری به روز رسانی بعد از download شدن تقریبا بصورت خودکار نصب می گردد .

در سالهای اخیر معمولا از سه روش عمده برای ارائه ی خدمات به روز رسانی استفاده شده است :

۱. برنامه هایی نظیر Microsoft windows ، شرکت ما کروسافت بسته های به روز رسانی را از طریق windows update منتشر می کند . یک برنامه ی نرم افزاری رایانه ی شما را بررسی کرده و فهرستی از به روز رسانی مورد نیاز سیستم را ارائه می نمایند ، و آنگاه شما می توانید آنها را انتخاب ، download و نصب کنید .

۲. گاهی اوقات بسته ی به روز رسانی که به روش فوق download می شود به روز رسانی واقعی نیست ، بلکه برنامه ای است که در زمان اجرا به روز رسانی واقعی را download می کند . این برنامه ممکن است تنها ۵۰۰ کیلو بایت حجم داشته باشد – که اندازه ی کوچکی برای بسته های به روز رسانی نرم افزار محسوب می شود ، اما در حقیقت این فقط برنامه ای است که به روز رسانی واقعی را download می کند و سپس آنرا نصب می کند ، و به روز رسانی واقعی شاید اندازه ای در حدود ۳۰ مگابایت داشته باشد .

۳. برخی از برنامه ها دارای توابع از پیش تعریف شده ای هستند که به صورت پویا به بررسی به روز رسانی های ارائه شده می پردازند و با اجازه ی کاربر آنها را download و نصب می نمایند .

این قابلیت ها برای آسانتر شدن کار شما طراحی شده اند در کلیه موارد وظیفه انتخاب دقیق بسته های به روز رسانی مورد نیاز (که برای سیستم عامل و نرم افزارهای کاربر خاص ، کار پیچیده ای است)

به وسیله ی برنامه ها و به صورت خودکار انجام می شود .

مشکل کشورهای در حال توسعه

همانطور که مشاهده می کنید بسیاری از فرایندهای به روز رسانی برای اجرا در محیط متصل به اینترنت طراحی شده اند و بسته های به روز رسانی چندین مگابایتی را download می کنند . لذا استفاده از این روش تنها در صورتی نتیجه بخش خواهد بود که یک ارتباط پرسرعت اینترنتی داشته باشید و یا بتوانید ارتباط تلفنی خود را تا چندین ساعت برقرار نگه دارید . اما معمولا در کشورهای در حال توسعه این امکان وجود ندارد .

دو روش برای مقابله با این مشکل موجود است :

۱. از خیر به روز رسانی نرم افزارهای کاربردی و سیستم عامل خود بگذرید .

۲. از فرد دیگری بخواهید بسته ی به روز رسانی را download کند و جزئیات دستور العمل نصب را ارائه دهد . در این صورت بسته ی به روز رسانی می تواند از طریق دیسکهای فشرده با شبکه محلی توزیع شود .

در شرایطی که احتمال خطرات امنیتی در حال افزایش است راه اول منطقی به نظر نمی رسد . بنابر این تنها گزینه مناسب download کردن و به اشتراک گذاشتن وصله ها و اصلاحهای download شده است.

چند را ه برای انجام این کار وجود دارد :

- اگر سازمانی دارای ماشینهای متعدد باشد ، راهبر فنی باید مسئولیت download و نصب بسته های به روز رسانی آنرا به عهده گیرد .
- کلوپهای رایانه ای یا گروههای دیگر می توانند بسته های به روز رسانی را download کنند و آنرا در اختیار اعضا قرار دهند .
- ارائه کنندگان خدمات اینترنتی (ISP ها) می توانند بسته های به روز رسانی محصولات رایج و سیستم عاملهای مشترک را تهیه و به صورت محلی میان کاربران خود توزیع کنند . با این کار نیازمندی ISP ها به پهنای باند بین المللی کم می شود و لذا هزینه ی آنها نیز کاهش می یابد .

- فروشگاههای رایانه ای می توانند بسته های به روز رسانی را در اختیار مشتریان خود قرار دهند.
- در سال ۲۰۰۳ هنگامیکه یک کرم اینترنتی باعث آسیب پذیری رایانه ها شد ، مایکروسافت در کشورهای مختلف برای مقابله با آن اقدام به توزیع بسته های به روز رسانی بر روی دیسکهای فشرده اقدام کرد . استفاده از این روش همچنان هم می تواند ادامه یابد.

هر چند سه شیوه اخیر توزیع بسته های به روز رسانی چندان رایج نیستند ، اما با توجه به نیاز برای به روز نگه داشتن نرم افزار ها می توانند به یک استراتژی موثر تجاری برای ISP ها و فروشندگان در کشورهای در حال توسعه تبدیل شوند . اگر چه از این استراتژیهای پشتیبانی استقبال می شود ، اما کاربران باید مطمئن شوند که منابع به روز رسانی های محلی نیز قابل اطمینان هستند . اگر منابع محلی قابل اطمینان نباشند ممکن است به مرکزی برای توزیع ویروسها و تراواها تبدیل شوند .

آیا بسته های به روز رسانی را باید پس از انتشار ،سریعا نصب نمود ؟

این بحث چندین دهه میان متخصصان رایانه در جریان بوده است . در این زمینه دو دیدگاه متفاوت وجود دارد :

موافقان :اگر سریعا بسته های به روز رسانی را نصب کنید ،خود را در مقابل آسیبهای شناخته شده ایمن کرده اید . با استفاده از ایمنی بسته ای به روز رسانی ، تا سطحی که سیستم اجازه می دهد می توانید از خود در برابر نفوذ و افشای اطلاعات محافظت نمایید .

مخالفان :امکان دارد برنامه نویسان هنگام برنامه نویسی دچار اشتباه شوند یا بخش دیگری از برنامه را مختل نمایند . همچنین ممکن است در بسته های به روز رسانی به اندازه ی برنامه های اصلی اشکال و آسیب پذیری وجود داشته باشد . لذا این احتمال وجود دارد که بسته ی به روز رسانی مشکلات جدیدی را به وجود بیاورد که به مشکل قبلی ارتباطی نداشته باشد .

انتشار هر از چند گاه نقایص امنیتی کشف شده که با استفاده از آن مهاجمان به سیستم نفوذ کرده و داده‌ها را تخریب می کنند دامنه ی این مسئله را تغییر داده است . هنگامی که یک نقص امنیتی اعلام می شود – حتی اگر این اعلام توسط یک وصله امنیتی صورت پذیرد – مهاجمان سریعا ابزارهایی برای سوء استفاده از آن نقص را به وجود می آورند ، و در نتیجه ممکن است سیستم رایانه ی افرادی که از وصله های امنیتی منتشر شده استفاده نمی کنند سریعا مورد تهاجم قرار گیرد .

پیشنهاد عملی :

- کاربران مبتدی و افرادی که رایانه هایشان برای کارهای غیر حساس استفاده می شود باید کلیه بسته های به روز رسانی را بلافاصله بعد از انتشار بکار گیرند . برای رایانه ای که به روز رسانی نشده ، خطر مشکلات جدید حاصل از بسته های به روز رسانی نشده است .
- کاربران حرفه ای و کارکنان بخش فنی باید بسته های به روز رسانی امنیتی را سریعا نصب کنند،اما می توانند بقیه ی بسته های به روز رسانی را با توجه به نوع عملکرد آنها اولویت بندی نمایند . تاخیر چند هفته ای یا چند ماهه در نصب این بسته ها به کاربران ماجراجو اجازه می دهد بسته های به روز رسانی را نصب کنند، مشکلات احتمالی را کشف و گزارش نمایند ، و با این کار – پیش از اینکه شما به روز رسانی ها را نصب کرده باشید – به تولید کننده فرصت اصلاح نقایص جدید را بدهند .
- هرگز نمی توان گفت که تغییرات جه زمانی می توانند یک نرم افزار کاربردی را از روند صحیح اجرا خارج کنند . به همین دلیل اگر از رایانه ی شما در فعالیتهای حساس تجاری استفاده می شود ، بهترین راهکار این است که پیش از اعمال به روز رسانی های جدید ، ابتدا تغییرات یک دستگاه مشابه و نه چندان حیاتی آزمایش کنید .

نرم افزارهای غیر سنتی و غیر تجاری

در بحث قبل بر محصولات تجاری شامل سیستم عاملها و برنامه های کاربردی عمده متمرکز شدیم که در بسیاری از محیط های عملیاتی موسوم هستند . اما در نرم افزارها ی دیگر چه تغییراتی می کنند؟

نرم افزارهای تجاری کوچک

نرم افزارهای زیادی وجود دارند که به صورت رایگان یا حداقل هزینه در اختیار عموم قرار می گیرند . سطح پشتیبانی فروشندگان این نرم افزار ها تفاوتهای بسیاری دارد . به طور کلی استفاده متناوب از بسته های به روز رسانی رایگان و یا کم هزینه کاملا توصیه می شود. این برنامه ها معمولا ضعفهای امنیتی ندارند ، بلکه برای حل مشکلات غیر امنیتی و یا افزودن قابلیتهای جدید طراحی شده اند . با اینحال برخی از نرم افزارهای رایگان نظیر دیواره ی آتش و یا ویروس یاب در حیطه ی بررسی ما هستند و در این کتاب در مورد آنها بحث خواهد شد .

اگر این برنامه هایی استفاده می کنید که دارای کارکردهای امنیتی هستند ، اطمینان حاصل کنید که سیاست فروشنده در ارائه به روز رسانی در درک کرده اید . مسلما نمی خواهید در موقعیتی قرار بگیرید که از یک نرم افزار حساس به امنیت استفاده کنید و ناگهان خدمات پشتیبانی ارائه به روز رسانی آن قطع شود و یا توانایی خرید آنرا نداشته باشید . استفاده از برخی نرم افزارها مانند ویروس‌یابها اگر بطور منظم (روزانه یا هفتگی) به روز رسانی نشوند ، می تواند بسیار خطرناک تر از حالتی باشد که از آنها استفاده نمی شوند ، زیرا از آن استفاده نمایند تصور می کنید که از شرایط امنیتی مناسبی برخوردارید .

نرم افزارهای متن باز

نرم افزار های متن بازی که به سرعت در حال گسترش هستند باید به صورت مناسبی مورد پشتیبانی قرار داشته باشند . در برخی از موارد با اینکه نرم افزار اصلی بصورت رایگان عرضه می شود اما امکان دارد در خدمات ارائه

به روز رسانی یا پشتیبانی آن هزینه بر باشد. نسخه رایگان RED HAT LINUX که در دسترس عموم قرار می گیرد نمونه خوبی از این قبیل نرم افزارها است . سازمانهایی که خواهان سطح بیشتری از پشتیبانی فنی هستند ممکن است بسته نرم افزاری اصلی و یا حداقل خدمات پشتیبانی آنرا خریداری کنند . اگر تصمیم به استفاده از نرم افزارهایی دارید که خرید و پشتیبانی آنها رایگان است (مثل بعضی از نرم افزار های آزاد و متن باز) توجه داشته باشید که مدت زمان در دسترس بوده نسخه های اصلاحی آن ممکن است کوتاه باشد . بنابر این اگر سیستم عامل یا زیر سیستم های مهم خود را از نوع نرم افزارهای بدون پشتیبانی انتخاب کرده اید باید نسخه جدید آنرا هر چند وقت یکبار (مثلا در هر شش ماه) به روز رسانی کنید .

روند به روز رسانی محصولات متن باز بسیار مشکل تر از به روز رسانی محصولاتی مثل MICROSOFT WINDOWS است ، اما با وجود دستورالعمل های نصب برای محصولات اصلی متن باز مبتنی بر windows نیز وجود دارد که به صورت کامپایل توزیع می شوند و از نصب کننده های ساده استفاده می کنند .

همانند سیستم های windows ، بسته های به روز رسانی و وصله های ارائه شده برای سیستم های متن باز بزرگ ، بسته به اندازه سیستمهای متن باز تغییر می کنند . شناسایی منابع محلی این بسته های به روز رسانی بمنظور کاهش زمان download آنها از اینترنت برای کاربران منفرد حائز اهمیت است.

آخرین نکته مربوط به نرم افزار متن باز کمی بحث می طلبد .

مباحثه ای میان طرفداران نرم افزار متن باز و طرفداران نرم افزارهای انحصاری سنتی وجود دارد که بالاخره کدامیک از این محصولات ایمن تر هستند .

طرفداران نرم افزارهای انحصاری معتقدند :

- از آنجا که متن برنامه ی محصولات متن باز در دسترس است ، نفوذ گران به سادگی می توانند برنامه را تجزیه و تحلیل کنند و تمامی اشکالاتی که از طریق آنها می توان به سیستم نفوذ کرد را شناسایی نمایند .

- چون افراد زیادی در مناطق مختلف و بدون رابط سازمانی ممکن است روی محصولات متن باز کار کنند، ممکن است استاندارد ها نادیده گرفته شوند و فقدان یکپارچگی در اجزای مختلف منجر به آسیب پذیری امنیتی گردد .
- به این دلیل که کاربران برای محصولات انحصاری به تولید کننده وجه می پردازند دستورات او را دنبال می کنند و انجام این کار باعث می شود کیفیت ملاحظات ایمنی در نرم افزارهای انحصاری بالا باشد .
- از آنجا که هیچ منبع معینی مسئولیتی در قبال محصولات متن باز بر عهده ندارد ، در صورتی که امنیت برای توسعه دهندگان انفرادی اهمیت نداشته باشد ، احتمال زیادی وجود خواهد داشت که نادیده گرفته شود .

طرفداران نرم افزارهای متن باز

- به دلیل اینکه افراد زیادی با متن برنامه نرم افزارها کار می کنند ، مسائل و مشکلات آنها توسط افراد خبره تشخیص داده می شوند و سریعا اصلاح می گردد .
- افرادی که با محصولات انحصاری کار می کنند ممکن است کد یکپارچه ای را تولید کنند ، اما اگر تولید کننده برای امنیت محصول خود ارزش خاصی قائل نشده باشد برنامه نمی تواند از سطح ایمنی مطلوبی برخوردار باشد .
- در برنامه های انحصاری برای اصلاح مشکلات موجود همیشه باید به تولید کننده ی محصول مراجعه کرد و این امر ممکن است باعث تاخیر زمانی زیادی شود . در واقع هر یک از این دلایل در جایگاه خود صحیح هستند . راهی برای کسب اطمینان از ایمن بودن نرم افزار متن باز وجود ندارد . همچنین نمی توان ادعا کرد که کشف و اصلاح مشکلات بوجود آمده در زمان مناسب صورت می گیرد یا خیر . در هر نوع نرم افزار ، نمونه هایی از رفتار ایده آل و همچنین بی دقتی طراحان و سازمانهای ارائه خدمات پشتیبانی دیده شده است .

