امنیت فناوری اطلاعات و کاربران منفرد

بخش دوم

فصل اول

مقدمه

تأکید بخش دوم بیشتر بر تأمین امنیت کاربران منفرد رایانه است – از مبتدیان گرفته تا کارشناسان؛ و اولین مسئله‌ای که در این زمینه باید شرح داده شود چگونگی حفاظت از رایانه‌های شخصی است.

می‌توان از رایانه بصورت ایمن استفاده کرد؛ ولی اینکار به اطلاعات، زیرکی و مراقبت شدید نیاز دارد. زبان بکار رفته در این بحث بعضاً حاوی مفاهیم نامأنوسی می‌باشد. بعضی از اصطلاحات و تعاریف در ضمیمهٔ انتهای این بخش آمده‌اند و بعضی از آنها نیز در پیوست ۱ کتاب بطور کامل طرح شده‌اند.

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

- داده‌ها و برنامه‌هایتان تنها درصورتی تغییر می‌کنند یا پاک می‌شوند که شما چنین خواسته‌ای داشته باشید؛
- برنامه‌های رایانه بگونه‌ای که طراح یا برنامه‌نویس آنرا تعیین کرده عمل می‌کنند (مگر عیب و نقصهای نرم‌افزاری، که وجود آنها در برنامه‌ها ناخواسته است)؛
- هیچکس نمی‌تواند بدون اجازهٔ شما از داده‌ها، 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 می‌کنید نیست؛
- کسی توانایی دستیابی به داده‌های شما، چه در شبکه‌های بی‌سیم و چه در شبکه‌های سیمی را ندارد؛
- روی سیستمها و یا پایگاههای وبی که به آنها دسترسی دارید کسی قادر به سرقت *نام کاربری*[1] و *رمز عبور*[2] نیست؛
- چنانچه شمارهٔ کارت اعتباری و یا اطلاعات مربوط به حساب بانکی خود را از طریق شبکهٔ اینترنت وارد کنید، داده‌های مربوطه از امنیت کامل برخوردار خواهند بود (مسلماً شما بر آنچه که در سوی دیگر شبکهٔ ارتباطی رخ می‌دهد کنترلی نخواهید داشت)؛
- و ...

چنانچه نکات امنیتی در رایانه‌های شخصی نادیده گرفته شوند پیامدهای گوناگونی به بار می‌آید: ممکن است این پیامدها منجر به آزار شخص گردند ولی هزینه‌ای 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 می‌شود 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 می‌آید که بتوان تمامی جوانب امنیتی رایانه‌های شخصی را کنترل نمود.

چنانچه راهنماییهای ارائه‌شده در این کتاب نیز بکار گرفته شوند می‌توان احتمال خطر را تا حد قابل قبولی کاهش داده و از جهان درحال تغییر فناوری اطلاعات استفادهٔ بهینه نمود.

طبیعتاً ارائه تمامی نکات امنیتی رایانه‌های شخصی صدها صفحه مطلب را به خود اختصاص می‌دهد، اما مخاطبین غالباً تمایل چندانی به مطالعه مطالب انبوه ندارند. در این نوشته خلاصه‌ای از اطلاعات لازم برای کاربران جهت درک و پیاده‌سازی نکات امنیتی رایانه‌های شخصی ارائه شده است. مراجع ذکرشده در بخش ضمایم شامل منابع الکترونیکی، سازمانهای مرتبط، و مستندات چاپی نیز می‌توانند کمکهای مفیدی باشند و کاربر را به مطالعهٔ بیشتر نکات امنیتی فناوری اطلاعات تشویق نمایند.

---

1 *Username*
2 *Password*

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 می‌شود. تعاریف کاملتر در ضمیمه ۱ همین فصل و نیز پیوست ۱ کتاب ذکر شده‌اند.

چرا تمهیدات امنیتی ضرورت دارند؟

در اولین روزهای استفاده از رایانه‌ها در سیستمهای به‌اشتراک گذاشته‌شده تنها از نام کاربری برای شناسایی افراد استفاده می‌شد 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 رایانه‌ها بیاندیشند. مهمترین دلایل این مسئله عبارتند از:

- *ارزش سرمایه‌گذاری روی تجهیزات سخت‌افزاری و برنامه‌های نرم‌افزاری* – نکتهٔ قابل توجه این است که رایانه‌ها و بسته‌های نرم‌افزاری بسیار گرانقیمت هستند و جایگزینی آنها پرهزینه و دشوار است. حتی اگر در یک رخداد امنیتی نرم‌افزارها و سخت‌افزارها کاملاً از بین نروند ممکن است مشکلات امنیتی ما را وادار به نصب مجدد همهٔ نرم‌افزارها کنند و متعاقباً لازم شود کلیهٔ نیازهای اساسی مجدداً تعریف گردند. این امر مستلزم صرف زمان بسیار زیادی است؛ خصوصاً اگر فرد مسئول، اطلاعات فنی کافی در این زمینه نداشته باشد.
- *ارزش داده‌های سازمانی* – این داده‌ها ممکن است شامل لیست مشتری‌ها، پروژه‌های مالی و یا برنامه‌های تجاری باشند که توسط کاربر نوشته شده‌اند.
- *ارزش داده‌های فردی* – ممکن است داده‌های فردی ارزش مادی چندانی نداشته باشند ولی از دست دادن آنها بسیار زیان‌آور باشد و برای ایجاد دوبارهٔ اطلاعات زمان بسیار زیادی لازم باشد (تعاریف مربوط به *سرقت هویت*[3] را مورد ملاحظه قرار دهید).
- *تهدیدات جنایتکاران رایانه‌ای* – همگام با پیشرفتهای فناوری، گروهی از خرابکاران که از دزدی داده‌های رایانه‌ای سود می‌برند نیز بوجود آمده‌اند. در مواردی اینکار صرفاً برای لذت و سرگرمی صورت می‌گیرد و برخی افراد نیز تنها بخاطر خودنمایی در برابر دوستان خود دست به چنین کارهایی می‌زنند؛ اما در بعضی موارد اینکار برای دستیابی به منافع شخصی و سازمانی انجام می‌گیرد (دزدی اطلاعات کارت اعتباری یا ورود به معاملات فریبکارانه). در تمامی موارد مذکور این اشخاص باعث ایجاد خسارت و گسترش بی‌اعتمادی می‌شوند و در حد گسترده‌تر مشکلات بحرانی بوجود می‌آورند که به اشخاص و موقعیتهای شغلی صدمه وارد می‌کند. باید گفت از زمانی که اینترنت در مقیاس جهانی در اختیار کاربران قرار گرفته، تعقیب و متوقف کردن مهاجمین هرچند همچنان امکانپذیر می‌باشد ولی بسیار پیچیده شده است.

چرا معمولاً در بعد امنیت ضعف وجود دارد؟

برنامه‌های نرم‌افزاری غالباً بدون درنظر گرفتن مسائل امنیتی تولید می‌شوند. این مسئله چند دلیل دارد:

- *سهل‌انگاری* – برنامه‌نویسان و طراحان از اهمیت نکات امنیتی اطلاعی ندارند.
- *اولویت پایین* – تا چندی قبل حتی کسانی که نسبت به نکات امنیتی آگاهی داشتند نسبت به آن اقدام چندانی نمی‌کردند و درنتیجه مسائل امنیتی مورد توجه لازم واقع نمی‌شد.

3 *Identity Theft*

- *محدودیت زمان و هزینه* – بعضی افراد تصور می‌کنند اقدامات امنیتی جهت طراحی، کد نویسی و آزمایش در طول فرآیند تولید نرم‌افزار هزینهٔ گزافی در بر داشته و زمان زیادی را به خود اختصاص می‌دهد.
- *بی‌نظمی برنامه‌نویسان* – در کارهای مربوط به برنامه‌نویسی اشتباهات مشابه چندین بار تکرار می‌شوند و باعث ایجاد نقایص امنیتی می‌گردند.
- *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 داده‌ها و سیستمهای خود نیستند.
- *نگاه غیرواقعی قربانیان* – برخی کاربران نسبت به نکات امنیتی آگاهی دارند ولی آنها را جدی نمی‌گیرند؛ چون گمان می‌کنند که حمله‌ای علیه آنها صورت نخواهد گرفت.

ارزیابی تهدیدات و هزینه‌های 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 داده‌های رایانهٔ شما پاک شوند.

...یک نسخه از تمام داده‌های شما به سرقت رود. این داده‌ها ممکن است شامل مواردی باشند از قبیل: اطلاعات حساب بانکی، فهرست نامهای کاربری و رمزهای عبورِ پایگاههای وب انجام *خریدهای برخط*[4]، گزارشهای کاری مهم و تکالیف درسی که ارزش آنها معادل ۵۰٪ نمرات درسهای ترم جاری شما است.

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

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

...یک ویروس رایانه‌ای مخرب به همه دوستانتان که نام آنها در دفترچهٔ آدرسهای 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 مطمئن هستید به این میزان از تلفن استفاده نکرده‌اید.

...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 نموده‌اید 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 می‌دهد؟
- چه مقدار هزینه صرف آن می‌شود؟
- چگونه می‌تواند سازمان شما را تحت تأثیر قرار دهد؟
- چه هزینه‌های جانبی در بر دارد؟ (مثلاً در شرایط نامناسب و در غیاب مسئول مربوطه)

تمامی این موارد اهمیت موضوع "امنیت رایانه" را مشخص می‌کنند. اکنون که متوجه شده‌اید امنیت موضوعی بسیار مهم است، گام بعدی بررسی یک طرح مناسب امنیتی برای ایمن شدن می‌باشد:

4 *Online Shopping*

- ایمن شدن برای شما چه هزینه‌ای خواهد داشت؟
- چه زمانی را به خود اختصاص می‌دهد؟
- تا چه حد مشکل‌آفرین خواهد بود؟
- آیا کارهایی وجود دارند که با اجرای طرح امنیتی، انجام آنها مشکل و یا غیر ممکن شود؟
- آیا می‌توانید 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 پروژهٔ 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 هزینه‌ای خواهد داشت؟

چند راهکار مناسب امنیتی وجود دارند که به تجهیزات چندانی نیاز ندارند و تجهیزات لازم نیز آنچنان گرانقیمت نیستند. حتی *ویروس‌یابها*[5] که رایجترین کالای امنیتی هستند در قالب *نرم‌افزارهای رایگان*[6] در دسترس می‌باشد. شایان ذکر است که فهرست سازمانهای ارائه‌کنندهٔ نرم‌افزارهای رایگان در بخش ضمائم موجود می‌باشد.

چه زمانی را به خود اختصاص می‌دهد؟

مسلماً اجرای طرح امنیتی و دنبال کردن آن زمانی را به خود اختصاص می‌دهد، اما میزان این زمان زیاد نیست. در این خصوص لازم است که نرم‌افزارهای 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 می‌دهید 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 ضمیمه‌ای فرستاده باشد، باید در مورد بازکردن و یا باز نکردن آن تصمیم‌گیری 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 – می‌رساند. بسته‌های نرم‌افزاری جدید قابلیتهای جذاب بسیاری دارند، اما استفاده از آنها – خصوصاً آندسته که برای گسترش شبکه و ارسال و دریافت پیام بکار می‌روند – باعث آسیب‌پذیری بیشتر در برابر حملات می‌گردند. بعنوان مثال ممکن است پایگاه وبی وجود داشته باشد که ارائه‌کنندهٔ خدمات مورد نظر شما باشد ولی برای دسترسی به آن لازم باشد که یک نرم‌افزار خاص آنرا download و بر روی رایانه خود اجرا کنید. اگر نسبت به اشخاصی که این خدمات را ارائه می‌دهند اعتماد کافی ندارید بهتر است از قابلیتهایی که آن برنامه می‌تواند برای شما به ارمغان بیاورد صرفنظر نمایید.

آیا می‌توانید 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.

- به‌روزرسانی نرم‌افزارها و *وصله‌های*[7] ارائه‌شده که بخش مهمی از فرآیند ایجاد امنیت است به *پهنای باند*[8] 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

5 *Virus Scanners*
6 *Freeware*
7 *Patches*
8 *Bandwidth*

از طریق تلفن برای بازه‌های طولانی‌مدت هم مقرون به صرفه نیست. به همین دلیل در چنین شرایطی بهتر است یکنفر نرم‌افزارهای معمول را به‌روز رسانی کرده و نسخه‌های download شدهٔ آنها را در اختیار دیگران قرار دهد. متأسفانه انجام اینکار معمولاً مشکلتر از download کردن مستقیم توسط هر کاربر است؛

- هشدارهای امنیتی به افراد حرفه‌ای در کار با رایانه کمک می‌کند. کاربران مبتدی معمولاً نسبت به چنین هشدارهایی حساسیت زیادی ندارند و اگر یک کاربر هشداری دریافت کند معمولاً قادر به فهم کامل آن و متعاقباً بروز واکنش مناسب نخواهد بود.[۹] بعضی اوقات ممکن است شما یک هرزنامه مشکل‌آفرین دریافت کنید که ادعا دارد یک به‌روزرسانی از مایکروسافت می‌باشد که شامل ضمیمهٔ "Update" است ولی باید دقت داشته باشید که معمولاً ضمیمه‌های این نامه‌ها چیزی جز ویروسهای خطرناک نیستند؛ و
- در محیطهایی که تعداد زیادی رایانه یافت می‌شوند (مراکز کاری، مدارس، اداره‌های دولتی) لازم است که شخصی بعنوان *راهبر سیستم*[۱۰] 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 سیستمها 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.

تصمیم‌گیری در مورد طرح امنیت فردی

برنامه‌های بسیاری وجود دارند که به نیازهای امنیتی رایانه‌ها 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 کرده‌اید، 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 برسید که مقابله با بعضی از خطرات حداقل در زمان حاضر ضروری نیست. طرح امنیتی شما به برنامه‌های نرم‌افزاری خاصی تکیه می‌کند اما کماکان باید فرآیندها، قوانین، و ملاحظات شخصی را در بر بگیرد.

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

بعضی از ملاحظات مناسب در زیر آمده‌اند:

- 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 سریعاً 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 می‌توان احتمال بروز تصادف را تا حد قابل توجهی کاهش داد. در تدوین اجزای یک طرح امنیتی، افراد باید لایه‌هایی از حفاظت را بکار گیرند که ممکن است حتی تا حدودی تکراری باشند. برای درک بهتر تصور کنید که می‌خواهید از یک تکه جواهر قیمتی محافظت کنید. مسلماً آنرا در یک جعبهٔ سربسته و سپس در یک اتاق قفل‌شده قرار می‌دهید؛ 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 می‌برند، ولی مسلماً بکارگیری تمام مراحل عاقلانه‌تر است، چراکه اگر در یک مرحله با

---

۹ *هرچند با گسترش آگاهی امنیتی جامعه، این وضع دچار تغییر می‌شود.*

شکست مواجه شوید مراحل دیگر در رسیدن شما به موفقیت کمک خواهد کرد (مثلاً اگر 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، پیاده‌سازی ضعیف و یا خطاهای انسانی باشد. این مسئله می‌تواند در مورد مشکلات ابزارهایی مثل ویروس‌یابها، *رمزگذاری*[11] 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 می‌کند نقش مهمی در تضمین ایمنی رایانه و نرم‌افزارهای 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 رایانه اطلاعات کافی ندارند خود از بزرگترین خطرات امنیت رایانه‌ای بشمار می‌روند.

امنیت یک هنر است، نه یک علم

در ایمن‌سازی رایانه‌ها و شبکه‌ها هیچ تضمین صد درصدی وجود ندارد، چراکه همیشه نقایص تازه و راههای جدید نفوذ و فرصتهای نو برای ایجاد مشکل – که خود ناشی از خطاهای انسانی است – وجود خواهد داشت. اما اگر مطالعهٔ دقیقی انجام بگیرد و از *تجارب موفق امنیتی*[12] استفاده شود می‌توان در عملکرد سیستم امنیت لازم را بوجود آورد. پایگاههای وب و گروههای پستی سازمانهای حفاظت از رایانه نیز می‌توانند کمکهای شایانی در این زمینه باشند، چراکه می‌توان در شرایط غیر معمول و بروز وضعیت غیرعادی از راهنماییهای آنها بهره گرفت.

11 *Encryption*
12 *Security Best Practices*

فصل سوم
امنیت رایانه و داده‌ها

کلیات

در این فصل به بررسی راههایی می‌پردازیم که از طریق آنها می‌توان رایانه را از لحاظ فیزیکی ایمن کرد و از سرقت داده‌ها و برنامه‌های رایانه‌ای جلوگیری نمود. مباحث عمدهٔ این فصل عبارتند از: امنیت فیزیکی، نسخه‌های پشتیبان، و تصدیق هویت با استفاده از نام کاربری و رمز عبور.

مقدمه

یکی از بهترین شیوه‌های درک مفهوم امنیت اطلاعات استفاده از یک *راهکار ضابطه‌مند*[۱۳] 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 فرآیندهای امنیتی برای رایانه‌های شخصی و گروه‌های کوچک رایانه‌ای را توضیح خواهیم داد. اطلاعات مربوط به جنبه‌های فنی امنیت برای سازمانهای بزرگتر و کاربران حرفه‌ای در بخش پنجم ارائه شده است. هنگامیکه با اطلاعات ارائه‌شده در این فصل با کلیات موضوع آشنا شدید، می‌توانید 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 داده‌اید یا اینکه رایانه و داده‌ها از چه حساسیتی برخوردار هستند یک قسمت جزئی یا یک قسمت بسیار مهم محسوب شود.

سرقت رایانه

سرقت رایانه‌ها مشکلی رو به رشد است. رایانه‌ها و خصوصاً رایانه‌های کیفی به سادگی دزدیده می‌شوند و بسیار سخت پیدا می‌شوند. چنانچه سارق مایل به استفادهٔ شخصی از رایانه نباشد مراکز بسیار زیادی وجود دارند که رایانه‌های دزدی و دست‌دوم را خریداری می‌کنند. برخی از سارقان، رایانه و نمایشگر آنرا بطور کامل به سرقت نمی‌برند بلکه قسمتهای مهم آن مانند حافظه و پردازشگر را می‌دزدند. 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 می‌باشد.

