امنیت فناوری اطلاعات

پروژه دات کام

www.Prozhe.com

مرجع دانلود رایگان پروژه، تحقیق و مقاله

فهرست

عنوان **صفحه**

بخش اول امنیت فناوری اطلاعات در عصر دیجیتال

مقدمه

انقلاب دیجیتال

امنیت چیست ؟

پیدایش و رشد اینترنت

موضوعات مطرح در حوزهٔ امنیت اطلاعات

مخاطرات محتمل در فضای سایبر چیستند؟

انگیزه خرابکاران امنیتی چیست؟

اهمیت امنیت برای سازمانهای کوچک و متوسط در کشورهای درحال توسعه

بسوی مفهوم نوینی از قابلیت اطمینان

جمع بندی

مقدمه :

ظهور فناوری دیجیتال یکی از بارزترین پیشرفتهای فناوری در نیم قرن اخیر به شمار می آید که در زندگی کنونی بشربصورت عاملی حیاتی درآمده است . برای بسیاری از ما این نوع فناوری در قالب رایانه های دیجیتالی تجلی کرده و به ابزاری لازم برای انجام کارها و رفع نیازهای شخصی تبدیل شده است . در سال ۱۹۵۱ میلادی زمانیکه اولین رایانه دیجیتال تجاری موسوم به UNIVAC I به سازمان آمار سرشماری ایالات متحده آمریکا تحویل داده شد، بسیاری ازمردم در مورد رایانه ها چیزی نمی دانستند و آن رایانه ها نیزتنها در تعداد انگشت شماری از دانشگاهها و آزمایشگاههای تحقیقاتی مورد استفاده قرار داشتند . این رایانه ها بزرگ ، گران و مملو از اشکال بودند . در مقابل ، رایانه های امروزی اندازه ای نسبتًا کوچک دارند ، ارزان و قابل اطمینان هستند و می توان آنها را در هر کشوری یافت. به فاصله کوتاهی پس از رواج رایانه ها در دانشگاهها،پروژه های تحقیقاتی برای مرتبط ساختن آنها با یکدیگر به نحوی که امکان مبادله اطلاعات میان آنها بوجود آید آغازشدند. از میان این پروژ ه ها، پروژه توسعه شبکه ARPANET موفقیت بیشتری کسب کرد و به آن چیزی تبدیل شد که امروز آنرا بعنوان «اینترنت» می شناسیم و درحال حاضر بیش از ۳۰۰ میلیون رایانه را در سراسر جهان به هم مرتبط کرده است.

شبکه جهانی وب که توسط تیم برنرز لی و رابرت کایلیو در مرکز تحقیقات هسته ای اروپا در اوایل دهۀ ۹۰ میلادی و در شهر ژنو ایجاد شد سرویس قدرتمندی است که از اینترنت برای ایجاد یک سیستم اطلاعاتی جهانی بهره جسته وبهره وری و جذابیت اینترنت را به مراتب افزایش داده است.

هر چند بسیاری از مردم تفاوتی میان شبکهجهانی وب و اینترنت قائل نیستند، ولی در واقع وب تنها یکی از این خدمات(و البته مهمترین آنها) است که اینترنت را به چنین ابزارقدرتمندی برای اطلاع رسانی و برقراری ارتباطات تبدیل کرده است.

طی ده سال اخیر اینترنت به یک ابزار مهم ارتباطی میان تمامی اقشار جامعه تبدیل شده و ما برای دسترسی آنی به اطلاعات، ارتباطات اختصاصی، تمامی انواع برنامه های کاربردی، تجاری، روابط کاری و نقل و انتقالات مالی به آن وابسته ایم. قابلیت اطمینان و دسترسی آسان به اینترنت برای موفقیت پایدار و مداوم کشورهای توسعه یافته یک عامل حیاتی بشمار می رود و اهمیت آن برای کشور های درحال توسعه نیز بسرعت رو به افزایش است . آثار استفاده از رایانه ها و نتایج حاصله از انقلاب اینترنت از مرز فواید مستقیم آنها فراتر رفته و پیش بینی می شود که تأثیرات بیشتری نیز در راه باشند.

اول از همه اینکه اینترنت مرزهای جغرافیایی میان کاربران متصل به خود را کمرنگ کرده و روند جهانی سازی را با ارائه قابلیتهای رسانه های ارتباطی تسهیل نموده و لذا هر کسی مستقل از محل فیزیکی خود قادر به برقراری ارتباط با آن میباشد. موتورهای جستجو بر روند این تغییر تأثیری مضاعف داشته اند؛ چراکه نتایج جستجو بر اساس موضوعات ظاهر می شوند و نه بر اساس فاصله ای که کاربر با آ نها دارد؛ بطوریکه پایگاه وب کارخانجات و شرکتهای واقع در کشورهای توسعه یافته و درحال توسعه از موقعیت یکسانی برای نظاره شدن توسط مراجعین برخوردار هستند.

دومین مسئله این است که اینترنت تأثیری شگرف در فرآیند حذف واسطه های تجاری داشته است . بعنوان مثال می توان به کاهش چشمگیر نرخ استخدام منشی در کشورهای توسعه یافته اشاره کرد که دلیل آن این است که نوشتن متن و چاپ و ارسال پیام شخصی برای افراد از طریق تسهیلاتی چون پردازشگر کلمات و پست الکترونیکی آسانتر از دیکته کردن متن برای یک منشی است. به همین ترتیب گردشگری دسته جمعی نیز درحال حاضر رو به انقراض است، چراکه گردشگران می توانند بلیطهای هوایی یا قطار و همچنین اتاقهای هتل مورد نظر خود را بصورت برخط رزرو کنند و این امر موجب صرفه جویی در هزینه و وقت مشتری شده و باعث شده بتوان با کمی دقت روی سفارشات، از یک سفر مفرح لذت بر د. پیدایش شرکتهای فروشندۀ کتاب،موسیقی و محصولات الکترونیکی بصورت برخط موجب تهدید و ضربه به فروشگاههای عرضه کننده اینگونه محصولات شده، اما در عین حال در بسیاری از بخشهای این صنف به گسترده تر شدن طیف بازار هدف نیز انجامیده است.

از آنجا که حرفه ها و صنایع سنتی به وجود خود ادامه می دهند، تمایل دارند افراد کمتری به استخدام درآورند و حتی ممکن است بجای ارائه خدمات عمومی به سمت بازارهای تخصصی حرکت کنند . تأثیرات مشهود روند حذف واسطه ها که با ظهور این فناوری شروع شد برای مدتی طولانی ادامه خواهد یافت و با اهمیت روز ا فزون فناوریاطلاعات، صنایع و حرفه های بیشتری با آن جایگزین خواهندشد. سومین پیامد این است که نرخ بهره وری حداقل در صنایع وابسته به فناوری اطلاعات با شتابی چشمگیر افزایش خواهدیافت. به کمک پست الکترونیکی امکان ارسال و تبادلاطلاعات در سراسر جهان طی تنها چن د ثانیه ممکن شده،بطوریکه مباحث و مذاکرات جهانی را می توان بسیار سریعتر از گذشته پیگیری کرد و به نتیجه رساند . امور بازرگانی که تا چندی قبل از طریق پست، تلکس و تلفن انجام می شدند اکنون با بکارگیری مفاهیمی نوین در صنعت مخابرات سیار، سریعتر و کارآمدتر به انجا م می رسند و این مسئله چرخه زمانی انجام فعالیتها را کاهش داده است.

نکتهٔ آخر اینکه ایمن نگاه داشتن محل ذخیرهٔ اطلاعات و خطوط ارتباطی مخابراتی نیز در این محیط جدید الزامی است. صنعت و فناوری امروز به شدت در تکاپوی یافتن راهی برای تضمین امنیت زیرساختهای خود هستند، چراکه دست اندرکاران آن دریافته اند که بیشتر نقایص امنیتی اینترنت ناشی از وجود سخت افزارها و نرم افزارهای ناامن در آن می باشند. در این محیط ایجاد اطمینان و اعتماد به رایانه ، شبکه و داده های ذخیره شده نسبت به محیطی که در آن روابط کاری بر اساس گفتگوهای رو در رو انجام می گیرد کمابیش از اهمیت یکسانی برخوردار است. این مطلب در مورد کشورهای درحال توسعه نیز واضح است:

سازمانهایی که به سطح امنیتی مناسبی در زیر ساختهای دیجیتالی خود دست نیافته و از ارسال اطلاعات خویش به نحو مطلوبی محافظت نمی کنند شایستهٔ اعتماد نخوا هند بود و از کاروان اقتصاد نوین جهانی عقب خواهند ماند.

انقلاب دیجیتال

امروزه فناوری دیجیتال از حیطه رایانه ها فراتر رفته است . پیشرفتهای فناوری در صنعت میکرو الکترونیک امکان ساخت ابزارهای پیچیده الکترونیکی در مقیاسهای بسیار کوچک را فراهم آورده بطوریکه اکنو ن شما می توانید تجهیزات ارتباطی و محاسباتی بسیار پیچیده را در جیب خود جای دهید . علاوه بر این بهبود نسبت قیمت به کارآیی برای این نوع فناوری در هر سال چیزی حدود ۳۰ ٪ است و احتمال برقراری این نسبت تا ده سال آینده نیز بسیار بالاست .انتظار ما این است که این فناوری مورد استقبال گسترده قرار گیرد و عرصه های نوینی در تجارت پدید آورد و نقطهٔ شروعی برای آغاز عصر طلایی فناوری دیجیتالی باشد.

تجهیزات تلفنی مدرن امروز کاملا دیجیتالی هستند و سیستم های هدفمند رایانه ای جایگزین تجهیزات Switching مبتنی بر رله مکانیکی شده اند. از زمان پیدایش دیسک فشرده در اواخر دههٔ ۸۰ میلادی، صدا و موسیقی شکل دیجیتالی به خود گرفته و با پیدایش قالب موسیقی MP3در اواخر دههٔ ۹۰ میلادی ضبط صدا حتی در محیطهای خانگی نیز کاملا دیجیتالی شده است . در دنیای عکاسی و فیلمبرداری نیز تصاویر دیجیتالی و دوربینها ی دیجیتالی ثبت تصاویر فیلمهای عکاسی گشته اند. امروز حتی فیلمهای سینمایی و کارتونها نیز دیجیتالی شده اند؛ چرا که بدین شکل هزینه های تولید آنها کمتر و کیفیتشان بیشتر است . رفته رفته نوارهای ویدئویی جای خود را به فناوری DVDداده اند و فیلمهای سینمایی با امکانا ت دیجیتالی ساخته و تدوین می گردند.

استانداردهای تلفنهای بی سیم درحال حرکت به سمت فناوری دیجیتال هستند و با وجود پروتکل هایی چون، CDMA،GSM TDMA و گونه های مختلف آنها بتدریج جایگزین نسل قدیمی استانداردهای فناوری آنالوگ خواهند شد . درکشورهای توسعه یافته تلویزیون دیجیتال به صحنه آمده است و دیری نخواهد گذشت که جای استانداردهای پخش برنامه را خواهد گرفت (هرچند که این تغییر کمی کندتر از بقیه خواهد بود؛ چرا که حجم گیرنده های خانگی موجود که به استانداردهای قدیمی تر وابسته اند بسیار وسیع است) سیستمهای امنیت فیزیکی نیز درحال تبدیل به انواع الکترونیکی خود هستند . در هتلها،

آپارتمانها و دفاتر اداری،کلیدهای فیزیکی جای خود را به کارتهای الکترونیکی داده اند. دوربینهای تلویزیونی مورد استفاده در سیستمهای نظارتی ساختمانها و تأسیسات نیز اغلب از تجهیزات الکترونیکی استفاده می کنند که بجای ارسال سیگنالهای تلویزیونی به یک مانیتور ویدئویی، تصاویر الکترونیکی را به ایستگاههای نظارت دیجیتالی ارسال می کنند.بسیاری از خدماتی که امروزه از آنها استفاده می کنیم بدون وجود رایانه ، شبکه و فناوری دیجیتال قابل ارائه نخواهند بود . خطوط هوایی نیز بدون سیستمهای رزرو رایانه ای و سیستمهای نگهداری و پشتیبانی پرواز قادر به رقابت با هم نیستند. هواپیماها تا اندازۀ زیادی به حسگرهای الکترونیکی و کنترلهای دیجیتالی وابسته اند و بدون آنها نمی توانند به خوبی کار کنند . حتی اتومبیلها نیز برای عملکرد مناسب و کمک به عیب یابی و نگهداری خود از ریزپردازنده ها استفاده می کنند . سیستمهای مکان یابی جهانی (GPS) نیز به شما این امکان را می دهند که بدانید در هر لحظه در چه مکانی روی کره زمین قرار گرفته اید و با داشتن چنین دستگاه نسبتا ارزانی درکنار رایانه ای که حاوی پایگاه د ادهای از نقشه ها باشد قادر به یافتن مسیر حرکت، نقاط مهم، رستورانها، تابلوهای راهنما، خدمات ارائه شده در طول مسیر، و در نهایت مقصد مورد نظر خواهی د بود.

این دستگاههای دیجیتال با سرعتی باورنکردنی در **شبکه** قرار می گیرند .تلفنهای بی سیم قادر به برقراری ارتباط با اینترنت هستند و ابتدا قادر به ارسال صوت و اکنون قادر به مبادلۀ تصاویر از طریق اینترنت می باشند و بزودی دارای قابلیت GPS نیز خواهند شد و به این ترتیب افرادی که در معرض خطر و حادثه قرار گرفته باشند را می توان با دقتی زیاد و تنها با یک تلفن مکانیابی کر د. بسیاری از خدماتی که اکنون مورد استفاده ما قرار می گیرند - مثل دستگاههای خودپرداز که برای تبادل و نقل و انتقال پول بکار می روند - بر اساس اصل « **در دسترس بودن شبکه** » کار می کنند. نقل و انتقالات مالی و اعتباری میان بانکی و بین المللی وابستگی زیادی به شبکه های اعتباری و مالی دارند .امروزه نقل و انتقالات بانکهای الکترونیکی از طریق **اینترنت** برای افراد میسر است. توسعۀ ابزارهای الکترونیکی دیجیتال و دستگاههای مرتبط با هم فواید بسیاری دارد؛ ولی نکات منفی نیز در آن قابل مشاهده است . پیدا کردن محل استقرار شما برای افراد آسانتر شده است . دیدن صفحات تبلیغاتی وب،

یافتن آنچه که بدنبال خرید آن در مغازه ها هستید، و مشاهدهٔ آنچه که درحال تماشا یا خواندن بصورت برخط هستید نیز ساده تر از قبل می باشد. اگر چنین نظارتی بر منافع شما حاکم باشد قاعدتًا شما از آن باخبر نخواهید شد، اما شاید بخواهید مطمئن شوید که چنین داده هایی با کسب اجازه از شما جمع آوری می شوند و تنها برای اهدافی بکار می روند که از آن اطلاع دارید و با آن موافق هستید . بسیاری از مردم برای حریم خصوصی خود اهمیت زیادی قائل هستند و دولتها نیز مایل به حفظ حقوق افراد می باشند، گرچه میزان و شدت اجرای قوانین از یک کشور تا کشور دیگر متفاوت است . مسئله اصلی برای دولتها این است که منافع حاصل از فناوریهای نوظهور را تشخیص دهند و در عین حال ارزشها و آزادیهایی که بدون آن فناوریها می توان از آنها برخوردار بود را همچنان حفظ کنند . موضوع این است که دولتها باید فناوریهای جدید را درک کرده و تأثیر قابلیتها و امکانات نوین بر آزادیها را ارزیابی نمایند . همچنین دولتها باید گامهای مؤثری بردارند تا مطمئن شوند اگر قوانین و سیاستهای عمومی در این زمینه آزادیهای فعلی را تقویت نمی کنند، حداقل یک وفاق جمعی در مورد آنها وجود داشته باشد. دنیای دیجیتالی معمولا با عنوان **فضای سایبر** شناخته می شود و تعریف آن تمامی رایانه ها و ابزار های دیجیتالی که با شبکه های داخلی و خارجی به هم متصل می شوند و می توانند با یکدیگر ارتباط داشته باشند را در بر می گیرد. در فضای سایبر هم مثل فضای فیزیکی می توان دربارهٔ ملاقاتها و انجام کارها صحبت کرد، اما باید میان رفتار در فضای سایبر و دنیای حقیقی که در آن زندگی ، کار و بازی می کنیم تفاوت قائل شد.

گسترش و رواج سریع رایانه های شخصی و اینترنت در بخشهای مختلف کشورهای درحال توسعه منافع بسیاری داشته است . با اینحال اینترنت بخودی خود رسانه ای نیست که نسبت به رفتار تبهکارانه ایمنی داشته باشد . هزینهٔ عدم توجه کافی به امنیت می تواند از دست دادن داد ه های مورد نیاز برای انجام کار یک سازمان بزرگ یا مؤسسهٔ دولتی باشد. اینترنت ماهیتًا از ایمنی لازم برخ وردار نیست اما هزینهٔ امن کردن آن نیز در مقایسه با هزینهٔ از دست رفتن داده های ارزشمند سازمانها و مؤسسات چندان قابل توجه نمی باشد . از دیگر مواردی که می تواند بسیار مهم باشد آنست که تأثیرسرقت و وقوع تخلف مالی در یک شرکت تنها محصور به آن شرکت نیست و در کل صنعت کشور تأثیر میگذارد.

با گسترش اینترنت و افزایش چشمگیر نگرانیهای ناشی از **حملات سایبر** ، تعداد چنین حوادثی نیز رو به افزایش است: **با وجود اینکه رایانه ها نقطهٔ مناسبی برای انجام حملات تروریستی هستند، اما این نکته را نیز باید درنظر داشت که برخی اقدامات خرابکا رانه توسط افرادی صورت می گیرند که از این راه بدنبال کسب درآمد ستند.مرکز فوریتهای امنیت رایانه ای (CERT)در سال ۲۰۰۱ میلادی رقمی برابر با[b] ۵۲۶۵۸** رخداد امنیتی اینترنتی را شناسایی کرده که دو برابر تعداد یکسال قبلتر است و نسبت به دو سال پیش از آن چهار برابر می باشد[/b] .