نرم افزار های مسروقه

نه نویسندگان و نه ناشران این کتاب هیچکدام مروج سرقت نرم افزاری نیستند ، اما ساده انگارانه است اگر وانمود کنیم چنین مسئله ای وجود ندارد . سرقت نرم افزار مشکلی است که در سراسر دنیا وجود دارد ،ولی بیشتر در کشورهایی اتفاق می افتد که در آنها هزینه نسبی تهیه نرم افزارهای قانونی در مقایسه با دستمزدها بسیار بیشتر از کشورهای در توسعه یافته است – که در آنها دوایر قوانین محلی و نیروهای انتظامی با همکاری هم انجام تخلفات را بسیار غیر محتمل می سازند .

گذشته از وظیفه قانونی مسئولین برای جلوگیری از خدشه دار شدن حقوق مالکیت سازنده محصول ، دو نکته در مورد امنیت نرم افزار مسروقه وجود دارد که باید مورد بررسی قرار گیرند . هیچکدام از این دو مورد در نرم افزارهای مسروقه چندان رایج نیستند ، اما به هر حال این امکان وجود دارد که هر دو با هم نیز وجود داشته باشند .

۱. ممکن است نرم افزار مسروقه قابل به روز رسانی شدن نباشد یا انجام به روز رسانی آنرا از کار بیاندازد .

۲. امکان دارد در برخی از نرم افزارهای مسروقه حاوی کارکردهایی باشند که انتظار آنها را ندارید . این کارکردها ممکن است شامل دربهای مخفی ، ثبت کننده های صفحه کلید ، یا سایر انواع نرم افزارهای مخرب باشند .

فصل سوم

نرم افزارهای مخرب

ویروس

ویروس برنامه ای است که به انتهای برنامه دیگر متصل می شود و یا وارد بدنه یک برنامه دیگر می گردد. وقتی آن برنامه به اجرا در می آید، ویروس نیز اجرا می شود و نسخه های خود را وارد فایلها یا دیسکهای دیگر می کند و بدین صورت خود را تکرار می نماید، و هنگامیکه هر یک از فایلها یا برنامه های آلوده اجرا می شوند این روند بار دیگر تکرار می گردد. ویروس ممکن است علاوه بر این موارد کارهای دیگری نیز انجام دهد.

کرم اینترنتی

کرمها از این جهت که نسخه ای از خود را تکرار می کنند مشابه ویروسها هستند، اما برای اینکار به برنامه میزبان نیاز ندارند همانند ویروسها ،یک کرم ممکن است تنها نسخه هایی از خود را در جاهای مختلف تکرار کند و یا اینکه علاوه بر آن عملیات دیگری نیز انجام دهد. کرم تنها زمانی کار می کند که سیستم قابلیت پذیرفتن منابع خارجی را داشته باشد و از طریق آن منابع بتواند. به اجرای برنامه بپردازد. برخی از فروشندگان ابزارهای شناسایی بدافزارها، کرم را نیز نوعی ویروس به حساب می آورند.

اسب تراوا

نام این نوع نرم افزار از افسانه جنگ شهر تراوا در یونان برگرفته شده است. در آن افسانه، یونانی ها یک اسب چوبی بزرگ را از دروازه شهر به داخل می فرستند و هنگامیکه اسب وارد شهر می شود تعداد زیادی سرباز یونانی از آن خارج می شوند و شهر را به تصرف خود رد می اورند. از آن زمان به بعد اسب تراوا به معنای چیزی است که ظاهری عادی اما محتویاتی خطرناک دارد.

در مفاهیم رایانه ای ، اسب تراوا می تواند خرابیهای زیادی به بار آورد و یا اعمالی غیر از آنچه که کاربر انتظار آنرا دارد انجام دهد. این اصطلاح در سالهای اخیر به برنامه های مخربی اطلاق می شود که معمولاً بدون اطلاع و اجازه کاربر وارد سیستم می شوند و به جمع آوری و ارسال اطلاعات می پردازند.

نرم افزار BONUS

نرم افزار BONUS نرم افزاری است که بدون آگاهی شما حاوی بسته های دیگر نرم افزاری در آن وجود دارد. قرار گرفتن بسته های دیگر در یک نرم افزار تجاری مرسوم است. بعنوان مثال اگر یک مرورگر وب نصب کنید ممکن است شامل برنامه هایی چون Adobe Acrobat یا نرم افزارهای چند رسانه ای باشد. این امر به این علت است که معمولاً با اینکار کارآیی نرم افزار اصلی افزایش می یابد و روند فعالیت نیز معمولاً بدنی ترتیب است که در صورت تمایل شما آن نرم افزارهای جانبی را نصب می کند یا اینکه در آغاز نصب آن برنامه ها شما را از انجام اینکار آگاه می سازد. عملکرد نرم افزارهای BONUS معمولاً متفاوت از نرم افزار اصلی است و اگر چاره ای داشته باشید مسلماً نباید آنها را نصب کنید.

قابلیتهای تراوا، ویروس و کرم برای یک برنامه «انحصاری» نیستند به عبارت دیگر مهاجمین میتواند بدافزاری با بیش از یک ویژگی بنویسند مانند تراوای خود تکرار شونده.

بدافزاری که دارای بیش از یک خصوصیت مخرب است تهدید چند وجهی نامیده می شود. همانطور که مشاهده می کنید این عناوین عموماً از روی نحوه گسترش نرم افزارهای مخرب تعریف شده اند و نه با توجه به نحوه عملکرد آنها بررسی می شود. در فصلهای بعد نیز روشهای ایمن ساختن رایانه ها و شبکه ها در برابر این نرم افزارها مورد بحث قرار می گیرد.

عملکرد نرم افزارهای مخرب

هیچ محدودیتی در چگونگی فعالیت نرم افزاارهیا مخرب روی رایانه شما وجود ندارد، اما معمولاً این برنامه ها در فعلیتهای خود واجد ویژگیهای مشترکی هستند:

ارسال نامه الکترونیکی

ارسال نامه الکترونیکی یکی از رایجترین عملکردهای برنامه های مخرب است. نامه الکترونیکی ممکن است ضمیمه ای شامل ویروس یا کرم داشته باشد. متن آن نیز می تواند در مورد اطلاعات خاصی تنظیم شده باشد (نظیر هشدارهای مایکروسافت در مورد یک مشکل امنیتی) یا حتی می تواند دارای یک قسمت تصادفی از برنامه های الکترونیکی پیشین شما باشد که در رایانه موجود است. اگر ضمیمه نامه فایل خطرناکی باشد، معمولاً متن آن به نحوی دریافت کننده را تشویق می نماید که ضمیمه را باز کند. فیلدهای موضوع و فرستنده نیز معمولاً بگونه ای تنظیم می شوند که کاربر را تشویق کنند که فایل ضمیمه را باز کند (مثل کرم مشهوری که موضوع آن « I love you» بود.) این نوع پیامها معمولاً برای افرادی ارسال می شوند که ادرس انها در فهرست آدرسها یا فایلهای دیگر رایانه آلوده وجود دارد. گاهی اوقات وقتی پیامها برای همه این افراد ارسال شد برنامه متوقف می گردد، و گاهی اوقات باز هم فعلیت خود را- چه از رایانه اولیه و چه از مبادی جدید- از سر می گیرد. توجه داشته باشید که اگر رایانه فرد دیگری با ویروس یا کرم آلوده شده باشد و آن ویروس آدرس شما را در فیلد فرستنده نامه الکترونیکی آلوده گذاشته باشد (شاید به این دلیل که آدرس شما را در ماشین آلوده یافته است) این شما هستید که متهم به توزیع این ویروس خواهید شد! (این فن گمراه کنندگی نامه الکترونیکی نام دارد و رد صورت استفاده برنامه مخرب از آن، بسادگی نمی توان مشخص کرد که رایانه آلوده واقعی متعلق به چه کسی است)

جمع آوری اطلاعات

نرم افزار مخرب می تواند اطلاعاتی در مورد رایانه شما و فایلهای موجود در آن بدست آورد و این اطلاعات را در اختیار نویسنده خود قرار دهد. این برنامه می تواند همه فایلهای رایانه شما (حتی فایلهای رمزگذاری شده) را بخواند، اگر اطلاعات حساب بانکی یا کارتهای اعتباری خود را در رایانه ذخیره می کنید ممکن است این داده ها مورد علاقه نفوذگران باشند. اگر از امضای خود در رایانه تصویری تهیه کرده باشید تا از آن در چاپ و یا ارسال نامه ها استفاده کنید، ان هم ممکن است بکار مهاجمان بیاید. جمع آوری این بسته های اطلاعاتی در کنار هم می تواند. برا یمهاجم این امکان را بوجود آورد که بتواند از هویت شما سوءاستفاده کند. اگر در یک شرکت تجاری کار می کنید که شماره های کارت اعتباری افراد دیگر را روی رایانه خود ذخیره مینمایید، در صورت دزدیده شدن این شماره ها مشکلات جدی برایتان پیش خواهد آمد.

بازنویسی یا حذف داده ها

برخی از نرم افزارهای مخرب واقعاً آسیب رسان هستند،به این ترتیب که با وارد کردن داده به رایانه شما بسرعت می توانند فایلهای موجود در دیسک سخت را پاک کنند یا آنها را با اطلاعات نادرست بازنویسی نمایند. این برنامه ها گاهی اوقات با روشهایی که احتمال شناسایی کمتری دارند تغییرات گفته شده را بوجود می آورند.

نصب یک تروا

این عملکرد نرم افزارهای مخرب بسیار رایج شده است. روی رایانه شما معمولاً برنامه هایی نصب شده و لذا برنامه مخرب می تواند با برنامه ای که شما یا سیستم عامل از آن استفاده زیادی می کنید. جایگزین شود (معنای اصلی تراوا) از این گذشته ممکن است برنامه های دیگری را وارد سیستم کند که در یک زمان از پیش تعیین شده یا

هنگام روشن شدن رایانه به اجرا در آیند، در بخش «نرم افزارهای سربار» بسیاری از این روشها توضیح داده شده اند.

زمانبندی برای آینده

هر یک از عملکردهای گفته شده ممکن است بلافاصله اتفاق بیفتند و یا برای وقوع در آینده برنامه ریزی شوند. برای مثال ممکن است نویسندگان نرم افزارهای مخرب علاقه مند باشند که اعلام شود یک کرم خاص در روزهای اولیه ژانویه سال ۲۰۰۰ یک خرابی بزرگ به بار آورد.

نرم افزارهای سربار

نرم افزار مخرب معمولاً به شکل برنامه ای ظاهر می شود که روی رایانه شما می نشیند و زمانی که رایانه خود را روشن یا برنامه خاصی را آغاز میکنید به اجرا در می آید، تنها محدودیتی که عملکرد این برنامه ها می تواند داشته باشد تصورات و مهارت پدید آورنده آنها است.

نرم افزار ردیابی و اعمال تغییر در شبکه

این دسته از برنامه ها پایگاههایی که شما مشاهده می کنید را نظاره می کنند و می توانند علاوه بر آنچه که شمار در حالت معمول مشاهده می کنید صفحات دیگری را به نمایش درآورند. همچنین می توانند آنچه که در پایگاه وب است را با تبلیغات خود جایگزین نمایند و اطلاعاتی در مورد رایانه شما و تعاملاتی که با تولید کنندگان آن انجام داده اید. برای پدید آورده خود بفرستند، این نرم افزارها در بسیاری از موارد دارای کنترل کامل بر روی مرورگر شما هستند، آنچه وارد می کنید را نظاره می کنند و می توانند آنچه که می بینید را تغییر دهند و هنگامیکه

مشاهدات شما را تحت نظر دارند می توانند فعالیتهای شما را به یک مقصد از پیش تعیین شده گزارش دهند. در internet explorer، این قابلیت طراحی شده و BHO نام دارد. اگر چه کاربر می تواند BHOهای سالم و بسیار مفیدی را پدید آورد، اما این قابلیت برای ایجاد برنامه های کاربردی که اخلاقیات در آنها کمتر رعایت شده نیز امکانات قابل توجهی بوجود آورده است.

دربهای مخفی

معمولاً برای دسترسی به یک سیستم رایانه ای نیاز به وارد کردن نام کاربری و رمز عبور دارید، اگر چه این سطح از امنیت گاهی اوقات برای سیستمهایی که از لحاظ فیزیکی ایمن هستند و تنها اشخاص خاصی می توانند از پشت صفحه کلید آنها وارد سیستم شوند وجود ندارد، نرم افزار درب مخفی یا بی اثر کردن کلیه حفاظهای امنیتی این چنینی به کاربر راه دور اجازه دسترسی به رایانه شما را می دهد. این نرم افزار حتی ممکن است حفاظهای امنیتی خود را کار بگذارد تا تنها پدید آورنده آن بتواند از سیستم استفاده نماید. اگر چه این جزئیات از یک مورد تا مورد دیگر متفاوت است، اما کاربر راه دور ممکن است روی سیستم شما کنترل کامل پیدا کرده باشد. حتی ممکن است این نرم افزارها اگر بخواهند بتوانند شما را از ادامه کارتان بازدارند. در این حالت رایانه شما تحت فرمان شخص دیگری قرار دارد و شما از این مسئله آگاهی ندارید. اما سوالی که پیش می آید این است که چرا مهاجم مایل است کنترل سیستم شما را در دست بگیرد؟ انجام اینکار می تواند دلایل متعددی داشته باشد ، از جمله اینکه:

- هیچ دلیلی غیر از اثبات توانایی خود به دو ستانش برای انجام این کار وجود نداشته باشد.
- بطور کلی بخواهد تخریبگر باشد
- برای هدف قرار دادن شما دلیل شخصی داشته باشد
- از رایانه شما برای فعالیتهای مخرب دیگر استفاده کند مثل فرستادن هرزنامه یا انجام حمله تخریب سرویس Dos علیه رایانه های دیگر و یا اینکه بخواهد اطلاعات با ارزشی را به سرقت ببرد.

- بخواهد اطلاعات با ارزشی را به سرقت ببرد.

توجه داشته باشید نرم افزارهایی با کاربرد مشابه تحت عناوینی چون ابزارهای دسترسی راه دور یا ابزارهای راهبری راه دور برنامه های مشروع و بسیار و پراستفاده ای هستند، اگر از این ابزارها برای اهداف کاری خود استفاده می کنید مطمئن شوید که ملاحظات مناسب امنیتی مانده نام کاربری و رمزهای عبور را بکا رگرفته اید.