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 می‌گردد و در شرایط بدتر، سرقت رایانه باعث از دست دادن شغل می‌شود. با اینحال چنانچه در این خصوص چند روش ساده و ارزان‌قیمت بکار گرفته شود می‌توان از سرقت رایانه‌های 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 کار خود با همکاران دیگری کار می‌کنید رایانه را در معرض دید آنان قرار دهید. رایانه خود را در محافل عمومی مانند فرودگاه‌ها بدون مراقبت رها نکنید.
- اگر تصور می‌کنید که در زمان عدم حضور شما در محل کارتان ممکن است شخصی شبانه وارد اتاق

13 *Rule-Based Approach*

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 نسبتاً عمومی مثل مدارس و یا کتابخانه‌ها استفاده می‌شود. اکثر رایانه‌ها دارای محلی مخصوص اتصال می‌باشند. رایانه‌های کیفی نیز برای اینکار معمولاً دارای کابلها و قفلهای بخصوصی هستند.
- چنانچه رایانه دارای قفلی می‌باشد که از باز شدن *بدنه*[14] جلوگیری می‌کند از آن استفاده نمایید. می‌توان از پیچهای مخصوص که براحتی قابل باز کردن نیستند نیز برای این منظور استفاده کرد.
- چنانچه اطلاعات ارزشمندی (مثل داده‌های کاری یا اطلاعات شخصی) در رایانهٔ شما وجود دارد، لازم است زمانی که آنرا بدون مراقبت قرار داده و یا از آن دور هستید (مثلاً اگر از هتل خارج می‌شوید و رایانه در اتاق است) امکان *دسترسی منطقی*[15] 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 صفحه‌نمایش 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).
- رایانه‌های کیفی و *PDAها*[16] کوچک می‌باشند و به همین دلیل دزدیدن آنها آسان است. چنانچه از آنها استفادهٔ زیادی نمی‌کنید حتماً آنها را از محیط کار خارج نمایید.

کاری کنید که میل به دزدیدن رایانه کاهش یابد

افرادی که مایل به خرید رایانه‌های 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 نمی‌توان آنها را از بین برد بر بدنهٔ رایانه حک و یا نقاشی کنید. این اطلاعات می‌تواند 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.

رایانه‌ها آسیب‌پذیرند

رایانه‌ها 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 رایانه‌ها همچنین نسبت به فرورفتگیها و برآمدگیهای سطحی که روی آن قرار دارند نیز حساس می‌باشند.

جنبه‌های دیگر امنیت فیزیکی

چنانچه شما برای نصب یک قطعه سخت‌افزاری بدنهٔ رایانه خود را باز کرده‌اید باید به اخطارهایی که دربارهٔ شوکهای الکترواستاتیک داده شده توجه کنید (شوک الکترواستاتیک باعث صدمه‌دیدن سخت‌افزار می‌شود و باید از وقوع آن جلوگیری کرد). ضمناً توجه کنید که برای جلوگیری از برق‌گرفتگی لازم است بدن شما با زمین در تماس دائم باشد.

برای محافظت از داده‌های خود نسخه‌های پشتیبان[17] تهیه نمایید

در قسمت قبل مطالبی در مورد ایجاد امنیت فیزیکی آمد. در این قسمت مواردی شرح داده خواهند شد که بوسیلهٔ آنها می‌توان اطمینان حاصل کرد که داده‌ها و برنامه‌ها از حفاظت کامل برخوردارند. شما چگونه از داده‌ها و برنامه‌های رایانهٔ خود حفاظت می‌کنید؟

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

- پاک شدن اتفاقی فایل؛
- دزدیده شدن رایانه؛

14 *Case*
15 *Logical Access*
16 *Personal Digital Assistants*
17 *Backups*

- ذخیرهٔ ناخواسته یک فایل بر روی فایل دیگر؛
- روند نادرست به اجرا در آمدن یک برنامه بگونه‌ای که باعث تغییر یا پاک شدن داده‌ها شود؛
- وجود یک برنامهٔ مخرب (مثل ویروس) که باعث تغییر، بازنویسی و یا حذف داده‌ها شود؛
- بروز مشکل در سخت‌افزار (مثل مشکلات *دیسک سخت*[18]، دیسک‌گردان، پردازشگر و یا منبع تغذیه) بگونه‌ای که باعث از بین رفتن داده‌ها گردد؛
- آتش‌سوزی و استفاده از آب برای خاموش کردن رایانهٔ سوخته، که باعث غیرقابل بازیابی شدن داده‌ها می‌شود؛
- و ...

یکی از راه‌حلها برای مقابله با این تهدیدات، تهیهٔ نسخه‌های پشتیبان می‌باشد. نسخه پشتیبان به خودی خود یک کپی از فایل یا مجموعه‌ای از فایلها است که با انتقال به یک دیسک فلاپی و یا دیسک فشرده از آن نگهداری می‌شود. چنانچه فایل اصلی به هر دلیلی از بین برود یا پاک شود می‌توان 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.

نسخه‌های پشتیبان می‌توانند بسیار ساده و یا بسیار پیچیده باشند (از ساده‌ترین انواع پشتیبان می‌توان به یک دیسک فلاپی که از آن در کشوی میز کار خود نگهداری می‌کنید اشاره کرد). اکثر بسته‌های نرم‌افزاری پشتیبان‌گیر به شما اجازه می‌دهند فایلی را که در رایانه خود دارید به روی نوارهای مغناطیسی و یا مجموعه‌ای از دیسکهای فشرده[19] کپی کنید. چنانچه رایانهٔ شما دزدیده شود، با خرید یک رایانهٔ جدید با ساختاری مشابه رایانهٔ قدیمی و با استفاده از نسخه‌های پشتیبان قادر خواهید بود فایلهای از دست رفته را مجدداً بکار گیرید.

نقایص، تصادفات، بلایای طبیعی و حملات مهاجمین قابل پیش‌بینی نیستند. معمولاً علیرغم تلاشهای زیاد برای برقراری امنیت نمی‌توان از بروز بعضی از مشکلات جلوگیری نمود، ولی اگر پشتیبان مناسب تهیه کرده باشید حداقل داده‌های خود را از دست نمی‌دهید و در اکثر مواقع می‌توانید سیستم خود را بازیابی کرده و به یک حالت متعادل و ماندگار برسانید. حتی درصورتیکه داده‌های رایانه تماماً از دست رفته باشد، چنانچه یک مجموعهٔ کامل از نسخه‌های 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 صرفاً زمانی کارآمد است که نسخه‌های پشتیبان در جایی غیر از رایانهٔ قربانی ذخیره شده باشند.

دلایل گوناگونی وجود دارند که باعث می‌شوند نسخه‌های پشتیبان اجزای کلیدی و مهمی در امنیت رایانه‌ها محسوب شوند:

خطای کاربر

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

نقص در سخت‌افزار

سخت‌افزار مورد استفاده در هر زمانی ممکن است دچار خرابی شود و باعث از بین رفتن داده‌ها در طول یک فرآیند گردد. صدمه‌هایی که به دیسک وارد می‌شود نیز می‌تواند منجر به تخریب کامل دیسک شود. ولی چنانچه از فایلها پشتیبان تهیه شده باشد می‌توان داده‌ها را مجدداً روی دیسک‌گردان و یا سیستم جدید بازیابی نمود.

نقص در نرم‌افزار

اکثر برنامه‌های کاربردی مثل Microsoft Word و Excel و Access می‌توانند باعث از بین رفتن ناخواستهٔ فایلهای داده شوند. اگر نسخهٔ پشتیبان داشته باشید و برنامهٔ کاربردی شما ناگهان نیمی از اطلاعات حیاتی فایلِ کاری شما را پاک کند، باز هم قادر خواهید بود داده‌های خود را بازیابی نمایید.

18 *Hard Disk*
19 *CD-ROMs*

نفوذها و تخریبهای الکترونیکی

مهاجمین و ویروسهای مخرب مرتباً باعث تغییر و یا پاک‌شدن داده‌ها می‌شوند. وجود نسخه‌های پشتیبان در این زمینه نیز به کاربران کمک شایانی می‌کند.

اطلاعات بایگانی

نسخه‌های پشتیبان بعنوان اطلاعات بایگانی‌شده تلقی می‌شوند که امکان مقایسهٔ نرم‌افزارها و داده‌های رایج با نرم‌افزارها و داده‌های قدیمی را بوجود می‌آورند. این قابلیت باعث می‌شود بتوانید مشخص کنید که چه چیزهایی عمداً یا سهواً دچار تغییر شده‌اند. برای این منظور اگر نخواهید به عقب برگشته و تاریخچهٔ یک پروژه را بازسازی کنید نسخه‌های پشتیبان منابع ارزشمندی بشمار می‌آیند.

سرقت

سرقت رایانه‌ها و فروش آنها کار بسیار آسانی است. با توجه به این مسئله، تهیهٔ نسخه‌های 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 شده‌اند.

بلایای طبیعی

وقوع اتفاقاتی نظیر سیل، زلزله و آتش‌سوزی اهمیت حفاظت از رایانه را بیشتر روشن می‌کنند. در این زمینه نگهداری پشتیبانها در محلهای دیگر بسیار مفید خواهد بود.

بلایای دیگر

بعضی مواقع نشت لوله‌های گاز و متعاقباً آتش‌سوزی ناشی از آن یا ریخته‌شدن مواد مایع روی دستگاه تهویه باعث بروز مشکل می‌گردد. در این موارد نیز وجود نسخه‌های پشتیبان بسیار حیاتی است.

با توجه به نقش مؤثری که پشتیبانها می‌توانند داشته باشند وجود اَشکال 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 شیوه‌های تهیهٔ پشتیبان آمده است:

- فایلهای حساس خود را روی دیسک فلاپی، دیسکهای نوری، و یا دیسکهای مغناطیسی با ظرفیت بالا که قابلیت پاک‌کردن نیز در آنها وجود دارد کپی کنید.
- محتویات دیسک را روی یک *دیسک انعکاسی*[20] یا اگر فضای کافی موجود است روی یک شاخه در همان دیسک مادر کپی کنید. البته اینکار در خرابیهای اساسی کمک چندانی نمی‌کند و صرفاً اگر تعدادی از فایلها بطور ناخواسته پاک شوند بکار می‌آید.
- هر از چندگاه آرشیو فشرده‌سازی‌شده‌ای از فایلهای مهم خود ایجاد کنید. البته می‌توان پشتیبانهای مربوطه را روی همان سیستم اولیه و یا روی رایانه‌های 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 نرم‌افزار یا سخت‌افزاری که از هر فایل یک پشتیبان تهیه می‌کند استفاده نمایید. البته لازم به ذکر است که با رعایت تمامی این موارد بازهم تهیهٔ مداوم پشتیبان جهت حفاظت در برابر مشکلات دیگر ضروری می‌باشد.

از چه چیزهایی باید پشتیبان تهیه کرد؟

دو دیدگاه در این زمینه وجود دارد:

۱. از تمام فایلهایی که اختصاصی رایانهٔ شما است – البته غیر از برنامه‌های کاربردی – پشتیبان تهیه کنید. این امر در قدم اول شامل فایلهای داده‌ای می‌شود ولی دقت داشته باشید که باید از تمام فایلهایی که

20 *Mirror Disks*

سازگاری[۲۱] سیستم‌عامل و برنامه‌های 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 می‌توانید تمام فایلهای داده‌ای خود را در چند شاخه اصلی نگهداری کنید و پشتیبانها را بگونه‌ای تهیه نمایید که تنها اطلاعات یکتا و اختصاصی شما را پوشش دهند.

۲. از همه چیز پشتیبان تهیه کنید. با تهیهٔ پشتیبان از تمام سیستم – بسته به نوع استفاده‌ای که از آن می‌شود – می‌توان 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 می‌کنیم:

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

۲. از داده‌های شخصی خود طبق یک زمانبندی با دوره‌های کوتاهتر پشتیبان تهیه کنید. بسته به نوع کاربرد، برای پشتیبان‌گیری روشهای گوناگونی وجود دارد:

- از تمام داده‌های شخصی خود پشتیبان تهیه نمایید (هر چند ماه یکبار) مگر اینکه حجم وسیعی داشته باشند و امکان اینکار وجود نداشته باشد.
- چنانچه داده‌های شخصی شما زیاد است متناوباً از آن پشتیبان تهیه نمایید، ولی در فاصله‌های کوتاه فقط از فایلهایی پشتیبان‌گیری کنید که دچار تغییر شده‌اند. به این نوع پشتیبان‌گیری *پشتیبان‌گیری افزایشی*[۲۲] می‌گویند. 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.

گونه‌های دیگری از پشتیبان‌گیری نیز وجود دارد. معمولاً برنامه‌های پشتیبان‌گیر در مورد چگونگی تهیه پشتیبان پیشنهاداتی به کاربر ارائه می‌کنند.

نسخه‌های پشتیبان باید در کجا نگهداری شوند؟

پاسخ این سؤال وابسته به دلیل شما برای استفاده از پشتیبانها است. اگر پشتیبان‌گیری برای حفاظت از داده‌ها در مقابل سرقت و یا آتش‌سوزی است محل ذخیره‌سازی 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 داده‌های پاک شده یا تغییر کرده صورت می‌پذیرد، باید محل آن طوری انتخاب شود که دسترسی به آن آسان باشد.

یک راه حل این است که پشتیبانهای کامل را در یک محل امن و پشتیبانهای افزایشی را در محلی نزدیک قرار دهید. راه دیگر این است که جدیدترین پشتیبان تهیه‌شده از داده‌ها را در دسترس و نسخه‌های قدیمی‌تر را در محلهای امن‌تر بگذارید. بعضی افراد از پشتیبانها دو نسخه تهیه می‌کنند و یک نسخه را در دسترس و دیگری را دور از دسترس قرار می‌دهند.

اگر در رایانهٔ خود داده‌هایی 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 داده‌ها 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 تهیه‌شده استفاده کنید:

- نسخهٔ مربوطه بسیار کهنه و یا از لحاظ فیزیکی صدمه دیده باشد. بروز این مشکل در دیسکهای فلاپی و رسانه‌های مغناطیسی بیش از همه به چشم می‌خورد.
- دستگاهی که پشتیبان بوسیلهٔ آن نوشته‌شده دارای اشکال بوده و به همین دلیل دادهٔ نوشته‌شده در پشتیبان قابل خواندن نباشد. در این موارد امکان دارد

21 *Compatibility*
22 *Incremental Backup*

بتوان با 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 می‌شد چندان تعجب کسی را بر نمی‌انگیخت. دیسکهای فشرده بعنوان رسانه‌های بسیار ماندگارتر شهرت داشتند، اما یک مطالعه در سالهای اخیر نشان داد دیسکهای فشرده‌ای که کیفیت چندان مطلوبی ندارند ممکن است بعد از گذشت حدود دو سال از زمان نوشته‌شدن اطلاعات روی آنها غیرقابل خواندن شوند.

خواندن نسخه‌های 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 قابلیت پاک کردن استفاده می‌کنید (مثل دیسکهای Zip و فلاپی)، از دیسکهای نو و تمیز استفاده نمایید.

بعضی اشخاص پشتیبانها را برای مدت بسیار طولانی نگه می‌دارند؛ اما سؤال این است که قرار است چه زمانی از نسخه‌هایی که چند سال قبل از اسناد و تصاویر و برنامه‌ها 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 داده‌ای در یک فلاپی پنج اینچی که در سال ۱۹۸۰ رایج بوده ذخیره شده باشد آیا امروز می‌توان رایانه‌ای با دیسک‌گردان پنج اینچی برای بازیابی آن پیدا کرد؟

چند نسخهٔ پشتیبان باید نگهداری شود؟

اگر شما هفته‌ای یکبار از آنچه دارید پشتیبان تهیه کنید درصورت مواجهه با یک فاجعهٔ مصیبت‌بار، حداکثر اطلاعات یک هفته را از دست خواهید داد. انجام اینکار از دیدگاه امنیتی قابل توجیه است ولی در طول زمان فضای اشغال‌شده بوسیلهٔ پشتیبانها بیشتر و بیشتر می‌شود. چه تعداد از این پشتیبانها را باید نگه داشت؟ اگر از دیسکهای مغناطیسی و یا دیسکهای فشرده استفاده می‌کنید 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 را نگهدارید. در تمام مثالهای بالا می‌توان 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 کرده‌اید قابل خواندن نباشد، گم شود، و یا به سرقت رود. در اینصورت واضح است که اگرچه نسخه‌های 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 نرم‌افزار خریداری‌شده پشتیبان تهیه کنید

اگر گواهی نرم‌افزارهایی که خریداری کرده‌اید این اجازه را می‌دهد، همیشه از دیسکهای فشردهٔ نرم‌افزارها یک نسخهٔ ثانویه تهیه کرده و از آن برای عملیات نصب و پشتیبانی استفاده نمایید.

مهمترین نکته در مورد نسخه‌های پشتیبان

مهمترین نکته در مورد نسخه‌های پشتیبان این است که تهیهٔ پشتیبان باید در فواصل زمانی منظم صورت بگیرد. بعضی اشخاص زحمت تهیهٔ پشتیبان را به خود نمی‌دهند و ممکن است به عواقب اینکار خود گرفتار شوند. این افراد عموماً وقتی هم که با مشکلی روبرو می‌شوند تصور می‌کنند مشکل دیگر تکرار نخواهد شد. همچنان توصیهٔ ما این است که از مخاطرهٔ احتمالی پیشگیری کنید و نسخهٔ پشتیبان تهیه نمایید.