بحث **امنیت** رایانه ها و شبکه ها برای کشورهای درحال توسعه از اهمیت خاصی برخوردار است. اینترنت میتواند فواصل را از میان بردارد و دسترسی به مطالب بی شماری را فراهم کند. با وجود شبکهٔ جهانی وب، اینترنت قادر خواهد بود از اطلاعات موجود دربارهٔ شرکتها، امکانات، و محصولات کشورهای درحال توسعه استفاده کند و تجارت را در آنها توسعه دهد. علاوه بر این، موتورهای جستجو از نظر جغرافیایی تمایزی میان پایگاههای وب قائل نمی شوند؛ وبدین ترتیب تأمین کنندگان خدمات و کالاهای اساسی و مواد اولیهٔ کشورهای درحال توسعه روی وب در کنار تأمین کنندگان کالاها و خدمات کشورهای توسعه یافته قرار میگیرند. این امر را گاهی « **مرگ فاصله ها** » می نامند؛

واژ های که روند جریان اطلاعات در اینترنت را نشان می دهد. ولی با اینحال همواره مخاطراتی جدی مانند از دست دادن سوابق، حملات تخریب سرویس، خراب شدن اطلاعات و سایر انواع حملات خصمانه وجود دارد . از دست رفتن تمام یا بخشی از سوابق الکترونیکی می تواند یک شرکت را زمینگیر کند. برای کشوری که امنیت فناوری اطلاعات آن ضعیف است این احتمال وجود دارد که منابع حیاتی آن در معرض خطر قرار گیرند و به آنها صدمات جبرا ن ناپذیری وارد شود. عدم توجه کافی به امنیت برای کشورهایی که به روابط خارجی در صنایع خود اهمیت می دهند می تواند موجب خسارتهای جدی و پیش بینی نشده ای گردد . نیل به اهداف توسعهٔ هزاره (MDG) به توانایی کشورهای درحال توسعه در استفادهٔ مؤثر از فناوری اطلاعات و افز ایش بودجهٔ آنها با عضویت دائمی در سازمان تجارت جهانی بستگی دارد .توانایی کسب و تأمین اطلاعات مناسب می تواند در تمامی زمینه های اقتصادی به کشورهای درحال توسعه کمک کند .

متأسفانه همهٔ ظواهر خوب و بد انسانی را می توان در فضای سایبر نیز مشاهده نمود . از آنجا که نسخه برداری از مضامین دیجیتالی و ویرایش آنها آسان است، مغالطه و تحریف اطلاعات مثل جعل مستندات اداری و رسمی آسان می شود . به دلیل آنکه اینترنت از یک محیط پژوهشی و تعاونی شروع به کار کرد و هدف آن اشتراک آسان اطلاعات بود، ساختار آن باعث تسهیل حمله به رایانه ها و سرقت اطلاعات محرمانه می گردد. انگیزهٔ افرادی که در فضای سایبر چنین رفتاری از خود بروز میدهند شبیه انگیزه هایی است که در دنیای واقعی آنها را به کارهای مشابه وادار می کند، اما با یک تفاوت عمده : محیطی که توسط رایانه ها و اینترنت بوجود آمده باعث شده در افرا د این تمایل بوجود بیاید که بخواهند ثابت کنند که می توانند به سیستمها وارد شوند و مشکلاتی بوجود بیاورند . بیشتر مشکلات مو جود در فضای سایبر از جانب خرابکارها ناشی می شود. خرابکارها افرادی هستند که می خواهند ثابت کنند می توانند از هر سد امنیتی که سر راهشان قرار داشته باشد عبور کنند . اگر بخواهیم چنین رفتاری را در دنیای واقعی مدل کنیم باید فردی مورد اشاره قرار دهیم که می خواهد ثابت کند می تواند به خانه شما وارد شود و سپس بدون دست زدن به چیزی خارج شود ! چنین پدیده ای نه تنها موجب بروز نوعی احساس عدم اطمینان می شود، بلکه این سؤال را نیز پدید می آورد که چه چیزی درحال تغییر یافتن یا کم شدن است یا اینکه چه اقداماتی می توان برای جلوگیری از نفوذهای بعدی انجام داد . همانطور که چنین رفتاری در دنیای واقعی قابل تحمل نیست، در فضای سایبر هم نمیتوان این رفتار را تحمل کرد.

امنیت چیست ؟

مفهوم امنیت در دنیای واقعی برای بسیاری از ما حیاتی است. در دوران ماقبل تاریخ، امنیت عبارت بود از اصول حفظ بقا؛ نظیر امنیت در برابر حملهٔ دیگران یا حیوانات، و نیز امنیت تأمین غذا. نیازهای دیگر چون امنیت در مقابل حوادث طبیعی یا بیماریهاعموماًبرای انسانهای ما قبل تاریخ مطرح نبود . با پیشرفت تمدن، محدودهٔ امنیت فراتر رفته و ابعاد وسیعتری مانند در اختیار داشتن مکانی برای آسایش و زندگی بی خطر را در بر گرفت و امروزه مفهوم اموال شخصی نیز به تعریف امنیت اضافه شده است. بیشتر آنچه که ما در دنیای

واقعی انجام می دهیم با مخاطره همراه است؛ هرچند بسیاری از فعالیتهایمان مخاطرهٔ کمی در پی دارد . مثلا وقتی به همراه شخصی ناآشنا به سفر می رویم و یا به شهر یا کشوری ناآشنا وارد می شویم این حقیقت را میدانیم که برای امنیت جسمی مان تهدیداتی وجود دارد.

تهدیدات موجود در اطراف ما وقتی جدی خواهند شد که ما در مکانی حفاظت نشده قرار بگیریم و با فردی روبرو شویم که بتواند از موقعیت ما سوء استفاده کند . اگر به اندازهٔ کافی به مخاطرات اطراف خود توجه کنیم موفق خواهیم شد مکانی امن پیدا کنیم یا راه چاره ای بیابیم؛ مثلا همراه کسی شویم که ما را به مکان امنی هدایت کند، یا یک تاکسی بگیریم. بعضی از کارها مخاطرات روانشناختی یا مالی به همراه دارند ولی مخاطرهٔ جسمی ندارند . وقتی سرمایه گذاری می کنیم (در هریک از اشکال خرید زمین، سهام یا حتی فعالیت در تجارت و یا کار در بازار) انتظار داریم که این سرمایه هرچه زودتر به ما بازگردد. همانطور که می دانیم بعضی از سرمایه گذاریها دیر یا زود بازخواهند گشت؛ حال آنکه بعضی از سرمایه گذاریها اینگونه نیستند و بعضی از آنها هم به زیان منجر می شوند. مثلا وقتی با شخص جدیدی ارتباط برقرار می کنیم امیدواریم که این رابطهٔ جدید برایمان آورده ای داشته باشد، هرچند خطر این مسئله که ممکن است این رابطه از فایدهٔ لازم برخوردار نباشد را نیز میپذیریم.

در بعضی زمینه ها دستیابی به سطحی از امنیت که انتظار آنرا داریم ممکن نیست . مثلا همیشه مایلیم عمری طولانی و جسمی سالم داشته باشیم؛ ولی آنچه که در معدل آماری طول عمر وجود دارد نشان می دهد که این مسئله برای بسیاری از افراد صدق نمی کند. بعضی از ما در سنین پائین می میریم، تعدادی در طول حیات با بیماریهای مختلف دست و پنجه نرم می کنیم، و برخی تا سالیان دراز زنده می مانیم و عمری به سلامت روزگار می گذرانیم. عدم توانایی خود در تعیین سرنوشت را با بیمه جبران می کنیم تا ما را در برابر اثرات منفی مالی، حوادث و بیماریها حفاظت کند. این مقدمه حقیقتی را دربارهٔ امنیت پیش روی ما قرار می دهد: امنیت مطلق چه در زندگی واقعی و چه در فضای سایبر غیرممکن و محال است؛ ولی با اینحال امنیتی که به اندازهٔ کافی مناسب باشد تقریباً در تمامی شرایط محیطی دستیافتنی میباشد.

راههای گوناگونی برای در اختیار گرفتن مکانیزمهای تقویتی افزایش و حفظ امنیت وجود دارد . ما از مکانیزمهای فیزیکی برای تضمین امنیت خود برخوردار هستیم : ساختمانهای بلند و مستحکم و درهای محکم و نفوذناپذیر به همراه قفلها و کلیدهای بی شمار. ما می توانیم به مرزهای فیزیکی دیگر مثل دیوارها و دیگر موانع جداساز نیز تکیه کنیم . همچنین می توانیم روی مناطقی که از طریق آنها احتمال نفوذ می رود نور کافی متمرکز کنیم . نهایتًا اینکه درصورت لزوم می توان با این فرض که اقدامات نفوذی اولیه موفق باشند از سیستمهای هشداردهنده و محافظهای قویتر برای شناسایی و مقابله با کسانیکه موفق به نفوذ شده اند استفاده نمود . مهمتر از همه اینکه می توانیم از پشتیبانی قوانین عمومی و جزایی و نیروهای انتظامی نیز درخواست کمک نماییم. ما معمولا از چندین روش مختلف برای افزایش امنیت خود استفاده می کنیم تا درصورتیکه یکی از تدابیر مفید واقع نشد دیگری خلاء آنرا پر کند . اگر یکی از کلیدها به سرقت رفت و قفل در از آن پس حفاظ مطمئنی به شمار نمی رفت، می توان از علائم هشداردهنده برای اعلام خطر نفوذ استفاده کرد. البته تعداد مرزها و عوامل سد کننده به ارزش چیزی که مورد حفاظت قرار می گیرد و انتظارات معقولانه ای که در زمینهٔ حمله به آن وجود دارد باز میگردد. تمامی این تدابیر و روشهای حفاظتی در فضای سایبر به شکلی دیگر مطرح می شوند و ما به آن اندازه که با تدابیر امنیت فیزیکی آشنا هستیم با ماهیت آنها در فضای سایبر آشنا نیستیم، اما لازم است که آنها را درک کنیم و درصورت نیاز به تأمین امنیت در فضای سایبر ، روش کاربرد آنها را بدانیم. هم در دنیای واقعی و و هم در فضای سایبر نیازمند حفاظت و دفاع از سرمایه های خود در برابر حملات دیگران و درصورت موفقیت آمیز بودن حملات، بازپس گیری سرمایه های از دست رفته می باشیم.

تعاریف و توضیحاتی که در فرهنگهای لغات و واژه نامه ها برای واژه امنیت وجود دارد به مواردی اشاره دارند که با سلامتی مرتبط هستند، نظیر « کیفیت یا حالتی از اطمینان، آزادی از خطر و رهایی از ترس یا اضطراب ». با اینحال هیچیک از این تعاریف نمی توانند برای توصیف دقیق امنیت در فضای سایبر بکار روند.

در عوض ما تعریف زیر را پیشنهاد می کنیم : هنگامی در فضای سایبر ایمن هستید که دسترسی به منابع

اطلاعاتی شما تحت کنترل خودتان باشد، یعنی هیچ کس بدون کسب اجازه از جانب شما قادر به دسترسی به این منابع اطلاعاتی نباشد. این منابع شامل داده ها و منابع رایانه ای، شبکه ای، تراکنشی، پردازشی، و اطلاعاتی می باشند. طبیعتًا ممکن است برخی از این منابع از جانب دیگران و برای استفادۀ شما ا رائه شده باشند، مثل حساب کاربری در یک رایانۀ اشتراکی یا دسترسی به اینترنت از طریق یک ارائه کنندۀ خدمات اینترنتی.(ISP)

از آنجا که این موارد هیچگاه کاملا ایمن نیستند، تنها تا وقتیکه دستورالعمل های فروشندۀ خدمات برای استفادۀ صحیح از آنها را دنبال کنید می توانید بر دسترسی مداوم و استفادۀ مناسب از خدمات اشراف داشته باشید.

مثالی در مورد ماهیت امنیت سایبر در اینجا ارائه می شود. برای این منظور به آخرین نقصی که (تا پیش از انتشار این کتاب(یافته شده در هستۀ سیستم عامل **Microsoft Windows**) میپردازیم:

مایکروسافت تقریباً در تمامی نسخه های موجود از سیستم عاملهای Windows خود یک آسیب پذیری بسیار مهم را کشف کرد که اولین تأثیر آن می تواند از کار افتادن کاملMicrosoft Windows Server 2003 باشد . مایکروسافت گفته که این آسیب پذیری می تواند نفوذگرها را قادر کند که از طریق اینترنت کنترل سیستم عامل Windows رایانه های قربانیان خود را بدست گرفته، اطلاعات آنها را بدزدند، فایلها را حذف کنند و یا از طریق پست الکترونیکی انتقال دهند . این شرکت به مشتریان خود اطمینان داد که بلافاصله یک وصله رایگان برای برطرف ساختن این اشکال روی پایگاه وب مایکروسافت قراردهد.

این اشکال که توسط پژوهشگرانی از کشور لهستان کشف شد نسخه های رایج Windows در میان کاربران خانگی را نیز تحت تأثیر قرار داد : « این مورد یکی از بدترین آسیب پذیریهایWindowsاست که تا کنون وجود داشته » ، این گفتۀ مارک مایفرت مدیر اجرا یی مؤسسۀ امنیت دیجیتال چشم الکترونیکی واقع در آلیسو ویه جو در ایالت کالیفرنیاست که محققان آن نظیر همین آسیب پذیری خطرناک را در سه نسخۀ قبلی Windows کشف کرد ه اند.

مایفرت دربارهٔ شرکتهای آسیب دیده عنوان کرد : « تا زمانیکه آنها این وصلهٔ نرم افزاری را نصب نکنند سیستمهایشان مثل یک تکه پنیر سوئیسی خواهد بود و هرکس می تواند براحتی به سرویس دهند ههای آنها وارد شود. »

اما همان زمان چهار پژوهشگر لهستانی که با عنوان Last Stage of Delirium Research Group شناخته می شدند پیدا کرده اند که راهی برای عبور از وصله های جدید مایکروسافت می دانند و این زمانی بود که تنها سه ماه از انتشار این وصله ها می گذشت . هرچند پژوهشگران لهستانی ابزاری برای اثبات وجود آسیب پذیریهای جدی تر طراحی کرده و با استفاده از آن به چند رایانه نفوذ کردند، ولی متعهد شدند که هیچ اثری از این آسیبپذیریهای جدید در اینترنت بجای نگذارند . بعضی از متخصصان انتظار داشتند که نفوذگران طی چند ماه آینده از این اشکال جدید برای نفوذ به رایانه ها استفاده کنند . حتی بدون اعلام این مسئله از سوی آن پژوهشگران، نفوذگران نوعًا قادر به عبور از وصلههای مایکروسافت هستند. همانند کاربران و کارمندان درون یک سازمان، ما هیچ کنترلی روی متن برنامه هایی نظیر Windows نداریم . میدانیم که برای فروشندگان نرم افزار بسیار مهم است که برنامه هایشان ایمن و عاری از هرگونه خطا باشد، اما زمانی که چنین مشکلاتی بروز می کنند با اتخاذ تدابیر و تصمیمات مناسب می توانیم نسبت به تهیه و نصب نسخه های اصلاحی فروشندگان اقدام کنیم و این تنها روش مقابله ای است که در اختیار داریم.

در دنیای واقعی می دانیم که چطور باید از منابع اطلاعاتی خود حفاظت نماییم و همچنین میدانیم که بعضی از اطلاعات را باید بصورت محرمانه نگهداری کرد و برخی از آنها را می توان بصورت آزادانه انتقال داد برای این منظور درهای دفاتر و کمدهای حاوی فایلها را قفل می کنیم و حتی ممکن است نسخه هایی از اطلاعات مهم را خارج از محل اداره نگهداریم تا در مواقعی چون بروز آتش سوزی و یا سایر بلایای طبیعی از آنها حفاظت کرده باشیم . بعضی اطلاعات را تنها می توان به تعداد محدودی از افراد انتقال داد و بسته به درجهٔ اهمیت اطلاعات می توان به افراد مختلف در سطوح متفاوتی اعتماد کرد.

از نظر مفهومی میان ماهیت تهدیدات فضای سایبر و تهدیداتی که در دنیای واقعی وجود دارند هیچ تفاو تی نیست، بلکه تفاوت این دو مقوله برخاسته از خصوصیات فضای الکترونیکی و تهدیدات این حوزه است که باعث می شود بتوان از بروز آنها جلوگیری کرد و آنها را خنثی، یا شناسایی و رفع نمود. عناوین حریم خصوصیو محرمانگی با مسئله امنیت در ارتباط هستند . اطلاعاتی که « خصوصی » بشمار می روند تنها زمانی می توانند واقعًا خصوصی بمانند که بصورت ایمن ذخیره شده باشند . برای این منظور در دنیای واقعی بگونه ای رفتار می کنیم که گویی چنین اطلاعاتی وجود خارجی ندارند . این سیاست را امنیت گمنامی می نامند .

به همین ترتیب اطلاعاتی که باید بصورت محرمانه به اشتراک گذارده شوند باید برای کسانیکه آنها را به اشتراک گذاشته اند بصورت ایمن باقی بمانند . اگر این افراد همیشه در یک مکان نیستند هنگام انتقال این اطلاعات باید سیاستهای امنیتی کافی در مورد آنها اعمال شود. موقعیتهایی نظیر این مسئله در فضای سایبر نیز وجود دارد، ولی با فرض طبیعت خاص فضای سایبر و ارتباط میان رایانه های موجود در آن، امنیت گمنامی یا استفاده از پنهان سازی سیاستی ضعیف می نماید و باید از آن اجتناب کرد.

پیدایش و رشد اینترنت

محیط رایانه ای و شبکه ای اینترنت امروز در ابتدا با هدف پژوهش و آموزش بوجود آمده بود . زمانیکه ARPANET(اینترنت اولیه) برای اولین بار ایجاد شد، هدف اصلی آن اشتراک منابع گروههای متعدد پژوهشگران در موقعیتهای جغرافیایی مختلف بود . این گروهها اهداف یکسان داشتند و با هدف به اشتراک گذاشتن منابع و داده ها کار می کردند؛ دسترسی به شبکه محدود به اعضای این گروهها می شد و لذا در آن زمان نگرانی چندانی در مورد تأمین امنیت اطلاعات وجود نداشت.

طراحی شبکه جهانی وب نیز بر همین اساس شکل گرفت تا یک ابزار قوی برای کشف منابع اطلاعاتی و قراردادن آن در اختیار افراد دیگر باشد؛ بدون استفاده از مکانیزمی برای کسب مجوز یا تسهیل سرمایه گذاریهای مالی. فرهنگ به اشتراک گذاری اطلاعات میان پژوهشگران و دانشگاهیان طی دهۀ ۹۰توسط ARPANETمطرح شد و هنوز هم نشانه هایی از آن دیده می شود . بر اساس این فرهنگ، اطلاعات در

شبکهٔ جهانی وب تا حد ممکن در دسترس و رایگان است و امکان استفاده از آن برای صدها میلیون نفر از مردم در سرتاسر جهان وجود دارد . این مسئله بسیار مهم است و پاسخی به این سؤال می باشد که چرا اینترنت تا امروز به این سطح از رشد رسیده است . جنبه اخلاقی این فرهنگ در گفتگوهای عامیانه مردمی که اینترنت را منبعی بسیار خوب و معتبر توصیف می کنند مشاهده می شود؛ چراکه قدرت رسانه ای اینترنت و اثرات کار با آنرا دیده اند. گاهی اوقات در مورد ماهیت اینترنت گفته میشود که اطلاعات در آن تمایل به آزاد بودن دارند. یک توجیه دیگر برای آسیب پذیریهای حال حاضر اینترنت آن است که نسل اول اینترنت بر اساس اعتماد متقابل ایجاد شده بود و کاربران آشکارا برای کار با یکدیگر به هم اعتماد می کردند. با گسترش وسیع اینترنت و به عضویت درآمدن افراد بیشتر با علایق و اهداف مختلف در آن، اعتماد متقابل معنای خود را از دست داد . درحال حاضر یکی از مباحث عمده در اینترنت توسعهٔ مفهوم نوین اعتماد متقابل است بگونهای که مؤثر، واقع گرایانه، و بسادگی قابل پیاده سازی باشد.