ثبت کننده کلید

مفهوم «ثبت کننده کلید» از نام آن مشخص است، آنها تمامی کلیدهای فشرده شده صفحه کلید را ثبت و در یک فایل ذخیره می کنند. این فایل می تواند در آینده با دسترسی از طریق درب مخفی مورد استفاده قرار بگیرد و یا از طریق پست الکترونیکی یا وب برای نویسنده برنامه ارسال گردد.

شایان ذکر است که ثبت کننده کلید تمامی آنچه که واقعاً تایپ می کنید را نظاره می کند و نه آنچه که از طریق شبکه ارسال می شود. بنابراین حتی اگر شماره کارت اعتباری را روی صفحه وب ایمن وارد کنید (یعنی اگر هنگام انتقال اطلاعات از رمزنگاری استفاده شود)،این برنامه دقیقاً آنچه که تایپ می کنید را بصورت رمزگذاری شده ثبت می نماید.

سرقت مالی

در اکثر سرقتهایی که در نتیجه حملات به رایانه های شخصی اتفاق افتاده اند، از رایانه قربانی سرقت اطلاعات صورت گرفته است، با این حال مواردی وجود دارند که در آنها با استفاده از برنامه های سربار، پول مسروقه بصورت خودکار به مصرف رسیده است. ساده ترین مثال این است که برنامه، یک مودم را روی رایانه شما شناسایی کند و از آن برای برقراری تماس با مقاصد دوردست استفاده نماید. از آنجا که برنامه نمی تواند صحبت

کند انجام اینکار برای مهاجم هیچ مزیتی ندارد، بجز نوعی احساس رضایت شیطانی مبنی بر اینکه شما در پایان ماده یک صورتحساب سنگین از شرکت مخابرات دریافت می کنید.

در موارد دیگر مهاجم می تواند از انجام اینکار بهره شخصی ببرد، در بسیاری از کشورها ممکن است شماره تلفن خاصی وجود داشته باشد که وقتی با آن تماس گرفته می شود شرکت مخابرات در هر دقیقه هزینه بیشتری برای تماس گیرنده ثبت کند و در عوض مقداری از این هزینه به حساب کسی برود که با او تماس حاصل شده است. این امر در انواع مختلف معاملات مورد استفاده قرار می گیرد، اما بیشتر مورد استفاده شرکتهای نرم افزاری است که خواهان راه ساده ای هستند تا بری پشتیبای بدون ضمانت هزینه ای را از حساب شما کسر نمایند. در چنین وضعیتی شرکت مخابرات هزینه های تماس گیرنده ها را بگونه ای محاسبه می کند که بتواند قسمتی از آنرا بعنوان هزینه تماسهای پشتیبانی به شرکتی که با آن تماس حاصل شده است ارسال کند. اگر نفوذگر چنین شماره ای داشته باشد می تواند رایانه شما را طوری برنامه ریزی کند که با این شماره تماس بگیرد و برای مدتی تماس را برقرار نگهدارد، در آنصورت این هزینه در صورتحساب پایان ماه تلفن شما در ج خواهد شد.

این نرم افزار ها چگونه شناسایی می شوند؟

چند سال قبل تنها راه آلوده شدن رایانه های شخصی بوسیله ویروس یا نرم افزارهای مخرب، استفاده از دیسکهای آلوده بود و اگر با افرادی که آلوده شده بودند تبادل فایل انجام نمی دادید در امنیت به سر می بردید سیستمهای UNIX چندان مستعد دریافت ویروس نبودند اما به دلیل قابلیتهای بسیار زیاد برقراری ارتباط و همچنین اشکالات امنیتی در سیستم عاملها و برخی از نرم افزارهای کاربردی رایج، حتی در آن روزها هم گاهی اوقات نفوذگران می توانستند به سیستمها دستیابی پیدا کنند و روی آنها نرم افزارهای درب مخفی نصب نمایند. اولین حادثه جدی امنیتی اینترنت گرمی بود که در سال ۱۹۸۸ به یک سیستم UNIX حمله کرد. امروز ممکن است شما به روشهای متفاوتی مورد حمله قرار بگیرید. روشهایی که در ادامه ذکر شده اند مربوط به سیستمهای مبتنی بر windows می شوند.

سیتسمهای macintosh و UNIX به نوعی نسبت به این حمله ها کمتر مستعد هستند، البته نه الزاماً به این علت که ایمن تر هستند، بلکه به این دلیل که معمولاً سیستمهای windows برای مهاجمین اهداف جذاب تری به شمار می روند. سیستمهای UNIX در رده بعدی قرار دارند و سیستمهای macintodh تا به امروز کمترین صدمه را از آسیب پذیریهای خود دیده اند.

نامه الکترونیکی

چند سال قبل میان کاربران پست الکترونیکی شایعاتی گسترش یافت مبنی بر اینکه با رد یافت نامه الکترونیک ممکن است به ویروس آلوده شوید. مدیران و مسئولان سیستم مجبور بودند مدلوماً به کاربران اطمینان دهند که این امر «غیرممکن» است ، و تا زمانیکه فایل ضمیمه به اجرا در نیاید ماشین و کاربران آن در امنیت کامل هستند.

آلوده شدن از طریق نامه الکترونیکی امروز دیگر امر محالی نیست و در واقع بسیار هم محتمل است. دو قابلیت اضافه شده به نرم افزارهای پست الکترونیکی باعث این مسئله شده اند.

اولین تغییر این است که امروزه برنامه هایی برای پست الکترونیکی وجود دارند که می توانند ضمایم را بصورت خودکار اجرا نمایند. در گذشته کاربر فایل ضمیمه را ذخیره و سپس آنرا اجرا می کرد، اما در حال حاضر اجرای خودکار ضمایم کارها را- مخصوصاً برای کاربران مبتدی که می خواهند بدون انجام عملیات اضافه آنچه که فرستاده شده است را ببینند- ساده تر کرده است.

دومین تغییر این است که چون تلاش بر این بوده که نرم افزار پست الکترونیکی ساده و قوی تر گردد، امروز امکان برنامه نویسی HTML در بدنه اصلی نامه الکترونیکی وجود دارد، علیرغم اینکه HTML می تواند حاوی دستورالعملهای مشکل ساز باشد. بعنوان مثال HTML می تواند مرورگر وب را بصورت خودکار به سمت یک پایگاه وب از پیش تعیین شده هدایت کند که شاید برای شما یا فرزندانتان مناسب نباشد.

توجه داشته باشید افرادی که نامه های الکترونیکی این چنین ارسال می کنند می توانند بسیار خلاق باشند. اخیراً تعدادی نامه الکترونیکی آلوده به ویروس منتشر شد که ادعا می کرد از طرف مایکروسافت است و حاوی آخرین وصله های امنیتی می باشد که در برابر ویروسها و کرمها از شما محافظت می نماید. این نامه ها شامل تصاویر و نمادهایی هستند که قابل اطمینان و معتبر بنظر می رسند و لذا کاربر را متقاعد می سازند که ضمایم باید به سرعت به اجرا در بیایند. واضح است که اگر کسی ضمیمه ها را اجرا کند دچار دردسرهای اساسی خواهد شد .

پایگاه وب

هنگامیکه شبکه گسترده جهانی راه اندازی شد صفحات وبی ایجاد شدند که شامل متنها وتصاویر بودند. اکنون این صفحات شامل محتویات بیشتری هستند مثل برنامه های پویایی که روی ماشین شما download شده و اجرا می گردند (ACTIVEX, JAVA, JAVASCRIPT) اگر به مرورگر خود اجازه دهید این برنامه ها را بدون بررسی قابلیت اطمینان پایگاه وب مورد نظر اجرا نماید . برنامه Javascriptبطور کلی ایمن است اما Java و ACtvex می توانند بسیار خطرناک باشند. معمولاً می‌توان مرورگرها را طوری تنظیم کرد که به این برنامه ها اجازه اجرا ندهند و یا قبل از اجرای آنها از کاربر اجازه بگیرند.

Add-on و plug-in

مرورگرهای وب و بسیاری برنامه های دیگر (مثل پردازشگر های کلمه و صفحات گسترده به برخی از برنامه ها اجرا شدن از داخل برنامه اصلی را می دهند. نمونه رایج آن برنامه Adobe Acrobat Reader است که به شما اجازه می دهد هنگام مرور وب ، فایلهای pDF را مشاهده کنید هنگامیکه

Plug-in ها یا add-on ها نصب می شوند می توانند هر کاریکه برنامه اصلی انجام میدهد – مانند خواندن از دیسک و نوشتن روی آن یا استفاده از ارتباط شبکه- را انجام دهند و لذا تنها باید زمانی نصب شوند و مورد اطمینان باشد

حفره های امنیتی

حفره های امنیتی اشکالاتی در بخشهایی از سیستم عامل یا دیکر اجزای سیستم هستند که به مهاجم اجازه دسترسی به اطلاعات موجود در سیستم یا کنترل آنرامی دهند. در سالهای اخیر اکثر تولیدکنندگان نرم افزار با سرعت قابل قبولی به مشکلات امنیتی که در سیستمها یشان کشف می شود پاسخ می دهند. بنابر این اگر بصورت منظم وصله های امنیتی را روی سیستم خود اعمال کنید می توانید قبلاز انتشار گسترده اشکالات ، راههای نفوذ را بر مهاجمان ببندید.

اشتراک فایلها

به اشتراک گذاری فایل در اشکال مختلف در همه سیستم عاملها وجود دارد اشتراک فایل در میان کارمندان یک شرکت کار بسیار مفیدی است. اگر چندین دستگاه مختلف دارید ، اشتراک فایل میان آنها یک قابلیت بسیار مورد نیاز خواهد بود . با این وجود اگر از روش اشتراک فایل از طریق اینترنت استفاده می کنیدو سیاست امنیتی مناسبی برای اینکار (مثل استفاده از نام کاربر و رمز عبور مناسب و محدود بودن امتیاز نوشتن و به روز رسانی) ندارید آنگاه هر مهاجمی در دنیا هم خواهدتوانست فایلهای شما رابه اشتراک بگذارد . علاوه بر این اگر به دیگران اجازه دهید که روی دیسکهای شما امکان نوشتن داشته باشند، آنگاه مهاجم خواهد توانست رایانه شما را به شکل دلخواه خود تنظیم کند.

هدایت بوسیله download ها

هدایت بوسیله download ها زمانی رخ می دهدکه به یک پایگاه وب مراجعه می کنید و برنامه HTML موجود در صفحه بصورت خودکار یک برنامه Java یا Activex را در خواست می کندو آن برنامه نیز یک برنامه دیگر را download می نماید ،آنرا اجرا می نماید یا طوری برنامه ریزی می کند که در آینده بتواند آنرا به اجرا در آورد همچنین کد HTML می تواند وارد نامه الکترونیکی گردد . اگر به برنامه های Java یا Activex بدون اینکه از شما اجازه بگیرند و یا حتی به شما اطلاع دهند اجازه نصب کردن برنامه داده باشید ، آنگاه خواهند توانست downlcad شوند و هر چه را که می خواهند نصب نمایند.

بی اعتمادی به نرم افزارهای مسروقه

مفهوم نرم افزار تجاری مسروقه مفهوم تازه ای نیست . چندین سال است که دیسکهای فشرده جعلی فروخته می شوند و نسخه های اینترنتی آنها- warez نامیده می شوند- نیز رایج هستند . از مدتها پیش این سوءظن وجود داشته که این دیسکهای فشرده می توانند حاوی ویروس باشند اما احتمال بیشتری که وجود دارد این است که این نوع نرم افزار ممکن است تعمداً حاوی وصله ای باشند

.

فصل چهارم

امنیت خدمات شبکه

اصول اولیه

وصله های امنیتی را باید بصورت منظم بری نرم افزارهای خود به روز رسانی کنید. از آنجا که مشکلات امنیتی می توانند با روشهای متعددی به شما آسیب برسانند، هنگامیکه به اینترنت متصل می شوید، احتمال آسیب پذیری بیشتر می گردد. اگر در سیستم عامل یا نرم افزار کاربردی شما اشکال امنیتی وجود داشته باشد مطمئن باشید مهاجمین از آن اطلاع دارند و با استفاده از آن روشهایی برای نفوذ به رایانه شما طراحی می کند.

قانون چهارم :

سیستم عامل و نرم افزارهای کاربردی مهم خود را به روز رسانی کنید.

به روز رسانی الزاماً به معنای استفاده از آخرین نسخه ها نیست. بیشتر شرکتها و توسعه دهندگان، اشکالات امنیتی نسخه های رایج را برطرف می کنند. توجه داشته باشید که این مسئله در مورد نرم افزارهای رایگان معمولاً فقط برای آخرین نسخه های موجود صادق است، این بدان معناست که اگر می خواهید از اشکالات امنیتی مصون بمانید باید بطور منظم نرم افزار خود را به آخرین نسخه موجود آن ارتقا دهید.

پست الکترونیکی

سیر تکامل

اگر تاریخچه شبکه را بررسی کنی (۱۰ تا ۳۰ سال گذشته) مشاهده می کنید که در ابتدا از پست الکترونیکی تنها برای ارسال پیامهای متنی استفاده می شد. اکثر سیستمهایی که از پست الکترونیکی استفاده می کردند از روشهای مختلفی برای انتقال فایلها بهره می گرفتند . روشهای انتقال فایل تا حدودی نامأنوس بودند و استفاده از آنها سخت

بود، البته در اوایل کار که بیشتر کاربران پست الکترونیکی متخصصین فناوری بودند این مسئله چندان مهم نبود، اما هنگانیکه استفاده از آن عموم گسترده تری یافت، باید برای استفاده توسط عموم ساده تر می گشت.

مشکل این بود که پست الکترونیکی اولیه تنها برای انتقال منتهای ساده طراحی شده بود و فایلهایی چون برنامه های اجرایی در متن خود کاراکترهای غیر چاپی داشتند که در متون ساده قابل نمایش نبودند. راه حل پیشنهادی این بود که اطلاعات غیر چاپی بگونه ای کدگذاری شوند که بتوان آنها را در متون ساده به نمایش درآورد. در این روش بعد از دریافت پیام، فایل کدگذاری شده کدگشایی می گردد و به شکل اصلی خود در می آید.

بعد از آن مفهوم ضمیمه بوجود آمد تا با استفاده از آن بتوان انواع بیشتری از فایلها را کدگذرای نمود. امروزه این روش جدید MIME نامیده می شود. هنگامیکه کاربرد طوری تغیر کردند که بتوانند ضمایم را بطور خودکار باز کند بنابراین دریافت کننده پیام می توانست آنچه برای وی فرستاده شده است را بدون انجام فعالیت اضافه مشاهده نماید.

در همان زمان شبکه گسترده جهانی نیز مرسوم شد و از HTML برای قالب بندی صفحات وب بهره گرفت. HTML تبدیل به یکی از روشهای کدگذاری MIME را فراهم می کرد (تغییر فونت ها، رنگها، تصاویر، و اشاره گرها به صفحات وب) در حال حاضر برنامه های پست الکترونیکی بصورت خودکار دستورات HTML درون صفحات ارسال شده را نیز اجرا می کنند.