تصدیق هویت

تصدیق هویت[۲۳] این امکان را فراهم می‌کند که رایانه بداند شما چه کسی هستید. این دانایی باعث می‌شود که بتوان از تقلب جلوگیری کرد. معمولاً شما با یک نام کاربری و رمز عبور شناسایی می‌شوید، هرچند گونه‌های مختلفی از این سیستمهای شناسایی وجود دارد. نکتهٔ قابل توجه این است که باید کلماتی بعنوان رمز عبور بکار گرفته شوند که نتوان

23 *Authentication*

آنها را براحتی حدس زد تا مهاجمان نتوانند آنها را پیدا کنند. در عین حال باید یادآوری آن کلمات در حافظه نیز امکانپذیر باشد و شخص آنها را فراموش نکند. اگر شما مرتباً با رایانه و پایگاه وب در تماس باشید قاعدتاً تا کنون نامهای کاربری و رمزهای عبور زیادی به خاطر سپرده‌اید، اما اگر آنها را بر روی یک کاغذ نزدیک رایانه نوشته‌اید باید بدانید که از امنیت زیادی برخوردار نیستند.

شناسایی کاربر

اکثر سیستمها برای شناسایی افراد از آنها می‌خواهند که بگونه‌ای هویت خود را احراز کنند. این مسئله می‌تواند با دریافت اطلاعات مختلفی انجام شود: نام کاربری، شمارهٔ عضویت، اسم عضو و...؛ که در این مباحث عموماً از نام کاربری استفاده می‌شود. در بعضی سیستمها بجای نام کاربری از آدرس پست الکترونیکی استفاده می‌شود. در حقیقت در این سیستمها آدرس پست الکترونیکی بعنوان نمادی خاص از نام کاربری تلقی می‌گردد. در خصوص نام کاربری قوانین مختلفی می‌تواند وجود داشته باشد:

- بعضی از سیستمها طول اسم را محدود می‌کنند ولی بعضی دیگر برای آن محدودیتی قائل نمی‌شوند.
- در بعضی از سیستمها می‌توان از هر علامتی – که بوسیلهٔ صفحه‌کلید 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 می‌کنند.
- بعضی سیستمها حروف بزرگ و کوچک را یکسان درنظر می‌گیرند 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 کاربر 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 الکترونیکی معمولاً بعنوان یک چنین نمادی از کاربر تلقی می‌شود.
- آیا می‌خواهید با انتخاب نام مورد نظر هویت واقعی خود را پنهان نگه دارید؟ اگر بوسیلهٔ این نام کاربری در یک فعالیت گروهی شرکت می‌کنید (مثلاً یک بازی اینترنتی) شاید نخواهید دیگران هویت واقعی شما را بدانند.
- آیا می‌خواهید نامی انتخاب کنید که یادآوری آن آسان باشد؟ چنانچه از یک *خدمت برخط*[24] استفاده کنید که به ندرت آنرا بکار می‌گیرید ممکن است مایل باشید از اسمی استفاده کنید که براحتی در ذهن بماند. بعضی افراد برای خدمات مختلف از یک نام کاربری استفاده می‌کنند، خصوصاً اگر آن خدمات با نکتهٔ مهم و حساسی در ارتباط نباشند.
- آیا می‌خواهید حدس زدن نامی که بکار می‌برید برای دیگران مشکل باشد؟ نام کاربری حساب بانکی شما باید بگونه‌ای تعیین شود که دیگران نتوانند به راحتی آنرا حدس بزنند (جهت تأمین امنیت لازم باید از پشتیبانی چندلایه استفاده کرد. اگر از آدرس پست الکترونیک عمومی خود برای ورود به سیستم بانکی استفاده کنید، حدس‌زدن آن برای سارقان ساده‌تر خواهد بود).

رمز عبور

در بعضی سیستمها نام کاربری از سوی سیستم تعیین می‌شود، ولی رمز عبور کلمه‌ای است که در هر صورت توسط کاربر تعیین می‌گردد و شکل آن نیز باید بگونه‌ای باشد که حدس زدنش توسط اشخاص دیگر دشوار باشد.

زمانیکه رمزهای عبور در سیستم میزبان ذخیره می‌شوند معمولاً رمزگذاری می‌شوند تا اگر کسی به دیسک دسترسی پیدا کرد قادر به مشاهدهٔ رمزهای عبور نباشد. در بعضی موارد این رمزگذاری بگونه‌ای است که امکان رمزگشایی رمزهای عبور وجود ندارد که به آن *رمزگذاری یکسویه*[25] می‌گویند. در این سیستمها وقتی برای ورود به سیستم رمز عبور را وارد می‌کنید، ابتدا رمزگذاری می‌شود و سپس با نسخهٔ ذخیره‌شده

24 *Online Service*
25 *One-way Encryption*

در دیسک مقایسه می‌گردد (برای جزئیات بیشتر به ضمیمهٔ ۱ همین بخش رجوع کنید).

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

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

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

- هرگز از یک کلمهٔ منفرد در زبان مادری خود بعنوان رمز عبور استفاده نکنید. انتخاب یک عبارت، یک جمله، و یا قطعاتی از کلمات برای این منظور مناسب‌تر است.
- چنانچه سیستم هم حروف بزرگ و هم حروف کوچک را در رمزهای عبور بعنوان حروف مجاز قلمداد می‌کند، از هر دوی آنها استفاده کنید – ولی نه در جای صحیح و قابل پیش‌بینیِ خود.
- درصورت امکان از اعداد ترکیبی، علامتهای مجاز و همچنین فضاهای خالی استفاده کنید.
- اگر سیستم اجازه می‌دهد که از فضای خالی استفاده کنید یا رمز عبور شما به شکل یک عبارت است می‌توانید در رمز عبور خود بعضی از فاصله‌ها را حذف کنید (یعنی رمز متشکل از لغاتی باشد که به یکدیگر چسبیده‌اند).
- برای اینکه رمز عبور خود را به آسانی به خاطر بسپارید می‌توانید 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 می‌کردید نیز به خطر خواهد افتاد. بنابراین چنین رمز عبوری را برای سیستمهایی انتخاب کنید که نیاز به حفاظت خاصی ندارند. بعنوان مثال برای استفاده از مطالب روزنامه‌ها و دیگر مطالب، نیازی به پرداخت پول یا ارائه اطلاعات محرمانه نیست، اما برای خواندن مقالات بعضی از روزنامه‌ها در پایگاه وب مربوطه باید یک نام کاربری و رمز عبور وارد کنید. درواقع آنها فقط می‌خواهند شما به سیستم آنها وارد شوید؛ بنابر این می‌توانید برای خواندن مطالب روزنامه‌های مختلف از یک رمز عبور مشابه استفاده نمایید.
- بعضی افراد حروف را با علائم یا ارقام مشابه عوض می‌کنند؛ مثلاً از رقم "1" بجای حروف "I" یا "L"، از شمارهٔ "3" یا علامت "#" بجای حرف "E"، از رقم "0" بجای حرف "O"، از علامت "@" بجای حرف "A"، و از رقم "5" بجای حرف "S" استفاده می‌نمایند. اینکار ترفند خوبی است، اما به یاد داشته باشید که یک مهاجم حرفه‌ای با این حقه‌ها کاملاً آشناست. این حقه‌ها کار وی را کمی سخت می‌کند، اما غیر ممکن نمی‌سازد.
- حرف "I" را به جای "eye" (چشم) یا "aye" یا هر کلمهٔ معنادار در زبان خودتان عوض کنید. اینکار بخصوص برای لغاتی مثل "icon" که پس از این تغییر به "eyecon" تبدیل می‌شود مفید است.

- از سرنام‌ها (حروف اول لغتهای سازنده یک عبارت) استفاده نمایید. بعنوان مثال "tgbwc" سرنامی برای شعار معروف کوکاکولا ("Things Go Better With Coke") می‌باشد.
- هجی‌کردن لغات بصورت برعکس آنها را کمی مبهم می‌کند، اما شناسایی‌شان را سخت نمی‌نماید.
- 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 می‌شوید؛
  - رمزهای عبور کلاسیک مثل "Xyzzy" یا "Plover" (رمزهای عبور مورد استفاده در بسیاری از بازی‌های رایانه‌ای)، و "open sesame"؛
  - لغاتی که در فیلمهای محبوب و معروف، اخبار، داستانها و یا ادبیات از آنها استفاده می‌شود؛ مثل "Harry Potter"، "Lord of the Rings" و "Gone with the Wind"؛
  - حروف روی صفحه‌کلید که در کنار هم قرار گرفته‌اند مانند "SDFGHJ"؛
  - مثالهای قبل به اضافهٔ یک رقم قبل و بعد از آنها؛
  - تکرار حروف یا ارقام در کنار هم یا بصورت ترتیبی مثل "۱۲۳۴۵۶"، "aaaa9999" یا "ABCDE".
- 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 صفحه‌کلید نگاه کند، خواهد توانست رمز عبور شما را بفهمد.
- رمز عبور هرچه که باشد باید بدون نوشتن آنرا بخاطر بسپارید. هرگز رمز عبور را جایی ننویسید و آنرا در محل کار یا روی برچسبهای عناوین قرار ندهید.
- هرگز فهرست رمزگذاری‌نشدهٔ رمزهای عبور را در فایلهای رایانه‌ای ذخیره نکنید.

بهترین رمز عبور، رشته‌ای 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 صفحه‌کلید نوشته شده باشد. مثالهایی از رمزهای عبور مناسب برای سیستمهایی که حروف، شماره‌ها، نشانه‌های خاص و جاهای خالی را می‌پذیرند و میان حروف کوچک و بزرگ تفاوت قائل می‌شوند ذیلاً ارائه شده‌اند. این رمزها بسادگی به خاطر سپرده می‌شوند، اما یافتن آنها در فرهنگهای لغات و یا حدس زدنشان بسیار دشوار می‌باشد.

رمز عبور	توضیحات
Computers Are Useful	عبارتی که بسیاری از کاربران رایانه با آن موافق هستند.
Computers aReuseFul	قرار دادن یک جای خالی مناسب و استفاده طنزآمیز از حروف بزرگ.
C0mputer5@ reus#fv1	رقم "0" بجای حرف "O"، "5" بجای "S"، "@" بجای "a"، "#" بجای "E"، "V" بجای "U"، و "1" بجای حرف "L"؛ در این مثال جای خالی وجود ندارد.
Comp9uter8sa re7usef6ul	عبارت اولیه بدون جای خالی و قراردادن شماره‌هایی بین هر ۴ حرف.
Comutrsa reusful	عبارت اولیه با چند حرف جا افتاده.

بخش دوم

Onupatithwa

در بسیاری از کشورهایی که سنّت قصه‌گویی وجود دارد اشکال استانداردی برای آغاز داستان وجود دارد. در زبان انگلیسی داستانهای کودکان معمولاً با عبارت Once upon a time, there was شروع می‌شوند. در این مثال از ابتدای هر لغت دو حرف گرفته شده تا طول کلمه عبور محدود شود و در عین حال قابل شناسایی نباشد.

oNup@T-1thuua

همان عبارت قبلی که در آن جایگزینی‌ها و علامتهای گفته‌شده بکار رفته است.

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 کرده‌اند که رمز عبور خود را در فواصل زمانی کوتاه تغییر دهید؛ اما عده‌ای معتقدند که اینکار باعث می‌شود رمزهای عبور ساده انتخاب شوند و یا برای جلوگیری از فراموش شدن در جایی نوشته شوند. برای کاربردهای معمولی نکات زیر توصیه می‌شوند:

- اگر فکر می‌کنید رمز عبورتان در معرض سرقت بوده سریعاً آنرا عوض کنید.
- اگر رمز عبورتان را به هر دلیلی به شخص دیگری داده‌اید بسرعت آنرا تغییر دهید. به اشتراک گذاشتن رمزهای عبور کار صحیحی نیست و باید از آن اجتناب کرد؛ مگر اینکه واقعاً چاره‌ای جز آن وجود نداشته باشد.
- رمزهای عبور را بصورت متناوب عوض کنید. معنی کلمهٔ "متناوب" از دیدگاه افراد مختلف، متفاوت است. شاید دوره‌هایی بین ۶ ماه تا یکسال به نظر مناسب باشند.
- اگر سیاست سازمانی شما در این مورد دقیقتر است از آن پیروی کنید.

امتیازات را محدود کنید

اکثر سیستمها به کاربران *امتیازات*[۲۶] محدودی ارائه می‌دهند که از امتیازات راهبر سیستم کمتر است. هنگامیکه راهبر و کاربر رایانه یکی باشند (نظیر بسیاری از رایانه‌های شخصی) کاربر کلیهٔ کارهای خود را با استفاده از امتیاز دسترسی کامل (*امتیازات ریشه*[۲۷] یا *امتیازات راهبر*[۲۸]) انجام می‌دهد؛ درحالیکه بهتر است برای فعالیتهای غیرراهبری از یک نام کاربری مجزا استفاده کند. اینکار احتمال خراب شدن ناخواستهٔ سیستم را کاهش می‌دهد و درصورت نفوذ مهاجم نیز از آسیب وارده به سیستم تا حد قابل توجهی می‌کاهد.

26 *Privilege*
27 *Root Privilege*
28 *Administrator Privilege*

فصل چهارم
امنیت سیستم‌عامل و نرم‌افزارهای کاربردی

کلیات

در این فصل به بررسی فنونی می‌پردازیم که از آنها برای کاهش آسیب‌پذیری سیستم‌عامل و نرم‌افزارهای کاربردی در برابر نفوذهای امنیتی استفاده می‌شود.

مقدمه

اصل اول: رایانه‌ها برنامه‌ها را اجرا می‌کنند.
اصل دوم: برنامه‌ها اشکال دارند.

اصل اول بدیهی است؛ و اصل دوم نیز با توجه به اینکه برنامه‌نویسان افراد بدون نقص نیستند کاملاً مورد انتظار است. معلوم نیست چرا این حجم زیاد از مسائل امنیتی مربوط به اشکالات برنامه‌نویسی هستند. هنگام توسعه برنامه براحتی می‌توان از بروز اشکالاتی نظیر *سرریز شدن بافر*[۲۹] جلوگیری کرد، اما با این وجود بنظر می‌رسد تقریباً نیمی از مشکلات جدی امنیتی از این دسته‌اند.

نرم‌افزارهای تجاری

یک نرم‌افزار تجاری معمولاً چگونه کار می‌کند؟

چند سال قبل هنگامیکه یک نرم‌افزار را می‌خریدید، تا زمان عرضهٔ نسخهٔ جدید آن به بازار هیچ به‌روزرسانی در آن اعمال نمی‌شد. امروزه بدلایل مختلف – بخصوص به دلیل مسائل امنیتی – بیشتر نرم‌افزارها بصورت منظم به‌روزرسانی می‌شوند. برای برخی از نرم‌افزارها مثل سیستم‌عاملها، "به‌روزرسانی منظم" به معنی انجام اینکار بصورت روزانه است[۳۰]. به‌روزرسانی اغلب محصولات معمولاً برای کاربران هزینه‌ای در بر ندارد.

بسیاری از شرکتهایی که نرم‌افزار تجاری ارائه می‌دهند برای رفع اشکالات و آسیب‌پذیریهای امنیتی نرم‌افزار، به‌روزرسانی‌های آنرا نیز ارائه می‌کنند. برای دریافت خدمات به‌روزرسانی فروشندگان بزرگ معمولاً می‌توانید به پایگاه وب آنها مراجعه کنید و از قسمت "Support" یا "Download" اصلاحات ارائه‌شده برای محصولات را بیابید.

وقتی به پایگاه وب فروشندهٔ نرم‌افزار مراجعه می‌کنید بسته‌های نرم‌افزاری و نسخه‌های مورد استفادهٔ خود را تعیین می‌نمایید و سپس پایگاه وب فهرستی از به‌روزرسانی‌های قابل دریافت را ارائه خواهد کرد. در برخی از موارد کاملاً مشخص است که به‌روزرسانی‌های ارائه‌شده برای رایانه شما قابل استفاده هستند، اما در بعضی موارد دیگر این مسئله وضوح کمتری دارد. وقتی شما به‌روزرسانی‌های مورد نظرتان را انتخاب کردید، آنها را download می‌کنید و در مرحلهٔ بعد آنها را نصب می‌نمایید. با توجه به نوع نرم‌افزار امکان دارد برنامه‌ای که download کرده‌اید بسادگی و در یک مرحله اجرا شود و یا اینکه برای نصب شدن نیازمند اجرای دستورالعملهای خاصی باشد. در برخی موارد بستهٔ نرم‌افزاری به‌روزرسانی بعد از download شدن تقریباً بصورت خودکار نصب می‌گردد.

در سالهای اخیر معمولاً از سه روش عمده برای ارائه خدمات به‌روزرسانی استفاده شده است:

۱. برای برنامه‌هایی نظیر Microsoft Windows، شرکت مایکروسافت بسته‌های به‌روزرسانی را از طریق پایگاه وب "Windows Update" منتشر می‌کند. یک برنامهٔ نرم‌افزاری رایانهٔ شما را بررسی کرده و فهرستی از به‌روزرسانی‌های مورد نیاز سیستم را ارائه می‌نماید، و آنگاه شما می‌توانید آنها را انتخاب، download و نصب کنید.

29 *Buffer Overflow*

۳۰ *در اکتبر ۲۰۰۳ و بدنبال یک مشکل امنیتی جدی در Microsoft Windows، مایکروسافت نتیجه‌گیری کرد که شاید غیر واقع‌بینانه و نامعمول باشد که توقع داشته باشد کاربران وصله‌های امنیتی را بطور هفتگی نصب کنند؛ و لذا از آن پس وصله‌ها را بصورت ماهانه منتشر می‌کند، مگر در حالتی که مشکل بسیار جدی و فوری باشد.*

۲. گاهی اوقات بستهٔ به‌روزرسانی که به روش فوق download می‌شود به‌روزرسانی واقعی نیست، بلکه برنامه‌ای است که در زمان اجرا به‌روزرسانی واقعی را download می‌کند. این برنامه ممکن است تنها ۵۰۰ کیلو بایت حجم داشته باشد – که اندازهٔ کوچکی برای بسته‌های به‌روزرسانی نرم‌افزار محسوب می‌شود؛ اما در حقیقت این فقط برنامه‌ای است که به‌روزرسانی واقعی را download می‌کند و سپس آنرا نصب می‌نماید؛ و به‌روزرسانی واقعی شاید اندازه‌ای در حدود ۳۰ مگا بایت داشته باشد.