اینترنت با سیستمهای ارتباطی قبل از خود چندین تفاوت اساسی د ارد که هر کدام از اهمیت خاصی برخوردارند . بعضی از این تفاوتها هنگامیکه اینترنت را با شبکهٔ تلفن عمومی(PSTN) که روزانه در سراسر دنیا استفاده میشود مقایسه کنیم بهتر درک میشوند . اینترنت براساس مدلی از انتقال اطلاعات کار می کند که Packet Switching نام دارد. هر زمان که اطلاعات از طریق اینترنت عبور می کند به چندین بستهٔ داده شکسته می شود. این بسته ها رمزگذاری شده و هر کدام بصورت مستقل در شبکه ارسال و پس از دریافت در مقصد مجدداً سرهم بندی می شوند (مسیر ارسال آنها می تواند متفاوت باشد). این روش انتقال د ر نقطهٔ مقابل - Circuit Switchingکه PSTN از آن استفاده می کند - قرار دارد . در این روش به هر مکالمه تلفنی یک مدار واحد اختصاص داده می شود و لذا در آن حجم صدای انتقال یافته در هر لحظه مهم نیست. اینترنت رسانه ای نادان است، چراکه تمام آنچه که می داند این است که باید یک بسته را از یک مبدأ متصل به شبکه به یک مقصد متصل به شبکه برساند . تمامی خدمات اینترنتی در انتها و در لبه ها به رایانه هایی می رسند که متصل به شبکه هستند.در عوض در PSTN اساس کار شبکه «هوشمندی » است و ابزار کاربر در نقاط انتهایی کاربرد اندکی برای صحبتکردن یا گوشدادن دارند.

اینترنت جهانی است و بسیاری از کشورها را به هم متصل می کند و اطلاعات از طریق آن فراتر از مرزهای جغرافیایی به افراد مختلف جریان پیدا می کنند .این ویژگی بارزترین و جالبترین خصوصیت آن است که البته ارتباط چندانی بهامنیت ندارد. شبکهٔ PSTN نیز جهانی است، اما روشهای دسترسی تلفنی به کشورهای مختلف به آسانی اینترنت نیست و مثلا کاربر تلفن می داند که با یک کشور خارجی تماس گرفته است؛ اما وقتیکه به یک پایگاه وب دسترسی پیدا می کند لزومی ندارد که بداند سرویس دهندهٔ آن در کجای دنیا قرار دارد.

اینترنت باز است و می توان آنرا بعنوان شبکه ای از شبکه ها درنظر گرفت که هر شبکه ای که به خانواده ای از پروتکل TCP/IP تعلق داشته باشد می تواند به آن متصل شود و بخشی از آن محسوب گردد . استانداردهایی که مجموعه این پروتکلها را تعریف می کنند توسط IETF ارائه می شوند و معمولا بدنه فنی غیررسمی آنها بر اساس شایسته سالاری فنی و پیاده سازی استانداردهای توافقی تدوین میگردد. اینترنت غیرمتمرکز است و در آن هیچ سیستم مرکزی ارتباطی وجود ندارد و همینکه شما از پروتکلهای اصلی آن نظیر TCP/IP پیروی کنید می توانید رایانه یا شبکه خود را به اینترنت متصل نمایید. اینترنت در همه جا رایج است و موانع ورود به آن اندک هستند. مقدار پهنای باند (سرعتی که می توانید داده ها را با آن انتقال دهید) نیز به ظرفیت حمل سیمهای مسی، اتصالات فیبری یا کانالهای ماهواره ای واقع در مسیر انتقال بستگی دارد. در شاهراه آن طیفهای الکترومغناطیسی کمیاب وجود ندارند. هرجا که از طیف رادیویی استفاده گردد - مانند شبکه های محلی بی سیم (WLANs) که معمولا با عنوان Wi-Fi از آنها نام برده می شود - قوانین و پروتکلهای مرتبط یک محیط اشتراکی را پدید می آورند که دسترسی را ساده میکند.

اینترنت برای کاربران متوسط واقع در بخشهایی از دنیا که مکالمات تلفنی محلی در آنها رایگان است نسبتًا ارزان تمام میشود. قیمت دسترسی به اینترنت از طریق خطوط تلفن و کافی نت و دیگر نقاط دسترسی عمومی در این کشورها بسیار اندک است و درنتیجه دسترسی به اینتر نت برای درصد زیادی از مردم جهان بسیار ساده تر میباشد. اینترنت مانع موجود میان مؤلف و ناشر را از بین برده است؛ شما می

توانید یک ناشر باشید و روی رایانهٔ خود خدمات شبکه ای ایجاد کنید و برای اینکار تنها کافیست رایانهٔ شما همواره به اینترنت وصل باشد . همچنین می توانید درباره خدماتی که ارائه می دهید تصمیم گیری کنید و هر کس دیگری نیز درصورت اتصال به اینترنت و کسب اجازه از جانب شما می تواند به رایانه شما وصل شده و از آن خدمات استفاده نماید . اینترنت توسط کاربران قابل کنترل و شنود است، اما در بسیاری از کشورها شما می توانید انتخاب کنید که پیامها و سایر داده های ارسالیتان برای مقابله با شنود رمزگذاری شوند یا خیر. بعلاوه غربال کردن پیامها تحت کنترل شما می باشد، هرچند که می توانید از یک منبع خارجی درخواست کنید اینکار رابرای شما انجام دهد - مثلا ازISP خود بخواهید که پیامهای نامطلوب را براساس ضوابطی که خودتان تدوین می کنید غربال نماید. اینترنت یک رسانهٔ تعاملی است؛ می توانید به آسانی و با سرعت چندین پایگاه وب را مشاهده کنید، یا از افراد بسیاری پیامهای الکترونیکی دریافت و یا به آنها پیام ارسال نمایید . از آنجا که زمان انتظا ر برای خدمات برخط بستگی به میزان پهنای باند خط ارتباطی شما دارد، ممکن است دریافت پاسخ از این خدمات کمی طول بکشد.

اینترنت می تواند آسیب پذیر باشد؛ چراکه در ابتدا اساس آن بر ارائه خدمات به گروههای همکار و نسبتًا مشابه مردم قرار داشت و بجای استفاده از مکانیزم های تصدیق هویت مطمئن، در آن به همه اعتماد می شد . این کتاب آسیب پذیریهای اینترنت را به شما شناسانده و مجموعه ای از الگوهای سرآمدی امنیتی را برای کمک به شما در کاهش آسیبپذیری ارائه میکند.

بر اساس مشخصه های فوق تاکنون باید در ذهن خود تصویری از اینترنت داشته باشید که در آن هر نوع فعالیت مجاز است و چیزی در آن محدودیت ندارد و تحت کنترل نیست. این فضای باز بخوبی ریشه های پژوهشی و دانشگاهی اینترنت را نشان می دهد و فواید آنرا برای تمامی اقشار جامعه می نمایاند. اینترنت با هدف برقراری امنیت طراحی نشده، بلکه برای افزا یش ثمرات فعالیتهای مشترک بوجود آمده است . این میزان آزادی عمل فرصتهایی برای افراد ایجاد می کند که بتوانند از شبکه ها سوء استفاده کنند و به دیگران آسیبهای جدی وارد نمایند . ما ابتدا باید ماهیت این نوع سوءاستفاده ها را درک کرده و سپس شبکه های خود را در مقابل آنها امن کنیم.

موضوعات مطرح در حوزهٔ امنیت اطلاعات

مفاهیم رایانه ، شبکه و امنیت داده ها در فضای سایبر همانندنیای واقعی هستند، ولی مکانیزمهای پیاده سازی روالهای مرتبط با آنها متفاوت است . مثلا برای استفاده از حسابهای کاربری که اجازهٔ دسترسی به اطلاعات یا خد مات را فراهم می آورند، به جای کلیدهای فیزیکی یا الکترونیکی، دارای شناسهٔ کاربری و رمز عبور هستیم و بجای استفاده از پاکتهای دربسته برای انتقال اطلاعات می توانیم دادهٔ انتقالی را به نحوی رمزگذاری کنیم که توسط افراد ناشناس، غیرقابل خواندن باشد. در مقایسهٔ دنیا ی واقعی با فضای سایبر می توانیم تخلفات مشابهی را در مورد قابلیت اطمینان و محرمانگی ببینیم . در هر دوی آنها ممکن است آدرسهای نادرست و یا امضاهای جعلی وجود داشته باشد . در هر دو فضا امکان ارائه اطلاعات غلط یا گمراه کننده نیز وجود خواهد داشت . همچنین امکان به اشتباه انداختن اشخاص با اطلاعات - چه بصورت تصادفی و چه از روی عمد - وجود دارد که باعث می شود نتوان تعیین کرد که چه اطلاعاتی مهم و قابل تأیید هستند.(کاپیتان کشتی معروف تایتانیک از رادیوی اولیه برای برقراری تماس از کشت ی با ساحل استفاده می کرد. منشی رادیو که اولین سفر دریایی خود را تجربه می کرد آنقدر پیامهای شخصی دریافت مینمود که یک پیام مهم - هشدار در مورد یک کوه یخی بزرگ در مسیر حرکت کشتی - بعنوان یک پیام مهم و شایستهٔ پیگیری شناسایی نشد . نتیجه این بود که کشتی با کوه ی خی برخورد کرد و چند ساعت بعد غرق شد.)دست آخر اینکه در هر دو فضا امکان دسترسی غیرمجاز به اطلاعات محرمانه و استفاده از آنها برای مقاصد غیرقانونی نیز وجود دارد. اما با همهٔ این شباهتها سه تفاوت عمده میان این دو فضا مشاهده میشود:

اول: هر نوع نقض امنیت در فضای سایبر می تواند بسیار سریع اتفاق بیافتد؛ یعنی تا زمانیکه بخواهید آگاه شوید چه اتفاقی برای سرمایه های شما افتاده، ممکن است دیگر برای جلوگیری از وارد آمدن خسارت بسیار دیر شده باشد . البته تمامی حملات سریع اتفاق نمی افتند؛ بلکه بعضی از آنها در هنگام وقوع قابل مشاهده اند و برای به نتیجه رسیدن زمان زیادی می برند. درسی که از این مطلب گرفته می شود آن است که تدابیر امنیتی و بازدارنده باید از استیلای کافی برای تشخیص نقض حریم امنیتی در حین وقوع جرم یا پس از آن برخوردار باشند. به گزارشهای زیر دربارهٔ کرم Slammer که در اوایل سال ۲۰۰۳ میلادی باعث خرابی

شدید در کار اینترنت شد توجه کنید. در اثر فعالیتهای این کرم، کشورهای زیادی از تمامی پنج قارهٔ جهان آلوده شدند و بخشع عمده خرابیها نصیب کشورهای درحال توسعه شد:

slammer(که گاهی اوقات Sapphireنیز نامیده می شود)سریعترین کرم رایانه ای است که در طول حیات رایانه ها منتشر شده . با شروع گسترش آن در سراسر اینترنت، بیش از ۹۰ ٪ میزبانهایآسیب پذیر در عرض ۱۰ دقیقه آلوده شدند و این ا مر موجب اختلال در انجام داد و ستدهای مالی و امور حمل و نقل مؤسسات دولتی شد و جایی برای عکس العمل انسانی باقی نگذاشت .

Slammerقبل از ساعت ۵:۳۰ UTC روز شنبه ۲۵ ژانویه ۲۰۰۳ میلادی با بهره برداری از یک آسیب پذیری سرریزی بافر با نفوذ به رایانه های متصل به اینترنت که نر م افزار Microsoft SQL Server یا Microsoft SQL Desktop Engine (MSDE)2000 را اجرا میکردند نفوذ کرد و به آرامی اقدام به آلوده ساختن تمامی رایانه های میزبان نمود.

دیوید لیچفیلد در جولای سال ۲۰۰۲ میلادی این آسیب پذیری را کشف کرد و مایکروسافت نیز قبل از انتشار کرم Slammer وصل های برای اصلاح آن منتشر کرده بود .

طبق گزارشهای رسمی کرم مذکور با استفاده از این آسیب پذیری حداقل هزار رایانهٔ میزبان را آلوده کرد که البته تعداد واقعی بسیار بیش از این میزان است- و موجب اختلال شدید در کار اینترنت و بروز نتایج پیش بینی نشده ای چون لغو پروازهای هوایی، اختلال در انتخابات، و بروز اشکال در کار ستگاههای خودپرداز شد .

دوم : لازم نیست شما در یک محل بصورت فیزیکی حضور داشته باشید تا بتوانید امنیت فضای سایبر را خدشه دار کنید. این بدان معناست که مثلا یک نفر در اروپا می تواند امنیت رایانه های یک هدف در هند را به آسانی کسی که در هند تنها به اندازه عرض یک خیابان با آن هدف فاصله دارد خدشه دار نماید . تهدید امنیتی در فضای سایبر می تواند از هر جای شبکه شروع شود و به سمت هدفی معلوم و مشخص جهت گیری کند؛ و هدف نیز می تواند بصورت تصادفی انتخاب شده باشد . این تهدیدات خطرناک باعث می شوند که ما نحوهٔ تفکر خود در مورد امنیت را تغییر دهیم . می توان گفت این هیچ ارزشی ندارد که در آیین نامهٔ

حق تکثیرDigital Millennium طراحی نرم افزارهای قفل شکن غیرقانونی اعلام شود؛ چراکه درحال حاضر کمیته های ملی و جهانی حق تکثیر در این موضوع و سایر موارد مرتبط به حفاظت از داده ها، هنوز مشغول تدوین راهکارهای اجرایی هستند.

سوم : فضای سایبر محیطی قدرتمند اما پیچیده را بوجود آورده که در آن نقش تأمین امنیت بر عهدهٔ چند بازیگر است. مثلا اگر شما یکی از کاربران یک ISP باشید، راههای مختلفی برای حفاظت از خود و رایانه شخصی تان پیش رودارید؛ هرچند نمی توانید سیاستهای امنیتی ISPمورد استفاده خود یا نحوه پیاده سازی آنرا کنترل کنید . همچنین نمی توانید نرم افزارهای مشتریان خود را تحت کنترل داشته باشید؛ حتی اگر در ارتباط نزدیک با سیستمهای آنها باشید . پس باید یک استراتژی حفاظتی برای سرمایه هایتان اتخاذ کنید، چراکه میدانید برقراری ارتباط با دنیای بیرون باعث می شود نتوانید تمام آسیب پذیریهای شبکه را خنثی نمایید.

مخاطرات محتمل در فضای سایبر چیستند؟

اگر هیچ ملاحظهٔ امنیتی را مد نظر قرار نداده باشید بعضی نتایجی که ممکن است به بار بیایند عبارتند از:

تخریب اطلاعات - داده های ذخیره شده روی رایانه شما ممکن است حذف شوند . البته معمولا امکان بازیابی آنها وجود دارد، اما فرآیندی زمان بر و احتمالا ناقص خواهد بود . اگر یک مؤسسهٔ دولتی باشید ممکن است فعالیتهایتان حین این دوره دچار اختلال شود.

سرقت اطلاعات و نقض حریم خصوصی - ممکن است از سرقت اطلاعات بلافاصله یا با تأخیر مطلع شوید و این مسئله از اینکه متوجه شوید چه کسی داده های شما را در اختیار گرفته، چه اطلاعاتی در اختیار اوست، یا با آنها چه کارهایی انجام خواهد داد کاملا مجزاست . اگر حجم وسیعی از اطلاعات شخصی شما به سرقت رفته باشد به احتمال زیاد سارق اطلاعات کلیدی شما را در اختیار دارد و همین امر می تواند نتایجی نامعلوم و تا اندازه ای خطرناک در پی داشته باشد. نقض یکپارچگی اطلاعات - اطلاعات موجود در رایانه

ممکن است بدون اطلاع شما تغییر کنند و دستکاری شوند. بر اساس نوع اطلاعاتی که نگهداری می کنید نتایج این دستکاری می تواند مقطعی یا درازمدت باشد.

اگر این داده ها شامل سوابق مالی ، اطلاعات مشتریان ، وضعیت سفارشات یا پرونده های کارمندان باشند، پیامدهای نقض یکپارچگی آنها ممکن است بسیار پرهزینه و زیانبار باشد. نقض انسجام شبکه از طریق سایر سیستمها و شبکه ها - هرچند در این مورد به طور مستقیم مورد حمله قرار نگرفتهاید، ولی ممکن است رایانه های دیگری که به آنها دسترسی داشته اید مورد حمله قرار گیرند و این مسئله روی شما نیز تأثیرگذار باشد . در اینصورت اگر مثلا یک مؤسسهٔ مالی و اعتباری باشید حین دورهٔ بازیابی اطلاعات قادر به تکمیل تراکنشهای مالی خود نخواهید بود .

ثبت کلیدها نرم افزارهای پنهانی می توانند روی رایانه شما نصب شوند که فشرده شدن دکمه های صفحه کلید توسط شما را ثبت کرده و آنها را به رایانه ای دیگر ارسال نمایند . این مسئله می تواند دسترسی به منابع خارجی نظیر دسترسی به یک سرویس دهندهٔ وب محافظت شده، دسترسی به یک سرویس دهندهٔ پست الکترونیکی، نقل و انتقالات مالی، و یا دریافت اطلاعات محرمانه را دچار اشکال کند . در اینحالت سارق می تواند نشانهای تصدیق هویت ، شمارهٔ کارت اعتباری، و رمزهای عبور شما را بدست آورد و در آینده برای منافع شخصی خود مورد استفاده قرار دهد. منع دسترسی ممکن است شما از دسترسی به اطلاعات خود محروم شوید، حتی اگر آن اطلاعات پاک نشده باشند . مثلا امکان دارد اطلاعات شما در قالبهای رمزگذاری شده ای ظاهر شوند و تنها مهاجم کلید رمزگشایی آنها را در اختیار داشته باشد. هزینه ترمیم موفقیت آمیز از هر یک از این حملات قابل ملاحظه است و بازیابی در برخی موارد ناممکن بنظر می آید.