تأثیر ارتقای پست الکترونیکی

افزوده شدن این قابلیتها (امکانات قالب بندی) به برنامه های پست الکترونیکی ،کاربرد آنها را مفیدتر ساخت. کاربران از آن پس می توانستند انواع فایلها را بسادگی تبادل کنند. با استفاده از فونت ها، رنگها و تصاویر، نامه شکل مطلوب تری پیدا می کرد و قالب بندی ساده آن بدون نیاز به برنامه پردازشگر کلمات صورت می پذیرفت. با این وجود، این ارتقا ابعاد منفی نیز در پی داشت.

همانطور که قبلاً ذکر شد تا قبل از ایجاد این پیشرفتها کسی از طریق پست الکترونیکی تحت تأثیر مستقیم ویروسها و کرمها قرار نمی گرفت. همچنین تا زمانیکه برنامه دریافت شده موجود رد ضمائم نامه دریافتی را اجرا نیم کردید از خطرات امنیتی مصون بودید. اکنون اما برنامه هایی که دریافت می کنید می توانند بصورت خودکار به اجرا در آیند که مفهوم آن این است که این برنامه ها خواهند تواسنت شما را به پایگاه وبی هدایت کنند که در ان اعمال مخربی مثل download نرم افزارهای مخرب صورت می پذیرد. علاوه بر این، دستورات ویژه HTML می توانند مهاجم را به راهبر رایانه شما تبدیل کنند که البته چگونگی آن بستگی به اشکالات موجود در برنامه مفسر دستورات HTML رایانه شما دارد.

پست الکترونیکی گمراه کننده است

در بسیاری از مواقع آدرس پست الکترونیک که جلوی عبارت «فرستنده» قرار میگیرد معتبر نیست. این قابلیتی است که هرزنامه نویس آنرا برای سوء استفاده از سیستم شما بکار می برند . گاهی اوقات اگر گل سرآیند را بررسی کنید ممکن است بتوانید متوجه شوید که این نامه واقعاً از کجا و از سوی چه کسی ارسال شده است.

چگونه می توانید از خود محافظت نمایید؟

قانون پنجم:

برنامه پست الکترونیکی خود را طوری پیکربندی نمایی که ضمائم را بصورت خودکار باز نکند.

هر فردی که آدرس پست الکترونیکی شما را بداند یا بتواند آنرا حدس بزند می تواند برای شما نامه حاوی ضمیمه ارسال کند. این ضمیمه ممکن است مفید و قابل استفاده و یا ویروس ، کرم، یا تراوایی باشد که بتواند آسیبهای جدی به سیستم شما ارسال وارد نماید. اکثر برنامه های جدید پست الکترونیکی ضمایم را قبل از اجازه شما باز نمی کنند، اما اگر برنامه شما بگونه ای باشد که آنرا بصورت خودکار باز نماید، باید بتوانید این گزینه را غیر فعال کنید.

قانون ششم:

قبل از باز کردن هر ضمیمه به نام آن دقت کنید تا مطمئن شوید که یک برنامه اجرایی نیست.

نویسندگان ویروس بسیار زیرک هستند. آنها معمولاً ضمایم را با نامهایی چون budgest.xls.vbs ارسال می کنند ناظری که نمی داند vbs چیست تصور می کند. یک فایل Excel با نام budget از سوی مایکروسافت برای وی ارسال شده (خصوصاً در حالتی از تنظیمات که سیستم عامل پسوندهای شناخته شده را به کاربر نمایش نمی دهد) اما این فایل در حقیقت یک برنامه اجرایی visual Basic است که نام آن budgest.xls می باشد، xis تنها بخشی از نام این فایل است و هیچ ارتباطی با Excel ندارد. در بدترین حالات این برنامه ممکن است بتواند تمامی دیسک سخت سیستم شما را پاک نماید.

قانون هفتم:

هرگز ضمیمه ای را که از جانب افراد ناشناس برایتان ارسال شده است باز نکنید، مگر اینکه اطمینان داشته باشید که آن نوع فایل نمی تواند حاوی کد مخرب باشد.

به خاطر داشته باشید برنامه هایی مثل Microsoft word (پردازشگر کلمات) و Microsoft Excel (صفحه گسترده داده) و تمامی برنامه های مشابه، دارای قابلیت استفاده از Macro هستند که می تواند حاوی ویروس باشد. حتی فایلهای PDF نیز می توانند حاوی قطعه برنامه های مخرب باشند (اگر چه این فایلها تنها زمانی می توانند خطرناک باشند که با نرم افزار کاربردی Adobe acrobat professional باز شوند و باز کردن انها با برنامه هایی چون Adobe acrobat reaser که کاربرد بیشتری میان افراد دارد خطر خاصی در پی نخواهد داشت) با استفاده از راهنمای کاربری و یا صفحات راهنما می توانید بررسی کنید که چگونه می توان بعضی قابلیتها (خصوصاً آنهایی که در سیستم بندرت مورد استفاده قرار میگیرند) را از کار انداخت.

قانون هشتم:

هرگز ضمائم ارسالی از جانب افراد شناخته شده و قابل اعتماد را نیز باز نکنید، مگر اینکه اطمینان داشته باشید که فرد مورد نظر این ضمایم را بررسی کرده و با ملاحظه کامل برایتان ارسال نموده است.

امکان دارد که ماشین دوست شما ویروسی داشته باشد که بدون اطلاع وی فایلهای آلوده را به همه افرادی که در فهرست آدرسهای وی هستند ارسال نماید.

قانون نهم:

پیکر بندی برنامه پست الکترونیکی خود را بررسی کنید تا فایلهای HTML تفننی را پردازش نکند و فایلهای آلوده را به رایانه های دیگر ارسال ننماید.

این بدان معناست که ممکن است بعضی از قابلیتهای تزئینی نامه های الکترونیکی را از دست بدهید، ولی در عوض کنترل بهتری روی عملکرد برنامه پست الکترونیکی خود بدست آورید. توجه داشته باشید که در برخی از برنامه های پست الکترونیک برای اجرا شدن کد HTML حتی لازم نیست پیامی که حاوی کد HTML است را باز نمایید و به نمایش در آمدن ان پیام در صفحه پیش نمایش برای اجرا شدن کد کافی است. علیرغم اینکه نامه الکترونیکی می تواند حاوی قطعه برنامه های HTML باشد اما بسیاری از مرورگرها و برنامه های پست الکترونیکی به شما اجازه می دهند plug-in, javasscrpt, cookie صفحاتی که بعنوان بخشی از نامه الکترونیکی دریافت می شوند را غیر فعال نمایید.

قانون دهم:

از ISP خود سوال کنید که آیا قبل از ارسال نامه های الکترونیکی، آنها را از نظر داشتن ویروس و تهدیدات مشابه بررسی می کند یا خیر.

به دلیل افزایش روز افزون فعالیت کرمها و ویروسها اکثر ISPها اینکار را انجام می دهند. توجه داشته باشید که نباید توقع داشت که غربال سازی ISP شما صد در صد ثمربخش باشد اما عملکرد پیشگیرانه ISPها می تواند به تلاشهای شما در برقراری امنیت کمک کند. اگر ISP شما از مسائل امنیتی آگاه نیست بهتر است برای ارائه خدمات امن تر به خودتان و نیز دیگر مشتریان با آنه همکاری کنید. مثلاً می توانید یک نسخه از کتابی که هم اکنون مشغول مطالعه آن هستید را بصورت رایگان به آنها هدیه نمایید؟

هرزنامه

هرزنامه نامی است که برای نامه های الکترونیکی ناخواسته بکار می رود خصوصاً نامه های تجاری که از طرف افراد ناشناس و بصورت متعدد- احتمالاً براساس این باور که دریافت کننده به محصولات آنها علاقه مند خواهد شد- ارسال می شوند. در سالهای اخیر تعداد هرزنامه ها بطور چشمگیری افزایش یافته است. در سال ۲۰۰۳ بیش از ۵۰٪ از کل نامه های الکترونیکی تبادل شده در اینترنت هرزنامه بوده است۱ بسیاری افراد هم اکنون به ازای دریافت هر یک نامه معتبر حدود ۱۰ هرزنامه دریافت می کنند.

اگر در فیلد «موضوع» هرزنامه ها عبارتهایی نظیر «SPAM» وجود می داشت، آنگاه می توانستیم به آسانی تمامی انها را حذف کنیم. قوانین مصوب قضایی حکم می کند که هر نامه الکترونیکی ناخواسته که از سوی شرکتها تجاری ارسال شود پیگرد قانونی خواهد داشت. با این وجود به دلیل حجم وسیع هرزنامه ها و نیز توانائی های محدود نیروهای انتظامی در حال حاضر اجرای این نوع قوانین چندان عملی نیست. هر کس باید بدون خواندن هرزنامه و یا ارسال اخطار به یک سیستم شلوغ دریافت شکایت، یک روش منطقی برای تشخیص و حذف آن داشته باشد.

آشنایی بیشتر با هرزنامه

برای آشنایی با مشکلاتی که هرزنامه در پی دارد باید سه نکته را در نظر گرفت:

اف) چگونه هرزنامه نویس ها آدرس شما را بدست می آورند.

ب) چه چیزی هرزنامه تلقی می شود (با جزییات دقیق) .

ج) چرا نویسندگان هرزنامه، آنها را ارسال می کنند.

الف) اگر یکی از فعالیتهای زیر را انجام داده باشید هرزنامه نویس ها موقعیت بدست آوردن آدرس شما را دارند:

- نامه یا امضای خود را به یک فهرست آدرس عمومی ارسال کرده باشید.
- به یک هرزنامه پاسخ داده باشید، مثلاً خواسته باشید که از فهرست دریافت کنندگان حذف شوید.
- برای گروه های خبری نامه فرستاده باشید.
- به هر دلیلی در یک فرم بو ثبت نام کردهباشید و آدرس خود را در آن وارد نموده باشید (حتی اگر کاملاً مطمئن باشید که به سازمان معتبری مراجعه نموده اید).
- از رایانه ای که یک برنامه شناسایی روی آن در حال اجرا بوده استفاده کرده باشید (این برنامه شناسایی در بسیاری از سیستمهای UNIX نام کاربری شما را به هر کس که انرا سوال کند ارائه می دهد).
- به مرورگر اجازه داده باشید ادرس شما را ذخیره کند.
- از نرم افزارهای ارسال پیام فوری استفاده کرده باشید.
- آدرس پستی خود را در یک صفحه وب قرار داده باشید، یعنی اجازه داده باشید که آدرس پستی شما برای همه قابل مشاهده باشد.
- یک نام دامنه برای خود ثبت کرده باشید و یا آدرس خود را در گروه پشتیبانی فنی یک پایگاه وب قرار داده باشید.
- از آدرسهای پستی قابل حدس زدن استفاده کرده باشید.

- آدرس خود را روی یکی از سیستمهایی که قبلاً به آنها نفوذ شده است قرار داده باشید.

اگر هر یک از این موارد در مورد شما صدق کند احتمال زیادی وجود خواهد داشت که آدرس شما مورد سوء استفاده قرار بگیرد و یا حتی به نویسندگان هرزنامه فروخته شود. به عبارت دیگر اگر به هر دلیلی از اینترنت استفاده می کنید این امکان وجود دارد که در فهرست دریافت کنندگان هرزنامه ها قرار بگیرید.

ب) برخی از نامه های تجاری به دلیل تعداد زیاد و نامربوط بودنشان کاملاً شناخته شده هستند و همه می دانند که هرزنامه می باشند. در مورد بعضی نامه های دیگر این مسئله کمتر آشکار است. در برخی موارد این بستگی به دریافت کننده دارد که یک نامه الکترونیکی دریافتی را هرزنامه بداند یا خیر. مثالهای زیر به روشن شدن بیشتر موضوع کمک خواهند کرد:

- آیا یک نامه الکترونیکی که حاوی اطلاعاتی در مورد چگونگی مراقبت از اجزای صورت است یک هرزنامه به شمار می رود؟ پاسخ: بله، هرزنامه است، مگر اینکه شما جراح پلاستیک باشید و این نامه الکترونیکی یک مقاله دانشگاهی باشد و نه یک آگهی تجاری.
- آیا درخواست مقاله از شما برای یک گردهمایی دانشگاهی با موضوعی مبهم که به چندین فهرست آدرس فرستاده شده یک هرزنامه بشمار می رود؟ پاسخ: شاید. مگر اینکه بطور اتفاقی موضوع آن مورد علاقه شما باشد و مایل باشید به آن پاسخ دهید.
- شرکتی که به شما محصولی فروخته و اطلاعاتی را در مورد محصول بعدی خود برای شما و بسیاری از مشتریهای دیگر ارسال می کند، آیا هرزنامه فرستاده است؟ پاسخ: خیر. اما برنامه غربال ساز هرزنامه در ISP شما ممکن است زمان زیادی را صرف شناسایی این کند که تشخیص دهد چنین نامه ای هرزنامه است یا خیر.
- اگر یک نامه الکترونیکی حاوی مطلبی باشد که با تمام تعاریف یک هرزنامه تلقی شود، آیا حتماً هرزنامه است؟ پاسخ: بله، اما تنها در صورتکیه اصل آن فرستاده شده باشد. اما مثلاً اگر این نامه از سوی یکی از

خوانندگان برای نویسندگان این کتاب فرستاده و در ان مثالهای جالبی در ارتباط با هرزنامه ها ذکر شده باشد مطمئناً هرزنامه نیست و نباید غربال شود.

- ج) چرا هرز نامه نویس ها برای افراد هرزنامه ارسال می کنند؟ ساده ترین جواب: چوناینکار جواب می دهد۱ اگر هرزنامه را مورد بررسی قرار دهیدسریعاً متوجه یک الگو در ان می شوید. معمولاً هرزنامه ها در مورد مسائلی هستند چون بدست آوردن، پول یا پس انداز آن، ارتقای زندگی عاطفی یا خصوصی ، و افزاش سلامتی . این موضوعات یک نقطه مشترک مهم دارند: اغلب ما در مورد این مسال نگرانیهای جدی داریم و تعدادی از ما نیز توجه بسیار اندکی از دریافت کنندگان، این نامه ها را پیگیری کنند (مثلاً چیزی حدود ۱ نامه در میان هر ۱۰۰٫۰۰۰ در یافت کننده) هرزنامه نویس هایی که چندین میلیون پیام در روز ارسال می کنند می توانند پول زیادی از این راه بدست آورند.