۳. برخی از برنامه‌ها دارای توابع از پیش تعریف شده‌ای هستند که بصورت پویا به بررسی به‌روزرسانی‌های ارائه‌شده می‌پردازند و با اجازهٔ کاربر آنها را download و نصب می‌نمایند.

این قابلیتها برای آسانتر شدن کار شما طراحی شده‌اند. در کلیهٔ موارد وظیفهٔ انتخاب دقیق بسته‌های به‌روزرسانی مورد نیاز (که برای سیستم‌عامل و نرم‌افزارهای کاربردی خاص، کار پیچیده‌ای است) بوسیلهٔ برنامه‌ها و بصورت خودکار انجام می‌شود.

مشکل کشورهای درحال توسعه

همانطور که مشاهده می‌کنید بسیاری از فرآیندهای به‌روزرسانی برای اجرا در محیط متصل به اینترنت طراحی شده‌اند و بسته‌های به‌روزرسانی چندین مگابایتی را download می‌کنند. لذا استفاده از این روش تنها در صورتی نتیجه‌بخش خواهد بود که یک ارتباط پرسرعت اینترنتی داشته باشید و یا بتوانید ارتباط تلفنی خود را تا چندین ساعت برقرار نگه دارید. اما معمولاً در کشورهای درحال توسعه این امکان وجود ندارد.

دو روش برای مقابله با این مشکل موجود است:

۱. از خیر به‌روزرسانی نرم‌افزارهای کاربردی و سیستم‌عامل خود بگذرید.

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

در شرایطی که احتمال خطرات امنیتی درحال افزایش است راه اول منطقی بنظر نمی‌رسد. بنابراین تنها گزینهٔ مناسب download کردن و به‌اشتراک‌گذاشتن وصله‌ها و اصلاحهای downloadشده است.

چند راه برای انجام اینکار وجود دارد:

- اگر سازمانی دارای ماشینهای متعدد باشد، راهبر فنی باید مسئولیت download و نصب بسته‌های به‌روزرسانی آنرا بر عهده گیرد.
- کلوپهای رایانه‌ای یا گروههای دیگر می‌توانند بسته‌های به‌روزرسانی را download کنند و آنها را در اختیار اعضا قرار دهند.
- ارائه‌کنندگان خدمات اینترنتی (ISPها)[۳۱] می‌توانند بسته‌های به‌روزرسانی محصولات رایج و سیستم‌عاملهای مشترک را تهیه و بصورت محلی میان کاربران خود توزیع کنند. با اینکار نیازمندی ISPها به پهنای باند بین‌المللی کم می‌شود و لذا هزینهٔ آنها نیز کاهش می‌یابد.
- فروشگاههای رایانه‌ای می‌توانند بسته‌های به‌روزرسانی را در اختیار مشتریان خود قرار دهند.
- در سال ۲۰۰۳ هنگامیکه یک کرم اینترنتی باعث آسیب‌پذیری رایانه‌ها شد، مایکروسافت در کشورهای مختلف برای مقابله با آن اقدام به توزیع بسته‌های به‌روزرسانی بر روی دیسکهای فشرده اقدام کرد. استفاده از این روش همچنان هم می‌تواند ادامه یابد.

هرچند سه شیوهٔ اخیر توزیع بسته‌های به‌روزرسانی چندان رایج نیستند، اما با توجه به افزایش نیاز برای به‌روز نگهداشتن نرم‌افزارها می‌توانند به یک استراتژی مؤثر تجاری برای ISPها و فروشندگان در کشورهای درحال توسعه تبدیل شوند. اگرچه از این استراتژیهای پشتیبانی استقبال می‌شود، اما کاربران باید مطمئن شوند که منابع به‌روزرسانی‌های محلی نیز قابل اطمینان هستند. اگر منابع محلی قابل اطمینان نباشند ممکن است به مرکزی برای توزیع ویروسها و تراواها تبدیل شوند.

31 *Internet Service Providers*

آیا بسته‌های به‌روزرسانی 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 سریعاً بسته‌های به‌روزرسانی را نصب کنید، خود را در مقابل آسیبهای شناخته‌شده ایمن کرده‌اید. با استفاده از ایمنی حاصل از بسته‌های به‌روزرسانی، تا سطحی که سیستم اجازه می‌دهد می‌توانید از خود در برابر نفوذ و افشای اطلاعات محافظت نمایید.

مخالفان: امکان دارد برنامه‌نویسان هنگام برنامه‌نویسی دچار اشتباه شوند یا بخش دیگری از برنامه را مختل نمایند. همچنین ممکن است در بسته‌های به‌روزرسانی به اندازهٔ برنامه‌های اصلی اشکال و آسیب‌پذیری وجود داشته باشد. لذا این احتمال وجود دارد که بستهٔ به‌روزرسانی مشکلات جدیدی را بوجود بیاورد که به مشکل قبلی ارتباطی نداشته باشد.

انتشار هر از چندگاه نقایص امنیتی کشف‌شده که با استفاده از آنها مهاجمان به سیستم نفوذ کرده و داده‌ها را تخریب می‌کنند دامنهٔ این مسئله را تغییر داده است. هنگامیکه یک نقص امنیتی اعلام می‌شود – حتی اگر این اعلام توسط یک وصلهٔ امنیتی صورت پذیرد – مهاجمان سریعاً ابزارهایی برای سوء استفاده از آن نقص را بوجود می‌آورند، و درنتیجه ممکن است سیستم رایانهٔ افرادی که از وصله‌های امنیتی منتشرشده استفاده نمی‌کنند سریعاً مورد تهاجم قرار گیرد.

پیشنهاد عملی:

- کاربران مبتدی و افرادی که رایانه‌هایشان برای کارهای غیرحساس استفاده می‌شود باید کلیهٔ بسته‌های به‌روزرسانی را بلافاصله بعد از انتشار بکار گیرند. برای رایانه‌ای که به‌روزرسانی نشده، خطر مشکلات جدید حاصل از بسته‌های به‌روزرسانی به مراتب کمتر از خطرات آسیب‌پذیریهای به‌روزرسانی‌نشده است.
- کاربران حرفه‌ای و کارکنان بخش فنی باید بسته‌های به‌روزرسانی امنیتی را سریعاً نصب کنند، اما می‌توانند بقیهٔ بسته‌های به‌روزرسانی را با توجه به نوع عملکرد آنها اولویت‌بندی نمایند. تأخیر چند هفته‌ای یا چند ماهه در نصب این بسته‌ها به کاربران ماجراجو اجازه می‌دهد بسته‌های به‌روزرسانی را نصب کنند، مشکلات احتمالی را کشف و گزارش نمایند، و با اینکار – پیش از اینکه شما به‌روزرسانی‌ها را نصب کرده باشید – به تولیدکننده فرصت اصلاح نقایص جدید را بدهند.

هرگز نمی‌توان گفت که تغییرات چه زمانی می‌توانند یک نرم‌افزار کاربردی را از روند صحیح اجرا خارج کنند. به همین دلیل اگر از رایانهٔ شما در فعالیتهای حساس تجاری استفاده می‌شود، بهترین راهکار این است که پیش از اعمال به‌روزرسانی‌های جدید، ابتدا تغییرات را روی یک دستگاه مشابه و نه‌چندان حیاتی آزمایش کنید.

نرم‌افزارهای غیرسنتی و غیرتجاری

در بحث قبل بر محصولات تجاری شامل سیستم‌عاملها و برنامه‌های کاربردی عمده متمرکز شدیم که در بسیاری از محیطهای محاسباتی مرسوم هستند. اما در نرم‌افزارهای دیگر شرایط چه تغییراتی می‌کنند؟

نرم‌افزارهای تجاری کوچک

نرم‌افزارهای زیادی وجود دارند که بصورت رایگان یا با حداقل هزینه در اختیار عموم قرار می‌گیرند. سطح پشتیبانی فروشندگان این نرم‌افزارها تفاوتهای بسیاری دارد. بطور کلی استفادهٔ متناوب از بسته‌های به‌روزرسانی رایگان و یا کم‌هزینه کاملاً توصیه می‌شود. این برنامه‌ها معمولاً ضعفهای امنیتی ندارند، بلکه برای حل مشکلات غیرامنیتی و یا افزودن قابلیتهای جدید طراحی شده‌اند. با اینحال برخی از نرم‌افزارهای رایگان نظیر *دیوارهٔ آتش*[۳۲] و یا *ویروس‌یاب*[۳۳] در حیطهٔ بررسی ما هستند و در این کتاب در مورد آنها بحث خواهد شد.

اگر از برنامه‌هایی استفاده می‌کنید که دارای کارکردهای امنیتی هستند، اطمینان حاصل کنید که سیاست فروشنده در ارائه به‌روزرسانی را درک کرده‌اید. مسلماً نمی‌خواهید در موقعیتی قرار بگیرید که از یک نرم‌افزار حساس به امنیت

32 *Firewall*
33 *Virus Scanner*

استفاده کنید و ناگهان خدمات پشتیبانی ارائه به‌روزرسانی آن قطع شود و یا توانایی خرید آنرا نداشته باشید. استفاده از برخی نرم‌افزارها مانند ویروس‌یابها اگر بطور منظم (روزانه یا هفتگی) به‌روزرسانی نشوند، می‌تواند بسیار خطرناکتر از حالتی باشد که از آنها استفاده نمی‌شود؛ زیرا اگر از آن استفاده نمایید تصور می‌کنید از شرایط امنیتی مناسبی برخوردارید.

نرم‌افزارهای متن‌باز[۳۴]

نرم‌افزارهای متن‌بازی که بسرعت درحال گسترش هستند باید بصورت مناسبی مورد پشتیبانی قرار داشته باشند. در برخی موارد با اینکه نرم‌افزار اصلی بصورت رایگان عرضه می‌شود اما امکان دارد خدمات ارائه به‌روزرسانی یا پشتیبانی آن هزینه‌بر باشد. نسخهٔ رایگان Red Hat Linux که در دسترس عموم قرار می‌گیرد نمونهٔ خوبی از این قبیل نرم‌افزارها است. سازمانهایی که خواهان سطح بیشتری از پشتیبانی فنی هستند ممکن است بستهٔ نرم‌افزاری اصلی و یا حداقل خدمات پشتیبانی آنرا خریداری کنند. اگر تصمیم به استفاده از نرم‌افزارهایی دارید که خرید و پشتیبانی آنها رایگان است (مثل بعضی از نرم‌افزارهای آزاد و متن‌باز) توجه داشته‌باشید که مدت‌زمان در دسترس بودن نسخه‌های اصلاحی آنها ممکن است کوتاه باشد. بنابراین اگر سیستم‌عامل یا زیرسیستمهای مهم خود را از نوع نرم‌افزارهای بدون پشتیبانی انتخاب کرده‌اید باید نسخهٔ جدید آنرا هر چند وقت یکبار (مثلاً در هر شش ماه) به‌روزرسانی کنید.

روند به‌روزرسانی محصولات متن‌باز بسیار مشکلتر از به‌روزرسانی محصولاتی مثل Microsoft Windows است؛ اما با وجود دستورالعملهای نصب برای محصولات اصلی متن‌باز این مشکل هم برطرف می‌شود. نرم‌افزارهای متن‌باز مبتنی بر Windows نیز وجود دارند که بصورت کامپایل‌شده توزیع می‌شوند و از نصب‌کننده‌های ساده استفاده می‌کنند.

همانند سیستمهای Windows، بسته‌های به‌روزرسانی و وصله‌های ارائه‌شده برای سیستمهای متن‌باز بزرگ، بسته به اندازهٔ سیستمهای متن‌باز تغییر می‌کنند. شناسایی منابع محلی این بسته‌های به‌روزرسانی بمنظور کاهش زمان download آنها از اینترنت برای کاربران منفرد بسیار حائز اهمیت است.

آخرین نکته مربوط به نرم‌افزار متن‌باز کمی بحث می‌طلبد. مباحثه‌ای میان طرفداران نرم‌افزار متن‌باز و طرفداران نرم‌افزارهای انحصاری سنتی وجود دارد که بالاخره کدامیک از این محصولات ایمن‌تر هستند.

طرفداران نرم‌افزارهای انحصاری معتقدند:

- از آنجا که متن برنامهٔ محصولات متن‌باز در دسترس است، نفوذگران به سادگی می‌توانند برنامه را تجزیه و تحلیل کنند و تمامی اشکالاتی که از طریق آنها می‌توان به سیستم نفوذ کرد را شناسایی نمایند.
- چون افراد زیادی در مناطق مختلف و بدون روابط سازمانی ممکن است روی محصولات متن‌باز کار کنند، ممکن است استانداردها نادیده گرفته شوند و فقدان یکپارچگی در اجزای مختلف منجر به آسیب‌پذیریهای امنیتی گردد.
- به این دلیل که کاربران برای محصولات انحصاری به تولیدکننده وجه می‌پردازند، دستورات او را دنبال می‌کنند و انجام اینکار باعث می‌شود کیفیت ملاحظات امنیتی در نرم‌افزارهای انحصاری بالا باشد.
- از آنجا که هیچ منبع معینی مسئولیتی در قبال محصولات متن‌باز بر عهده ندارد، درصورتیکه امنیت برای توسعه‌دهندگان انفرادی اهمیت نداشته باشد، احتمال زیادی وجود خواهد داشت که نادیده گرفته شود.

طرفداران نرم‌افزارهای متن‌باز معتقدند:

- به دلیل اینکه افراد زیادی با متن برنامه نرم‌افزارها کار می‌کنند، مسائل و مشکلات آنها توسط افراد خبره تشخیص داده می‌شود و سریعاً اصلاح می‌گردد.
- افرادی که با محصولات انحصاری کار می‌کنند ممکن است کد یکپارچه‌ای را تولید کنند؛ اما اگر تولیدکننده برای امنیت محصول خود ارزش خاصی قائل نشده باشد برنامه نمی‌تواند از سطح ایمنی مطلوبی برخوردار باشد.
- در برنامه‌های انحصاری برای اصلاح مشکلات موجود همیشه باید به تولیدکنندهٔ محصول مراجعه کرد و این امر ممکن است باعث تأخیر زمانی زیادی شود.

34 *Open Source Software*

در واقع هریک از این دلایل در جایگاه خود صحیح هستند. راهی برای کسب اطمینان از ایمن بودن نرم‌افزار انحصاری یا نرم‌افزار متن‌باز وجود ندارد. همچنین نمی‌توان ادعا کرد که کشف و اصلاح مشکلات بوجود آمده در زمان مناسب صورت می‌گیرد یا خیر. در هر دو نوع نرم‌افزار، نمونه‌هایی از رفتار ایده‌آل و همچنین بی‌دقتی طراحان و سازمانهای ارائه خدمات پشتیبانی دیده شده است.

نرم‌افزارهای مسروقه[۳۵]

نه نویسندگان و نه ناشران این کتاب هیچکدام مروج سرقت نرم‌افزاری نیستند، اما ساده‌انگارانه است اگر وانمود کنیم چنین مسئله‌ای وجود ندارد. سرقت نرم‌افزار مشکلی است که در سراسر دنیا وجود دارد، ولی بیشتر در کشورهایی اتفاق می‌افتد که در آنها هزینهٔ نسبی تهیه نرم‌افزارهای قانونی در مقایسه با دستمزدها بسیار بیشتر از کشورهای توسعه‌یافته است – که در آنها دوایر قوانین محلی و نیروهای انتظامی با همکاری هم انجام تخلفات را بسیار غیر محتمل می‌سازند.

گذشته از وظیفهٔ قانونی مسئولین برای جلوگیری از خدشه‌دار شدن حقوق مالکیت سازندهٔ محصول، دو نکته در مورد امنیت نرم‌افزار مسروقه وجود دارد که باید مورد بررسی قرار گیرند. هیچکدام از این دو مورد در نرم‌افزارهای مسروقه چندان رایج نیستند، اما به هر حال این امکان وجود دارد که هر دو با هم نیز وجود داشته باشند.

۱. ممکن است نرم‌افزار مسروقه قابل به‌روزرسانی شدن نباشد یا انجام به‌روزرسانی آنرا از کار بیندازد.

۲. امکان دارد برخی از نرم‌افزارهای مسروقه حاوی کارکردهایی باشند که انتظار آنها را ندارید. این کارکردها ممکن است شامل دربهای مخفی، ثبت‌کننده‌های صفحه‌کلید، یا سایر انواع نرم‌افزارهای مخرب باشند.

35 *Pirated Software*

فصل پنجم
نرم‌افزارهای مخرب

کلیات

در این فصل مفهوم و انواع مختلف نرم‌افزارهای مخرب (نظیر ویروسها، کرم‌های اینترنتی، و تراواها) و مکانیزمهایی که برای توزیع آنها استفاده می‌شود مورد مطالعه قرار می‌گیرد.

مقدمه

نرم‌افزار مخرب[۳۶]

علامت اختصاری نرم‌افزارهای مخرب *بدافزار*[۳۷] است. این نرم‌افزارها معمولاً برای آسیب رساندن یا خراب‌کردن سیستم طراحی می‌شوند.

اولین ویروس رایانه‌ای در سال ۱۹۸۱ شناسایی شد. مفهوم *کرم رایانه‌ای*[۳۸] در کتاب "Science Fiction" در سال ۱۹۷۵ معرفی شد و اولین فعالیت واقعی آن مربوط به اوایل دهۀ ۱۹۸۰ است. جالب است بدانید که این کرمها اولین بار برای این طراحی شدند که عملکرد مثبت و مفید داشته باشند. پیدایش *اسبهای تراوای رایانه‌ای*[۳۹] هم به اولین روزهای اشتراک زمانی (دهۀ ۱۹۶۰) باز می‌گردد. علیرغم تاریخ و سابقۀ طولانی این نرم‌افزارها، در سالهای اخیر است که تأثیرات مخرب آنها برای کاربران عادی شدید و خطرناک شده است.