اگر شما مدیر یک رسانهٔ تبلیغاتی باشی د که به منابع داده ای الکترونیکی خود وابستگی شدید دارد، یک حملهٔ مخرب می تواند موجب ورشکستگی مؤسسه شما گردد . توجه داشته باشید که کرم Slammer سیستمهایی را آلوده می کرد که وصله ارائه شده توسط مایکروسافت روی آنها نصب نشده بود. یکی از نفوذهای امنیتی که بیش از یکسال فعالیت موفقی تآمیز داشت روشهای نوینی را به تصویر کشید که

با آنها میتوان امنیت را در فضای سایبر خدشهدار کرد: آسوشیتد پرس (نیویورک) برای بیش از یکسال، جوجو جیانگ بدون اطلاعِ افرادی که از پایانه های اینترنتی در فروشگاههای کینکودرنیویورک استفاده می کردند، آنچه که آنها تایپ می کردند را ثبت می کرد. جیانگ بصورت مخفیانه نرم افزاری را در حداقل چهارده فروشگاه کینکو نصب کرده بود که می توانست فشردن کلیدهای افراد را ثبت نماید . این نرم افزار در طول فعالیت یکسالهٔ خود بیش از ۴۵۰ شناسهٔ کاربری و رمز عبور ثبت کرده و از آنها برای دسترسی و حتی بازکردن حسابهای بانکی برخط استفاده مینمود. این پرونده که در اوایل این ماه پس از دستگیری جیانگ منجر به تعیین مجازات برای وی شد خطرهای استفاده از پایانه های عمومی اینترنت در کافی نت ها، کتابخانه ها، فرودگاهها و دیگر مؤسسات ر ا آشکار می سازد . نیل مهتا مهندس پژوهش در مؤسسه سیستمهای ایمن اینترنتی هشدار می دهد که «هنگام استفاده از هر یک از پایانه های عمومی از دانش عرفی خود بهره بگیرید . برای بسیاری از ارتباطات روزمره نظیر اتصال به وب ممکن است با مشکلی مواجه نشوید اما برای انجام هر کاری که ممکن است حساسیت ایجاد کند ابتدا کمی فکر کنید ». جیانگ زمانی دستگیر شد که مطابق سوابق موجود در دادگاه از یکی از رمزهای عبور مسروقه برای دسترسی به رایانه ای مجهز به نرم افزار GoToMyPC استفاده کرده بود . این نرم افزار به افراد امکان می دهد که از راه دور و از هر مکانی به رایانهٔ خود دسترسی پیدا کنند . شخصی که برنامهٔ GoToMyPCروی رایانهٔ وی نصب شده بود در زمان وقوع جرم در خانه بود و ناگهان متوجه شد مکان نمای رایانهٔ او روی صفحه شروع به حرکت کرد و فایلها خود به خود باز شدند.

سپس دید که یک حساب بانکی باز و نام او در یک سرویس خرید اینترنتی درج شد . جیانگ که منتظر صدور حکم دادگاه است، نهایتاً در چهاردهم فوریه ۲۰۰۱ به نصب کردن نرم افزار مخفی ثبت کنندهٔ کلید در فروشگاههای کینکو اعتراف کرد. این کتاب راهنمایی دربارهٔ امنیت کاربران هم در محیط خانه و هم در محیط تجاری می باشد و لذا حاوی اطلاعات وسیعی دربارهٔ موضوعات امنیتی مانند مخاطرات، نتایج حملات، روشهای حفاظت از رایان هها، شبک هها و داد ه ها، و نیز سیاستهایی است که باید قبل از پیاده سازی استراتژی امنیتی مؤثر مورد بررسی قرار گیرند . هدف نهایی این کتاب دور ساختن کاربرا ن از

منابع ارائه شده در محیطهای دیجیتالی جدید نیست، بلکه قدرت بخشیدن به کاربران برای لذت بردن از این دنیای نوین به روشی ایمن و مطمئن است . در یک کلام می توان گفت هدف از انتشار این کتاب توسعهٔ درک واقع گرایانه و عمیق از ماهیت مشکلات امنیتی موجود به منظور کاهش آسیب پذیریها و افزایش نقاط قوت فناوری اطلاعات و ارتباطات میباشد.

انگیزه خرابکاران امنیتی چیست؟

در زندگی واقعی انگیزه های زیادی برای انجام تخلفات جنایی علیه یک شخص یا سازمان وجود دارد . یکی از دلایل عمده، انتقامگیری فرد خرابکار از شخصی که فکر می کند به او آسیبی رسانده، و یا بدست آوردن پول است.

نظیر همین تخلفات نیز در فضای سایبر وجود دارد، اما تخلف در این فضا از جنس دیگری است . فضای سایبر برای گروهی از افراد – که عموماً« خرابکار » نامیده می شوند و قادرندوارد حسابهای کاربری افراد شوند و یا بعنوان تفریح و سرگرمی به افراد دیگر آسیب برسانند - یک محیط چالش برانگیز است. بعبارت دیگر، آنها قدرت نفوذ به حسابهای کاربری، پایگاههای داده و تجهیزات شبکه ای را یک افتخار برای خود میدانند. مشابه این رفتار در دنیای واقعی بسیار نادر است. خرابکارها معمولا فعالیتهای خودرا « جنایات بدون قربانی » به حساب می آورند .استدلال آنها این است که وقتی یک حساب کاربری یا پایگاه داده مورد نفوذ قرار می گیرد ولی چیزی تغییر نمی یابد و دزدیده نمی شود چه آسیبی به کسی وارد شده است؟ در واقع این افراد به تأثیرات حقوقی و پیامدهای اینکار توجه نمی کنند و به احساس ناامنی قربانیانشان که ناشی از انجام این فعالیتها می شود نیز اهمیتی نمی دهند.

مشابه این رفتار در دنیای واقعی مثل این است که فردی واردخانهٔ شما شود و هر زمان که بخواهد نیز بتواند اینکاررا تکرار کند. مسلماً این مسئله برای شما غیرقابل تحمل خواهد بود. متأسفانه اینترنت به ناقضان امنیت کمک زیادی می کند. برخی از خرابکارها دارای ابزارهای نفوذ هستند که به نفوذگران تازه کار هم امکان بهره برداری موفقیت آمیز از برخی آسیبپذیریها را می دهد. چنین ابزارهایی معمولا به گروههای خبری Usenet که بسیار مشهور هستند فرستاده می شوند و افراد مختلف می توانند ابزار را از آنجا پیدا

کرده و مورد استفاده قرار دهند . از آنجا که بسیاری از این ابزارها ممکن است بدون خطر باشند، هرگز کسی مطمئن نیست آثار استفاده از هریک از آنها دقیقا چیست . علاوه بر آن این امکان وجود دارد که با انجام تغییراتی در بعضی از این ابزار به اصطلاح بی خطر بتوان به رایانه ها و حسابهای کاربری که از طریق آنها مورد دسترسی قرار گرفته اند آسیب وارد کرد . درادامه، یک نمونه از این موارد ذکر شده است:

سند CA-203-18 مرکز فوریتهای امنیت رایانه ای آخرین حفره Windows را مستند کرده، و CNetنیز گزارش داده که با بهرهبرداری از این آسیبپذیری برای نفوذ به Windows راه برای ظهور برق آسا و حملهٔ شدید یک کرم دیگر هموار میشود: پژوهشگران امنیتی هشدار داده اند که یک گروه از نفوذگران برنامه ای منتشر کرده اند که برای سوء استفاده از یک اشکا ل عمدهٔ Windows طراحی شده و راه را برای انجام یک حملهٔ بزرگ تا اواخر هفتهٔ جاری باز می کند. این هشدار روز جمعه اعلام شد؛ بعداز آنکه نفوذگران چینی گروه امنیتی X Focusمتن برنامه ای را برای چندین مرکز امنیتی دنیا منتشر کردندکه با طراحی ماهرانه به رایانه های د ارای سیستم عامل Windows نفوذ میکرد .

برنامهٔ گروه X Focus از اشکال موجود در سیستم عامل مایکروسافت بهره برداری می کند و به نفوذگران امکان نفوذ به سیستم از راه دور را می دهد . این اشکال توسط چند نفر از متخصصین بعنوان بزرگترین اشکالی که تا کنون در Windowsیافت شده معرفی شده است. حملات روزافزونی که توسط افراد نسبتًا غیرحرفه ای انجام میشوند نیز ماجرایی طولانی و دنباله دار است . البته تمامی نقض حریمهای امنیتی مختص رایانه ها و اینترنت نیستند . دستگاههای خودپرداز نیز تا کنون برای سرقت اطلاعات محرمانه مورد استفاده قرا ر گرفته اند. در یک مورد (در ایالت کانکتیکات ایالات متحده) سارقین اقدام به نصب دستگاهی شبیه دستگاه خودپرداز در یک مرکز خرید کردند هنگامیکه مردم برای گرفتن پول از این ماشین کارت و شمارهٔ رمز خود را وارد می کردند، این دستگاه جعلی با ذخیرهٔ رمزهای عبور دسترسیه ای غیرمجاز بعدی به این حسابها رابسیار ساده می کرد، اما چون اتصالی با مراکز واقعی اعتباری نداشت قادر به تکمیل عملیات مالی نبود . در یک مورد دیگر سارقین از دستگاههای خودپرداز به نحوی استفاده کردند که

امکان انتقال پول هم وجود داشته باشد، اما مدتی بعد و بااستفاده ازاطلاعات ثبت شده اقدام به سرقت می نمود.

اگرچه بیشتر جرائم قابل مشاهده در دنیای سایبر توسط افرادانجام می شود، ولی سازمانها و مؤسسات نیز قادر به سوء استفاده از خصوصیات این فضا برای رسیدن به اهداف سازمانی خود هستند . جرائم سازماندهی شده ممکن است دستکاری در شبکهٔ اینترنت برای رسیدن به نتایج مطلوب آنها باشد، اما می تواند باعث ارتکاب جرم علیه دیگران نیز بشود. ممکن است برخی سازمانها علاقه داشته باشند که نتیجهٔ یک نظرسنجی یا حتی انتخابات را دستکاری کنند تا به نتایج مطلوب خود برسند . برخی از مؤسسات درحال حا ضر روی این مسئله سرمایه گذاری زیادی انجام داده اند و ممکن است بتوانند تا مدتها آنرا همچنان با قوت ادامه دهند. واضح است که منافع بالقوهٔ موجود در عصر نوین دیجیتال بیشمار هستند . بسیار حائز اهمیت است که با ایمن سازی محیط فیزیکی، زیرساختها، رایانه ها، خطوط ارتب اطی و منابع اطلاعاتی خود از این منافع حفاظت کنیم . اولین گام در انجام این مهم رسیدن به سطح شناخت کافی و صحیح از فناوری است که می تواند در اتخاذ تصمیمات عاقلانه دربارهٔ چگونگی رسیدن به سطح مطلوبی از امنیت به ما کمک کند . بسیاری از ما در این زمینه چندین نقش را بر عهده داریم : ممکن است بعنوان یک کاربر عادی از این منابع استفاده کنیم، در قبال سیستمهای دیجیتال و خدمات موجود در یک سازمان مسئولیت داشته باشیم، و یا به همکاری با دولت در اجرای سیاستهای حمایتی از امنیت علاقهمند باشیم. همهٔ ما در هریک از این نقشها در قبا ل تحقق سطح مطلوبی از امنیت مسئول هستیم . متأسفانه امنیت در یک محیط پیچیده معمولا به اندازهٔ امنیت ضعیفترین جزءِ آن محیط استحکام دارد؛ از اینرو باید مطمئن شویم که اجزای محیطی که روی آن کنترل داریم آنقدر قوی هستند که ضعیفترین آنها هم از توانایی دفاع در برابر تهدیدات موجود برخوردار است.

اهمیت امنیت برای سازمانهای کوچک و متوسط در کشورهای درحال توسعه

با اینکه امنیت برای همه حائز اهمیت است، اما برای سازمانهای کوچک و متوسط کشورهای درحال توسعه اهمیت ویژه ای دارد . نتایج حاصل از ورود به بازار جهانی با کمک فناوری اطلاعات و ارتباطات بسیار مطلوب است، ولی مخاطرات انجام اینکار بصورت ناامن نیز بسیار اساسی است. در بسیاری از اصناف تجاری، عملیات دستی به مدیریت با استفاده از رایانه ها تغییر یافته است . از رایانه های مستقل می توان در بسیاری از عرص ههای اقتصادی کشورهای توسعه یافته برای مدت زمانی مشخص استفاده کرد . با معرفی منابع رایانه ا ی جدید، مدیران به سمت و سوی کسب دانش و، اطلاعات دربارۀ موضوعات کاربردی چون پشتیبان گیری نگهداری شبکه، به روزرسانی نرم افزارها و ممیزی (بازبینی)رایانه ا ی در حرکت هستند . کسب موفقیت در همگی موارد فوق مستلزم آشنایی با رایانه، شبکه، و مفاهیم امنیت اطلاعات است. با معرفی ارتباطات شبکه ای و امکان ورود به عرصۀ تجارت الکترونیکی، فرآیندهای سیستم و فرآیندهای مدیریت باید از دو دیدگاه متفاوت نظاره شوند . سیستمهای مستقل عموماً فرآیندمحور هستند (مثل انبارداری، سفارشات یا فرآیندهایی نظیر تولید، ثبت در دفاتر عمومی، و حسابهای پرداختنی و دریافتنی)، اما سیستمهای موفق تجارت الکترونیکی برخط به روش دیگری سازماندهی می شوند. در این سیستمها برای کسب موفقیت لازم است که طراحی مشتری مدار باشد و سیستم به تعقیب رفتار مشتری در فرآیندهای جستجو و ارزیابی محصولات، ارائه سفارش، تکمیل تراکنشهای مالی و ردگیری محصول ارسال شده بپردازد . در این سیستمها نگرانی در مورد محصولات و فرآیندها همچنان مهم است، اما در مقابل نیاز به تعقیب رفتار مشتری در پایگاه وب و انجام هرمعامله ای که مشتری آنرا درخواست می کند در اولویت بعدی قرار می گیرد. این طراحی مجدد برای دستیابی به موفقیت ضروری است، اما به یک راهکار جایگزین برای مدیریت درخواستهای خرید مشتری نیاز دارد؛ روشی که اگر بدون توجه کافی پیاده سازی شود ممکن است راه را برای روشهای جدید نفوذهای امنیتی باز بگذارد. سازمانهای کوچک و متوسط باید آگاه باشند که اصلاح نگرش سیستمهای تجاری برای بکارگیری اینترنت،مخاطرات جدیدی برای آنها به همراه دارد . یکی از این خطرات از همه جدیدتر است : احتمال به سرقت رفتن و در معرض فروش قرار گرفتن سرمایه های موجود

در شر کت. درعصری که کالاها و خدمات فروخته شده را محصولات اطلاعاتی تشکیل می دهند، احتمال توزیع و تهیهٔ غیرقانونی آنها بصورت رایگان و یا در بازار سیاه وجود دارد که در این حالت منافع اینکار به سارقان می رسد، و نه به شرکتی که اطلاعات را تولید کرده است. بارزترین نمونهٔ نسخه برداری غیرقانونی که امروزه می توان مشاهده کرد در صنعت موسیقی رواج دارد که به توزیع محصولات مسروقه و غالباً هم در قالب دیسک فشرده منجرشده است . درحال حاضر حفاظت از سرمایه های دیجیتالی مسئله ای حل نشده می باشد، هرچند برای حل آن اقدامات زیادی صورت گرفته است . دیرزمانی است که از محصولات اطلاعاتی دیجیتالی نسخه برداریهای نسبتًا کاملی انجام می شود، چراکه نسخه برداری از آنها آسان بوده و حین فروش لزومی ندارد که به دنبال نسخه اصلی آن بود . فناوری مورد استفاده در صنعت موسیقی را می توان در شرایط و محیطهای دیگر نیز مورد استفاده قرار داد، به این معنی که فوت و فنهای تجاری یا دیگر اطلاعات محرمانه را نیز می توان باروشهایی تهیه و منتشر نمود که موجب تخریب شدید آن تجارت و صنعت گردد . سرمایه های با ارزش نیاز به حفاظت کافی و مناسب دارند . البته این سطح از امنیت می تواند برقرار شود، اما مخاطرات و روشهای کار برای شرکتی که در قالب تجارت الکترونیکی کار میکند با مخاطرات و روشهای کار در شرکتی که بصورت سنتی به تجارت میپردازد متفاوت است.

بسوی مفهوم نوینی از قابلیت اطمینان

محیط دیجیتالی جدید از ما می خواهد که در تعریف خود از قابلیت اطمینان بازنگری کنیم . در دنیای واقعی از معیارهای گسترده ای برای تصمیمگیری دربارهٔ میزان اطمینان به یک شخص، یک فرآیند، یا یک سازمان استفاده می کنیم؛ مثلا از تطابق مشاهدات فعلی با تجربیات و دانسته های قبلی مان استفاده می نماییم. حین تبادل اطلاعات در فضای سایبر بیشتر شاخصهای غیر شفاهی ارتباطات از دست می روند .هنگامیکه یک نامهٔ الکترونیکی دریافت می کنیم یا صفحهٔوبی را می خوانیم، نمی توانیم همیشه بگوئیم که اگر اطلاعات دقیق بود و اگر آنها را بررسی می کردیم مشخص می شد که صحیح نیستند . همچنین نمی دانیم که خطاهای واقع شده نتیجه سهل انگاری هستند یا تلاشهایی تعمدی برای فریب دادن ما . در غیاب اطلاعات حتی دیگر نمی دانیم که آیا نویسندهٔ یک پیام همان شخصی است که خودش ادعای آنرا دارد یا

خیر. مسلم است که فریبکاری در جهان واقعی نیز رخ می دهد، ولی معمولا تعیین حقیقت در شرایطی که ا فراد بصورت فیزیکی و مکانها بصورت واقعی وجود دارند ساده تر است. خوشبختانه از طریق مراکز صدور گواهی به این بعد از امنیت دنیای سایبر کمک زیادی شده است . این مراکز برای شناسایی افراد و سازمانها به طور رسمی گواهی صادر می کنند. این مفهوم در دنیای واقعی نیز وجود دارد: اگر گذرنامۀ ملی داشته باشید یعنی دولت یک کشور هویت شما را تأیید کرده و لذا گذرنامه نشانه ا ی خواهد بود که می توانید برای تصدیق هویت خود از آن استفاده کنید . بطور مشابه اگر گواهینامۀ وسیلۀ نقلیۀ موتوری داشته باشید به این معنی است که یک سازمان ملی یا ناحیه ای دولت برای شما مجوزی صادر کرده که هم هویت شما را تأیید می کند و هم جواز رانندگی با یک وسیلۀ نقلیه را به شما می دهد.