با هرزنامه ها چه باید کرد؟

روشهای بسیاری وجود دارند که با استفاده از آنها می توان هرزنامه را محدود و کنترل کرد. برخی از دولتها در حوزه قضایی خود قوانینی را برای جلوگیری از گسترش هرزنامه تصویب کرده اند. اکثر ISP ها معتقدند که استفاده از تسهیلات آنها برای فرستادن هرزنامه بر خلاف توافقنامه های کاری آنها است. تصویب چنین قوانینی می تواند مؤثر باشد، اما تاکنون اعمال اکثر قوانین مربوط به هرزنامه بسیار مشکل و پر هزینه بوده و در بسیاری موارد هیچ راهکار اجرایی برای آن اندیشیده نشده است.

برخی از کاربران عمده پست الکترونیکی از پذیرفتن نامه های الکترونیکی که از سوی ISPهای منتشر می شود که اجازه فعالیت به هرزنامه نویس ها را می دهند امتناع می ورزند. اینکار می تواند موثر واقع شود، زیرا ISPها را وادار می کند که فعالیتهای مرتبط با هرزنامه را متوقف سازند. با این وجود معمولاً این روش به مشتریان بی گناهی

که تعداد کمی نامه الکترونیکی به مقاصد مختلف ارسال می کنند هم آسیب می رسانند. برنامه های زیادی وجود که برای تشخیص هرزنامه، حذف آن و یا هشدار به دریافت کننده مبنی بر دریافت یک هرزنامه بکار می روند . این برنامه ها را می توان در پایگاه وب ISP یا سرویس گیرنده پستی به اجرا در آورد. این برنامه ها محتوای نامه و منشأ ارسال آنرا بررسی می کنند ف اما از انجا که این معیارها به سختی قابل ارزیابی هستند عملکرد این برنامه ها نیز معمولاً دارای تشخیص منفی نادرست (flash negative) و تشخیص مثبت نادرست (flash positive) می باشد.

flash negative

flash negative زمانی رخ می دهد که برنامه جستجوگر اعلام می کند که یک نامه الکترونکی هرزنامه نیست، اما در حقیقت هرزنامه است. این بدان معناست که برنامه به هرزنامه اجازه می دهد که از غربال عبور کند و به همین دلیل است که گفته می شود این برنامه ممکن است ۱۰۰٪ موثر نباشد.

flash positive

flash positive بدین معناست که برنامه جستجوگر اظهار می کند که برخی از نامه های بی ضرر هرزنامه هستند. این اتفاق خسارتهای زیادی به بار می آورد، بخصوص اگر در اثر این تشخیص ، نامه فرستاده شده بجای تحویل شدن، حذف گردد. ممکن است با flash positive نامه های الکترونیکی عادی و بی ضرر از دست بروند و غیر قابل بازیابی شوند.

هدف برنامه های جستجوی هرزنامه به حداقل رساندن flash negative و از بین بردن flash positive می باشد. متاسفانه کاهش flash negative معمولاً flash positive را افزایش می دهد. افرادی که به هر دلیلی نیاز به دریافت نامه های الکترونیکی شبیه به هرزنامه دارند ممکن است از این طریق آسیب ببینند. آخرین نمونه گزارش

شده این اتفاق در مورد یک خبرنامه دانشگاهی بود که در آن در ارتباط با هرزنامه ها مطالبی مطرح شده بود. از آنجا که خبرنامه دارای مثالهایی در مورد هرزنامه ها بود، توسط جستجوگرها بعنوان یک هرزنامه شناسایی شد و isp های جستجوگرها بعنوان یک هرزنامه شناسایی شد و isp های متعددی آنرا غربال و حذف نمودند.

علاوه بر جستجوگرهای هرزنامه ، روشهای غربال سازی هرزنامه نیز وجود دارند که از فنون پرسش – پاسخ استفاده می کنند. در این روش هنگامیکه نامه ای از یک فرستنده ناشناس دریافت می شود، در میان راه (قبل از اینکه گیرنده آنرا باز کند) متوقف میگردد. سپس پرسشی برای فرستنده ارسال می شود و در آن از وی درخواست میگردد نامه ای که فرستاده است را تائید کند تا ثابت شود آن نامه از سوی همان فرد است و نه از جانب شخص دیگر یا یک نرم افزار.

فرم تائیدیه چنان طراحی شده که بطور خودکار نمی تواند مدیریت شود و نیز برای هرزنامه های بعدی موثر نیت . اگر تا چند روز هیچ تائیدیه ای دریافت نشود، نامه بجای تحویل شدن، حذف می گردد. مشکل این روش این است که نیازمند مداخله دستی فرستنده است. اگر نامه ای را بفرستید و قادر نباشید که به درخواست تائیدیه سریعاً پاسخ دهید نامه شما تحویل نخواهد شد. همچنین اگر دو ISP بصورت متقابل از این سرویس استفاده کنند ممکن است هرگز از یکدیگر نامه ای دریافت نکنند، زیرا اولین دریافت کننده نامه را نمی بیند مگر اینکه تائید شده باشد، و تقاضای تائید نیز ارسال نخواهد شد، چون فرستنده آن ناشناس است. برخی از صافیهای هرزنامه بجای اینکه نامه های مشکوک را حذف کنند آنها را در یک پوشه مخصوص قرار می دهند. بنابراین شما می توانید بطور متناوب پوشه هرزنامه را بررسی کنید تا مطمئن شوید که محتویات آن قربانیهای flash positive نیستند.

روش امیدوار کننده جدید ضد هرزنامه روشی به نام Bayesian filtering است. در این روش قوانین غربال سازی با شناخت شما از هرزنامه اصلاح می شود. این قوانین می توانند در مورد هر دریافت کننده ای متغیر باشند. هدف از این روش، آموزش دیدن برنامه غربال ساز از رفتار شما است تا بتوانند فرد مورد اطمینان شما را تشخیص دهد و محتویاتی که معمولاً بعنوان هرزنامه شناسایی نمی شوند اما به هر دلیلی مورد توجه شما نیستند را رد کند.

صافیهای Bayesian از فنون زبان شناسی استفاده می کنند تا به نامه هایی اجازه عبور دهند که حاوی لغات مخصوصی هستند و براساس تجربیات گذشته رفتار پست الکترونیکی شما در نامه های واقعیتان بکار می روند اما بندرت در هرزنامه ظاهر می شوند. صافیهای Bayesian برای اکثر برنامه های پست الکترونیکی قابل استفاده هستند.

اگر هرزنامه برای شما مشکل آفرین شده است باید بررسی کنید که آیا ISP شما قابلیتهای شناسایی و غربال سازی هرزنامه را ارائه می دهد یا خیر. همچنین باید نرم افزارهای پست الکترونیکی خود را بررسی کنید تا معلوم شود آیا می توانند هرزنامه ها را غربال نمایند یا نه.

استفاده از شبکه جهانی وب

هنگامیکه این کتاب در سال ۲۰۰۳ نوشته شد، وب حدود ۱۰ سال با سطوح دسترسی مختلف در اختیار عموم قرار داشته است. در حال حاضر وجود وب برای آندسته از افرادی که مرتباً در کارف مدرسه و تفریح از شبکه استفاده می کنند ضروری است. از آنجا که وب بصورت ابزاری مفید و رایج در آمده، فراموش شده که می تواند محیطی خصومت آمیز باشد.

ایمن نگهداشتن مرورگرها

بطور کلی وب نسبتاً ایمن است اما استفاده از آن خطرات بالقوه ای نیز در پی دارد. پایگاه های وب معمولاً دارای متنها و تصاویر ایستا هستند، اما می توانند برنامه های پویایی نیز داشته باشند که برای اجرا در رایانه شما در نظر گرفته شده باشند.

قانون یازدهم

به پایگاههای وب اجازه ندهید که برنامه های مخرب را در رایانه شما download و اجرا نمایند، مگر اینکه به آن پایگاه وب کاملاً اطمینان داشته باشید.

Download پویای برنامه ها گاهی اوقات می تواند بسیار مفید باشد. این قابلیت به شما اجازه می دهد که از خدمات برخط استفاده کنید، مثلاً به ویروس یابی و رفع مشکلات امنیتی بپردازید. همچنین باعث می شود نرم افزار شما بتواند بسادگی نصب و به روزرسانی شود، بدون اینکه لازم باشد کاربر روالهای چند مرحلهای پیچیده و فنی انجام دهد.

متاسفانه download پویا و خودکار برنامه ها می تواند خطرناک و مخرب نیز باشد. کلیه مرورگرها به شما اجازه می دهند که برنامه های activex, java,javascript و دیگر ابزارهای برنامه نویسی را روی رایانه خود download و اجرا کنید، اما اگر می خواهید کاملاً ایمن باشید نباید اجازه اجرای این برنامه های را صادر نمایید . البته با غیر فعال نمودن این ویژگیها متوجه خواهید شد که بسیاری از پایگاههای وب نمی توانند مثل گذشته کار کنند.

بجای مسدود کردن دسترسی به این همه پایگاه وب باید بدنبال یک راه حل منطقی بود:

- قابلتیهای نسبتاً ایمن و رایج مانند javascript را فعل نمایید. با اینکار به پایگاه های وب زیادی اجازه می دهید که بتوانند بطور صحیح عمل کنند.
- قابلتیهای مانند java و activex که ایمنی کمتری دارند و کمتر نیز استفاده می شوند را غیر فعال کنید یا مرورگر خود را طوری تنظیم نمایید که قبل از بکارگیری آنها از شما اجازه بگیرد . غیر فعال نمودن این قابلیتها بدین معناست که از آن پس بعضی از توابع مرورگر کارنخواهند کرد. باانجام اینکار بعضی از پایگاه های وب ممکن است به شما هشدار دهند و برخی دیگر از ادامه فعالیت باز بمانند. اگر مایل نیستید

چنین اتفاقی رخ دهد، مرورگر باید بتواند نیازهای پایگاه وب را شناسایی کند و برای download و اجرای برنامه مورد نیاز جهت مشاهده صحیح محتویات آن پایگاه از شما سوال نماید.

قانون دوازدهم:

به آدرس پایگاه وب و آدرسی که به آن متصل می شوید دقت کنید و هنگام مشاهده یک پایگاه وب ناشناخته، به آن توجه نمایید، خصوصاً اگر به آن پایگاه اجازه اجرای یک برنامه روی رایانه خود را داده اید.

مرورگرهای وب می توانند طوری تنظیم شوند که آدرس پایگاه وب در حال مشاهده را نشان دهند (این قابلیت معمولاً navigation bar یا address bar نامیده می شود.) هنگامیکه مکان نمای شما به یک ارتباط اشاره می کند، این ویژگی می تواند نشان دهد که آن ارتباط به چه ادرسی اشاره دارد (نوار وضعیت). با مشاهده آن آدرس متوجه می شوید که به چه پایگاه وب دیگری فرستاده خواهید شدف پایگاهی که ممکن است غیر قابل اطمینان باشد، یا شاید نخواهید انرا مشاهده کنید. در عمل ممکن است نخواهید با هر کلیک navigation bar و status bar را بررسی کنید، اما وقتیکه در یک پایگاه وب ناآشنا هستید- بخصوص اگر java یا activex را فعل کرده باشید- باید از این ابزار بگونه ای استفاده نمایید که چنانچه بصورت ناخواسته به پایگاه وب جدیدی هدایت شدید از آن آگاهی یابید.

Cookieها

Cookie اطلاعاتی است که به مرورگر هنگام مشاهده یک پایگاه وب راه دور روی دیسک سخت رایانه می نویسد. هنگامیکه بعدها دوباره همان پایگاه وب را مشاهده کنید، Cookieهای مربوط به شما مجدداً برای آن پایگاه ارسال می شوند. ر واقع هر Cookie مربوط به پایگاه وب مبدأ خود است، اگرچه برخی از اشکالات

موجود در مرورگرها باعث می شوند که پایگاه ها بتوانند Cookieهای یکدیگر را مشاهده نمایند. Cookie به پایگاه وب متذکر می شود که شما چه کسی هستید، میل و سلیقه شما چیست،و قبلاً در آن پایگاه چه فعالیتهایی انجام داده اید. بعنوان مثال هنگامیکه با نام کاربری و رمز عبور خود وارد یک پایگاه وب می شوید، پایگاه وب این اطلاعات را در یک Cookie بر روی رایانه شما ذخیره می کند. وقتی که مثلاً پس از یک هفته دوباره به آن مراجعه می کنید ممکن است براساس اطلاعات موجود در Cookie مذکور بصورت خودکار وارد آن پایگاه شوید. Cookie ها همچنین به پایگاههای وب اجازه می دهند انچه را که در یک جلسه انجام داده اید ردیابی نمایند.

اگر چه یک Cookie به شکل معمول تنها می تواند از پایگاه وب مبدا خود بازیابی شود، اما ممکن است پایگاه وبی که مشاهده می کنید حاوی تصاویر و اشیاء پایگاه وبی که مشاهده می کنید حاوی تصاویر و اشیاء دیگری باشد که مربوط به یک پایگاه وب ثانویه هستند (که پایگاه وب خارجی یا پایگاه وب شخص ثالث نامیده می شود) و آن پایگاه وب ثانویه نیز بتواند Cookieها را ذخیره و بازیابی نماید. از آنجا که تصاویری می توانند نامرئی باشند، ممکن است اصلاً متوجه نشوید که چنین اتفاقی رخ داده است. این تصاویر غیر قابل رویت می توانند با ردیابی پایگاههای وبی که شما آنها را مشاهده می کنید برای اهداف تبلیغاتی بکار روند.

قانون سیزدهم

چگونگی وضعیت ذخیره Cookie ها بر روی رایانه را مورد بررسی قرار دهید. اگر نمی توانید آنها را کنترل نمایید (مانند زمانیکه از رایانه ای در یک مکان عمومی استفاده می کنید) اطلاعات خصوصی خود را وارد رایانه نکنید.

کلیه مرورگرها وب تا سطح کنترل خاصی به شما امکان می دهند که وجود Cookie ها را مجاز بدانید یا خیر. در برخی موارد ممکن است مرورگر میان Cookieهای که در رایانه شما ذخیره شده اند، Cookieهایی که هنگام

بستن مرورگر ناپدید می شوند و آندسته که هنگام مشاهده پایگاه های وب و پایگاه های وب خارجی ذخیره می گردند تفاوت قائل شود. اساساً شما می توانید اجازه ذخیره همه Cookieها ا بدهید، از ذخیره آنها جلوگیری کنید، و یا از مرورگر بخواهید که قبل از ذخیره آنها از شما سوال نماید. شما هرگز مطلع نمی شوید که چه زمانی اطلاعات ذخیره شده در یک Cookie به پایگاه وب مبدا باز می گردد.