در آغاز باید معنا و مفهوم این اصطلاحات را تعریف کنیم.

ویروس ویروس برنامه‌ای است که به انتهای برنامۀ دیگر متصل می‌شود و یا وارد بدنۀ یک برنامۀ دیگر می‌گردد. وقتی آن برنامه به اجرا در می‌آید، ویروس نیز اجرا می‌شود و نسخه‌های خود را وارد فایلها یا دیسکهای دیگر می‌کند و بدینصورت خود را تکرار می‌نماید، و هنگامیکه هریک از فایلها یا برنامه‌های آلوده اجرا می‌شوند این روند بار دیگر تکرار می‌گردد. ویروس ممکن است علاوه بر این موارد کارهای دیگری نیز انجام دهد.

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

اسب تراوا نام این نوع نرم‌افزار از افسانۀ جنگ شهر تراوا در یونان برگرفته شده است. در آن افسانه، یونانی‌ها یک اسب چوبی بزرگ را از دروازۀ شهر به داخل می‌فرستند و هنگامیکه اسب وارد شهر می‌شود تعداد زیادی سرباز یونانی از آن خارج می‌شوند و شهر را به تصرف خود در می‌آورند. از آن زمان به بعد "اسب تراوا" به معنای چیزی است که ظاهری عادی اما محتویاتی خطرناک دارد.
در مفاهیم رایانه‌ای، اسب تراوا می‌تواند خرابیهای زیادی به بار آورد و یا اعمالی غیر از آنچه که کاربر انتظار آنرا دارد انجام دهد. این اصطلاح در سالهای اخیر به برنامه‌های مخربی اطلاق می‌شود که معمولاً بدون اطلاع و اجازۀ کاربر وارد سیستم می‌شوند و به جمع‌آوری و ارسال اطلاعات می‌پردازند.

36 *Malicious Software*
37 *Malware*
38 *Computer Worms*
39 *Computer Trojan Horses*

نرم‌افزار "Bonus"

نرم‌افزار bonus نرم‌افزاری است که بدون آگاهی شما حاوی بسته‌های دیگر نرم‌افزاری در آن وجود دارد. قرار گرفتن بسته‌های دیگر در یک نرم‌افزار تجاری مرسوم است. بعنوان مثال اگر یک مرورگر وب نصب کنید ممکن است شامل برنامه‌هایی چون Adobe Acrobat یا نرم‌افزارهای چندرسانه‌ای باشد. این امر به این علت است که معمولاً با اینکار کارایی نرم‌افزار اصلی افزایش می‌یابد و روند فعالیت نیز معمولاً بدین ترتیب است که درصورت تمایل شما آن نرم‌افزارهای جانبی را نصب می‌کند یا اینکه در آغاز نصب آن برنامه‌ها شما را از انجام اینکار آگاه می‌سازد. عملکرد نرم‌افزارهای bonus معمولاً متفاوت از نرم‌افزار اصلی است و اگر چاره‌ای داشته باشید مسلماً نباید آنها را نصب کنید.

قابلیتهای تراوا، ویروس و کرم برای یک برنامه "انحصاری" نیستند. به عبارت دیگر مهاجمین می‌توانند بدافزاری با بیش از یک ویژگی بنویسند؛ مانند *تراوای خود تکرار شونده*[40]. بدافزاری که دارای بیش از یک خصوصیت مخرب است *تهدید چندوجهی*[41] نامیده می‌شود. همانطور که مشاهده می‌کنید این عناوین عموماً از روی نحوهٔ گسترش نرم‌افزارهای مخرب تعریف شده‌اند و نه با توجه به نحوهٔ عملکرد آنها. در این فصل چگونگی عملکرد این نرم‌افزارها و راههای انتشار آنها بررسی می‌شود. در فصلهای بعد نیز روشهای ایمن ساختن رایانه‌ها و شبکه‌ها در برابر این نرم‌افزارها مورد بحث قرار می‌گیرد.

عملکرد نرم‌افزارهای مخرب

هیچ محدودیتی در چگونگی فعالیت نرم‌افزارهای مخرب روی رایانه شما وجود ندارد، اما معمولاً این برنامه‌ها در فعالیتهای خود واجد ویژگیهای مشترکی هستند:

40 *Self-Replicating Trojan*
41 *Blended Threat*

ارسال نامهٔ الکترونیکی

ارسال نامهٔ الکترونیکی یکی از رایجترین عملکردهای برنامه‌های مخرب است. نامه الکترونیکی ممکن است *ضمیمه‌ای*[42] شامل ویروس یا کرم داشته باشد. *متن*[43] آن نیز می‌تواند در مورد اطلاعات خاصی تنظیم شده باشد (نظیر هشدارهای مایکروسافت در مورد یک مشکل امنیتی) یا حتی می‌تواند دارای یک قسمت تصادفی از نامه‌های الکترونیکی پیشین شما باشد که در رایانه موجود است. اگر ضمیمهٔ نامه فایل خطرناکی باشد، معمولاً متن آن به نحوی دریافت‌کننده را تشویق می‌نماید که ضمیمه را باز کند. فیلدهای *موضوع*[44] و *فرستنده*[45] نیز معمولاً بگونه‌ای تنظیم می‌شوند که کاربر را تشویق کنند که فایل ضمیمه را باز کند (مثل کرم مشهوری که موضوع آن "I Love You" بود). این نوع پیامها معمولاً برای افرادی ارسال می‌شوند که آدرس آنها در فهرست آدرسها یا فایلهای دیگر رایانهٔ آلوده وجود دارد. گاهی اوقات وقتی پیامها برای همهٔ این افراد ارسال شد برنامه متوقف می‌گردد، و گاهی اوقات باز هم فعالیت خود را – چه از رایانهٔ اولیه و چه از مبادی جدید – از سر می‌گیرد. توجه داشته باشید که اگر رایانهٔ فرد دیگری با ویروس یا کرم آلوده شده باشد و آن ویروس آدرس شما را در فیلد "فرستنده" نامهٔ الکترونیکی آلوده گذاشته باشد (شاید به این دلیل که آدرس شما را در ماشین آلوده یافته است) این شما هستید که متهم به توزیع این ویروس خواهید شد! (این فن *گمراه‌کنندگی نامهٔ الکترونیکی*[46] نام دارد و درصورت استفادهٔ برنامهٔ مخرب از آن، بسادگی نمی‌توان مشخص کرد که رایانهٔ آلودهٔ واقعی متعلق به چه کسی است)

جمع‌آوری اطلاعات

نرم‌افزار مخرب می‌تواند اطلاعاتی در مورد رایانهٔ شما و فایلهای موجود در آن بدست آورد و این اطلاعات را در اختیار نویسندهٔ خود قرار دهد. این برنامه می‌تواند همهٔ فایلهای رایانه شما (حتی فایلهای رمزگذاری‌شده) را بخواند. اگر اطلاعات حساب بانکی یا کارتهای اعتباری خود را در رایانه ذخیره می‌کنید ممکن است این داده‌ها مورد علاقهٔ نفوذگران باشند. اگر از امضای خود در رایانه تصویری تهیه کرده باشید تا از

42 *Attachment*
43 *Body*
44 *Subject Field*
45 *From Field*
46 *Email Spoofing*

آن در چاپ و یا ارسال نامه‌ها استفاده کنید، آن هم ممکن است بکار مهاجمان بیاید. جمع‌آوری این بسته‌های اطلاعاتی در کنار هم می‌تواند برای مهاجم این امکان را بوجود آورد که بتواند از هویت شما سوء استفاده کند. اگر در یک شرکت تجاری کار می‌کنید که شماره‌های کارت اعتباری افراد دیگر را روی رایانهٔ خود ذخیره می‌نمایید، درصورت دزدیده شدن این شماره‌ها مشکلات جدی برایتان پیش خواهد آمد.

بازنویسی یا حذف داده‌ها

برخی از نرم‌افزارهای مخرب واقعاً آسیب‌رسان هستند؛ به این ترتیب که با وارد کردن داده به رایانهٔ شما بسرعت می‌توانند فایلهای موجود در دیسک سخت را پاک کنند یا آنها را با اطلاعات نادرست بازنویسی نمایند. این برنامه‌ها گاهی اوقات با روشهایی که احتمال شناسایی کمتری دارند تغییرات گفته‌شده را بوجود می‌آورند:

نصب یک تروا

این عملکرد در نرم‌افزارهای مخرب بسیار رایج شده است. روی رایانه شما معمولاً برنامه‌هایی نصب شده و لذا برنامهٔ مخرب می‌تواند با برنامه‌ای که شما یا سیستم‌عامل از آن استفادهٔ زیادی می‌کنید جایگزین شود (معنای اصلی تراوا). از این گذشته ممکن است برنامه‌های دیگری را وارد سیستم کند که در یک زمان از پیش تعیین شده یا هنگام روشن شدن رایانه به اجرا در آیند. در بخش "نرم‌افزارهای سربار" بسیاری از این روشها توضیح داده شده‌اند.

زمانبندی برای آینده

هریک از عملکردهای گفته شده ممکن است بلافاصله اتفاق بیفتند و یا برای وقوع در آینده برنامه‌ریزی شوند. برای مثال ممکن است نویسندگان نرم‌افزارهای مخرب علاقه‌مند باشند که اعلام شود یک کرم خاص در روزهای اولیهٔ ژانویهٔ سال ۲۰۰۰ یک خرابی بزرگ به بار آورد.

نرم‌افزارهای سربار[47]

نرم‌افزار مخرب معمولاً به شکل برنامه‌ای ظاهر می‌شود که روی رایانهٔ شما می‌نشیند و زمانی‌که رایانهٔ خود را روشن یا برنامهٔ خاصی را آغاز می‌کنید به اجرا در می‌آید. تنها محدودیتی که عملکرد این برنامه‌ها می‌تواند داشته باشد تصورات و مهارت پدیدآورندهٔ آنها است.

نرم‌افزار ردیابی و اعمال تغییر در شبکه[48]

این دسته از برنامه‌ها پایگاههایی که شما مشاهده می‌کنید را نظاره می‌کنند و می‌توانند علاوه بر آنچه که شما در حالت معمول مشاهده می‌کنید صفحات دیگری را به نمایش درآورند. همچنین می‌توانند آنچه که در پایگاه وب است را با تبلیغات خود جایگزین نمایند، و اطلاعاتی در مورد رایانهٔ شما و تعاملاتی که با تولیدکنندهٔ آن انجام داده‌اید برای پدیدآورندهٔ خود بفرستند. این نرم‌افزارها در بسیاری از موارد دارای کنترل کامل بر روی مرورگر شما هستند: آنچه وارد می‌کنید را نظاره می‌کنند و می‌توانند آنچه که می‌بینید را تغییر دهند؛ و هنگامیکه مشاهدات شما را تحت نظر دارند می‌توانند فعالیتهای شما را به یک مقصد از پیش تعیین‌شده گزارش دهند. در Internet Explorer، این قابلیت طراحی شده و *BHO*[49] نام دارد. اگرچه کاربر می‌تواند BHOهای سالم و بسیار مفیدی را پدید آورد، اما این قابلیت برای ایجاد برنامه‌های کاربردی که اخلاقیات در آنها کمتر رعایت شده نیز امکانات قابل توجهی بوجود آورده است.

دربهای مخفی[50]

معمولاً برای دسترسی به یک سیستم رایانه‌ای نیاز به وارد کردن نام کاربری و رمز عبور دارید؛ اگرچه این سطح از امنیت گاهی اوقات برای سیستمهایی که از لحاظ فیزیکی ایمن هستند و تنها اشخاص خاصی می‌توانند از پشت صفحه‌کلید آنها وارد سیستم شوند وجود ندارد. نرم‌افزار "درب مخفی" با بی‌اثر کردن کلیهٔ حفاظهای امنیتی اینچنینی به *کاربر راه دور*[51] اجازهٔ دسترسی به رایانهٔ شما را می‌دهد. این نرم‌افزار حتی ممکن است حفاظهای امنیتی خود را کار بگذارد تا تنها پدیدآورندهٔ آن بتواند از سیستم استفاده نماید. اگرچه این جزئیات از یک مورد تا مورد دیگر متفاوت است، اما

47 *Payload Software*

48 *Web Tracking/Modification Software*
49 *Browser Helper Object - http://msdn.microsoft.com/library/enus/dnwebgen/html/bho.asp*
50 *Backdoors*
51 *Remote User*

کاربر راه دور ممکن است روی سیستم شما کنترل کامل پیدا کرده باشد. حتی ممکن است این نرم‌افزارها اگر بخواهند، بتوانند شما را از ادامهٔ کارتان بازدارند. در اینحالت رایانهٔ شما تحت فرمان شخص دیگری قرار دارد و شما از این مسئله آگاهی ندارید. اما سؤالی که پیش می‌آید این است که چرا مهاجم مایل است کنترل سیستم شما را در دست بگیرد؟ انجام اینکار می‌تواند دلایل متعددی داشته باشد، از جمله اینکه:

- هیچ دلیلی غیر از اثبات توانایی خود به دوستانش برای انجام این کار وجود نداشته باشد؛
- بطور کلی بخواهد تخریبگر باشد؛
- برای هدف قرار دادن شما دلیل شخصی داشته باشد؛
- از رایانهٔ شما برای فعالیتهای مخرب دیگر استفاده کند؛ مثل فرستادن هرزنامه یا انجام حملهٔ *تخریب سرویس* (DoS)[52] علیه رایانه‌های دیگر؛ و یا اینکه
- بخواهد اطلاعات با ارزشی را به سرقت ببرد.

توجه داشته باشید نرم‌افزارهایی با کاربرد مشابه تحت عناوینی چون *ابزارهای دسترسی راه دور*[53] یا *ابزارهای راهبری راه دور*[54] برنامه‌های مشروع و بسیار و پراستفاده‌ای هستند. اگر از این ابزارها برای اهداف کاری خود استفاده می‌کنید مطمئن شوید که ملاحظات مناسب امنیتی مانند نام کاربری و رمزهای عبور را بکار گرفته‌اید.

ثبت‌کننده‌های کلید[55]

مفهوم "ثبت‌کننده کلید" از نام آن مشخص است. آنها تمامی کلیدهای فشرده شدهٔ صفحه‌کلید را ثبت و در یک فایل ذخیره می‌کنند. این فایل می‌تواند در آینده با دسترسی از طریق درب مخفی مورد استفاده قرار بگیرد و یا از طریق پست الکترونیکی یا وب برای نویسندهٔ برنامه ارسال گردد.

شایان ذکر است که ثبت‌کننده کلید تمامی آنچه که واقعاً تایپ می‌کنید را نظاره می‌کند و نه آنچه که از طریق شبکه ارسال می‌شود. بنابراین حتی اگر شمارهٔ کارت اعتباری را روی صفحهٔ وب ایمن وارد کنید (یعنی اگر هنگام انتقال اطلاعات از رمزنگاری استفاده شود)، این برنامه دقیقاً آنچه که تایپ می‌کنید را – بصورت رمزگذاری نشده – ثبت می‌نماید.

سرقت مالی

در اکثر سرقتهایی که درنتیجهٔ حملات به رایانه‌های شخصی اتفاق افتاده‌اند، از رایانهٔ قربانی سرقت اطلاعات صورت گرفته است. با اینحال مواردی وجود دارند که در آنها با استفاده از برنامه‌های سربار، پول مسروقه بصورت خودکار به مصرف رسیده است. ساده‌ترین مثال این است که برنامه، یک مودم را روی رایانهٔ شما شناسایی کند و از آن برای برقراری تماس با مقاصد دوردست استفاده نماید. از آنجا که برنامه نمی‌تواند صحبت کند انجام اینکار برای مهاجم هیچ مزیتی ندارد، بجز نوعی احساس رضایت شیطانی مبنی بر اینکه شما در پایان ماه یک صورتحساب سنگین از شرکت مخابرات دریافت می‌کنید.

در موارد دیگر مهاجم می‌تواند از انجام اینکار بهرهٔ شخصی ببرد. در بسیاری از کشورها ممکن است شماره تلفن خاصی وجود داشته باشد که وقتی با آن تماس گرفته می‌شود شرکت مخابرات در هر دقیقه هزینهٔ بیشتری برای تماس‌گیرنده ثبت کند و در عوض مقداری از این هزینه به حساب کسی برود که با او تماس حاصل شده است. این امر در انواع مختلف معاملات مورد استفاده قرار می‌گیرد، اما بیشتر مورد استفادهٔ شرکتهای نرم‌افزاری است که خواهان راه ساده‌ای هستند تا برای پشتیبانی بدون ضمانت هزینه‌ای را از حساب شما کسر نمایند. در چنین وضعیتی شرکت مخابرات هزینه‌های تماس‌گیرنده‌ها را بگونه‌ای محاسبه می‌کند که بتواند قسمتی از آنرا بعنوان هزینهٔ تماسهای پشتیبانی به شرکتی که با آن تماس حاصل شده است ارسال کند. اگر نفوذگر چنین شماره‌ای داشته‌باشد می‌تواند رایانهٔ شما را طوری برنامه‌ریزی کند که با این شماره تماس بگیرد و برای مدتی تماس را برقرار نگهدارد. در آنصورت این هزینه در صورتحساب پایان ماه تلفن شما درج خواهد شد.