شرکتهایی که خدمات کارت اعتباری می دهند نیز از طریق صدور کارتهای اعتباری شما را تأیید می نمایند . کارفرما یا آموزشگاه شما هم ممکن است از طریق یک کارت شناسایی شما را تأیید کند و آن کارت ممکن است دسترسی شما را به سرویسهای خاصی که مخصوص کارمندان یا دانشجویان یک حوزۀ خاص هستند برقرار نماید.واضح است که تعداد مراکز صدور گواهی در دنیای واقعی اندک هستند . بطور کلی هریک از این مراکز از تأیید شما هدف خاصی را درنظر می گیرند. جامعیت تأیید هویت از یک مرکز تا مرکز دیگر متفاوت است؛ برخی از آنها ممکن است به اثبات کامل هویت شما نیاز داشته باشند، درحالیکه سایرین ممکن است آنچه که بیان می کنید را بپذیرند. مراکز صدور گواهی در دنیای سایبر این مشخصات را به اشتراک می گذارند. سطوح متعدد تأیید هویت برای درجات مختلف اطمینان ایجاد می شود و هریک از این گواهیها تنهادر سطح خود معتبر می باشند. لذاست که هرچند ممکن است بنظر برسد که وجود یک مرکز صدور گواهی برای دستیابی به تمامی اهداف مورد نظر کافی است؛ اما چندین مرکز صدور گواهی در دنیای مجازی وجود دارد . علاوه بر این با استفاده از گواهی الکترونیکی ۶۶ ، این گواهیها می توانندبصورت الکترونیکی امضا شوند و این اطمینان را ایجاد کنند که گواهی منتقل شده صحیح و حقیقی است . این سیستمهای صدور گواهی از روشهای تجربی و شهودی که در دنیای واقع ی مورد استفاده قرار می گیرند مستحکم تر هستند. در دنیای دیجیتالی برای برقراری اعتماد لازم جهت پشتیبانی از انجام تراکنشهای

تجاری و نقل و انتقالات مالی در شبکه های الکترونیکی، لازم است که روشهای مستحک متر مورد استفاده قرار گیرند.

دولتها در ایجاد اطمینان از و جود مکانیزمهای مناسب برای کارایی و مورد استفاده قرار گرفتن مدلهای جدید اعتماد نقش مهمی دارند . انجام تراکنشهای سازمانهای کوچک و متوسط بصورت الکترونیکی بسته به وجود این اعتماد است . در بعضی کشور ها دولتها بر این باورند که سازمانهای دولتی باید بعنوان مراکز صدو ر گواهی عمل کنند و در سایر کشورها دولتها معتقدند که وظیفهٔ مراکز صدور گواهی باید به بخش خصوصی واگذار شود . مستقل از جزئیات پیاده سازی، هدف از تأسیس این مراکز واضح است . سیاست دولت می تواند مکانیزمهای ایجاد اطمینان را تسهیل کند تا افراد، سازمانها وکاربران منف رد آن قادر باشند در تجارت الکترونیکی کشورهای دیگر هم مشارکت نمایند .

جمع بندی

فناوری دیجیتالی ابزارهای جدید و مهیجی را فراهم می کند که هریک می توانند نقش بسزایی در آموزش، بهداشت، رفاه، تجارت و سایر بخشهای جامعهٔ مدنی داشته باشند.تمام افراد و کشورها از فناو ری اطلاعات بهره می جویند، امااین فناوری برای کشورهای درحال توسعه جاذبهٔ خاصی دارد و می تواند جا افتادن آنها در جامعهٔ اقتصاد جهانی را تسریع کند. این فناوری هنوز در آغاز راه خود است ولی بسرعت درحال 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. مفهوم «ایمنی سایبر » یک مفهوم مهم است . مثالهای این فصل، میزان وقایع گزارش شده به ، CERTو رخدادهای جدیدی که روزانه در مطبوعات گزارش می شوند همگی نشان می دهند که چرا آگاهی از موضوعات امنیتی حائزاهمیت است و چرا باید گام هایی برای تضمین پشتیبانی ازرایان ههای شخصی، داد ه ها و تجارت برداشت.

این کتاب حاوی مجموعه ای از الگوهای سرآمدی در زمینهٔ 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 سازما نهایی 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 شبک های می باشند مفید خواهند بود.

این شرایط در کشورهای درحال توسعه از اهمیت خاصی برخوردار است . سرمایه گذاری مستقیم خارجی و اعتماد و قابلیت اطمینان در این کشورها بستگی به سطح امنیت و پیادهسازی موفقیت آمیز فناوری و زیرساختهای آن دارد.

دولتها، سازمانها و کاربران منفرد همگی نقش بسزایی درتأمین امنیت سرمایه های اطلاعاتی و الکترونیکی کشورها ایفا می کنند. شناخت تهدیدات بسیار سودمند است؛ و عملکردمناسب بر اساس چنین شناختی می تواند یک محیط قابل اطمینان ایجاد کند و باعث شود ساکنان کرۀ زمین تا سرحدامکان فواید عصر نوین دیجیتال را حس کنند .

بخش دوم امنیت فناوری اطلاعات و کاربران منفرد

فصل اول

مقدمه

نکات ایمنی

فصل اول

مقدمه

تأکید بخش دوم بیشتر بر تأمین امنیت کاربران منفرد رایانه است - از مبتدیان گرفته تا کارشناسان؛ و اولین مسئله ای که در این زمینه باید شرح داده شود چگونگی حفاظت از رایانه های شخصی است. میتوان از ر ایانه بصورت ایمن استفاده کرد؛ ولی اینکار به اطلاعات، زیرکی و مراقبت شدید نیاز دارد . زبان بکار رفته در این بحث بعضًا حاوی مفاهیم نامأنوسی می باشد . بعضی از اصطلاحات و تعاریف در ضمیمهٔ انتهای این بخش آمده اند و بعضی از آنها نیز در پیوست ۱ کتاب بطور کامل طرح شده اند.

نکات ایمنی

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 درصورتی تغییر می کنند یا پاک می شوند که شما چنین خواستهای 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 در برنامهها ناخواسته است)؛
- هیچکس نمی تواند بدون اجازهٔ شما از داده ها، رایانه و شبکهٔ شما استفاده کند؛
- رایانه بطور ناخواسته فایلهای آلوده به ویروس را منتشر نمیکند؛
- کسی قادر به مشاهدهٔ تغییراتی که در رایانه ایجاد می کنید نیست؛

- کسی توانایی دستیابی به داد ههای شما، چه در شبکه های ب یسیم و چه در شبک ههای سیمی را ندارد؛
- روی سیستمها و یا پایگاههای وبی که به آنها دسترسی دارید کسی قادر به سرقت نام کاربری ۱ و رمز عبور۲ نیست؛
- چنانچه شمارهٔ کارت اعتباری و یا اطلاعات مربوط به حساب بانکی خود را از طریق شبکهٔ اینترنت وارد کنید، داده های مربوطه از امنیت کامل برخوردار خواهند بود (مسلماً شما بر آنچه که در سوی دیگر شبکهٔ ارتباطی رخ می دهد کنترلی نخواهید داشت)

چنانچه نکات امنیتی در رایانه های شخصی نادیده گرفته شوند پیامدهای گوناگونی به بار می آید : ممکن است این پیامدها منجر به آزار شخص گردند ولی هزینه ای در بر نداشته باشند، و یا اینکه هزینهٔ گزافی تحمیل کنند و وقت بسیار زیادی را به خود اختصاص دهند . در مواردی که حفاظت از رایانه بعنوان حرفهٔ شخص قلمداد می شود ممکن است مشکل بوجود آمده باعث به خطر افتادن موقعیت شغلی وی گردد در تمامی موارد شخص باید به ارزیابی احتمال خطر بپردازد و طرح امنیتی لازم را بکار گرفته و آنرا اجرا نماید .با توجه به جزئیاتی که در رابطه با امنیت فناوری اطلاعات ارائه شده است این امکان بوجود می آید که بتوان تمامی جوانب امنیتی رایانه های شخصی را کنترل نمود. چنانچه راهنمایی های ارائه شده در این کتاب نیز بکار گرفته شوند می توان احتمال خطر را تا حد قابل قبولی کاهش داده و از جهان درحال تغییر فناوری اطلاعات استفادهٔ بهینه نمود. طبیعتاً ارائه تمامی نکات امنیتی رایانه های شخصی صدها صفحه مطلب را به خود اختصاص می دهد، اما مخاطبین غالباً تمایل چندانی به مطالعه مطالب انبوه ندارند . در این نوشته خلاصه ای از اطلاعات لازم برای کاربران جهت درک و پیادهسازی نکات امنیتی رایانه های شخصی ارائه شده است. مراجع ذکرشده در بخش ضمایم شامل منابع الکترونیکی، سازمانهای مرتبط، و مستندات چاپی نیز می توانند کمکهای مفیدی باشند و کاربر را به مطالعهٔ بیشتر نکات امنیتی فناوری اطلاعات تشویق نمایند .

بخش دوم امنیت فناوری اطلاعات و کاربران منفرد

فصل دوم : درک مفاهیم امنیتی

کلیات

چرا تمهیدات امنیتی ضرورت دارند؟

ارزیابی تهدیدات و هزینه های آنها

ایمن شدن برای شما چه هزینه هایی خواهد داشت؟

چه زمانی را به خود اختصاص میدهد؟

تا چه حد برای شما مشکل آفرین خواهد بود؟

آیا کارهایی وجود دارند که با اجرای طرح امنیتی،انجام آنها مشکل و یا غیر ممکن شود؟

آیا می توانید به تنهایی طرح را اجرا کنید یا برای اجرای آن به کمک دیگران نیاز دارید؟

تصمیم گیری در مورد طرح امنیت فردی

نقش کاربر در امنیت

امنیت یک هنر است، نه یک علم

فصل دوم

درک مفاهیم امنیتی

کلیات

این فصل به تبیین ضرورت برقراری امنیت و حفاظت از شبکه و رایانه اختصاص دارد . در این فصل به پیامدهای نفوذ امنیتی، اقدامات اولیه جهت مقابله با آن، و نیز چند تعریف فنی از مباحث امنیتی پرداخته می شود .

چرا تمهیدات امنیتی ضرورت دارند؟

در اولین روزهای استفاده از رایانه ها در سیستمهای به اشتراک گذاشتهشده 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 سخ ت افزاری و برنامه های نرم افزاری - نکتهٔ قابل توجه این است که رایانه ها و بسته های نرم افزاری بسیار گرانقیمت هستند و جایگزینی آنها پرهزینه و دشوار است . حتی اگر در یک رخداد امنیتی نرم افزارها و سخ تافزارها کاملاً از بین نروند ممکن است مشکلات امنیتی ما را وادار به نصب مجدد همهٔ نرم افزارها کنند و م تعاقبًا لازم شود کلیهٔ نیازهای اساسی مجدداً تعریف گردند .

این امر مستلزم صرف زمان بسیار زیادی است؛ خصوصاًاگر فرد مسئول، اطلاعات فنی کافی در این زمینه نداشته باشد.

ارزش داده های سازمانی این داده ها ممکن است شامل لیست مشتر یها، پروژ ههای 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 دادنآنها بسیار زیان آور باشد و برای ایجاد دوبارۀ 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 صرفًا برای لذت و سرگرمی صورت می گیرد و برخی افراد نیز تنها بخاطر خودنمایی در برابر دوست ان 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 میشوند و در حد گس ترده 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 هرچند همچنان امکانپذیر می باشد ولی بسیار پیچیده شده است.

چرامعمولاً در بعد امنیت ضعف وجود دارد؟

برنامه های نرم افزاری غالباً بدون درنظر گرفتن مسائل امنیتی تولید میشوند .این مسئله چند دلیل دارد:

سهل انگاری برنامه نویسان و طراحان از اهمیت نکات امنیتی اطلاعی ندارند. اولویت پایین تا چندی قبل حتی کسانی که نسبت به نکات امنیت ی آگاهی داشتند نسبت به آن اقدام چندانی نمی کردند و درنتیجه

مسائل امنیتی مورد توجه لازم واقع نمی شد. محدودیت زمان و هزینه بعضی افراد تصور می کنند اقدامات امنیتی جهت طراحی، کد نویسی و آزمایش در طول فرآیند تولید نرم افزار هزینهٔ گزافی در بر داشته و زمان زیادی را به خود اختصاص می دهد.

بی نظمی برنامه نویسان در کارهای مربوط به برنامه نویسی اشتباهات مشابه چندین بار تکرار می شوند و باعث ایجاد نقایص امنیتی می گردند.

خلاقیت تبهکاران انسان موجود خلاقی است و افراد باانگیزه همیشه برای غلبه بر موانع امنیتی و کشف اشتباهاتی که منجر به نقایص امنیتی شوند راهی پیدا خواهند کرد.

سطح پایین آگاهی کاربران کاربران معمولی (قربانیان تخلفات امنیتی) بطور طبیعی از تهدیدهای اطراف خود آگاهی ندارند و به همین دلیل در پی راههای مناسب جهت تضمین امنیت داد هها و سیستمهای خود نیستند.

نگاه غیرواقعی قربانیان برخی کاربران نسبت به نکات امنیتی آگاهی دارند ولی آنها را جدی نمی گیرند؛ چون گمان می کنند که حمله ای علیه آنها صورت نخواهد گرفت.

ارزیابی تهدیدات و هزینه های آنها

جهت درک اهمیت نکات امنیتی لازم است به چند سؤال پاسخ داده شود . ابتدا فرض کنید مسائل زیر اتفاق افتاده باشند و سپس سعی کنید نتایج احتمالی هریک را ارزیابی نمایید و در هر مورد به چند سؤال کلیدی که در ابتدای صفحه بعدی آمده پاسخ دهید.

چه اتفاقی خواهد افتاد اگر...

... شخصی به خانه و یا محل کار شما حمله کند و رایانهٔ شما را بدزدد و علاوه بر آن دیسک نسخهٔ پشتیبان شما که ممکن است در آن نزدیکی باشد را نیز با خود ببرد.

... همهٔ داده های رایانهٔ شما پاک شوند.

..یک نسخه از تمام داده های شما به سرقت رود . این داده ها ممکن است شامل مواردی باشند از قبیل :اطلاعات حساب بانکی، فهرست نامهای کاربری و رمزهای عبورِ پایگاههای وب انجام خریدهای برخط ۴، گزارشهای کاری مهم و تکالیف درسی که ارزش آنها معادل ۵۰ % نمرات درسهای ترم جاریشما است.

... شخصی لحظه به لحظه هر آنچه را که شما با رایانه انجام می دهید مشاهده کند و به خاطر بسپارد. زمانیکه شمارهٔ کارت اعتباری خود را و ارد می کنید از آن آگاه شود، از گشت و گذار شما در پایگاههای وب مختلف مطلع باشد، و زمانیکه با پایگاه وب یا سیستمها ارتباط برقرار می کنید بتواند نام کاربری و رمز عبور را به سرقت ببرد.

... هنگامیکه روی یک پروژهٔ مهم کار می کنید و زمان در آن نقش بسیار مهمی دارد، رایانهٔ شما دچار مشکل گردد.

... یک ویروس رایانه ای مخرب به همه دوستانتان که نام آنها در دفترچهٔ آدرس های رایانهٔ شما ثبت شده ارسال شود.

... وقتی صورتحساب تلفن را دریافت کردید ملاحظه کنید که مبلغ آن حتی از حقوق ماهیانهٔ شما هم بیشتر است و این در شرایطی است که مطم ئن هستید به این میزان از تلفن استفاده نکرد هاید.

... یک صورتحساب کارت اعتباری برای شما ارسال شود و مشاهده کنید که این صورتحساب شما نیست؛ ولی بانک سعی دارد شما را متقاعد کند که به این میزان از کارت خود استفاده نموده اید و برای این مدعا دلیل هم دارد. سؤالات کلیدی که در هر مورد باید به آنها پاسخ داده شود به شرح زیر هستند:

- ✓درصورت وقوع، آیا امکان ترمیم وجود دارد؟
- ✓این رخداد چقدر زمان به خود اختصاص می دهد؟
- ✓چه مقدار هزینه صرف آن می شود؟

- ✓چگونه می تواند سازمان شما را تحت تأثیر قرار دهد؟
- ✓چه هزینه های جانب ی در بر دار د؟ (مثلاًدر شرایط نامناسب و در غیاب مسئول مربوطه)

تمامی این موارد اهمیت موضوع « امنیت رایانه » را مشخص می کنند .اکنون که متوجه شده اید امنیت موضوعی بسیار مهم است، گام بعدی بررسی یک طرح مناسب امنیتی برای ایمن شدن میباشد

- ✓ایمن شدن برای شما چه هزین های خواهد داشت؟
- ✓چه زمانی را به خود اختصاص می دهد؟
- ✓تا چه حد مشک لآفرین خواهد بود؟
- ✓آیا کارهایی وجود دارند که با اجرای طرح امنیتی، انجام آنها مشکل و یا غیر ممکن شود؟
- ✓آیا می توانید به تنهایی طرح را اجرا کنید یا برای اجرای آن به کمک دیگران نیاز دارید؟

سؤالات مطرح شده سؤالات بسیار مهمی هستند؛ چراکه شما برای اجرای یک طرح امنیتی نیاز به تخمین مناسبی از هزینه و زمان لازم و نیز مشکلات جانبی آن دارید . بدون وجود چنین اطلاعاتی ممکن است در طول فرآیند دچار ناامیدی شوید؛ یا پروژۀ مربوطه را لغو نموده و سپس خود را بدون پشتیبان بیابید . در ادامه در مورد هریک از موارد توضیح بیشتری داده شده است.

ایمن شدن برای شما چه هزینه هایی خواهد داشت؟

چند راهکار مناسب امنیتی وجود دارند که به تجهیزات پ چندانی نیاز ندارند و تجهیزات لازم نیز آنچنان گرانقیمت نیستند . حتی ویروس یابها که رایجترین کالای امنیتی هستند در قالب نرم افزارهای رایگان در دسترس می باشد.

چه زمانی را به خود اختصاص میدهد؟

مسلماً اجرای طرح امنیتی و دنبال کردن آن زمانی را به خود اختصاص می دهد، اما میزان این زمان زیاد نیست . در این خصوص لازم است که نرم افزارهای مناسب را نصب کنید و سپس وظایف حفاظتی معمول را طبق یک روال مشخص به انجام رسانید.

تا چه حد برای شما مشکل آفرین خواهد بود؟

میزان مشکلات به دیدگاه شما بستگی دارد . باید در مورد آنچه انجام می دهید آگاهی داشته باشید و هرگز نباید فکر کنید که هر چیزی در نوع خود واجد امنیت است . برای مثال اگر شخصی در نامهٔ الکترونیکی خود برای شما ضمیمه ای فرستاده باشد، باید در مورد بازکردن و یا باز نکردن آن تصمیم گیری کنید . این میزان احتیاط در زندگی روزمره نیز ضروری است . بعنوان مثال بسیار خوشایند خواهد بود اگر بتوانید هر زمان که بخواهید از خیابان عبور کنید؛ اما لازم است برای عبور از خیابان مراقب آمد و رفت ماشینها باشید.