Cookieها را می توان بررسی نمود زیرا در قالب متنی هستند، اما چون اطلاعات موجود در آن توسط پایگاه وب مبدا رمزگذاری می شود معمولاً قابل فهم نمی باشند. برخی از مرورگرها اجزاه نمایش و حذف Cookieها را می دهند و برنامه های ثالثی وجود دارند که اجازه مدیریت آنها را نیز برای شما فراهم می آورند.

اگر می خواهید اطلاعاتی که یک پایگاه وب در مورد شما می داند را کنترل کنید باید زمان و چگونگی ذخیره شدن Cookieها روی رایانه خود را کنترل نمایید. توجه داشته باشید که برخی از پایگاههای وب برای اینکه بتوانند بدرستی عمل نمایند نیازمند ذخیره Cookieها روی رایانه کاربر می باشند. عموماً این پایگاه های وب در صورت غیرفعال بودن Cookieها به شما اطلاع می دهند که قادر به انجام یا تکمیل عملیات نیستند.

اگر در اماکن عمومی (مثل کافی نت، کتابخانه ها، مدراس) از مرورگرهای وب استفاده می کنید توجه داشته باشید Cookieهایی که حاوی اطلاعات شما هستند در آنها ذخیره می شوند. در بسیاری از موارد راهبر رایانه ممکن است به شما آنقدر دسترسی نداده باشد که بتوانید Cookieها را کنترل ، نظاره و یا پاک کنید. بنابراین اطلاعات شما در این رایانه می ماند و ممکن است بوسیله فرد دیگری که همان پایگاه وب را مشاهده می کند مورد استفاده قرار گیرد. اگر به پایگاه وبی وارد شده باشید و اطلاعات معتبر شما رد یک Cookie ذخیره شده باشد و کاربر دیگری به همان پایگاه وب مراجعه نماید، ممکن است بصورت خودکار بجای شما وارد ان پایگاه گردد. در نتیجه احتمال دارد که پایگاه وب اطلاطعات ذخیره شده شما (مانند نام، آدرس و اطلاعات کارت اعتباری) را در اختیار این کاربر قرار دهد.

این مورد حتی در یک رایانه خصوصی که چند نفر از آن استفاده می کنند نیز می تواند مشکل ساز شود. در این مواردCookie ها نه تنها یک مشکل برای حریم خصوصی هستند، بلکه یک آسیب پذیری امنیتی نیز بشمار می روند.

حافظه نهان مرورگر وب

هنگامیکه یک مرورگر صفحه یا تصویری را از یک پایگاه وب بازیابی می کند معمولاً یک نسخه از صفحه در حال نمایش را نیز در دیسک سخت رایانه ذخیره می نماید. این مجموعه صفحات و تصاویر ذخیره شده حافظه نهان نامیده می شوند. اگر این پایگاه وب را مجدداً مشاهده کنید و صفحه آن تغییر نکرده باشد ممکن است مرورگر کل صفحه را از ابتدا download نکند، بلکه برای نمایش آن از حافظه نهان استفاده نماید. در برخی موارد صفحات وبی که در حافظه نهان وجود دارند می توانند بصورت offline (یعنی دون اتصال اینترنتی) نیز دیده شوند. این بدان معناست که هر آنچه توسط مرورگر مشاهده می کنید در دیسک سخت رایانه ذخیره شده است . بنابراین اگر برای انجام معاملات مالی از وب استفاده می کنید، اطلاعات خرید، کارتهای اعتباری و حسابهای بانکی شما در آن رایانه کاملاً قابل خواندن و بازیابی خواهندشد. با توجه به میزان مرور و اندازه حافظه نهان، این صفحات و تصاویر می توانند تا مدتهای متفاوتی روی رایانه باقی بمانند.

قانون چهاردهم:

در صورتیکه اطلاعات خصوصی شما در صفحه وب نمایش داده شدف پس از اتمام کار باید حافظه نهان را پاک نمایید. اگر نمی توانید اینکار را انجام دهید (مثلاً هنگامیکه از یک رایانه عمومی استفاده می کنید) نباید از آن رایانه برای تبادل اطلاعات محرمانه شخصی استفاده نمایید.

کلیه مرورگرها اجزاه می دهند حافظه نهان (که فایلهای موقتی اینترنت نامیده می شود) را از روی سیستم پاک کنید، اما بسیاری از رایانه هایی که در اماکن عمومی مورد استفاده قرار می گیرند اجازه کنترل و حذف حافظه نهان را نمی دهند. اگر چه پاک کردن این حافظه پس از ورود اطلاعات حساس از اهمیت بسیار زیادی برخوردار است، اما تا بحال هیچ مرور گری در نوار ابزار خود نمایه ای قرار نداده که با کلیک بر روی آن بتوان به آسانی حافظه نهان را پاک نمود.

انتقال امن

کلیه پیامهایی که در وب دریافت و ارسال می کنید بصورت متن ساده هستند. این بدان معناست که اگر فردی بتواند این منتها را میان راه بدزد، برای وی قابل فهم و خواندن خواهند بود. اگر بخشی از ارتباط قابل اطمینان نباشد دزدی پیام از میان راه راحت تر می شود و لذا توجه به آن اهمیت بسیار بیشتری پیدا می کند.

مرورگرها و سرویس دهنده های وب برای حل این مسئله از رمزگذاری پیان را تغییر می دهد، بنابراین برای افراد غیر مجاز بسیار سخت و حتی غیرممکن می شود که بتوانند پیام رمزگذاری شده را بخوانند نام پروتکل رمزگذرای SSL است. می توانید برای پیامهایی که دریافت می کنید از SSL استفاده نمایید. در اکثر مرورگرها تصویر کوچکی از یک قفل وجود دارد که برای انتقال عادی پیام باز است و برای انتقالاتی از نوع SSL به حالت بسته در https آغاز می شود. در صورتیکه در کشورتان امکان آن وجود داشته باشد، بهرت است همواره از قوی ترین روش رمزگذاری استفاده نمایید .

توجه داشته باشید که این قفل مشخص نمی کند پیامی که از طرف شما به سرویس دهنده اراسل می شود برای رمزگذاری از ssl استفاده کرده است یا نه، اما فرض بر این سات که ارگ صفحه ارسالی رمزگذاری شده باشد،پیام بازگشتی نیز بصورت رمزگذرای شده منتقل می شود.

SSL تنها زمانی کار می کند که مرورگر بداند مخاطب آن کیست. این امر به کمک گواهی امنیتی و امضای دیجیتالی صورت می پذیرد. بطور کلی اگر سرویس دهنده وب بخواهد قابل اطمینان باشد باید از یک مرکز معتبر صدور گواهی، گواهی امنیتی تهیه نماید. اگر این مرکز بخواهد بدرستی به وظیفه خود عمل نماید باید بررسی کند فردی که درخواست گواهی نموده همان کسی است که خودش ادعای آنرا دارد. سپس این مرکز گواهی را بصورت دیجیتالی امضا می کند و مرورگر شما جداولی را برای شناسایی این گواهی ها ذخیره می نماید.

گاهی اوقات از سوی یک پایگاه وب پیامی دریافت می کنید مبنی براینکه گواهی دیجیتالی آن منقضی شده یا متعلق به مکان دیگری است. حالت اول زمانی است که تاریخ اعتبار گواهی بتازگی به پایان رسیده و پایگاه وب برای تمدید آن باید تشریفات اداری تمدید گواهی را دنبال کند. در حالت دوم نیز معمولاً پایگاه مورد نظر تغییر نام داده و این تغیر در گواهی آن منعکس نشده است. با این و جود اگر خواستار سطح مناسبی از ایمنی هستید در هر دو حالت باید تا زمانیکه مشکل بگونه ای رفع شود به ارتباط خود با آن پایگاه خاتمه دهید.

آیا انتقال امن کافی است؟

یک قفل کوچک برای انتقال امن در وب طراحی شده و ایمن بودن انتقال را نشان میدهد. با این وجود انتقال تنها موردی نیست که برای تامین امنیت باید مورد بررسی قرار گیرد. تنها درصد کمی از کلاهبرداریها یا سرقتهای هویت در اثر انتقال ناامن صورت می گیرد. در صد عمده مسائل مواردی هستند چون:

- فقدان اصول اخلاقی در بعضی پایگاههای وب
- سوء استفاده از پایگاه های وب شخصی
- سوء استفاده از رایانه های شخصی

سیاستهای حریم خصوصی

بسیاری از پایگاههای وب برای حفاظت از حریم خصوصی افراد، سیاستهای اعلام شده دارند. این سیاستها مشخص می کنند که چه نوع اطلاعاتی را می توان در پایگاه وب جمع آوری نمود، با آن داده ها چه کاری را می توان یا نمی توان انجام داد، و نیز اینکه چگونه باید از این داده ها حفاظت کرد. کلیه پایگاههای وبی که اطلاعات فردی یا مالی جمع آوری می کنند باید از یک سیاست حریم خصوصی مناسب و اعلام شده برخوردار باشند.

انتقال بی سیم

استفاده از فناوری بی سیم در کشورهای در حال توسعه و توسعه یافته رو به افزایش است. این فناوری معمولاً کم هزینه تر از فناوریهای سیمی است، در اماکن خصوصی راحت رت و سریعتر نصب می شود و اشکالات تنظیمی کمتری دارد. با این وجود فناوری بی سیم دارای دو مشکل بالقوه است:

- امکان دارد اطلاعات در میانه انتقال دزدیده سود.
- با توجه به مکان، آب و هوا، زمان روز، نزدیک بودن تجهیزات رادیویی، سرعت انتقال خط، کیفیت نصب و تداخلهای مخرب، سرعت و کیفیت انتقال ممکن است متفاوت باشد.

در مورد دسته دوم مشکلات، کار زیادی نمی توان انجام داد. این موارد از خصوصیات فناوری بی سیم و از هزینه هایی هستند که برای استفاده از ارتباطات بی سیم باید پرداخت شوند. راه مقابله با دزدی میان راه نیز استفاده از روشهای مختلف رمزگذاری است . اگر سرویس دهنده ای دارید که از روشهای رمزگذاری پشتیبانی می کند حتماً از آن استفاده نمایید (مثل پایگاه های وب مبتنی بر SSL) اگر از پست الکترونیکی مبتنی بر POP استفاده می کنید باید گزینه APOP را انتخاب نمایید تا رمزهای عبور قبل از ارسال رمزگذاری شوند. این ویژگی-مستقل از رسانه

انتقال- امنیت پایانه به پایانه را برآورده می کند. اگر سرویس دهنده از رمزگذاری استفاده نکند باید از محدودیتهای فناوری آگاه باشید و رد صورت لزوم تصمیم بگیرید که از ارتباط چگونه استفاده کنید.

802.11 یا WI-FI

802.11 مجموعهای از استانداردهای در حال توسعه IEEE برای شبکه های محلی بی سیم می باشد. 802.11 که معمولاً WI-FI نامیده می شود، بعنوان جایگزین اترنت سیمی برای اتصال رایانه های خانگی و رایانه های کیفی محبوبیت یافته و مزیتش ارزان بودن و سرعت نسبی آن است.

متاسفانه چندین آسیب پذیری در اغلب پیاده سازیهای WI-FI وجود دار:

- ایستگاه های اصلی، ارتباط ایمن و مطمئنی با یکدیگر ندارند.
- اگر بخواهید ارتباط شبکه ای خود را با فرد دیگری به اشتراک بگذارید، باید نام شبکه خود (SSID) را از حالت پیش فرض تغییر دهید و آنرا طوری تنظیم کنید که نام آن برای افراد غیر مجاز قابل رویت نباشد. در صورت انجام اینکار تنها افرادی که SSID را می دانند خواهند توانست آن ارتباط شبکه ای را ببینند .
- الگوریتم رمزنگاری آن (WEP)ضعیف است و بسادگی می تواند شکسته شود . با این وجود رد غیاب روشهای بهرت می توانید آنرا فعال سازید. به یاد داشته باشید که اگر فردی واقعاً بخواهد انتقال اطلاعات شما (مانند رمز عبور) را بررسی کند استفاده ازاین روش بسیار آسیب پذیر خواهد بود. البته یک روش جدید رمزنگاری (WPA) وجود دارد که کاستیهای WEP را رافع می کند و در تجهیزات جدیدتر قابل استفاده می باشد.استفاده از این روش در شبکه هیا مبتنی بر WI-FI اکیداً توصیه می شود.

تلفنهای سیار

تلفنهای سیار (که تلفنهای دستی یا تلفنهای همراه نیز نامیده می شوند) به شکل گسترده ای برای انتقال صوت بکار می روند و گاهی اوقات نیز می توانند برای انتقال اطلاعات مورد استفاده قرار گیرند. بسیاری از فناوریهای تلفن سیار می توانند مورد استراق سمع و شنود قرار بگیرند و لذا ایمن نمی باشد.

خطوط دور برد

ارتباطات طولانی خصوصاً برای مناطق دوردست معمولاً با استفاده از فناوریهای بی سیم مهیا می شود. این خطوط می توانند به چندین کاربر بطور همزمان خدمات ارائه دهند. اگر روش انتقال بصورت مستقیم باشد (با استفاده از آنتنهای بشقابی یا آنتنهای یاگی) استراق سمع بدون تجهیزات خاص دشوار خواهد بود. این ارتباطات در صورت لزوم می توانند با استفاده از تجهیزات سخت افزاری رمزنگاری بصورت رمزی درایند.

تلفنهای بی سیم حلقه محلی

این فناوری در منازل و ادارات بسیاری از کشورها بکار می رود و نصب کم هزینه و بین قص خطوط تلفن را میسر می سازد و مشکلاتی که تجهیزات زیرساختهای سیمی دراند را ندارد. از طرف دیگر بر خلاف سیمهای مسی، تجهیزات بی سیم در میانه راه قابل دزدیدن و فروختن نیستند، اما همانند تلفنهای سیمی هنگامی که یک مودم به این خطوط متصل می شود می توانند بجای اطلاعات صوتی، سایر انواع اطلاعات را انتقال دهند. فناوری بی سیم ممکن است قابل شنود باشد. بسته به موقعیت محلی، قوانین کشوری و مقررات محلی می توانید از ISP خود درخواست کنید که رمزگذاری شدن ارتباط را بررسی نماید.

اشتراک فایل

در صورت وجود بیش از یک رایانه، استفاده از فایلهای اشتراکی یکی از مهمترین و کاربردی ترین ابزار موجود در شبکه می باشد. در ساده ترین حالت، این ویژگی شما را قادر می سازد در حالیکه در یک سیستم فعالیت می کنید به فایلهای موجود در یک سیستم دیگر دسترسی یابید، آنها را تغیر دهید، در آن سیستم فایل جدید بسازید ، و یا فایلهای موجود در آنرا حذف نمایید. دو سیستم مجزا می توانند هر دو در یک اتاق یا هر کدام در یک نیمکره زمین باشند. اشتراک فایل این امکان را فراهم می سازد که در طول مسافرتها بتوانید به فایلهای رایانه خود دسترسی داشته باشید.