این نرم‌افزارها چگونه شناسایی می‌شوند؟

چند سال قبل تنها راه آلوده شدن رایانه‌های شخصی بوسیلهٔ ویروس یا نرم‌افزارهای مخرب، استفاده از دیسکهای آلوده

52 *Denial of Service Attack*
53 *Remote Access Tools*
54 *Remote Administration Tools*
55 *Keyloggers*

بود و اگر با افرادی که آلوده شده بودند تبادل فایل انجام نمی‌دادید در امنیت به سر می‌بردید. سیستمهای UNIX چندان مستعد دریافت ویروس نبودند اما به دلیل قابلیتهای بسیار زیاد برقراری ارتباط و همچنین اشکالات امنیتی در سیستم‌عاملها و برخی از نرم‌افزارهای کاربردی رایج، حتی در آن روزها هم گاهی اوقات نفوذگران می‌توانستند به سیستمها دستیابی پیدا کنند و روی آنها نرم‌افزارهای درب مخفی نصب نمایند. اولین حادثهٔ جدی امنیتی اینترنت کرمی بود که در سال ۱۹۸۸ به یک سیستم UNIX حمله کرد. امروز ممکن است شما به روشهای متفاوتی مورد حمله قرار بگیرید. روشهایی که در ادامه ذکر شده‌اند مربوط به سیستمهای مبتنی بر Windows می‌شوند. سیستمهای Macintosh و Unix به نوعی نسبت به این حمله‌ها کمتر مستعد هستند؛ البته نه الزاماً به این علت که ایمن‌تر هستند، بلکه به این دلیل که معمولاً سیستمهای Windows برای مهاجمین اهداف جذاب‌تری به شمار می‌روند. سیستمهای Unix در ردهٔ بعدی قرار دارند و سیستمهای Macintosh تا به امروز کمترین صدمه را از آسیب‌پذیریهای خود دیده‌اند.

نامهٔ الکترونیکی

چند سال قبل میان کاربران پست الکترونیکی شایعاتی گسترش یافت مبنی بر اینکه با دریافت نامهٔ الکترونیکی ممکن است به ویروس آلوده شوید. مدیران و مسئولان سیستم مجبور بودند مداوماً به کاربران اطمینان دهند که این امر "غیر ممکن" است، و تا زمانیکه فایل ضمیمه به اجرا در نیاید، ماشین و کاربران آن در امنیت کامل هستند.

آلوده شدن از طریق نامهٔ الکترونیکی امروز دیگر امر محالی نیست و درواقع بسیار هم محتمل است. دو قابلیت اضافه‌شده به نرم‌افزارهای پست الکترونیکی باعث این مسئله شده‌اند.

اولین تغییر این است که امروزه برنامه‌هایی برای پست الکترونیکی وجود دارند که می‌توانند ضمایم را بصورت خودکار اجرا نمایند. در گذشته کاربر فایل ضمیمه را ذخیره و سپس آنرا اجرا می‌کرد، اما درحال حاضر اجرای خودکار ضمائم کارها را – مخصوصاً برای کاربران مبتدی که می‌خواهند بدون انجام عملیات اضافه آنچه که فرستاده شده است را ببینند – ساده‌تر کرده است.

دومین تغییر این است که چون تلاش بر این بوده که نرم‌افزار پست الکترونیکی ساده و قوی‌تر گردد، امروز امکان برنامه‌نویسی HTML در بدنهٔ اصلی نامهٔ الکترونیکی وجود دارد؛ علیرغم اینکه HTML می‌تواند حاوی دستورالعملهای مشکلساز باشد. بعنوان مثال HTML می‌تواند مرورگر وب را بصورت خودکار به سمت یک پایگاه وبِ از پیش تعیین‌شده هدایت کند که شاید برای شما یا فرزندانتان مناسب نباشد.

توجه داشته باشید افرادی که نامه‌های الکترونیکی اینچنینی ارسال می‌کنند می‌توانند بسیار خلاق باشند. اخیراً تعدادی نامهٔ الکترونیکی آلوده به ویروس منتشر شد که ادعا می‌کرد از طرف مایکروسافت است و حاوی آخرین وصله‌های امنیتی می‌باشد که در برابر ویروسها و کرمها از شما محافظت می‌نماید. این نامه‌ها شامل تصاویر و نمادهایی هستند که قابل اطمینان و معتبر بنظر می‌رسند و لذا کاربر را متقاعد می‌سازند که ضمایم باید به سرعت به اجرا در بیایند. واضح است که اگر کسی ضمیمه‌ها را اجرا کند دچار دردسرهای اساسی خواهد شد.

پایگاه وب

هنگامیکه *شبکهٔ گستردهٔ جهانی*[56] راه‌اندازی شد صفحات وبی ایجاد شدند که شامل متنها و تصاویر بودند. اکنون این صفحات شامل محتویات بیشتری هستند، مثل برنامه‌های پویایی که روی ماشین شما download شده و اجرا می‌گردند (Javascript، Java، و ActiveX). اگر به مرورگر خود اجازه دهید این برنامه‌ها را بدون بررسی قابلیت اطمینان پایگاه وب مورد نظر اجرا کند، ممکن است برخی از موارد را برخلاف آنچه که باید، اجرا نماید. برنامهٔ Javascript بطور کلی ایمن است، اما Java و ActiveX می‌توانند بسیار خطرناک باشند. معمولاً می‌توان مرورگرها را طوری تنظیم کرد که به این برنامه‌ها اجازه اجرا ندهند و یا قبل از اجرای آنها از کاربر اجازه بگیرند.

Plug-inها و Add-onها

مرورگرهای وب و بسیاری برنامه‌های دیگر (مثل *پردازشگرهای کلمه*[57] و *صفحات گسترده*[58]) به برخی از برنامه‌ها اجازهٔ اجرا شدن

56 *World-Wide Web*
57 *Word Processors*
58 *Spreadsheets*

از داخل برنامهٔ اصلی را می‌دهند. نمونهٔ رایج آن برنامهٔ "Adobe Acrobat Reader" است که به شما اجازه می‌دهد هنگام مرور وب، فایلهای PDF را مشاهده کنید. هنگامیکه plug-inها یا add-onها نصب می‌شوند می‌توانند هر کاری که برنامهٔ اصلی انجام می‌دهد – مانند خواندن از دیسک و نوشتن روی آن یا استفاده از ارتباط شبکه – را انجام دهند، و لذا تنها باید زمانی نصب شوند و مورد استفاده قرار بگیرند که مبدأ بطور کامل مورد اطمینان باشد.

حفره‌های امنیتی

حفره‌های امنیتی اشکالاتی در بخشهایی از سیستم‌عامل یا دیگر اجزای سیستم هستند که به مهاجم اجازهٔ دسترسی به اطلاعات موجود در سیستم یا کنترل آنرا می‌دهند. در سالهای اخیر اکثر تولیدکنندگان نرم‌افزار با سرعت قابل قبولی به مشکلات امنیتی که در سیستمهایشان کشف می‌شود پاسخ می‌دهند. بنابراین اگر بصورت منظم وصله‌های امنیتی را روی سیستم خود اعمال کنید می‌توانید قبل از انتشار گستردهٔ اشکالات، راههای نفوذ را بر مهاجمان ببندید.

اشتراک فایلها[59]

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

هدایت بوسیلهٔ downloadها[60]

"هدایت بوسیله downloadها" زمانی رخ می‌دهد که به یک پایگاه وب مراجعه می‌کنید و برنامه HTML موجود در صفحه بصورت خودکار یک برنامهٔ Java یا ActiveX را درخواست می‌کند و آن برنامه نیز یک برنامهٔ دیگر را download می‌نماید، آنرا اجرا می‌نماید، یا طوری برنامه‌ریزی می‌کند که در آینده بتواند آنرا به اجرا در آورد. همچنین کد HTML می‌تواند وارد نامهٔ الکترونیکی گردد. اگر به برنامه‌های Java یا ActiveX بدون اینکه از شما اجازه بگیرند و یا حتی به شما اطلاع دهند اجازهٔ نصب کردن برنامه داده باشید، آنگاه خواهند توانست download شوند و هرچه را که می‌خواهند نصب نمایند.

بی‌اعتمادی به نرم‌افزارهای مسروقه

مفهوم نرم‌افزار تجاری مسروقه مفهوم تازه‌ای نیست. چندین سال است که دیسکهای فشردهٔ جعلی فروخته می‌شوند و نسخه‌های اینترنتی آنها – که Warez نامیده می‌شوند – نیز رایج هستند. از مدتها پیش این سوء ظن وجود داشته که این دیسکهای فشرده می‌توانند حاوی ویروس باشند، اما احتمال بیشتری که وجود دارد این است که این نوع نرم‌افزار ممکن است تعمداً حاوی وصله‌ای باشد که یک فرد غیر مجاز را قادر می‌سازد که از طریق اینترنت به رایانهٔ شما دسترسی پیدا کند. از آنجا که نصب اغلب نرم‌افزارها به امتیاز دسترسی راهبری نیاز دارد، این روش فرصت مناسبی برای نصب شدن برنامه‌هایی که شما آنها را درخواست نکرده‌اید فراهم می‌آورد.

عملکردهای پنهان نرم‌افزارهای سالم

اگرچه ممکن است اکثر نرم‌افزارهایی که download می‌کنید سالم باشند، اما احتمال زیادی وجود دارد که نرم‌افزار download شده (مخصوصاً نرم‌افزارهای رایگان) برنامه‌های دیگری را روی دستگاه شما نصب نماید. برنامه‌های *اشتراک متقابل فایلها*[61] بسیار مستعد چنین وضعیتی هستند. این برنامه‌ها معمولاً شامل برنامه‌های دیگری می‌باشند که بسیاری از آنها در نوع برنامه‌های ردیابی و اعمال تغییر در وب طبقه‌بندی می‌شوند و گردش وب شما را نظاره می‌کنند،

59 *File Sharing*

60 *Drive By Downloads*
61 *Peer-to-Peer File Sharing*

انواع تبلیغات را به نمایش درمی‌آورند و فعالیتهای شما را به مدیر خود گزارش می‌نمایند. برخی از این برنامه‌ها دسیسه‌آمیز هستند، بدین صورت که سعی دارند خود را پنهان کنند و تقریباً غیر قابل حذف باشند. چنین برنامه‌ای دارای یک ابزار uninstall است که اگر آنرا اجرا کنید، آن ابزار uninstall را پاک می‌کند، ولی برنامهٔ اصلی هنوز وجود خواهد داشت و به اجرا در خواهد آمد.

بدافزارهای غیرماندگار[۶۲]

همهٔ بدافزارها روی رایانهٔ شما اجرا نمی‌شوند. بسیار رایج شده که این نرم‌افزارها یک نامهٔ الکترونیکی بفرستند و در آن کاربر را به نحوی ترغیب به مشاهدهٔ پایگاه وب مورد نظر خود نمایند. روش سنتی حیله این است که نامهٔ الکترونیکی به شما چیزی پیشنهاد می‌دهد که بدان علاقمند هستید اما هنگامیکه مشغول مشاهدهٔ پایگاه وب معرفی‌شده هستید تعدادی نرم‌افزار مخرب به سیستم شما حمله می‌کنند و شاید نوعی نرم‌افزار را روی سیستم download کرده (مشابه "هدایت بوسیله downloadها") و یا عملیات دیگری انجام دهند.

در روشهای جدیدتر، نامهٔ الکترونیکی ادعا می‌کند که صورتحسابی از eBay (پایگاه وب مزایده در اینترنت) یا PayPal (یک پایگاه وب برای پرداختهای اینترنتی) و یا از طرف بانک شما است. نامهٔ الکترونیکی بسیار مطمئن بنظر می‌رسد و به شما پایگاههای وبی نشان می‌دهد که در آنها می‌توانید شمارهٔ کارت اعتباری خود را تأمین اعتبار نمایید. معمولاً URLهایی که این نامه‌ها معرفی می‌کنند نیز با URLهای معتبر بسیار مشابهت دارد. بعنوان مثال URL واقعی PayPal، آدرس www.paypal.com است، و URLی که در نامه الکترونیکی نمایش داده می‌شود نیز ممکن است دقیقاً همان آدرس باشد. با این وجود آنچه که در صفحه نشان داده می‌شود، URL واقعی نیست که برای دسترسی به آن صفحه مورد استفاده قرار گرفته است. URL واقعی که به آن اشاره شد معمولاً پنهان می‌باشد و ممکن است بصورت زیر باشد:

http://www.paypal.com:user=3245329:transaction=43293:code=4333033.33@218.5.79.162

اگر فردی با ریزه‌کاریهای قالب URL آشنا نباشد تصور می‌کند که این آدرس همان www.paypal.com است و لذا قابل اطمینان می‌باشد، اما در حقیقت نباید کاراکترهایی که قبل از علامت @ قرار گرفته‌اند را درنظر گرفت؛ زیرا این URL به آدرس 218.5.79.162 متصل می‌شود. معمولاً در این پایگاه وب نیز صفحه‌ای مشابه صفحهٔ واقعی PayPal قرار داده شده و از شما می‌خواهد که وارد آن شوید و شمارهٔ کارت اعتباری خود را وارد نمایید. درواقع این پایگاه وب هرگز به PayPal متصل نمی‌شود، بلکه متعلق به فردی است که سعی دارد کارت اعتباری شما و اطلاعات مربوط به آنرا به سرقت ببرد. این حیله‌ها در عمل بسیار موفقیت‌آمیز بوده‌اند. توجه داشته باشید که نامه‌های الکترونیکی مشابه ممکن است نامه‌های سالم و مشروع باشند که واقعاً از طرف PayPal ارسال شده‌اند.

نامهٔ الکترونیکیِ رسمی که برای این منظور ارسال می‌شود معمولاً شامل اطلاعات منحصر به فردی است که از آدرس پست الکترونیکی شما نمی‌توان آنها را بدست آورد؛ اطلاعاتی نظیر نام کامل و یا چهار رقم آخر کارت اعتباری شما. اگر این نامهٔ الکترونیکی شما را به یک پایگاه وب هدایت کند، به شما آدرس آنرا نیز خواهد داد، اما در آن هیچ *ارتباط صفحه وب*[۶۳] وجود ندارد. همچنین صفحات وب مقصد شامل اطلاعاتی هستند که هیچ کلاهبردار یا هرزنامه‌نویسی نمی‌تواند از آن اطلاع داشته‌باشد. اگر بازهم در این مورد تردید داشتید، برای کسب اطمینان بیشتر می‌توانید از طریق تلفن (و نه نامهٔ الکترونیکی) با شرکت مربوطه تماس بگیرید و از اصالت نامهٔ ارسالی مطمئن شوید.

62 Non-Resident Malware

63 Hyperlink

فصل ششم
امنیت خدمات شبکه

کلیات

پست الکترونیکی و وب از کاربردهای اصلی اینترنت هستند. در این فصل عملکرد این خدمات را بطور جزئی توضیح می‌دهیم و استفادهٔ نامناسب از آنها که باعث ایجاد ناامنی می‌گردد را بررسی می‌کنیم. مواردی مثل ارتباطات بی‌سیم، 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

وصله‌های امنیتی را باید بصورت منظم برای نرم‌افزارهای خود به‌روزرسانی کنید. از آنجا که مشکلات امنیتی می‌توانند با روشهای متعددی به شما آسیب برسانند، هنگامیکه به اینترنت متصل می‌شوید احتمال آسیب‌پذیری بیشتر می‌گردد. اگر در سیستم‌عامل یا نرم‌افزار 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 می‌کنند.

قانون چهارم:
سیستم‌عامل و نرم‌افزارهای کاربردی مهم خود را به‌روزرسانی کنید.

به‌روزرسانی الزاماً به معنای استفاده از آخرین نسخه‌ها نیست. بیشتر شرکتها و توسعه‌دهندگان، اشکالات امنیتی نسخه‌های رایج را برطرف می‌کنند. توجه داشته باشید که این مسئله در مورد نرم‌افزارهای رایگان معمولاً فقط برای آخرین نسخه‌های موجود صادق است. این بدان معناست که اگر می‌خواهید از اشکالات امنیتی مصون بمانید باید بطور منظم نرم‌افزار 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 می‌کنید که در ابتدا از پست الکترونیکی تنها برای ارسال پیامهای متنی استفاده می‌شد. اکثر سیستمهایی که از پست الکترونیکی استفاده می‌کردند از روشهای مختلفی برای انتقال فایلها بهره می‌گرفتند. 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 گسترده‌تری یافت، باید برای استفاده توسط عموم ساده‌تر می‌گشت.

مشکل این بود که پست الکترونیکی اولیه تنها برای انتقال *متنهای ساده*[64] طراحی شده بود و فایلهایی چون برنامه‌های اجرایی در متن خود کاراکترهای غیرچاپی داشتند که در متون ساده قابل نمایش نبودند. راه‌حل پیشنهادی این بود که اطلاعات غیرچاپی بگونه‌ای کدگذاری شوند که بتوان آنها را در متون ساده به نمایش درآورد (جزئیات بیشتر در مورد کدگذاری در ضمیمهٔ ۱ ذکر شده است). در این روش بعد از دریافت پیام، فایل کدگذاری‌شده کدگشایی می‌گردد 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 روشِ جدید *MIME*[65] نامیده می‌شود. هنگامیکه کاربرد ضمیمه وسعت بیشتری پیدا کرد، برنامه‌های پست الکترونیکی طوری تغییر کردند که بتوانند ضمایم را بطور خودکار باز کنند. بنابراین دریافت‌کنندهٔ پیام می‌توانست 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 قالب‌بندی صفحات وب بهره گرفت. HTML تبدیل به یکی از روشهای کدگذاری MIME شد که امکان قالب‌بندی نامه‌های الکترونیکی را فراهم می‌کرد (تغییر فونتها، رنگها، تصاویر، و اشاره‌گرها به صفحات وب). درحال حاضر

64 *Clear Text*
65 *Multipurpose Internet Mail Extensions*

برنامه‌های پست الکترونیکی بصورت خودکار دستورات HTML درون صفحات ارسال‌شده را نیز اجرا می‌کنند.