آیا کارهایی وجود دارند که با اجرای طرح امنیتی،انجام آنها مشکل و یا غیر ممکن شود؟

بله؛ شما برای ایمن شدن باید عملکرد خود را تا حدودی تغییر دهید . انتخاب طرحی برای امنیت بیشتر، شما را به آگاهی بیشتر در برابر مشکلات بالقوه - که باید تا حد امکان از بروز آنها جلوگیری کنید - می رساند .بسته های نرم افزاری جدید قابلیتهای جذاب بسیاری دارند، اما استفاده از آنها- خصوصاً آ ندسته که برای گسترش شبکه و ارسال و دریافت پیام بکار می روند - باعث آسیب پذیری بیشتر در برابر حملات می گردند .بعنوان مثال ممکن است پایگاه وبی وجود داشته باشد که ارائه کنندهٔ خدمات مورد نظر شما باشد ولی برای دسترسی به آن لازم باشد که یک نرم افزار خاص آنرا download و بر روی رایانه خود اجرا کنید . اگر نسبت به اشخاصی که این خدمات را ارائه می دهند اعتماد کافی ندارید بهتر است از قابلیتهایی که آن برنامه می تواند برای شما به ارمغان بیاورد صرفنظر نمایید.

آیا می توانید به تنهایی طرح را اجرا کنید یا برای اجرای آن به کمک دیگران نیاز دارید؟

فرض بر این است که شما مسئول تمام ابعاد امنیتی سیستم خود هستید، اما در عمل شاید بهتر باشد که برای بهتر انجام شدن کار از دیگران نیز کمک بگیرید.

به روز سانی نرم افزارها و وصله های ارائه شده که بخش مهمی از فرآیند ایجاد امنیت است به پهنای باند شما بستگی دارد . مسلماً این مسئله برای کسی که به اینترنت متصل شده و سرعت ارتباط وی در حد مگابایت است مشکلساز نیست؛ ولی پهنای باند در کشورهای درحال توسعه به شدت محدود و بسیاری اوقات پرهزینه و گرانقیمت است و اتصال به اینترنت از طریق تلفن برای بازه های طولا نیمدت هم مقرون به صرفه نیست . به همین دلیل در چنین شرایطی بهتر است یکنفر نرم افزارهای معمول را به روز رسانی کرده و نسخه های download شده آنها را در اختیار متأسفانه انجام اینکار معمولا مشکلتر از download کردن مستقیم توسط هر کاربر است ؛ هشدارهای امنیتی به افراد حرفه ای در کار با رایانه کمک می کند . کاربران مبتدیمعمولاً نسبت به چنین هشدارهایی حساسیت زیادی ندارند و اگر یک کاربر هشداری دریافت کندمعمولاً قادر به فهم کامل آن و متعاقبًا بروز واکنش مناسب نخواهد بود . ۹ بعضی اوقات ممکن است شما یک هرزن امه مشک ل آفرین دریافت کنید که ادعا دارد یک به روزرسانی از مایکروسافت می باشد که شامل ضمیمه update ولی باید دقت داشته باشید کهمعمولاً ضمیمه های این نامه ها چیزی جز ویروسهای خطرناک نیستند؛ و در محیطهایی که تعداد زیادی رایانه یافت می شوند (مراکز کاری، مدارس، اداره های دولتی) لازم است که شخصی بعنوان راهبر سیستم جهت اعمال برخی از تدابیر امنیتی بکار گرفته شود.

اگر بخواهید کارهای مربوط به امنیت سیستمها را به دیگران نیز واگذار کنید باید از یک طرح تعامل مناسب استفاده نمایید .اطلاعات بیشتر در زمینهٔ ادارهٔ سیس تمها در بخشهای دیگر کتاب ارائه خواهد شد دقت داشته باشید که مشخص کردن مسئولیتها در فرآیندهای امنیتی تحت گروههای یک یا چند نفره بخش مهمی از هر طرح امنیتی است.

تصمیم گیری در مورد طرح امنیت فردی

برنامه های بسیاری وجود دارند که به نیازهای امنیتی رایانه ها میپردازند .اکنون که شما مفهوم خطرات را درک کرده و در رابطه با انواع خطراتی که باید کاهش یافته و یا از بین بروند تصمیمگیری کرده اید، قادر هستید یک طرح امنیت فردی را به اجرا در آورید .پس از ارزیابی قیمتها، زمان لازم و دردسرهای انجام کار ممکن است به این نتیجه ب رسید که مقابله با بعضی از خطرات حداقل در زمان حاضر ضروری نیست . طرح امنیتی شما به برنامه های نرمافزاری خاصی تکیه میکند اما کماکان باید فرآیند ها، قوانین، و ملاحظات شخصی را در بر بگیرد.

یک طرح امنیتی مناسب از لایه های چندگانه تشکیل شده و هر لایه انواع خاصی از خطرات را از بین می برد . چنانچه از لایههای مختلف استفاده کنید مسلماً در پیشگیری از مشکلات بیشتری موفق خواهید بود . عمل رانندگی را درنظر بیاورید .بنظر شما چه تدابیری می توان اندیشید که احتمال وقوع تصادف کاهش یابد؟

بعضی از ملاحظات مناسب در زیر آمده اند:

- چنانچه ماشین نیاز به تعمیر داشته باشد باید به درستی تعمیر شود.
- رانندگی باید با دقت انجام گیرد.
- چنانچه کارخانه نسبت به وجود عیبی در ماشین هشدار دهد که با سلامت افراد مرتبط باشد، آن عیب باید سریعًا رفع گردد.
- هنگام رانندگی باید احتیاط کرد، چراکه ممکن است ماشینهای دیگر برایتان مشکل بیافرینند.
- اگر در روزنامه هشدار داده شده که پلی شکسته است، باید از رانندگی بر روی آن پرهیز شود.

هیچکدام از عوامل بالا به تنهایی قادر به تضمین سلامت شما نخواهند بود، ولی با درنظر گرفتن همهٔ آنها می توان احتمال بروز تصادف را تا حد قابل توجهی کاهش داد . در تدوین اجزای یک طرح امنیتی،

افراد باید لایه هایی از حفاظت را بکار گیرند که ممکن است حتی تا حدودی تکراری باشند . برای درک بهتر تصور کنید که می خواهید از یک تکه جواهر قیمتی محافظت کنید . مسلماً آنرا در یک جعبهٔ سربسته و سپس در یک اتاق قفل شده قرارمی دهید؛ و جهت کسب اطمینان بیشتر، آنرا در برابر سرقت نیز بیمه خواهید نمود . در این مثال عمل محافظت در چندین مرحله انجام گرفته است . هرکدام از این مراحل به تنهایی ضریب حفاظت از جواهر را کمی بالا می برند، ولی مسلماً بکارگیری تمام مراحل عاقلانه تر است، چراکه اگر در یک مرحله با شکست مواجه شوید مراحل دیگر در رسیدن شما به موفقیت کمک خواهد کرد(مثلاًاگر شخصی غیرقابل اعتماد در خانه باشد،

مسلماً قفل کردن در، راه مناسبی نیست. نکتهٔ قابل توجه این است که بعضی مواقع احتمال دارد فنون امنیتی نیز با شکست مواجه شوند . این امر ممکن است ناشی از مشکلات طراحی، پیاده سازی ضعیف و یا خطاهای انسانی باشد .این مسئله می تواند در مورد مشکلات ابزارهایی مثل ویروس یابها، رمزگذاری و رمزهای عبور صدق کند . بنابراین چون امکان شکست برای هرکدام از ابزارها در هر زمانی وجود دارد نباید تنها بر یک شیوه تکیه نمود.

نقش کاربر در امنیت

اولین کاربر که از رایانه استفاده می کند نقش مهمی در تضمین ایمنی رایانه و نرم افزارهای آن دارد . درمجموع کاربران دیگر نیز در تضمین دقت در عملیات حفاظت و ایمنی نقش بسزایی دارند . دقت داشته باشید کاربرانی که نسبت به امنیت رای انه اطلاعات کافی ندارند خود از بزرگترین خطرات امنیت رایانه ای بشمار می روند.

امنیت یک هنر است، نه یک علم

در ایمن سازی رایانه ها و شبکه ها هیچ تضمین صد درصدی وجود ندارد، چراکه همیشه نقایص تازه و راههای جدید نفوذ و فرصتهای نو برای ایجاد مشکل - که خود ناشی ا ز خطاهای انسانی است - وجود

خواهد داشت . اما اگر مطالعهٔ دقیقی انجام بگیرد و از تجارب موفق امنیتی استفاده شود می توان در عملکرد سیستم امنیت لازم را بوجود آورد.

پایگاههای وب و گروههای پستی سازمانهای حفاظت از رایانه نیز می توانند کمکهای شایانی در این زمینه باش ند، چراکه می توان در شرایط غیر معمول و بروز وضعیت غیرعادی از راهنمایی های آنها بهره گرفت.

بخش دوم امنیت فناوری اطلاعات و کاربران منفرد

فصل سوم : امنیت رایانه و داده

کلیات

مقدمه

امنیت فیزیکی

سرقت رایانه

قانون اول

رایانه ها آسیب پذیرند

جنبه های دیگر امنیت فیزیکی

برای محافظت از داده های خود نسخه های پشتیبان تهیه نمایید

قانون دوم

خطای کاربر

نقص در سخت افزار

نقص در نرم افزار

نفوذها و تخریبهای الکترونیکی

اطلاعات بایگانی

از چه چیزهایی باید پشتیبان تهیه کرد؟

تصدیق هویت

شناسایی کاربر

رمز عبور

قانون سوم

امتیازات را محدود کنید

فصل سوم

امنیت رایانه و داده ها

کلیات

در این فصل به بررسی راههایی می پردازیم که از طریق آنها می توان رایانه را از لحاظ فیزیکی ایمن کرد و از سرقت داده ها و برنامه هایرایانه ای جلوگیری نمود . مباحث عمدهٔ این فصل عبارتند از : امنیت فیزیکی، نسخه های پشتیبان، و تصدیق هویت با استفاده از نام کاربری و رمز عبور.

مقدمه

یکی از بهترین شیوه های درک مفهوم امنیت اطلاعات استفاده از یک راهکار ضابطه مند است . با شروع از معرفی امنیت فیزیکی در این فصل، در سایر فصول بخش دوم به بررسی جوانب دیگر امنیت خواهیم پرداخت و اساس استقرار فرآیند های امنیتی برای رایانه های شخصی و گروه های کوچک رایانه ای را توضیح خواهیم داد . اطلاعات مربوط به جنبه های فنی امنیت برای سازمانهای بزرگتر و کاربران حرفه ای در بخش پنجم ارائه شده است .هنگامیکه با اطلاعات ارائه شده در این فصل با کلیات موضوع آشنا شدید، می توانید با استفاده از مطالب ارائه شده در بخش پنجم (امنیت فناوری اطلاعات و راهبران فنی) بر دانش فنی خود بیافزایید.

امنیت فیزیکی

اولین مرحله این است که اطمینان حاصل کنید رایانهٔ 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 خصوصاًرایانه های کیفی به سادگی دزدیده می شوند و بسیار سخت پیدا می شوند .چنانچه سارق مایل به استفادهٔ شخصی از رایانه نباشد مراکز بسیار زیادی وجود دارند که رایانه های دزدی و دست دوم را خریداری می کنند . برخی از سارقان، رایانه و نمایشگر آنرا بطور کا مل 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 هزینهٔ گزافی را بر شما تحمیل خواهد کرد . در بعضی مواقع سرقت اطلاعات باعث افشای امور شغلی و یا اسرار محرمانهٔ اشخاص می گردد و در شرایط بدتر، سرقت رایانه باعث از دست دادن شغل می شود .با اینحال چن انچه در این خصوص چند روش ساده و ارزان قیمت بکار گرفته شود می توان 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 برای 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 ک ار خود با همکاران دیگری کار می کنید رایانه را در معرض دید آنان قرار دهید رایانه خود را در محافل عمومی مانند فرودگاهها 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، رایانهٔ خود را بوسیلهٔ کابل سیمی و یا زنجیر به میله، لوله یا اشیایی که قابلیت جابجایی ندارند متصل کنید . از این روش در محافل نسبتًا عمومی مثل مدارس و یا کتابخانه ها استفاده می شود. اکثر رایانه ها دارای محلی م خصوص اتصال می باشند. رایانه های کیفی نیز برای اینکارمعمولاً 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 رایانهٔ شما وجود دارد، لازم است زمانی که آنرا بدون مراقبت قرار داده و یا از آن دور هستید (مثلاًاگر از هتل خارج می شوید و رایانه در اتاق است) امکان دسترسی منطقی به آنرا تا حد ممکن کاهش دهید .دسترسی منطقی به معنای استفادهٔ 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 رمزهای عبور گزینههای مناسبی برای شروع این نوع از حفاظت هستند(برای اطلاعات بیشتر به بحث مربوط به مجوز ورود در همین فصل رجوع کنید)
- رایانه های کیفی و PDA ها کوچک می باشند و به همین دلیل دزدیدن آنها آسان است . چنانچه از آنها استفادهٔ زیادی نمی کنید حتمًا 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 اینکه سارقان تمایلی به دزدیدن رایانه نداشته باشند این است که مشخصات خود را با علائم ثابت و ماندگار که نمی توان آنها را از بین برد بر بدنۀ 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 میتواند 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 آنجا وجود دارد مرتباً باید با دقت زیاد آنرا تمیز کرد تا شکاف تهویه مسدود نشود . برخی رایانه ها همچنین نسبت به ف رورفتگیها و برآمدگیهای سطحی که روی آن قرار دارند نیز حساس میباشند.

جنبه های دیگر امنیت فیزیکی

چنانچه شما برای نصب یک قطعه سخت افزاری بدنۀ رایانه خود را باز کرده اید باید به اخطارهایی که دربارۀ شوکهای الکترواستاتیک داده شده توجه کنید (شوک الکترواستاتیک باع ث صدمهدیدن سخت افزار می شود و باید از وقوع آن جلوگیری کرد) .ضمنًا 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 بوسیلۀ آنها میتوان اطمینان حاصل کرد که داده ها و برنامه ها از حفاظت کامل برخوردارند . شما چگونه از داده ها و برنامه های رایانۀ خود حفاظت 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؛
- ذخیرۀ ناخواسته یک فایل بر روی فایل دیگر؛ روند نادرست به اجرا در آمدن یک برنامه بگونه ای که باعث تغییر یا پاک شدن داد ها شود؛ وجود یک برنامۀ مخرب (مثل ویروس) که باعث تغییر، بازنویسی و یا حذف داد ها شود؛بروز مشکل در سخت افزار(مثل مشکلات دیسک سخت دیسکگردان، پردازشگر و یا منبع تغذیه)بگونهای که باعثاز بین رفتن داد ها گردد؛
- آتش سوزی و استفاده از آب برای خاموش کردن رایانۀ سوخته، که باعث غیرقابل بازیابی شدن داده ها می شود؛

یکی از راه حلها برای مقابله با این تهدیدات، تهیۀ 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 فشرده 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 بکار گیرید.

نسخه های پشتیبان می توانند 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 دارید به روی نوارهای مغناطیسی و یا مجموعه ای از دیسکهای فشرده ۱۹ کپی کنید . چنانچه رایانهٔ شما دزدیده شود، با خر ید یک رایانهٔ جدید با ساختاری مشابه رایانهٔ قدیمی و با استفاده از نسخه های پشتیبان قادر خواهید بود فایلهای 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 بروز بعضی از مشکلات جلوگیری نمود، ولی اگر پشتیبان مناسب تهیه کرده باشید حداقل داده های خود را از دست نمی دهید و در اکثر مواقع می توانید سیستم خود را بازیابی کرده و به یک حالت متعادل و ماندگار برسانید .حتی درصورتیکه داده های رایانه تماماً از دست رفته باشد، چنانچه یک مجموعهٔ کامل از نسخه های پشتیبان در اختیار داشته باشید قادر خواهید بود همهٔ اطلاعات را روی رایانهٔ جدید بازیابی کنید و مجدداً به آنها دسترسی داشته باشید .البته این مسئله صرفًا زمانی کارآمد است که نسخه های پشتیبان در جایی غیر از رایانهٔ قربان ی ذخیره شده باشند.

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

خطای کاربر

بعضی از افراد برخی مواقع بطور ناخواسته فایلهای خود را پاک می کنند . در استفاده از واسطه ی گرافیکی کاربر این امکان وجود دارد که یک فایل یا شاخه بطور ناخواسته به مکانی نادرست منتقل شود . اما چنانچه مرتباً از فایل ها پشتیبان تهیه شده باشد امکان بازیابی فایل هایی 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 فرآیند گردد .صدمه هایی که به دیسک وارد می شود نیز می تواند منجر به تخریب کامل دیسک شود ولی چنانچه از فایلهای 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 Excelو Microsoft Word و Access می توانند باعث از بین رفتن ناخواستهٔ فایلهای داده شوند . اگر نسخهٔ پشتیبان داشته باشید و برنامهٔ کاربردی شما ناگه ان نیمی از اطلاعات حیاتی فایل کاری شما را پاک کند، باز هم قادر خواهید بود داده های خود را بازیابی نمایید.

نفوذها و تخریبهای الکترونیکی

مهاجمین و ویروسهای 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 مقایسهٔ نرم افزارها و داده های رایج با نرم افزارها و داده های قدیمی را بوجود می آورند .این قابلیت باعث می شود بتوانید مشخص کنید که چه چیزهایی عمداً یا سهواً دچار تغییر شده اند . برای این منظور اگر نخواهید به عقب برگشته و تاریخچهٔ 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، تهیهٔ نسخه های پشتیبان و ذخیرهٔ آنها در محلی خارج از رایانه و در مکانی امن کمک شایانی خواهد بود، چراکه موارد بسیاری وجود داشته که پشتیبانها نیز به همراه رایانه به سرقت برده شد هاند.

بلایای طبیعی

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

بلایای دیگر

بعضی مواقع نشت لوله های گاز و متعاقبا 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 . نکتهٔ قابل توجه این است که پشتیبان بکاررفته در هرکدام از شرایط فوق ممکن است برای شرایط دیگر کاربردی نداشته باشد . به خاطر داشته باشید که استفاده از حفاظت چندلایه و بکارگیری سیستمهای گوناگون تهیهٔ پشتیبان جهت ایجاد ایمنی در برابر خطراتی که در اداره و یا منزل با آن مواجه هستید، مؤثرترین راه است.