یک رایانه منفرد که بعنوان سرویس دهنده فایل عمل می کند می تواند بعنوان دیسک سخت تعداد یاید رایانه تلقی گردد. در اینصورت بیشتر فایلهای شما رد سرویس دهنده فایل قرار می گیرند و بنابراین می توانید از طریق شبکه به آنها دست یابید.

آسیب پذیری واضحی که در اینجا وجود دارد این است که اگر شما بتوانید به فایلهای خود از راه دور دست پیدا کنید، افراد دیگر نیز می توانند اینکار را انجام دهند. یک آسیب پذیری ضعیفتر این است که اگر فایلها را با دیگران به اشتراک بگذارید ، در برابر آسیب پذیریهایی که ممکن است برای رایانه آنها پیش آید در امان نخواهید بود. مثلاً اگر رایانه ای که به فایلهای شما دسترسی داشته توسط یک ویروس آلوده شود، ممکن است فایلهای شما نیز آلوده گردند.

قانون پانزدهم

اگر از قابلیت اشتراک فایل استفاده نمی کنید آنرا غیرفعال سازید. در صورت نیاز به ان، دسترسیهای خود را به آنچه که واقعاً لازم دارید محدود نمایید.

قانون شانزدهم

اگر از قابلیت اشتراک فایل استفاده می کنید، نام کاربری و رمزهای عبور مستحکم بکار گیرید و مجوز دسترسی را به کمترین حد ممکن که همچنان با آن می توانید کار خود را انجام دهید محدود سازید.

قانون هفدهم

اگر فایلها را با دیگران به اشتراک می گذارید مطمئن شوید آنها مسائل امنیتی را جدی می گیرند. قابلیتهای اشتراک فایل و دسترسی از راه دور این امکان را فراهم می سازند که برای کنترل دسترسی از نام کاربری و رمزهای عبور استفاده کنید، و نامهای کاربری و رمزهای عبور شما را قادر می کنند بتوانید آنچه که یک کاربر انجام می دهد (خواندن، نوشتن، ایجاد و پاک نمودن) را کنترل نمایید. بسیاری از سیستمها می توانند تمامی اعمال یک کاربر را کنترل نمایند. بعنوان مثال می توانید تسهیلات دسترسی از راه دور را بگونه ای محدود سازید که به فایلها تنها اجازه خوانده شدن بدهد. به عبارت دیگر اگر نیازی به دسترسی نوشتن ندارید باید انرا غیر فعال کنید.

سیستمهایی که از بعضی قابلیتهای اشتراک فایلها پشتیبانی می کنند می توانند چاپگرها را نیز به اشتراک بگذارند. اگر چه امکان دسترسی راه دور به چاپگر چندان پرمخاطره نیست، اما بهتر است که آنرا غیر فعال سازیم مگر آنکه ضروری باشد. ممکن است اشکالی در دسترسی راه دور چاپگر وجود داشته باشد که باعث شود مجوزهایی که اختصاصاً برای کارهای چاپی صادر شده، امکان اعمال خراب کارانه را فراهم کنند.

پیامهای فوری

قابلیت ارسال پیام فوری این امکان را فراهم می سازد که پیام تایپ شده روی یک رایانه همزمان روی رایانه های دیگر به نمایش درآید. برخلاف پست الکترونیکی، در این مورد فرستنده و گیرنده باید هر دو در یک زمان متصل

به شبکه باشند. قابلیت ارسال پیام فوری نرم افزارهای متفاوتی دارد. در میان آنها می توان به AIM, YAHOO CHAT, IRC, MSN MESSENGER اشاره نمود.

ارتباطات اینترنتی از قبیل AOL, MSN, YAHOO میزبانهای بازیهای اینترنتی و .. هر یک دارای MESSENGER و CHAT مخصوص به خود هستند. بعضی از آنها با سایرین تبادل اطلاعات می کنند وب برخی دیگر چنین کاری انجام نمی دهند.

بسیاری از سیستمهای ارسال پیام فوری به کاربر اجازه می دهند اسمی انتخاب کند که همراه پیامهای ارسالی اش به نمایش در آید و بدین ترتیب سایرین نیز بتوانند برای او پیام ارسال نمایند. این اسامی ممکن است موجب شوند که هویت اصلی شما پنهان بماند، اگر چه راهبران سیستم ممکن است بتوانند هویت شما را از طریق آدرس IP شناسایی کنند.

قانون هجدهم

قابلیت ارسال پیام فوری می تواند بسیار مفید باشد، اما از آن با آگاهی و دقت کامل استفاده کنید.

قابلیت ارسال پیام فوری به چند دلیل نقش مفیدی ایفا می کند:

- استفاده از آن نسبت به پست الکترونیکی راحتتر و سریعتر است و تقریباً هیچ تاخیری ندارد. این مسئله باعث می شود گفتگوهای انجام شده در آن عملی تر از نامه های الکترونیکی باشند .
- در حالیکه مشغول انجام کار دیگری هستید پیام در پنجره کوچکی روی صفحه شما دریافت و ارسال می گردد و چندان باعث ایاد وقفه در سایر کارهایتان نمی شود.
- نیازی نیست که آدرس پست الکترونیکی (و هویت) خود را برای سایر شرکت کنندگان در گفتگوهای انجام شده در پیامهای فوری فاش کنید.

در موارد خاص استفاده از قابلیت ارسال پیام فوری نسبت به نامه الکترونیکی ارجح است. در نظر بعضی افراد استفاده از این سرویس ایمن تر نیز هست، چرا که پیامها در مکانهای دیگر دیسک کپی نمی شوند، در صورتیکه در پست الکترونیکی این اتفاق می افتد. به ره حال هنوز به کاربران هشدار داده می شود که ممکن است پیامهای فوری آنها ایمن نباشد. مشکل اصلی سیستمهای ارسال پیام این است که بعضی از آنها را مانند سایر قابلیتهای اشتراک فایل هم دراند. این موضوع آنها را مانند سایر قابلیتهای اشتراک فایل- مثل ضمائم نامه های الکترونیکی- دچار مشکل می کند. برخی از سیستمهای ارسال پیام فوری اجزاء اجرای دستورات از راه دور را نیز می دهند و اینکار می تواند منجر به وقوع تهاجم گردد.

خدمات فعال غیر ضروری

سیستم عاملها و برنامه های کاربردی بسیار قدرتمند و کارا هستند . در بیشتر موارد کاربر عادی قابلیتهای موجود در نرم افزار را لازم ندارد. خدماتی که مورد نیاز نیستند باید غیر فعال شوند. متاسفانه بعضی از عرضه کنندگان نرم افزار تمامی قابلیتهای برنامه های خود را فعال می کنند و بستگی به کاربر دارد که از آنها استفاده کند یا نکند، و در غالب موارد هم کاربر از وجود این خدمات آگاه نیست. بعنوان مثال برای چندین سال متوالی بعضی از سیستمهای UNIX بگونه ای طراحی شده بودند که هر دستگاه مجهز به آنها بتواند بعنوان یک مرکز پست الکترونیکی غیرمحدود عمل نماید (البته اگر این قابلیت توسط کاربر غیرفعال نمی شد). این مسئله به هرزنامه نویس ها امکان داد که از این دستگاهها برای توزیع هرزنامه ها استفاده کنند، بدون آنکه بسیاری از صاحبان دستگاهها از وجود چنین قابلیتی آگاهی داشته باشد.

قانون نوزدهم

تمامی خدمات اینترنتی که مورد نیاز نیستند و از آنها کمتر استفاده می کنید را غیرفعال نمایید.

عرضه کنندگان نرم افزارها بطور فزاینده ای در حال آگاه شدن از مشکلات هستند. بنابراین علیرغم علاقه آنها به توسعه و عرضه سیستمهایی با توانمندیهای زیاد، برنامه های خود را با خدمات فرعی غیر فعال شده منتشر می کنند، و کاربر در صورت نیاز می تواند هر یک از آنها را فعال سازد. غیرفعال بودن خدماتی که از آنها استفاده خاصی نمی شود اهمیت زیادی دارد. چنین خدماتی شامل اشتراک فایلها و چاپگر، سرویس دهنده های و سرویس دهنده های پست الکترونیک ، سرویس دهنده های پروتکل انتقال فایل (FTP SERVERS) و غیره می باشند.

نتیجه گیری

تمام افراد و کشورها از فناوری اطلاعات بهره می جویند، اما این فناوری برای کشورهای در حال توسعه جاذبه خاصی دارد و می تواند جا افتادن آنها در جامعه اقتصاد جهانی را تسریع کند. این فناوری هنوز در آغاز راه خود است ولی بسرعت در حال پیشرفت می باشد. متأسفانه همانند سایر پیشرفتهای فناوری، اینترنت نیز می تواند هم برای اهداف مشروع و هم برای اهداف نامشروع مورد استفاده قرار گیرد. همانطور که مشاهده کردیم در دنیای سایبر مجرمان و خرابکارانی وجود دارند که از اینترنت برای حمله به کاربران منفرد و سازمانی استفاده می کنند.

این پروژه حاوی مجموعه ای از الگوها سرآمدی در زمینه امنیت است که در اجرای سیاستها و روشهایی که به موقعیت خاص شما مربوط هستند کمک می کنند. علاوه بر آن مراجع چاپی و الکترونیکی فراوانی که در بر دارنده ابعاد خاص امنیت فناوری اطلاعات هستند و همچنین سازمانهایی که به شکل تخصصی بر روی موضوعات امنیت فناوری اطلاعات تمرکز دارند را معرفی می کند. تمامی این منابع برای افراد و سازمانهایی که در پی گسترش آگاهی خود از امنیت در جهان شبکه ای می باشند مفید خواهند بود.

این شرایط در کشورهای در حال توسعه از اهمیت خاصی برخوردار است. سرمایه گذاری مستقیم خارجی و اعتماد و قابلیت اطمینان در این کشورها بستگی به سطح امنیت و پیاده سازی موفقیت آمیز فناوری و زیر ساختهای آن دارد. دولتها ، سازمانها و کاربران منفرد همگی نقش بسزای در تأمین امنیت سرمایه های اطلاعاتی و الکترونیکی کشورها ایفا می کنند. شناخت تهدیدات بسیار سودمند است، و عملکرد مناسب براساس چنین شناختی می تواند یک محیط قابل اطمینان ایجاد کند و باعث شود ساکنان کره زمین تا سرحد امکان فواید عصر نوین دیجیتال را حس کنند.

پیوست

آشنایی با کد و رمزگذاری

آشنایی با کدگذاری و رمزگذاری

کدگذاری و رمزگذاری فنونی هستند که رشته های حروف را به قالب و شکل دیگری تبدیل می کنند. کد گذاری در دنیای رایانه تغییر شکلی است که ظاهر پیام را تغییر می دهد، بطوریکه نتیجه آن معیارهای خاصی را برآورده سازد، و رمزگذرای نیز نوعی تغییر شکل است که برای مخفی کردن محتویات پیام بکار می رود.

کدگذاری

کدگذاری قالب موضوع را تغییر می دهد تا برخی از معیارهای مورد نظر را برآورده سازد. این فرایند برگشت پذیر استف بگونه ای که قالب کدگذاری شده بعداً می تواند که کدگشایی شود تا به شکل اصلی خود تبدیل گردد.

فرایند کدگذاری

فرض کنید می خواهید پیامی ارسال کنید که بصورت یک جمله عادی انگلیسی است:

Security is important.

اما در ارسال محدودیتی وجود دارد و این است که شما تنها می توانید ارقام دهدهی را ارسال کنید: ۰ ، ۱، ۲، ۳، ۴، ۵، ۶، ۷، ۸، ۹ . پس باید یک تابع نگاشت تهیه کنیم که بتواند آنچه می خواهیم ارسال کنیم را به اعداد دهدهی تبدیل کند، و بعد از ارسال نیز بتواند آنرا مجدداً به حالت قبلی خود بازگرداند.

برای این منظور از یکسری قوانین ساده استفاده می کنیم:

بجای A عدد ۰۱ را قرار می دهیم،

بجای B عدد ۰۲ را قرار می دهیم،

بجای C عدد ۰۳ را قرار می دهیم،

بجای D عدد ۰۴ را قرار می دهیم،

...

بجای X عدد ۲۴ را قرار می دهیم،

بجای Y عدد ۲۵ را قرار می دهیم،

بجای Z عدد ۲۶ را قرار می دهیم،

بجای فاصله عدد ۲۷ را قرار می دهیم،

بجای نقطه نیز عدد ۲۸ را قرار می دهیم.

جمله اصلی را در نظر بگیرید و هر حرف را با کد تعیین شده، جایگزین نمایید.

۱۹ را بجای S قرار دهید،

۰۵ را بجای E قرار دهید،

۰۳ را بجای C قرار دهید، و ...

حالا می توانیم رشته را اینگونه ارسال کنیم :

19050321180920252709192709131615182001142028

اگر میان ارقام فاصله قرار دهیم خواناتر هم می شود:

19 05 03 21 18 09 20 25 27 09 19 27 09 13 16 15 18 20 01 14 20 28

هنگامیکه پیام دریافت شد، دریافت کننده آنرا به حالت اول باز می گرداند :

S جایگزین ۱۹ می شود،

E جایگزین ۰۵ می شود،

C جایگزین ۰۳ می شود، و اینکار انقدر ادامه می یابد تا جمله اصلی بدست آید.

کاربردهای کدگذری

کاربرد اصلی کدگذاری که در ادامه به آن خواهیم پرداخت در انتقال ضمائم نامه های الکترونیکی است. پست الکترونیکی ابتدا برای فرستادن متون به زبان انگلیسی طراحی شد و مبنای این طراحی کد ASCLL بود که ۱۲۸ حرف منحصر به فرد داشت. این تعداد کد برای نمایش ۲۶ حرف الفبای انگلیسی به شکل کوچک و بزرگ، ۱۰ رقم، برخی از نشانه های دیگر مانند ویرگول، نقطه، کروشه و نیز تعدادی از کلیدهای کنترلی مثل Tab و End بکار می رفتند.

اما بسیاری از زبانها تعداد حروفشان بیشتر از زبان انگلیسی است. از طرف دیگر برنامه ها، فایلهای پردازش کلمه، عکسها و انواع دیگر فایلها از بایتهای ۸ بیتی تشکیل شده اند و مجموعاً ۲۵۶ حرف منحصر به فرد را می سازند، و هیچ یک نمی توانند توسط نامه الکترونیکی ارسال گردند.