تأثیر ارتقای پست الکترونیکی

افزوده شدن این قابلیتها (امکانات قالب‌بندی) به برنامه‌های پست الکترونیکی، کاربرد آنها را مفیدتر ساخت. کاربران از آن پس می‌توانستند انواع فایلها را بسادگی تبادل کنند. با استفاده از فونت‌ها، رنگها و تصاویر، نامه شکل مطلوب‌تری پیدا می‌کرد و قالب‌بندی سادهٔ آن بدون نیاز به برنامهٔ پردازشگر کلمات صورت می‌پذیرفت. با این وجود، این ارتقا ابعاد منفی نیز در پی داشت.

همانطور که قبلاً ذکر شد تا قبل از ایجاد این پیشرفتها کسی از طریق پست الکترونیکی تحت تأثیر مستقیم ویروسها و کرمها قرار نمی‌گرفت. همچنین تا زمانیکه برنامهٔ دریافت‌شدهٔ موجود در ضمائم نامهٔ دریافتی را اجرا نمی‌کردید از خطرات امنیتی مصون بودید. اکنون اما برنامه‌هایی که دریافت می‌کنید می‌توانند بصورت خودکار به اجرا درآیند که مفهوم آن این است که این برنامه‌ها خواهند توانست شما را به پایگاه وبی هدایت کنند که در آن اعمال مخربی مثل download نرم‌افزارهای مخرب صورت می‌پذیرد. علاوه بر این، دستورات ویژهٔ HTML می‌توانند مهاجم را به راهبر رایانهٔ شما تبدیل کنند که البته چگونگی آن بستگی به اشکالات موجود در برنامهٔ مفسر دستورات HTML رایانهٔ شما دارد.

پست الکترونیکی گمراه‌کننده است

در بسیاری از مواقع آدرس پست الکترونیکی که جلوی عبارت "فرستنده" قرار می‌گیرد معتبر نیست. این قابلیتی است که هرزنامه‌نویس‌ها آنرا برای سوء استفاده از سیستم شما بکار می‌برند. گاهی اوقات اگر کل *سرآیند*[66] را بررسی کنید ممکن است بتوانید متوجه شوید که این نامه واقعاً از کجا و از سوی چه کسی ارسال شده است.

چگونه می‌توانید از خود محافظت نمایید؟

قانون پنجم:

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

هر فردی که آدرس پست الکترونیکی شما را بداند یا بتواند آنرا حدس بزند می‌تواند برای شما نامهٔ 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 برنامه‌های جدید پست الکترونیکی ضمایم را قبل از اجازهٔ شما باز نمی‌کنند، اما اگر برنامهٔ شما بگونه‌ای 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 برنامهٔ اجرایی نیست.

نویسندگان ویروس بسیار زیرک هستند. آنها معمولاً ضمایم را با نامهایی چون budget.xls.vbs ارسال می‌کنند. ناظری که نمی‌داند vbs چیست تصور می‌کند یک فایل Excel با نام budget از سوی مایکروسافت برای وی ارسال شده (خصوصاً در حالتی از تنظیمات که سیستم‌عامل پسوندهای شناخته‌شده را به کاربر نمایش نمی‌دهد)؛ اما این فایل در حقیقت یک برنامهٔ اجرایی Visual Basic است که نام آن budget.xls می‌باشد: xls تنها بخشی از نام این فایل است و هیچ ارتباطی با Excel ندارد. در بدترین حالات این برنامه ممکن است بتواند تمامی دیسک سخت سیستم شما را پاک نماید.

قانون هفتم:

هرگز ضمیمه‌ای را که از جانب افراد ناشناس برایتان ارسال شده است باز نکنید؛ مگر اینکه اطمینان داشته باشید که آن نوع فایل نمی‌تواند حاوی کد مخرب باشد.

به خاطر داشته باشید برنامه‌هایی مثل Microsoft Word (پردازشگر کلمات) و Microsoft Excel (صفحه گستردهٔ داده) و تمامی برنامه‌های مشابه، دارای قابلیت استفاده از Macro هستند که می‌تواند حاوی ویروس باشد. حتی فایلهای PDF نیز می‌توانند حاوی قطعه برنامه‌های مخرب باشند (اگرچه این

66 Header

فایلها تنها زمانی می‌توانند خطرناک باشند که با نرم‌افزار کاربردی Adobe Acrobat Professional باز شوند و بازکردن آنها با برنامه‌هایی چون Adobe Acrobat Reader که کاربرد بیشتری میان افراد دارد خطر خاصی در پی نخواهد داشت). با استفاده از راهنمای کاربری و یا صفحات راهنما می‌توانید بررسی کنید که چگونه می‌توان بعضی قابلیتها (خصوصاً آنهایی که در سیستم بندرت مورد استفاده قرار می‌گیرند) را از کار انداخت.

قانون هشتم:

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

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

قانون نهم:

پیکربندی برنامهٔ پست الکترونیکی خود را بررسی کنید تا فایلهای HTML تفننی[67] را پردازش نکند و فایلهای آلوده را به رایانه‌های دیگر ارسال ننماید.

این بدان معناست که ممکن است بعضی از قابلیتهای تزئینی نامه‌های الکترونیکی را از دست بدهید، ولی در عوض کنترل بهتری روی عملکرد برنامهٔ پست الکترونیکی خود بدست آورید. توجه داشته باشید که در برخی از برنامه‌های پست الکترونیکی برای اجرا شدن کد HTML حتی لازم نیست پیامی که حاوی کد HTML است را باز نمایید و به نمایش در آمدن آن پیام در *صفحهٔ پیش‌نمایش*[68] برای اجرا شدن کد کافی است. علیرغم اینکه نامهٔ الکترونیکی می‌تواند حاوی قطعه برنامه‌های HTML باشد اما بسیاری از مرورگرها و برنامه‌های پست الکترونیکی به شما اجازه می‌دهند cookie، Javascript، و plug-in صفحاتی که بعنوان بخشی از نامهٔ الکترونیکی دریافت می‌شوند را غیرفعال نمایید.

67 *Fancy HTML*
68 *Preview Screen*

قانون دهم:

از ISP خود سؤال کنید که آیا قبل از ارسال نامه‌های الکترونیکی، آنها را از نظر داشتن ویروس و تهدیدات مشابه بررسی می‌کند یا خیر.

به دلیل افزایش روزافزون فعالیت کرمها و ویروسها اکثر ISPها اینکار را انجام می‌دهند. توجه داشته باشید که نباید توقع داشت که غربال‌سازی ISP شما صد درصد ثمربخش باشد، اما عملکرد پیشگیرانهٔ ISPها می‌تواند به تلاشهای شما در برقراری امنیت کمک کند. اگر ISP شما از مسائل امنیتی آگاه نیست بهتر است برای ارائه خدمات امن‌تر به خودتان و نیز دیگر مشتریان با آنها همکاری کنید. مثلاً می‌توانید یک نسخه از کتابی که هم اکنون مشغول مطالعه آن هستید را بصورت رایگان به آنها هدیه نمایید!

هرزنامه

هرزنامه[69] نامی است که برای نامه‌های الکترونیکی ناخواسته بکار می‌رود، خصوصاً نامه‌های تجاری که از طرف افراد ناشناس و بصورت متعدد – احتمالاً بر اساس این باور که دریافت کننده به محصولات آنها علاقه‌مند خواهد شد – ارسال می‌شوند. در سالهای اخیر تعداد هرزنامه‌ها بطور چشمگیری افزایش یافته است. در سال ۲۰۰۳ بیش از ۵۰٪ از کل نامه‌های الکترونیکی تبادل‌شده در اینترنت هرزنامه بوده است! بسیاری افراد هم‌اکنون به ازای دریافت هر یک نامهٔ معتبر حدود ۱۰ هرزنامه دریافت می‌کنند.

اگر در فیلد "موضوع" هرزنامه‌ها عبارتهایی نظیر "**SPAM**" وجود می‌داشت، آنگاه می‌توانستیم به آسانی تمامی آنها را حذف کنیم. قوانین مصوب قضایی حکم می‌کند که هر نامهٔ الکترونیکی ناخواسته که از سوی شرکتهای تجاری ارسال شود پیگرد قانونی خواهد داشت. با این وجود به دلیل حجم وسیع هرزنامه‌ها و نیز تواناییهای محدود نیروهای انتظامی درحال حاضر اجرای این نوع قوانین چندان عملی نیست. هرکس باید بدون خواندن هرزنامه و یا ارسال اخطار به یک سیستمِ شلوغِ دریافت شکایت، یک روش منطقی برای تشخیص و حذف آن داشته باشد.

69 *Spam*

آشنایی بیشتر با هرزنامه

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

الف) چگونه هرزنامه‌نویس‌ها آدرس شما را بدست می‌آورند.
ب) چه چیزی هرزنامه تلقی می‌شود (با جزئیات دقیق).
ج) چرا نویسندگان هرزنامه، آنها را ارسال می‌کنند.

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

- نامه یا امضای خود را به یک *فهرست آدرس عمومی*[۷۰] ارسال کرده باشید.
- به یک هرزنامه پاسخ داده باشید؛ مثلاً خواسته باشید که از فهرست دریافت‌کنندگان حذف شوید.
- برای *گروه‌های خبری*[۷۱] 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 نموده‌اید).
- از رایانه‌ای که یک *برنامه شناسایی*[۷۲] روی آن درحال اجرا بوده استفاده کرده باشید (این برنامه شناسایی در بسیاری از سیستمهای UNIX نام کاربری شما را به هر کس که آنرا سؤال کند ارائه می‌دهد).
- به مرورگر اجازه داده باشید آدرس شما را ذخیره کند.
- از نرم‌افزارهای ارسال پیام فوری استفاده کرده باشید.
- آدرس پستی خود را در یک صفحهٔ وب قرار داده باشید؛ یعنی اجازه داده باشید که آدرس پستی شما برای همه قابل مشاهده باشد.
- یک *نام دامنه*[۷۳] برای خود ثبت کرده باشید و یا آدرس خود را در گروه پشتیبانی فنی یک پایگاه وب قرار داده باشید.
- از آدرسهای پستی قابل حدس زدن استفاده کرده باشید.
- آدرس خود را روی یکی از سیستمهایی که قبلاً به آنها نفوذ شده است قرار داده باشید.

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

ب) برخی از نامه‌های تجاری به دلیل تعداد زیاد و نامربوط بودنشان کاملاً شناخته‌شده هستند و همه می‌دانند که هرزنامه می‌باشند. در مورد بعضی نامه‌های دیگر این مسئله کمتر آشکار است. در برخی موارد این بستگی به دریافت‌کننده دارد که یک نامهٔ الکترونیکی دریافتی را هرزنامه بداند یا خیر. مثالهای زیر به روشن شدن بیشتر موضوع کمک خواهند کرد:

- آیا یک نامهٔ الکترونیکی که حاوی اطلاعاتی در مورد چگونگی مراقبت از اجزای صورت است یک هرزنامه به شمار می‌رود؟ پاسخ: بله، هرزنامه است؛ مگر اینکه شما جراح پلاستیک باشید و این نامه الکترونیکی یک مقالهٔ دانشگاهی باشد و نه یک آگهی تجاری.
- آیا درخواست مقاله از شما برای یک گردهمایی دانشگاهی با موضوعی مبهم که به چندین فهرست آدرس فرستاده شده یک هرزنامه بشمار می‌رود؟ پاسخ: شاید. مگر اینکه بطور اتفاقی موضوع آن مورد علاقهٔ شما باشد و مایل باشید به آن پاسخ دهید.
- شرکتی که به شما محصولی فروخته و اطلاعاتی را در مورد محصول بعدی خود برای

70 *Public Mailing List*
71 *Newsgroup*
72 *Ident Daemon*
73 *Domain Name*

شما و بسیاری از مشتریهای دیگر ارسال می‌کند، آیا هرزنامه فرستاده‌است؟ پاسخ: خیر. اما برنامهٔ غربال‌ساز هرزنامه در ISP شما ممکن است زمان زیادی را صرف شناسایی این کند که تشخیص دهد چنین نامه‌ای هرزنامه است یا خیر.

- اگر یک نامهٔ الکترونیکی حاوی مطلبی باشد که با تمام تعاریف یک هرزنامه تلقی شود، آیا حتماً هرزنامه است؟ پاسخ: بله؛ اما تنها درصورتیکه اصل آن فرستاده شده باشد. اما مثلاً اگر این نامه از سوی یکی از خوانندگان برای نویسندگان این کتاب فرستاده و در آن مثالهای جالبی در ارتباط با هرزنامه‌ها ذکر شده باشد مطمئناً هرزنامه نیست و نباید غربال شود.

ج) چرا هرزنامه‌نویس‌ها برای افراد هرزنامه ارسال می‌کنند؟ ساده‌ترین جواب: چون اینکار جواب می‌دهد! اگر هرزنامه را مورد بررسی قرار دهید سریعاً متوجه یک الگو در آن می‌شوید. معمولاً هرزنامه‌ها در مورد مسائلی هستند چون بدست آوردن پول یا پس‌انداز آن، ارتقای زندگی عاطفی یا خصوصی، و افزایش سلامتی. این موضوعات یک نقطهٔ مشترک مهم دارند: اغلب ما در مورد این مسائل نگرانیهای جدی داریم و تعدادی از ما نیز توجه بسیار زیادی به آنها می‌کنیم. بنابراین حتی اگر درصد بسیار اندکی از دریافت‌کنندگان، این نامه‌ها را پیگیری کنند (مثلاً چیزی حدود ۱ نامه در میان هر ۱۰۰،۰۰۰ دریافت‌کننده) هرزنامه‌نویس‌هایی که چندین میلیون پیام در روز ارسال می‌کنند می‌توانند پول زیادی از این راه بدست آورند.

با هرزنامه‌ها چه باید کرد؟

روشهای بسیاری وجود دارند که با استفاده از آنها می‌توان هرزنامه را محدود و کنترل کرد. برخی از دولتها در حوزهٔ قضایی خود قوانینی را برای جلوگیری از گسترش هرزنامه تصویب کرده‌اند. اکثر ISPها معتقدند که استفاده از تسهیلات آنها برای فرستادن هرزنامه برخلاف توافقنامه‌های کاری آنها است. تصویب چنین قوانینی می‌تواند مؤثر باشد، اما تاکنون اعمال اکثر قوانین مربوط به هرزنامه‌ها بسیار مشکل و پرهزینه بوده و در بسیاری موارد هیچ راهکار اجرایی برای آن اندیشیده نشده است.

برخی از کاربران عمدهٔ پست الکترونیکی (مانند شرکتها) از پذیرفتن نامه‌های الکترونیکی که از سوی ISPهایی منتشر می‌شود که اجازهٔ فعالیت به هرزنامه‌نویس‌ها را می‌دهند امتناع می‌ورزند. اینکار می‌تواند مؤثر واقع شود، زیرا ISPها را وادار می‌کند که فعالیتهای مرتبط با هرزنامه را متوقف سازند. با این وجود معمولاً این روش به مشتریان بی‌گناهی که تعداد کمی نامهٔ الکترونیکی به مقاصد مختلف ارسال می‌کنند هم آسیب می‌رساند. برنامه‌های زیادی وجود دارند که برای تشخیص هرزنامه، حذف آن و یا هشدار به دریافت‌کننده مبنی بر دریافت یک هرزنامه بکار می‌روند. این برنامه‌ها را می‌توان در پایگاه وب ISP یا *سرویس‌گیرندهٔ پستی*[۷۴] به اجرا در آورد. این برنامه‌ها محتوای نامه و منشاء ارسال آنرا بررسی می‌کنند؛ اما از آنجا که این معیارها به سختی قابل ارزیابی هستند عملکرد این برنامه‌ها نیز معمولاً دارای *تشخیص منفی نادرست* (False Negative) و *تشخیص مثبت نادرست* (False Positive) می‌باشد.

False Negative

False Negative زمانی رخ می‌دهد که *برنامهٔ جستجوگر*[۷۵] اعلام می‌کند که یک نامهٔ الکترونیکی هرزنامه نیست، اما در حقیقت هرزنامه است. این بدان معناست که برنامه به هرزنامه اجازه می‌دهد که از غربال عبور کند و به همین دلیل است که گفته می‌شود این برنامه ممکن است ۱۰۰٪ مؤثر نباشد.

False Positive

False Positive بدین معناست که برنامهٔ جستجوگر اظهار می‌کند که برخی از نامه‌های بی‌ضرر هرزنامه هستند. این اتفاق خسارتهای زیادی به بار می‌آورد، بخصوص اگر در اثر این تشخیص، نامهٔ فرستاده‌شده بجای تحویل شدن، حذف گردد. ممکن است با False Positive نامه‌های الکترونیکی عادی و بی‌ضرر از دست بروند و غیرقابل بازیابی شوند.

74 *Mail Client*
75 *Scanning Program*

هدف برنامه‌های جستجوی هرزنامه به حداقل رساندن False Negative و از بین بردن False Positive می‌باشد. متأسفانه کاهش False Negative معمولاً False Positive را افزایش می‌دهد. افرادی که به هر دلیلی نیاز به دریافت نامه‌های الکترونیکی شبیه به هرزنامه دارند ممکن است از این طریق آسیب بینند. آخرین نمونهٔ گزارش‌شدهٔ این اتفاق در مورد یک خبرنامهٔ دانشگاهی بود که در آن در ارتباط با هرزنامه‌ها مطالبی مطرح شده بود. از آنجا که خبرنامه دارای مثالهایی در مورد هرزنامه‌ها بود، توسط جستجوگرها بعنوان یک هرزنامه شناسایی شد و ISPهای متعددی آنرا غربال و حذف نمودند.