ذیلاً چند مورد از شیو ههای تهیهٔ 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 صرفًا اگر تعدادی از فایلها بطور ناخواسته پاک شوند بکار می آید.

هر از چندگاه 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 رایانهٔ دیگری منتقل کنید.

اگر درنظر دارید که در مقابل خرابی دیسکهای سخت از ایمنی زیادی برخوردار باشید در رایانهٔ 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 بازهم تهیهٔ 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:

1 - از تمام فایلهایی که اختصاصی رایانهٔ شما است – البته غیر از برنامه های کاربردی - پشتیبان ته یه 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.

2 - از همه چیز پشتیبان تهی ه کنید . با تهیهٔ پشتیبان از تمام سیستم بسته به نوع استفاده ای که از آن می شود - می توان کل سیستم را درصورت لزوم بازیابی کرد . همچنین قادر خواهید بود فایلها و یا شاخههای خاص را بازیابی نمایید.

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

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

2 - 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 در فاصله های کوتاه فقط از فایلهایی پشتیبان گیری کنید که دچار تغییر شده اند .به این نوع پشتیبان گیری پشتیبانگیری افزایشی می گویند .توجه داشته باشید که برای بازیابی فایلها در این نوع پشتیبانگیری، هم به آخرین نسخهٔ پشتیبان کامل و هم به آخرین نسخهٔ پشتیبان افزایشی نیاز خواهید داشت. گونه های دیگری از پشتیبان گیری نیز وجود دارد. معمولاً برنامههای پشتیبان گیر در مورد چگونگی تهیه پشتیبان پیشنهاداتی به کاربر ارائه میکنند.

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 د ر 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 تهیهٔ پشتیبان فقط

برای بازیابی داده های پاک شده یا تغییر کرده صورت می پذیرد، باید محل آن طوری انتخا ب 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 در محلهای امن تر بگذارید .بعضی افراد از پشتیبانها دو نسخه تهیه می کنند و یک نسخه را در دسترس و دیگری را دور از دسترس قرار می دهند.

اگر در رایانهٔ خود داده هایی دارید که سارقان قصد سرقت آنها را دارند باید همیشه به یاد داشته باشید که آنها با سرقت نسخهٔ پشتیبان نیز قادر خواهند بود همان دا ده 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:

نسخهٔ مربوطه بسیار کهنه و یا از لحاظ فیزیکی صدمه دیده باشد . بروز این مشکل در دیسکهای فلاپی ورسانههای مغناطیسی بیش از همه به چشم می خورد.

دستگاهی که پشتیبان بوسیلهٔ آن نوشته شده دارای اشکال بوده و به همین دلیل دادهٔ نوشته شده در پشتیبان قابل خواندن نباشد . در این موارد امکان دارد بتوان ب ا یک دستگاه مشابه دیگر، پشتیبان مورد نظر را خواند.

رسانهای که پشتیبان روی آن قرار داده شده 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 ن می 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 نوشتهشدن اطلاعات روی آنها غیرقابل خواندن شوند.

خواندن نسخه های پشتیبان با دستگاهی غیر از آن که نسخهٔ پشتیبان با آن تهیه شده کنترل مناسبی برای کسب اطمینان از صحت رسانهٔ حاوی نسخه پشتیبان است . دقت داشته باشید که اگر برای نوشتن پشتیبان از دیسکهای مغناطیسی با و Zip قابلیت پاک کردن استفاده می کنید (مثل دیسکهای 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 و تصاویر و برنامه ها تهیه شده استفاده کنند؟ اگر درنظر 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 در سال ۱۹۸۰ رایج بوده ذخیره شده باشد آیا امروز می توان رایانه ای با دیسک گردان پنج اینچی برای بازیابی آن پیدا کرد؟

چند نسخهٔ پشتیبان باید نگهداری شود؟

اگر شما هفته ای یکبار از آنچه دارید پشتیبان تهیه کنید درصورت مواجهه با یک فاجعهٔ مصیبت بار، حداکثر اطلاعات یک هفته را از دست خواهید داد . انجام اینکار از دیدگاه امنیتی قابل توجیه است ولی در طول زمان فضای اشغال شده بوسیلهٔ پشتیبانها بیشتر و بی شتر می شود . چه تعداد از این پشتیبانها را باید 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 و قابلیت استفادهٔ مجدد هم ندارند؛ اما همواره باید چند نسخه از پشتیبانها ر ا نگهدارید . در تمام مثالهای بالا می توان از چهار نسخهٔ آخر نگهداری کرد.

چرا بهتر است اینگونه عمل شود؟ چرا باید نسخهٔ مربوط به ماه قبل را در شرایطی که نسخهٔ جدیدتری وجود دارد نگهداری کرد؟ دلیل آن ساده است : ممکن است نسخهٔ آخری که ایجاد کرده اید قابل خواندن

نباشد ، گم شود، و یا به سرقت رود . در اینصورت واضح است که اگرچه نسخه های ماههای قبلی کاملاً به روز نیستند، ولی بودنشان بهتر از نبودنشان است . این مورد یک مثال دیگر از این نکته است که ایمنی سطح بالا از معیارهای چندگانه و تا حدودی تکرارشده تشکیل میشود.

از نرم افزار خریداریشده پشتیبان تهیه کنید

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

مهمترین نکته در مورد نسخه های پشتیبان

مهمترین نکت ه در مورد نسخه های پشتیبان این است که تهیۀ پشتیبان باید در فواصل زمانی منظم صورت بگیرد. بعضی اشخاص زحمت تهیۀ پشتیبان را به خود نمی دهند و ممکن است به عواقب اینکار خود گرفتار شوند . این افرادعموماًوقتی هم که با مشکلی روبرو می شوند تصور می کنند مشکل دیگر تک رار نخواهد شد . همچنان توصیۀ ما این است که از مخاطرۀ احتمالی پیشگیری کنید و نسخۀ 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 ن ام کاربری و رمز عبور شناسایی می شوید، هرچند گونه های مختلفی از این سیستمهای شناسایی وجود دارد . نکتۀ قابل توجه این است که باید کلماتی بعنوان رمز عبور بکار گرفته شوند که نتوان آنها را براحتی حدس زد تا مهاجمان نتوانند آنها را پیدا کنند. در عین حال باید یادآور ی آن کلمات در حافظه نیز امکانپذیر باشد و شخص آنها را فراموش نکند . اگر شما مرتباً با رایانه و پایگاه وب در تماس باشید قاعدتًا تا کنون نامهای کاربری و رمزهای عبور زیادی به

خاطر سپرده اید، اما اگر آنها را بر روی یک کاغذ نزدیک رایانه نوشته اید باید بدانید که از امنیت زیادی برخوردار نیستند .

شناسایی کاربر

اکثر سیستمها برای شناسایی افراد از آنها می خواهند که بگونه ای هویت خود را احراز کنند . این مسئله می تواند با دریافت اطلاعات مختلفی انجام شود : نام کاربری، شمارهٔ عضویت، اسم عضو و... ؛ که در 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 سیستمها طول اسم را محدود می کنند ولی بعضی دیگر برای آن محدودیتی قائل نمی شوند.
- در بعضی از سیستمها می توان از هر علامتی – که بوسیلهٔ صفحه کلید قابل نوشتن باشد - در ترکیب نام کاربری استفاده کرد، ولی بعضی دیگر فقط در محدودهٔ حروف و اعداد و فقط اندکی در محدودهٔ علائم کار می کنند.
- بعضی سیستمها حروف بزرگ و کوچک را یکسان درنظر می گیرند ولی بعضی دیگر با آنها به منزلهٔ دو حرف متفاوت برخورد میکنند.

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

- آیا درنظر دارید نام کاربری نشاندهندهٔ هویت واقعی شما باشد؟ آیا قرار است این اسم کمک کند که دوستان و همکارانتان شما را بشناسند؟ یک آدرس پست الکترونیکیمعمولاً بعنوان یک چنین نماد ی از کاربر تلقی می شود.

- آیا می خواهید با انتخاب نام مورد نظر هویت واقعی خود را پنهان نگه دارید؟ اگر بوسیلهٔ این نام کاربری در یک فعالیت گروهی شرکت می کنید (مثلاًیک 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 برخطا استفاده کنید که به ندرت آنرا بکار می گیرید ممکن است مایل باشید از اسمی استفاده کنید که براحتی در ذهن بماند . بعضی افراد برای خدمات مختلف از یک نام کاربری استفاده میکنند، خصوصاًاگر آن خدمات با نکتهٔ 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 چندلایه استفاده کرد . اگر از آدرس پست ا لکترونیک 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 شوندمعمولاً لا رمزگذاری می شوند تا اگر کسی به دیسک دسترسی پیدا کرد قادر به مشاهدهٔ رمزهای عبور نباشد . در بعضی موارد این رمزگذاری بگونه ای است که امکان رمزگشایی رمزهای عبور وجود ندارد که به آن رمزگذاری یکسویه می گویند .در این سیستمها وقتی برای ورود به سیستم رمز عبور را وارد می کنید، ابتدا رمزگذاری می شود و سپس با نسخهٔ ذخیره شده در دیسک مقایسه می گردد .

قانون سوم:

از رمز عبور ی 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 رمزگذارِ ی 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 همۀ کلمات درون فرهنگ لغات و س ایر رمزهای عبور متداول استفاده کند .لذا مثلاًاگر شما کلمه birthday بعنوان رمز عبور استفاده کرده باشید مهاجم هنگام رمزگذاری کلمۀ birthday متوجه می شود . نسخۀ رمزگذاری شده آن با آنچه که روی دیسک استمطابقت دارد و لذا از آن پس رمز عبور شما را خواهد دانست.

از آنجا که کل ایدۀ استفاده از رمزهای عبور برای صدور اجازۀ 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 رمزعبور درنظر گرفته اند (حداقل و حداکثر طول، حروف مجاز برای استفاده، و سایر موارد)

- هرگز از یک کلمۀ 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 هم حروف بزرگ و هم حروف کوچک را در رمزهای عبور بعنوان حروف مجاز قلمداد می کند، از هر دوی آنها استفاده کنید - ولی نه در جای صحیح و قابل پیشبینی خود.
- درصورت امکان از اعداد ترکیبی، علامتهای مجاز و همچنین فضاهای خالی استفاده کنید.

- اگر سیستم اجازه می دهد که از فضای خالی استف اده کنید یا رمز عبور شما به شکل یک عبارت است می توانید در 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 اینکار 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 نیاز به حفاظت خا صی 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.

درواقع آنها فقط می خواهند شما به سیستم آنها وارد شوید؛ بنابر این می توانید برای خواندن مطالب روزنامههای مختلف از یک رمز عبور مشابه استفاده نمایید.

بعضی افراد حروف را با علائم یا ارقام مشابه عوض می کنند؛ مثلاً از رقم 1 بجای حروف l یا L از شماره 3 به جای علامت # به جای حرف E از رقم 0 به جای حرف O علامت @ 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.

- از سرنام ها (حروف اول لغتهای سازنده یک عبارت) استفاده نمایید .بعنوان مثال tgwbc سرنامی برا ی شعار معروف کوکاکولا("Things Go Better With Coke") می باشد.
- هجی کردن لغات بصورت برعکس آنها را کمی مبهم می کند، اما شناساییشان را سخت نمی نماید

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 و والدین؛

اسامی دوستان، رؤسا و یا همکاران؛

اسامی حیوانات خانگی؛

روز تولد خود یا هریک از دوستان و خویشاوندان؛

شمارهٔ تلفن، شمارهٔ گواهینامه یا مدارک مشابه؛

رنگ مورد علاقه؛

مقام یا عنوان شغلی؛

نام سازمانی که در آن کار میکنید؛

هر چیز دیگری که با آن شناخته می شوید .

در بعضی سیستمها تعداد حروف رمز عبور باید از مقدار معینی بیشتر باشد و یا تعداد مشخصی از حروف و ارقام به اتفاق هم را در 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 هرچه که باشد باید بد ون نوشتن آنرا بخاطر بسپارید .هرگز رمز عبور را جایی ننویسید و آنرا در محل کار یا روی برچسبهای عناوین قرار ندهید.

هرگز فهرست رمزگذاری نشدهٔ رمزهای عبور را در 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 میباشد .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 قائل می شوند ذیلاً ارائه شدهاند . این رمزها بسادگی به خاطر سپرده می شوند، اما یافتن آنها در فرهنگهای لغات و یا حدس زدنشان بسیار دشوار میباشد.

رمز عبور خود را تغییر دهید

- رمزهای عبور باید بصورت متناوب تغییر 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 سا ده انتخاب شوند و یا برای جلوگیری از فراموش شدن در جایی نوشته شوند .برای کاربردهای معمولی نکات زیر توصیه می شوند:
- اگر فکر می کنید رمز عبورتان در معرض سرقت بوده سریعًا 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 واقعًا چاره ای جز آن وجود نداشته باشد.
- رمزهای عبور را بصورت متناوب عوض کنید . معنی کلمهٔ" متناوب "از دیدگاه افراد مختلف، متفاوت است. شاید دوره هایی بین ۶ ماه تا یکسال به نظر مناس ب 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 کلیهٔ کارهای خود را با استفاده از امتیاز دسترسی کامل انجام می دهد؛ درحالیکه بهتر است برای فعالیتهای غیرراهبری از یک نام کاربری مجزا استفاده کند . اینکار احتمال خراب شدن ناخواستهٔ سیستم را کاهش می دهد و درصورت نفوذ مهاجم نیز از آسیب وارده به سیستم تا حد قابل توجهی میکاهد.

بخش دوم امنیت فناوری اطلاعات و کاربران منفرد

فصل چهارم : امنیت سیستم عامل و نرم افزارهای کاربردی

کلیات

مقدمه

نرم افزارهای تجاری

مشکل کشورهای درحال توسعه

آیا بسته های به روزرسانی را باید پس از انتشار، سریعًا نصب نمود؟

پیشنهاد عملی

نرم افزارهای غیرسنتی و غیرتجاری

نرم افزارهای تجاری کوچک

نرم افزارهای متن باز

نرم افزارهای مسروقه

فصل چهارم

امنیت سیستم عامل و نرم افزارهای کاربردی

کلیات

در این فصل به بررسی فنونی می پردازیم که از آنها برای کاهش آسیب پذیری سیستم عامل و نرم افزارهای کاربردی در برابر نفوذهای امنیتی استفاده می شود.

مقدمه

اصل اول : رایانه ها برنام ههها را اجرا می کنند.

اصل دوم : برنامه ها اشکال دارند.

اصل اول بدیهی است؛ و اصل دوم نیز با توجه به اینکه برنامه نویسان افراد بدون نقص نیستند کاملاً مورد انتظار است .معلوم نیست چرا این حجم زیاد از مسائل امنیتی مربوط به اشکالات برنامه نویسی هستند هنگام توسعه برنامه براحتی می توان از بروز اشکالاتی نظیر سرریز شدن بافر جلوگیری کرد ، اما با این وجود بنظر می رسد تقریباً نیمی از مشکلات جدی امنیتی از این دسته اند.

نرم افزارهای تجاری

یک نرم افزار تجاری معمولاً چگونه کار می کند؟

چند سال قبل هنگامیکه یک نرم افزار را می خریدید، تا زمان عرضهٔ نسخهٔ جدید آن به بازار هیچ به روزرسانی در آن اعمال نمی شد . امروزه بدلایل مختلف بخصوص به دلیل مسائل امنیتی بیشتر نرم افزارها بصورت منظم به روزرسانی می شوند .برای برخی از نرم افزارها مثل سیستم عاملها، « به روزرسانی منظم» به معنی انجام اینکار بصورت روزانه است . به روزرسانی اغلب محصولات معمولاً 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 روزرسانی های آنرا نیز ارائه می کنند .برای دریافت خدمات به روز سانی فروشندگان بزرگ معمولاً می توانید به پایگاه وب آنها مراجعه کنید و از قسمت suooort یا download اصلاحات ارائه شده برای محصولات را بیابید .

وقتی به پایگاه وب فروشندۀ نرم افزار مراجعه می کنید بسته های نرم افزاری و نسخه های مورد استفادۀ خود را تعیین می نمایید و سپس پایگاه وب فهرستی از به روزرسانی های قابل دریافت را ارائه خواهد کرد . در برخی از موارد کاملاً مشخص است که به روزرسانی 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 مرحلۀ بعد آنها را نصب می نمایید .با توجه به نوع نرم افزار امکان دارد برنامه ای که download کرده اید بسادگی و در یک مرحله اجرا شود و یا اینکه برای نصب شدن نیازمند اجرای دستورالعمل های خاصی باشد . در برخی موارد بستۀ نرم افزاری به روزرسانی بعد از download شدن تقریباً بصورت خودکار نصب می گردد

در سالهای اخیرمعمولاً از سه روش عمده برای ارائه خدمات به روزرسانی استفاده شده است:

۱ .برای برنامه هایی نظیر ،Microsoft Windows شرکت مایکروسافت بسته های به روزرسانی را از طریق پایگاه وب Windows Update منتشر می کند. یک برنامۀ نرم افزاری رایانۀ شما را بررسی کرده و فهرستی از به روز رسانی های مورد نیاز سیستم را ارائه مینماید، و آنگاه شما می توانید آنها را انتخاب، download و نصب کنید.

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

۳ .برخی از برنامه ها دارای توابع از پیش تعریف شده ای هستند که بصورت پویا به بررسی به روزرسانی های ارائه شده می پردازند و با اجازهٔ کاربر آنها را download و نصب مینمایند.

این قابلیتها برای آسانتر شدن کار شما طراحی شده اند . در کلیهٔ موارد وظیفهٔ انتخاب دقیق بسته های به روزرسانی مورد نیاز (که برای سیستم عامل و نرم افزارهای کاربردی خاص، کار پیچیده ای است) بوسیلهٔ برنام ههٔا و بصورت خودکار انجام میشود.

مشکل کشورهای درحال توسعه

همانطور که مشاهده می کنید بسیاری از فرآیندهای به روزرسانی برای اجرا در محیط متصل به اینترنت طراحی شده اند و بسته های به روزرسانی 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 . امامعمولاً در کشو ر های درحال توسعه این امکان وجود ندارد.

دو روش برای مقابله با این مشکل موجود است:

۱ .از خیر به روزرسانی نرم افزار های کاربردی و سیستم عامل خود بگذرید.

۲ .از فرد دیگری بخواهید بستهٔ به روزرسانی را download کند و جزئیات دستورالعمل نصب را ارائه دهد .در اینصورت بستهٔ به روز رسانی میتواند از طریق دیسکهای فشرده یا شبکهٔ محلی توزیع شود.

در شرایطی که احتمال خطرات امنیتی درحال افزایش است راه اول منطقی بنظر نمی رسد .بنابراین تنها گزینهٔ مناسب download کردن و به اشتراک گذاشتن وصله ها و اصلاحهای download شده است.