برای حل این مشکل مفهوم ضمائم بوجود آمد، که در آن فایلی که همراه نامه الکترونیکی ارسال می شود ابتدا کدگذاری می گردد تا محتوای آن به شکل حروف استاندارد ASCLL در آید. این فرایند مشابه همان فرایندی است که طی آن توانستیم آن جمله را تنها با استفاده از اعداد کدگذاری شده از اصل پیام طولانی تر است، اما می تواند بدون ایجاد اشکال خاصی انتقال یابد و هنگامیکه در یافت شد کد گشایی گردد و به شکل اصلی خود در آید.

Unicood

Unicood نوعی روش کدگذاری برای تمامی حروفی است که در زبانهای رایج مورد استفاده قرار می گیرند و رایانه ها می توانند بطور یکسان آنها را بکار برند. جزئیات بیشتر که در کنسرسیوم Unicood http://www.unicode.org مورد توافق قرار گرفته در ادامه به شکل خلاصه ذکر شده است:

اساساً رایانه ها با اعداد و ارقام سر و کار دارند. آنها حروف الفبا و دیگر علامتها را با اختصاص دادن یک عدد به هر یک از آنها ذخیره می کنند. پیش از پیدایش Unicood صدها سیستم کدگذاری مختلف برای این تبدیلات وجود داشت، اما هیچکدام از انها به اندازه کافی حروف و علامت را پشتیبانی نمی کردند، و مثلاً اتحادیه اروپایی به تنهایی نیاز به چندین کدگذاری مختلف داشت تا تمامی زبانهای اروپایی را پوشش دهد. حتی در مورد یک زبان منحصر به فرد مانند انگلیسی نیز یک کدگذاری واحد برای تمامی حروف، علائم و علامتهای دستوری و فنی کافی نبود.

همچنین سیستمهای کدگذاری مختلف با یکدیگر ناسازگار بودند، یعنی ممکن بود د و سیستم کدگذاری مختلف از اعداد مشابهی برای دو حرف متفاوت استفاده کرده و یا برای یک حرف، دو عدد مختلف را بکار برده باشند. هر رایانه (بویژه سرویس دهنده ها) باید از سیستمهای رمزگذاری مختلفی پشتیبانی کند. هر زمان که داده میان سیستمهای کدگذاری مختلف تبادل می شود ممکن است آسیب ببیند. Unicood آمده بود تا تمامی این مشکلات را حل کند.

Unicood برای هر یک از حروف، شماره مجزایی اختصاص میدهد. اهمیتی ندارد که چه بستر، برنامه یا زبانی مورد استفاده باشد. استاندارد Unicood با رهبری شرکتهایی چون apple,HP,IBM,JUSTSYSTEM, MICROSOFT,ORACLE, SAP,SUN, SYBASE, UNISYS و ... نهایی شده، و در تمام بسترها یکی استاندارد ثابت است.

رمزگذرای

رمزگذاری همانند کدگذاری است که در فرایند آن، متون یا موضوعات به قالب دیگری تبدیل می شوند. هدف اینکار مخفی کردن محتوای پیام است.

سه روش رمزگذاری مختلف وجود دارد:

- رمز گذاری متقارن
- رمزگذاری کلید عمومی
- رمزگذرای یکطرفه با استفاده از Hash

رمزگذاری متقارن

به زبان ساده، رمزگذاری متقارن مشابه کدگذاری است که حروف اصلی متن همگی در آن تغییر ظاهری می یابند.

یکی از ساده ترین الگوریتمها رمزگذاری این است که هر حرف را با حرف بعدی آن جایگزین کنیم. بنابراین در

این روش:

B بجای A قرار می گیرد،

C بجای B قرار می گیرد،

D بجای C قرار می گیرد،

...

Y بجای X قرار می گیرد،

Z بجای Y قرار می گیرد،

A بجای Z قرار می گیرد (در پایان حروف الفبا، دوباره به حرف اول بازگشته ایم).

اگر از این الگوریتم استفاده کنیم، مثال ذکر شده تبدیل می شود به (فاصله و نقطه را در نظر نگیرید):

TFDVSJUZ JT JNQPSUBOU

اکنون این پیام تغییر کرده است. دریافت کننده آن را بر می گرداند و هر حرف را با هر حرف قبلی خود جایگزین

می کند و بدین ترتیب جمله اصلی به دست می آید.

به جای آنکه هر حرف را یک واحد انتقال دهیم ،می توانیم آنها را چند واحد منتقل کنیم .تا زمانی که در یافت کننده مقدار این انتقال را بداند می تواند پیام را رمز گشایی نماید. تعداد تغیر مکان یک حرف را کلید رمز گذاری می گوید.

از این عدد هم برای رمز گذاری پیام استفاده می شود و هم برای رمز گشایی آن جولیوس سزار از این روش برای ارسال پیام های محرمانه و سری خود استفاده می نماید(او کلید رمز گشایی و رمز گذاری خود را برابر ۳ انتخاب کرده است).

با استفاده از این الگوریتم ساده اگر پیام شما دزدیده شود و سارق متوجه روح کلی رمز گذاری بشود ممکن است با حدس زدن بتواند محتوای آن را بفهمد. در صورتی که الگوریتم پیچیده تر از آن باشد که با اعمال چند جابجایی بتوان آنرا پیدا کرد آنگاه رمز گشایی بسیار مشکل تر خواهد بود. تا مدتی پیش الگوریتم های رمز گذاری متعددی از این روش ساده انتقال استفاده می کردند.

امروزه برای رمز گذاری به جای انتقال حروف از فرمولهای ریاضی استفاده می شود. البته هنوز هم از کلید استفاده می کنیم و این کلید بخشی از آن فرمول برای انجام رمزگذاری است. اگر بخواهید پیامی را رمزگشایی کنید حتماً باید از یک کلید استفاده نمایید. البته اگر کلید مخصوص را نداشته باشید می توانید کلیدهای دیگر را امتحان کنید تا به جواب برسید. در صورتیکه کلید محدود به شماره های ۱ تا ۱۰ باشد، عملیات حدس زدن زیاد طول نمی کشد. اما اگر مثلاً میان اعداد ۱ تا ۱۰۰ باشد ممکن است کمی بیشتر زمان ببرد. امروزه کلیدها معمولاً اعداد دودویی ۱۲۸ بیتی هستند. این رقم تقریباً برابر با:

۳۴۰٫۰۰۰٫۰۰۰٫۰۰۰٫۰۰۰٫۰۰۰٫۰۰۰٫۰۰۰٫۰۰۰٫۰۰۰٫۰۰۰٫۰۰۰ انتخاب مختلف است که حدس زدن صحیح کلید را تقریباً غیرممکن می کند.

رمز گذاری متقارن هنگامی مورد استفاده قرار می گیرد که فرستنده و دریافت کننده بتوانند از یک کلید مشابه استفاده کنند (در اینصورت آنها باید در مورد یک کلید مشخص به توافق رسیده باشند)از این روش در صورتی

برای رمز گذاری پیام استفاده می شود که بخواهید اطلاعاتی را از جایی به جای دیگر انتقال دهید ،مثلاً انتقال از طریق ارتباطات بی سیم، و یا اینکه بخواهید اطلاعات شما نیز مطمئناً از دست رفته اند.

رمزگذاری کلید عمومی

این نوع رمزگذاری مشابه رمزگذاری متقارن است، اما با یک تفاوت عمده: بجای یک کلید، در آن دو کلید وجود دارد. در واقع در اینجا کلیدی که برای رمزگذاری پیام استفاده می گردد متفاوت از کلیدی است که برای رمزگشایی پیام رمزگذاری شده بکار می رود. معمولاً کلید اول عمومی است و همه مجازند از آن اطلاع داشته باشند. اگر شما بخواهید برای شخصی یک پیام خصوصی ارسال کنید باید از کلید عمومی وی – که خود او آنرا برای رمزگذاری در اختیار همه قرار داده– استفاده نمایید. برای رمزگشایی پیام، نیاز به کلید خصوصی وی می باشد که متفاوت از کلید عمومی است و این کلید را نباید به هیچ وجه در اختیار دیگران قرار داد. با این توضیحات مشخص است که اگر پیام شما با استفاده از این مکانیزم برای کسی ارسال شود، هیچ شخص دیگری بجز گیرنده حقیقی نمی تواند آنرا بخواند.

توجه داشته باشید که با استفاده از این روش، شخص مطمئن نیست چه کسی پیام را برای وی ارسال کرده است، زیرا هر کسی ممکن است کلید عمومی وی را داشته باشد. اما فرستنده مطمئن خواهد بود که تنها صاحب آن کلید عمومی (کلیدی که برای رمزگذاری بکار رفته) می تواند با کلید خصوصی متناظر این پیام را رمزگشایی کند و بخواند.

کلیدهای عمومی و خصوصی می توانند عکس آنچه گفته شد نیز استفاده شوند. در اینحالت شما پیام را با کلید خصوصی خود رمزگذاری می کنید و هر کسی که کلید عمومی شما را داشته باشد می تواند آنرا رمزگشایی نماید. در اینصورت آنچه به اثبات می رسد این است که مطمئناً فرستنده پیام کسی نیست جز شما.

رمز گذاری یکطرفه با استفاده از در هم سازی

می توانید این روش را مشابه رمز گذاری کلید عمومی بدانید در حالتی که در آن هیچکس کلید خصوصی ندارد. بنابراین مطالب می توانند رمز گذاری شوند، اما نمسی توانند رمزگشاییی گردند ،و تفاوت آن با رمزگذاری کلید عمومی در این است که پیام رمز شده معمولآ حداکثر طول مشخصی دارد .یکی از رایجترین الگوریتمهای رمز گذاری یکطرفه با استفاده از در هم سازی ،الگوریتمیهای رمز گذاری یکطرفه با استفاده از درهم سازی، الگوریتمی بنام MD5است. خروجی الگوریتم MD5همیشه ۱۲۸ بیت (۱۶بایت)می باشد اگر یک کد درهم سازی شده برای دو پیام متفاوت ایجاد کنید احتمال اینکه خروجی دو کد درهم سازی شده مشابه یکدیگر باشند تقریبآ صفر خواهد بود .

این روش و کد خروجی تولید شده در آن دو کاربرد اصلی دارند :

تضمین جامعیت

شما می توانید یک سند طولانی یا یک برنامه را برگزینید کد شده در آن دو کاربرد اصلی دارند :

تضمین جامعیت شما می توانید یک سند طولانی یا یک برنامه را برگزینید کد MD5را برای آن محاسبه و آنرا در محلی امن ذخیره نمایید .مدتی بعد می توانید به اسناد خود مراجعه و دوباره روی آن همین عملیات را اعمال کنید .

طبیعتآ چنانچه کد جدید متایز از کد قبلی بود متوجه می شوید که برنامه یا سند تغییر کرده است

معمولآ یک تغییر بسیار جزیی در یک فایل بزرگ هم باعث ایجاد تغییرات زیادی در کد MD5مربوطه می شود .

ذخیره رمز عبور

در بسیاری از سیستمها هنگا میکه کاربر از کلمه ای بعنوان رمز عبور استفاده می کند این کلمه با استفاده از الگوریتم MD5 (یا یک الگوریتم مشابه) رمزگذاری می شود و نسخه رمزگذاری شده ذخیره می گردد. بار بعد که کاربر سعی می کند وارد سیستم شود، آنچه که وارد می کند مجدداً رمزگذاری می شود و با آنچه که در دیسک ذخیره شده بود مقایسه می گردد، و در صورت یکسان بودن آنها مشخص می شود که رمز عبور صحیح بوده است. البته اگر کاربر رمزعبور را فراموش کند رمزگشایی آنچه که روی دیسک ذخیره شده امکان پذیر نیست و باید یک رمز عبور جدید انتخاب گردد. از این روش برای این منظور استفاده می شود که اصل رمز عبور هیچگاه نتواند در قالب اصلی خود به نمایش درآید.

متأسفانه هنوز یک مشکل وجود دارد که به دلیل آن کاربر نباید از رمزهای عبور کوتاه، ساده و یا قابل حدس استفاده کند و آن اینکه اگر کسی فهرستی از رمزهای عبور رمزگذاری شده بدست آورد (مثلاً از سیستمی که به آن نفوذ کرده) بسیار ساده خواهد بود که همه رمزهای عبور ساده ممکن را رمزگذاری شده موجود در سیستم تطبیق دهد و بدین ترتیب رمزهای عبور ساده سیستم را پیدا کند.

امضای دیجیتالی

اگر شخصی بخواهد برای شما پیامی خصوصی ارسال کند و بخواهد شما مطمئن باشید که فرستنده آن پیام کسی جز او نیست، میتوان از ترکیب روشهای پیش گفته استفاده کرد:

۱. پیام را می نویسد و از MD5 برای ایجاد کد در هم سازی شده استفاده می کند.

۲. با استفاده از کلید خصوصی خود، کد درهم سازی شده را رمزگذری می کند.

۳. با استفاده از کلید عمومی شما متن پیام را رمزگذرای می نماید.

۴. پیام و کد در هم سازی رمزگذاری شده را ارسال می کند.

۵. شما پیام را دریافت می کنید.

۶. با استفاده از کلید عمومی وی کد در هم سازی را رمزگشایی می نمایید، که نتیجه آن بدست آمدن کد در هم سازی اصلی است.

۷. متن پیام ارسالی را با استفاده از کلید خصوصی خود رمزگشایی میکنید.

۸. برای متن پیام ارسالی، با استفاده از MD5 کد در هم سازی را محاسبه می نمایید.

۹. اگر دو کد در هم سازی بدست آمده یکسان بودند اطمینان می یابید متن ارسالی تغییر نکرده است و فرستنده نیز همان شخصی است که انتظار آنرا داشتید.

گواهی های دیجیتالی که بوسیله مرورگرهای وب برای تصدیق هویت ایمن مورد استفاده قرار می‌گیرند نیز براساس فنون امضای دیجیتالی (مثال فوق) کار می کنند.

منـابع

سایتهای

1. www. Scict.ir
2. www.infodov.security.net
3. www.tasmafair.ir
4. www.sigma.ir
5. www.websecurity
6. www.ifna.ir
7. www.itsecurity policies
8. www.it and data protection security softwer
9. www.iran. Eny. Com
10. www.e-mashhad.ir
11. www.parstech.org
12. www.ict.ir
13. www.ict.ir.group-article –strategic.pdf
14. SANS institute (http//:www.sans.org)
15. IEEE computer society Technical committee on security and privacy (http//:www.ieee-security.org)
16. International federation for information processing (http//:www.ifip.tu-graz.ac.at/TC11)
17. Internet sosieety (http//:www.isoc.org)

۱۸. نام نویسنده: سید احسان اعتباریان ، نام کتاب: امنیت شبکه، انتشارات: دانش پرور ، سال انتشار: ۱۳۸۳