چند راه برای انجام اینکار وجود دارد:

- اگر سازمانی دارای ماشینهای متعدد باشد، راهبر فنی باید مسئولیت download و نصب بسته های به روزرسانی آنرا بر عهده گیرد.

- کلوپهای رایانه ای یا گروههای دیگر می توانند بسته های به روزرسانی را download کنند و آنها را در اختیار اعضا قرار دهند. .
- ارائه کنندگان خدمات اینترنتی می توانند بسته های به روزرسانی محصولات رایج و سیستم عاملهای مشترک را تهیه و بصورت محلی میان کاربران خود توزیع کنند . با اینکار نیازمندی ISP ها به پهنای باند بین المللی کم می شود و لذا هزینهٔ آنها نیز کاهش می یابد. فروشگاههای رایانه ای می توانند بسته های به روزرسانی 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 روزرسانی بر روی دیسکهای فشرده اقدام کرد. استفاده از این روش همچنان هم میتواند ادامه یابد.

هرچند سه شیوهٔ اخیر توزیع بسته های به روزرسانی چندان رایج نیستند، اما با توجه به افزایش نیاز برای به روز نگهداشتن نرم افزار ها می توانند به یک استراتژی مؤثر تجاری برای ISP ها و فروشندگان در کشورهای درحال توسعه تبدیل شوند .اگرچه از این استراتژیهای پشتیبانی استقبال می شود، اما کاربران باید مطمئن شوند که منابع به روزرسانی 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 روزرسانی را باید پس از انتشار، سریعاً نصب نمود؟

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

موافقان : اگر سریعًا بسته های به روزرسانی را نصب کنید، خود را در مقابل آسیبهای شناخته شده ایمن کرده اید . با استفاده از ایمنی حاصل از بست ه های به روزرسانی، 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 روزرسانی به اندازهٔ برنامه های اصل ی اشکال و آسیب

پذیری وجود داشته باشد . لذا این احتمال وجود دارد که بستهٔ به روزرسانی مشکلات جدیدی را بوجود بیاورد که به مشکل قبلی ارتباطی نداشته باشد.

انتشار هر از چندگاه نقایص امنیتی کشف شده که با استفاده از آنها مهاجمان به سیستم نفوذ کرده و داده ها را تخری ب می کنند دامنهٔ این مسئله را تغییر داده اس ت . هنگامیکه یک نقص امنیتی اعلام می شود . حتی اگر این اعلام توسط یک وصلهٔ امنیتی صورت پذیرد - مهاجمان سریعًا ابزارهایی برای سوء استفاده از آن نقص را بوجود می آورند، و درنتیجه ممکن است سیستم رایانهٔ افرادی که از وصله های امنیتی منتشرشده استفاده نمی کنند سریعًا مورد تهاجم قرار گیرد.

پیشنهاد عملی:

- کاربران مبتدی و افرادی که رایانه هایشان برای کارهای غیرحساس استفاده می شود باید کلیهٔ بسته های به روزرسانی را بلافاصله بعد از انتشار بکار گیرند . برای رایانه ای که به روزرسانی نشده، خطر مشکلات جدید حاصل از بسته های به روزرسانی به مراتب کمتر از خطرات آسیب پذیریهای به روزرسانی نشده است
- کاربران حرفه ای و کارکنان بخش فنی باید بسته های به روزرسانی امنیتی را سریعاً نصب کنند، اما می توانند بقیهٔ بسته های به روزرسانی را با توجه به نوع عملکرد آنها اولویت بندی نمایند . تأخیر چند هفته ای یا چند ماهه در نصب این بسته ها به کاربران ماجراجو اجازه می دهد بسته های به روزرسانی را نصب کنند، مشکلات احتمالی را کشف و گزارش نمایند، و با اینکار پیش از اینکه شما به روز رسانی ها را نصب کرده باشید به تولیدکننده فرصت اصلاح نقایص جدید را بدهند.

هرگز نمی توان گفت که تغییرات چه زمانی می توانند یک نرم افزار کاربردی را از روند صحیح اجرا خارج کنند . به همین دلیل اگر از رایانهٔ شما در فعالیتهای حساس تجاری استفاده می شود، بهترین راهکار این است که پیش از اعمال به روز رسانی های جدید، ابتدا تغییرات را روی یک دستگاه مشابه و نه چندان حیاتی آزمایش کنید.

نرم افزارهای غیرسنتی و غیرتجاری

در بحث قبل بر محصولات تجاری شامل سیستم عاملها و برنامه های کاربردی عمده متمرکز شدیم که در بسیاری از محیط های محاسباتی مرسوم هستند . اما در ن رم افزارهای دیگر شرایط چه تغییراتی می کنند؟

نرم افزارهای تجاری کوچک

نرم افزارهای زیادی وجود دارند که بصورت رایگان یا با حداقل هزینه در اختیار عموم قرار می گیرند . سطح پشتیبانی فروشندگان این نرم افزارها تفاوتهای بسیاری دارد . بطور کلی استفادۀ متناوب از بسته های به روزرسانی رایگان و یا کم هزینه کاملاً توصیه می شود .این برنامه ها معمولاً ضعفهای امنیتی ندارند، بلکه برای حل مشکلات غیرامنیتی و یا افزودن قابلیتهای جدید طراحی شده اند .با اینحال برخی از نرم افزارهای رایگان نظیر دیوارۀ آتش و یا ویروس یاب در حیطۀ برر سی ما هستند و در این کتاب در مورد آنها بحث خواهد شد.

اگر از برنامه هایی استفاده می کنید که دارای کارکردهای امنیتی هستند، اطمینان حاصل کنید که سیاست فروشنده در ارائه به روزرسانی را درک کرده اید . مسلماً نمی خواهید در موقعیتی قرار بگیرید که از یک نرم افزار حس اس به امنیت استفاده کنید و ناگهان خدمات پشتیبانی ارائه به روز رسانیآن قطع شود و یا توانایی خرید آنرا نداشته باشید . استفاده از برخی نرم افزارها مانند ویروس یابها اگر بطور منظم (روزانه یا هفتگی) به روزرسانی نشوند، می تواند بسیار خطرناکتر از حالتی باشد که از آنها استفاده نمی شود؛ زیرا اگر از آن استفاده نمایید تصور میکنید از شرایط امنیتی مناسبی برخوردارید.

نرم افزارهای متن باز

نرم افزارهای متن بازی که بسرعت درحال گسترش هستند باید بصورت مناسبی مورد پشتیبانی قرار داشته باشند . در برخی موارد با اینکه نرم افزار اصلی بصورت رایگان عرضه می شود اما امکان دارد خدمات ارائه به روزرسانی یا پشتیبانی آن هزینه بر باشد .نسخۀ رایگان Red Hat Linux که در دسترس عموم قرار می گیرد نمونۀ خوبی از این قبیل نرم افزارها است . سازمانهایی که خواهان سطح بیشتری از پشتیبانی

فنی هستند ممکن است بستهٔ 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 افزارهای آزاد و متن باز) توجه داشته باشید که مدت زمان در دسترس بودن نسخه های اصلاحی آنها ممکن است کوتاه باشد . بنابراین اگر سیستم عامل یا زیرسیستم های مهم خود را از نوع نرم افزارهای بدون پشتیبانی انتخاب کرده اید باید نسخهٔ جدید آنرا هر چند وقت یکبار (مثلاً در هر شش ماه) به روزرسانی کنید روند به روزرسانی محصولات متنباز بسیار مشکلتر از به روزرسانی محصولاتی مثل Microsoft Windows است؛ اما با وجود دستورالعمل های نصب برای محصولات اصلی متن باز این مشکل هم برطرف می شود . نرم افزارهای متنباز مبتنی بر ویندوز نیز وجود دارند که بصورت کامپایل شده توزیع می شوند و از نصب کننده های ساده استفاده می کنند .

همانند سیستمهای windows بسته های به روزرسانی و وصله های ارائه شده برای سیستمهای متن باز بزرگ، بسته به اندازهٔ سیستمهای متن باز تغییر می کنند .شناسایی منابع محلی این بسته های به روزرسانی بمنظور کاهش زمان download آنها از اینترنت برای کاربران منفرد بسیار 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 ایم نتر هستند.

طرفداران نرم افزارهای انحصاری معتقدند:

- از آنجا که متن برنامهٔ محصولات متن باز در دسترس است، نفوذگران 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 روابط سازمانی ممکن است روی محصولات متن باز کار کنند، ممکن است استانداردها نادیده گرفته شوند و فقدان یکپارچگی در اجزای مختلف منجر به آسیب پذیریهای امنیتی گردد.

- به این دلیل که کاربران برای محصولات انحصاری به تولیدکننده وجه می پردازند، دستورات او را دنبال می کنند و انجام اینکار باعث می شود کیفیت ملاحظات امنیتی در نرم افزارهای انحصاری بالا باشد.
- از آنجا که هیچ منبع معینی مسئولیتی در قبال محصولات متن باز بر عهده ندارد، درصورتیکه امنیت برای توسعه دهندگان انفرادی اهمیت نداشته باشد، احتمال زیادی وجود خواهد داشت که نادیده گرفته شود.

طرفداران نرم افزارهای متنباز معتقدند:

- به دلیل اینکه افراد زیادی با متن برنامه نرم افزارها کار می کنند، مسائل و مشکلات آنها توسط افراد خبره تشخیص داده می شود و سریعًا اصلاح می گردد.
- افرادی که با محصولات انحصاری کار می کنند ممکن است کد یکپارچه ای را تولید کنند؛ اما اگر تولیدکننده 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 تولیدکنندۀ محصول مراجعه کرد و این امر ممکن است باعث تأخیر زمانی زیادی شود.

در واقع هریک از این دلایل در جایگ اه خود صحیح هستند. راهی برای کسب اطمینان از ایمن بودن نرم افزار انحصاری یا 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 دو نوع نرم افزار، نمونه هایی از رفتار ایده آل و همچن ین بی دقتی طراحان و سازمانهای ارائه خدمات پشتیبانی دیده شده است.

نرم افزارهای 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 سراس ر دنیا وجود دارد، ولی بیشتر در کشورهایی اتفاق میافتد که در آنها هزینۀ نسبی تهیه نرم افزارهای قانونی در مقایسه با دستمزدها بسیار بیشتر از کشورهای 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 وظیفۀ قانونی مسئولین برای

جلوگیری از خدشه دار شدن حقوق مالکیت سازندۀ 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 ای ن امکان وجود دارد که هر دو با هم نیز وجود داشته باشند.

۱. ممکن است نرم افزار مسروقه قابل به روز رسانیشدن نباشد یا انجام ب هروزرسانی آنرا از کار بیندازد.

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

بخش دوم امنیت فناوری اطلاعات و کاربران منفرد

فصل ششم امنیت خدمات شبکه

کلیات

اصول اولیه

قانون چهارم

پست الکترونیکی

تأثیر ارتقای پست الکترونیکی

پست الکترونیکی گمراه کننده است

چگونه می توانید از خود محافظت نمایید؟

قانون پنجم

قانون ششم

هرزنامه

آشنایی بیشتر با هرزنامه

سایر مسائل اینترنتی

اشتراک فایل

قانون هفتم

قانون هشتم

قانون نهم

پیامهای فوری

فصل پنجم امنیت خدمات شبکه

کلیات

پست الکترونیکی و وب از کاربردهای اصلی این ترنت هستند. در این فصل عملکرد این خدمات را بطور جزئی توضیح می دهیم و استفادهٔ نامناسب از آنها که باعث ایجاد ناامنی می گردد را بررسی می کنیم . مواردی مثل ارتباطات بی سیم، اشتراک فایلها و قابلیت ارسال پیام فوری از دیگر موضوعات حساس مرتبط با امنیت شبکه هستند که در این فصل به آنها پرداخته خواهد شد.

اصول اولیه

وصله های امنیتی را باید بصورت منظم برای نرم افزارهای خود به روزرسانی 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 رایانهٔ شما طراحی می کنند.

قانون چهارم:

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

به روزرسانی 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 نسخهٔ موجود آن ارتقا دهید.

پست الکترونیکی

سیر تکامل

اگر تاریخچهٔ شبکه را بررسی کنید (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 هنگامیکه استفاده از آن عموم گسترده تری یافت، باید برای استفاده توسط عموم ساده تر میگشت.

مشکل این بود که پست الکترونیکی اولیه تنها برای انتقال منتهای ساده طراحی شده بود و فایلهایی چون برنامه هایاجرایی در متن خود کاراکترهای غیرچاپی داشتند که در متون ساده قابل نمایش نبودند . راه حل پیشنهادی این بود که اطلاعات غیرچاپی 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 میآید.

بعد از آن مفهوم « ضمیمه» بوجود آمد تا با استفاده از آن بتوان انواع بیشتری از فایلها را کدگذاری نمود . امروزه این رو جدید *MIME* نامیده می شود . هنگامیکه کاربرد ضمیمه وسعت بیشتری پیدا کرد، برنامه های پست الکترونیکی طوری تغییر کردند که بتوانند ضمایم را بطور خودکار باز کنند.

بنابراین دریافت کنندهٔ 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* شد که امکان قالب بندی نامههای الکترونیکی را فراهم میکرد (تغییر فونت ها، رنگها، تصاویر، و اشاره گرها به صفحات وب)درحال حاضر برنامه های پست الکترونیکی بصورت خودکار دستوراتHTM درون صفحات ارسال شده را نیز اجرا میکنند.

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، ر نگها و تصاویر، نامه شکل مطلوب تری پیدا می کرد و قالب بندی سادۀ آن بدون نیاز به برنامۀ 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 تأثی ر مستقیم ویروسها و کرمها قرار نمی گرفت . همچنین تا زمانیکه برنامۀ دریافت شدۀ موجود در ضمائم نامۀ دریافتی را اجرا نمی کردید از خطرات امنیتی مصون بودید . اکنون اما برنامه هایی که دریافت می کنید می توانند بصورت خودکار به اجرا درآیند که مفهوم آن این است که این ب رنامهها خواهند توانست شما را به پایگاه وبی هدایت کنند که در آن اعمال مخربی مثل download نرم افزارهای مخرب صورت می پذیرد .علاوه بر این دستورات ویژه HTML می توانند مهاجم را به راهبر رایانۀ شما تبدیل کنند که البته چگونگی آن بستگی به اشکالات موجود در برنامۀ مفسر دستورات HTML رایانه شما دارد .

پست الکترونیکی گمراه کننده است

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

چگونه می توانید از خود محافظت نمایید؟

قانون پنجم:

برنامۀ پست الکترونیکی خود را طوری پیکربندی نمایید که ضمائم را بصورت خودکار باز نکند.

هر فردی که آد رس پست الکترونیکی شما را بداند یا بتواند آنرا حدس بزند می تواند برای شما نامۀ 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 وارد نماید .اکثر برنامه های جدید پست الکترونیکی ضمایم را قبل از اجازۀ شما باز نمی کنند، اما اگر برنامۀ شما بگونه ای باشد که آنرا بصورت خودکار باز نماید، باید بتوانید این گزینه را غیرفعال کنید.

قانون ششم:

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

نویسندگان ویروس بسیار زیرک هستند . آنها معمولاً ضمایم با نام هایی چون budget.xls.vbs ارسال می کنند . ناظری که نمی داند vbs چیست تصور می کند یک فایل Exel 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 budget.xls می باشد .

هرزنامه

هرزنامه نامی است که برای نامه های الکترونیکی ناخواسته بکار می رود، خصوصلاً نامه های تجاری که از طرف افراد ناشناس و بصورت متعدد احتمالا بر اساس 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 ا ست .در سال ۲۰۰۳ بیش از ۵۰ درصد از کل نامه های الکترونیکی تبادل شده در اینترنت هرزنامه بوده است ! بسیاری افراد هم اکنون به ازای دریافت هر یک نامۀ معتبر حدود ۱۰ هرزنامه دریافت می کنند.

اگر در فیلد « موضوع» هرزنامه ها عبارتهایی نظیر وجود می داشت، آنگاه می توانستیم به آسانی SPAM تمامی آنها را حذف کنیم . قوانین مصوب قضایی حکم می کند که هر نامۀ الکترونیکی ناخواسته که از سوی شرکتهای تجاری ارسال شود پیگرد قانونی خواهد داشت . با این وجود به دلیل حجم وسیع

هرزنامه ها و نیز تواناییهای محدود نیروهای انتظامی درحال حاضر اجر ای این نوع قوانین چندان عملی نیست . هرکس باید بدون خواندن هرزنامه و یا ارسال اخطار به یک سیستِ م شلوِ غ 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 درنظر گرفت:

الف) چگونه هرزنامه نویس ها آدرس شما را بدست م یآورند.

ب)چه چیزی هرزنامه تلقی میشود(با جزئیات دقیق) .

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

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 وب ثبت نام کرده باشید 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 درحال اجرا بوده استفاده کرده باشید

سایر مسائل اینترنتی

اشتراک فایل

درصورت 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 درحالیکه در یک سیستم فعالیت می کنید به فایلهای موجود در یک سیستم دیگر دسترسی یابید، آنها را تغییر 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 هرکدام در یک نیمکرهٔ زمین باشند . اشتراک فایل این امکان را فراهم می سازد که در طول مسافرتها بتوانید به فایلهای رایانهٔ خود دسترسی داشته باشید.

یک رایانهٔ منفرد که بعنوان سرویس دهندهٔ فایل عمل می کند می تواند بعنوان دیسک سخت تعداد زیادی رایانه تلقی گردد .در اینصورت بیشتر فایلهای شما در سرویس دهندهٔ 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 رایانهٔ 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 هفتم:

اگر از قابلیت اشتراک فایل استفاده نمی کنید آنرا غیرفعال سازید . درصورت نیاز به آن، دسترسیهای خود را به آنچه که واقعًا لازم دارید محدود نمایید.

قانون هشتم:

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 نهم:

اگر فایلها را با دیگران به اشتراک م ی گذارید مطمئن شوید آنها مسائل امنیتی را جدی میگیرند.

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 بگونهای محدود سازید که به فایلها تنها اجازۀ خوانده شدن بدهد . به عبارت دیگر اگر نیازی به دسترسی نوشتن ندارید باید آنرا غیر فعال کنید.

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

پیامهای فوری

قابلیت ارسال پیام فوری این امکان را فراهم می سازد که پیام تایپشده 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 . بسیاری از سیستمهای ارسال پیام فوری به کاربر اجازه می دهند اسمی انتخاب کند که همراه پیامهای ارسالی اش به نمایش درآید و بدین ترتیب سایرین نیز بتوانند برای او پیام ارسال نمایند . این اسامی ممکن است موجب شوند که هویت اصلی شما پنهان بماند، اگرچه راهبران سیستم ممکن است بتوانند هویت شما را از طریق آدرس IPشناسایی کند .