علاوه بر جستجوگرهای هرزنامه، روشهای غربال‌سازی هرزنامه نیز وجود دارند که از فنون *پرسش – پاسخ*[۷۶] استفاده می‌کنند. در این روش هنگامیکه نامه‌ای از یک فرستندهٔ ناشناس دریافت می‌شود، در میان راه (قبل از اینکه گیرنده آنرا باز کند) متوقف می‌گردد. سپس پرسشی برای فرستنده ارسال می‌شود و در آن از وی درخواست می‌گردد نامه‌ای که فرستاده است را تأیید کند تا ثابت شود آن نامه از سوی همان فرد است و نه از جانب شخص دیگر یا یک نرم‌افزار. فرم تأییدیه چنان طراحی شده که بطور خودکار نمی‌تواند مدیریت شود و نیز برای هرزنامه‌های بعدی مؤثر نیست. اگر تا چند روز هیچ تأییدیه‌ای دریافت نشود، نامه بجای تحویل شدن، حذف می‌گردد. مشکل این روش این است که نیازمند مداخلهٔ دستی فرستنده است. اگر نامه‌ای را بفرستید و قادر نباشید که به درخواست تأییدیه سریعاً پاسخ دهید نامهٔ شما تحویل نخواهد شد. همچنین اگر دو ISP بصورت متقابل از این سرویس استفاده کنند ممکن است هرگز از یکدیگر نامه‌ای دریافت نکنند؛ زیرا اولین دریافت‌کننده نامه را نمی‌بیند مگر اینکه تأیید شده باشد، و تقاضای تأیید نیز ارسال نخواهد شد، چون فرستندهٔ آن ناشناس است. برخی از صافیهای هرزنامه بجای اینکه نامه‌های مشکوک را حذف کنند آنها را در یک پوشهٔ مخصوص قرار می‌دهند. بنابراین شما می‌توانید بطور متناوب پوشهٔ هرزنامه را بررسی کنید تا مطمئن شوید که محتویات آن قربانیهای False Positive نیستند.

روش امیدوارکنندهٔ جدید ضد هرزنامه روشی به نام Bayesian Filtering است. در این روش قوانین غربال‌سازی با شناخت شما از هرزنامه اصلاح می‌شود. این قوانین می‌توانند در مورد هر دریافت‌کننده‌ای متغیر باشند. هدف از این روش، آموزش دیدن برنامه غربال‌ساز از رفتار شما است تا بتواند فرد مورد اطمینان شما را تشخیص دهد و محتویاتی که معمولاً بعنوان هرزنامه شناسایی نمی‌شوند اما به هر دلیلی مورد توجه شما نیستند را رد کند. صافیهای bayesian از فنون زبان‌شناسی استفاده می‌کنند تا به نامه‌هایی اجازهٔ عبور دهند که حاوی لغات مخصوصی هستند و بر اساس تجربیات گذشتهٔ رفتار پست الکترونیکی شما در نامه‌های واقعیتان بکار می‌روند اما بندرت در هرزنامه ظاهر می‌شوند. صافیهای bayesian برای اکثر برنامه‌های پست الکترونیکی قابل استفاده هستند.

اگر هرزنامه برای شما مشکل‌آفرین شده است باید بررسی کنید که آیا ISP شما قابلیتهای شناسایی و غربال‌سازی هرزنامه را ارائه می‌دهد یا خیر. همچنین باید نرم‌افزارهای پست الکترونیکی خود را بررسی کنید تا معلوم شود آیا می‌توانند هرزنامه‌ها را غربال نمایند یا نه.

استفاده از شبکهٔ جهانی وب

هنگامیکه این کتاب در سال ۲۰۰۳ نوشته شد، وب حدود ۱۰ سال با سطوح دسترسی مختلف در اختیار عموم قرار داشته است. درحال حاضر وجود وب برای آندسته از افرادی که مرتباً در کار، مدرسه و تفریح از شبکه استفاده می‌کنند ضروری است. از آنجا که وب بصورت ابزاری مفید و رایج در آمده، فراموش شده که می‌تواند محیطی خصومت‌آمیز باشد.

ایمن نگهداشتن مرورگرها

بطور کلی وب نسبتاً ایمن است اما استفاده از آن خطرات بالقوه‌ای نیز در پی دارد. پایگاههای وب معمولاً دارای متنها و تصاویر *ایستا*[۷۷] هستند، اما می‌توانند برنامه‌های *پویایی*[۷۸] نیز داشته باشند که برای اجرا در رایانهٔ شما درنظر گرفته شده باشند.

76 *Challenge-Response*

77 *Static*
78 *Dynamic*

قانون یازدهم

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

Download پویای برنامه‌ها گاهی اوقات می‌تواند بسیار مفید باشد. این قابلیت به شما اجازه می‌دهد که از *خدمات برخط*[۷۹] استفاده کنید؛ مثلاً به ویروس‌یابی و رفع مشکلات امنیتی بپردازید. همچنین باعث می‌شود نرم‌افزار شما بتواند بسادگی نصب و به‌روزرسانی شود؛ بدون اینکه لازم باشد کاربر روالهای چندمرحله‌ای پیچیده و فنی انجام دهد.

متأسفانه download پویا و خودکار برنامه‌ها می‌تواند خطرناک و مخرب نیز باشد. کلیهٔ مرورگرها به شما اجازه می‌دهند که برنامه‌های JavaScript، Java، ActiveX و دیگر ابزارهای برنامه‌نویسی را روی رایانهٔ خود download و اجرا کنید، اما اگر می‌خواهید کاملاً ایمن باشید نباید اجازهٔ اجرای این برنامه‌ها را صادر نمایید. البته با غیرفعال نمودن این ویژگیها متوجه خواهید شد که بسیاری از پایگاههای وب نمی‌توانند مثل گذشته کار کنند.

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

- قابلیتهای نسبتاً ایمن و رایج مانند Javascript را فعال نمایید. با اینکار به پایگاههای وب زیادی اجازه می‌دهید که بتوانند بطور صحیح عمل کنند.
- قابلیتهایی مانند Java و ActiveX که ایمنی کمتری دارند و کمتر نیز استفاده می‌شوند را غیرفعال کنید یا مرورگر خود را طوری تنظیم نمایید که قبل از بکارگیری آنها از شما اجازه بگیرد. غیرفعال نمودن این قابلیتها بدین معناست که از آن پس بعضی از توابع مرورگر کار نخواهند کرد. با انجام اینکار بعضی از پایگاههای وب ممکن است به شما هشدار دهند و برخی دیگر از ادامهٔ فعالیت باز بمانند. اگر مایل نیستید چنین اتفاقی رخ دهد، مرورگر باید بتواند نیازهای پایگاه وب را شناسایی کند و برای download و اجرای برنامهٔ مورد نیاز جهت مشاهدهٔ صحیح محتویات آن پایگاه از شما سؤال نماید.

قانون دوازدهم:

به آدرس پایگاه وب و آدرسی که به آن متصل می‌شوید دقت کنید و هنگام مشاهدهٔ یک پایگاه وب ناشناخته، به آن توجه نمایید؛ خصوصاً اگر به آن پایگاه اجازهٔ اجرای یک برنامه روی رایانهٔ خود را داده‌اید.

مرورگرهای وب می‌توانند طوری تنظیم شوند که آدرس پایگاه وب درحال مشاهده را نشان دهند (این قابلیت معمولاً Navigation Bar یا Address Bar نامیده می‌شود). هنگامیکه *مکان‌نمای*[۸۰] شما به یک *ارتباط*[۸۱] اشاره می‌کند، این ویژگی می‌تواند نشان دهد که آن ارتباط به چه آدرسی اشاره دارد (*نوار وضعیت*[۸۲]). با مشاهدهٔ آن آدرس متوجه می‌شوید که به چه پایگاه وب دیگری فرستاده خواهید شد؛ پایگاهی که ممکن است غیرقابل اطمینان باشد؛ یا شاید نخواهید آنرا مشاهده کنید. در عمل ممکن است نخواهید با هر کلیک Navigation Bar و Status Bar را بررسی کنید، اما وقتیکه در یک پایگاه وب ناآشنا هستید – بخصوص اگر Java یا ActiveX را فعال کرده باشید – باید از این ابزار بگونه‌ای استفاده نمایید که چنانچه بصورت ناخواسته به پایگاه وب جدیدی هدایت شدید از آن آگاهی یابید.

Cookieها

Cookie اطلاعاتی است که مرورگر هنگام مشاهدهٔ یک پایگاه وبِ راه دور روی دیسک سخت رایانه می‌نویسد. هنگامیکه بعدها دوباره همان پایگاه وب را مشاهده کنید، cookieهای مربوط به شما مجدداً برای آن پایگاه ارسال می‌شوند. درواقع هر cookie مربوط به پایگاه وب مبدأ خود است؛ اگرچه برخی از اشکالات موجود در مرورگرها باعث می‌شوند که پایگاهها بتوانند cookieهای یکدیگر را مشاهده نمایند. Cookie به پایگاه وب متذکر می‌شود که شما چه کسی هستید، میل و سلیقهٔ شما چیست، و قبلاً در آن پایگاه چه فعالیتهایی انجام داده‌اید. بعنوان مثال هنگامیکه

79 *Online Services*

80 *Cursor*
81 *Link*
82 *Status Bar*

با نام کاربری و رمز عبور خود وارد یک پایگاه وب می‌شوید، پایگاه وب این اطلاعات را در یک cookie بر روی رایانهٔ شما ذخیره می‌کند. وقتی‌که مثلاً پس از یک هفته دوباره به آن مراجعه می‌کنید ممکن است بر اساس اطلاعات موجود در cookie مذکور بصورت خودکار وارد آن پایگاه شوید. Cookieها همچنین به پایگاههای وب اجازه می‌دهند آنچه را که در یک *جلسه*[۸۳] انجام داده‌اید ردیابی نمایند.

اگرچه یک cookie به شکل معمول تنها می‌تواند از پایگاه وب مبدأ خود بازیابی شود، اما ممکن است پایگاه وبی که مشاهده می‌کنید حاوی تصاویر و اشیاء دیگری باشد که مربوط به یک پایگاه وب ثانویه هستند (که *پایگاه وب خارجی*[۸۴] یا *پایگاه وب شخص ثالث*[۸۵] نامیده می‌شود) و آن پایگاه وب ثانویه نیز بتواند cookieها را ذخیره و بازیابی نماید. از آنجا که تصاویر می‌توانند نامرئی باشند، ممکن است اصلاً متوجه نشوید که چنین اتفاقی رخ داده است. این تصاویرِ غیرقابل رؤیت می‌توانند با ردیابی پایگاههای وبی که شما آنها را مشاهده می‌کنید برای اهداف تبلیغاتی بکار روند.[۸۶]

قانون سیزدهم

چگونگی وضعیت ذخیرهٔ cookieها بر روی رایانه را مورد بررسی قرار دهید. اگر نمی‌توانید آنها را کنترل نمایید (مانند زمانیکه از رایانه‌ای در یک مکان عمومی استفاده می‌کنید) اطلاعات خصوصی خود را وارد رایانه نکنید.

کلیهٔ مرورگرهای وب تا سطح کنترل خاصی به شما امکان می‌دهند که وجود cookieها را مجاز بدانید یا خیر. در برخی موارد ممکن است مرورگر میان cookieهایی که در رایانهٔ شما ذخیره شده‌اند، cookieهایی که هنگام بستن مرورگر ناپدید می‌شوند و آندسته که هنگام مشاهدهٔ پایگاه‌های وب و پایگاههای وب خارجی ذخیره می‌گردند تفاوت قائل شود. اساساً شما می‌توانید اجازهٔ ذخیرهٔ همهٔ cookieها را بدهید، از ذخیرهٔ آنها جلوگیری کنید، و یا از مرورگر بخواهید که قبل از ذخیرهٔ آنها از شما سؤال نماید. شما هرگز مطلع نمی‌شوید که چه زمانی اطلاعات ذخیره شده در یک cookie به پایگاه وب مبدأ بازمی‌گردد.

Cookieها را می‌توان بررسی نمود زیرا در قالب متنی هستند، اما چون اطلاعات موجود در آن توسط پایگاه وب مبدأ رمزگذاری می‌شود معمولاً قابل فهم نمی‌باشند. برخی از مرورگرها اجازهٔ نمایش و حذف cookieها را می‌دهند و برنامه‌های ثالثی وجود دارند که اجازهٔ مدیریت آنها را نیز برای شما فراهم می‌آورند.

اگر می‌خواهید اطلاعاتی که یک پایگاه وب در مورد شما می‌داند را کنترل کنید باید زمان و چگونگی ذخیره‌شدن cookieها روی رایانهٔ خود را کنترل نمایید. توجه داشته باشید که برخی از پایگاههای وب برای اینکه بتوانند بدرستی عمل نمایند نیازمند ذخیرهٔ cookieها روی رایانهٔ کاربر می‌باشند. عموماً این پایگاههای وب درصورت غیرفعال بودن cookieها به شما اطلاع می‌دهند که قادر به انجام یا تکمیل عملیات نیستند.

اگر در اماکن عمومی (مثل کافی‌نت، کتابخانه‌ها، مدارس) از مرورگرهای وب استفاده می‌کنید توجه داشته باشید cookieهایی که حاوی اطلاعات شما هستند در آنها ذخیره می‌شوند. در بسیاری از موارد راهبر رایانه ممکن است به شما آنقدر دسترسی نداده باشد که بتوانید cookieها را کنترل، نظاره و یا پاک کنید. بنابراین اطلاعات شما در این رایانه می‌ماند و ممکن است بوسیلهٔ فرد دیگری که همان پایگاه وب را مشاهده می‌کند مورد استفاده قرار گیرد. اگر به پایگاه وبی وارد شده باشید و اطلاعات معتبر شما در یک cookie ذخیره شده باشد و کاربر دیگری به همان پایگاه وب مراجعه نماید، ممکن است بصورت خودکار بجای شما وارد آن پایگاه گردد. درنتیجه احتمال دارد که پایگاه وب اطلاعات ذخیره‌شدهٔ شما (مانند نام، آدرس و اطلاعات کارت اعتباری) را در اختیار این کاربر قرار دهد.

این مورد حتی در یک رایانهٔ خصوصی که چند نفر از آن استفاده می‌کنند نیز می‌تواند مشکل‌ساز شود. در این موارد

---

83 *Session*
84 *Foreign Site*
85 *Third-Party Site*
۸۶ *فرض کنید پایگاههای A و B و C و D همگی یک تصویر نامرئی از پایگاه Z نمایش می‌دهند. وقتی تصویر مربوطه در مرورگر شما به نمایش در می‌آید، Z مطلع می‌شود که از کدام پایگاه به آن اشاره شده است، و سپس cookieهایی ذخیره می‌کند تا به خاطر بسپارد که شما از کدام پایگاهها دیدن کرده بودید. از این پس Z در مورد اینکه چه چیزهایی مورد علاقهٔ شما است اطلاعات خوبی در اختیار دارد و می‌تواند از آن اطلاعات برای ارسال تبلیغات به شما استفاده کند.*

cookieها نه تنها یک مشکل برای حریم خصوصی هستند، بلکه یک آسیب‌پذیری امنیتی نیز بشمار می‌روند.

حافظهٔ نهان[87] مرورگر وب

هنگامیکه یک مرورگر صفحه یا تصویری را از یک پایگاه وب بازیابی می‌کند معمولاً یک نسخه از صفحهٔ درحال نمایش را نیز در دیسک سخت رایانه ذخیره می‌نماید. این مجموعهٔ صفحات و تصاویر ذخیره‌شده "حافظهٔ نهان" نامیده می‌شوند. اگر این پایگاه وب را مجدداً مشاهده کنید و صفحهٔ آن تغییر نکرده باشد ممکن است مرورگر کل صفحه را از ابتدا download نکند، بلکه برای نمایش آن از حافظهٔ نهان استفاده نماید. در برخی موارد صفحات وبی که در حافظهٔ نهان وجود دارند می‌توانند بصورت offline (یعنی بدون اتصال اینترنتی) نیز دیده شوند. این بدان معناست که هرآنچه توسط مرورگر مشاهده می‌کنید در دیسک سخت رایانه ذخیره شده است. بنابراین اگر برای انجام معاملات مالی از وب استفاده می‌کنید، اطلاعات خرید، کارتهای اعتباری و حسابهای بانکی شما در آن رایانه کاملاً قابل خواندن و بازیابی خواهند شد. باتوجه به میزان مرور و اندازهٔ حافظهٔ نهان، این صفحات و تصاویر می‌توانند تا مدتهای متفاوتی روی رایانه باقی بمانند.

قانون چهاردهم:

درصورتیکه اطلاعات خصوصی شما در صفحهٔ وب نمایش داده شد، پس از اتمام کار باید حافظهٔ نهان را پاک نمایید. اگر نمی‌توانید اینکار را انجام دهید (مثلاً هنگامیکه از یک رایانهٔ عمومی استفاده می‌کنید) نباید از آن رایانه برای تبادل اطلاعات محرمانهٔ شخصی استفاده نمایید.

کلیهٔ مرورگرها اجازه می‌دهند حافظهٔ نهان (که *فایلهای موقتی اینترنت*[88] نامیده می‌شود) را از روی سیستم پاک کنید؛ اما بسیاری از رایانه‌هایی که در اماکن عمومی مورد استفاده قرار می‌گیرند اجازهٔ کنترل و حذف حافظهٔ نهان را نمی‌دهند. اگرچه پاک کردن این حافظه پس از ورود اطلاعات حساس از اهمیت بسیار زیادی برخوردار است، اما تا به حال هیچ مرورگری در نوار ابزار خود نمایه‌ای قرار نداده که با کلیک بر روی آن بتوان به آسانی حافظهٔ نهان را پاک نمود.

انتقال امن

کلیهٔ پیامهایی که در وب دریافت و ارسال می‌کنید بصورت متن‌ساده هستند. این بدان معناست که اگر فردی بتواند این متنها را میان راه را بدزد، برای وی قابل فهم و خواندن خواهند بود. اگر بخشی از ارتباط اینترنتی به شکل بی‌سیم باشد و یا ISP انتهای ارتباط قابل اطمینان نباشد دزدی پیام از میان راه راحت‌تر می‌شود و لذا توجه به آن اهمیت بسیار بیشتری پیدا می‌کند.

مرورگرها و سرویس‌دهنده‌های وب برای حل این مسئله از رمزگذاری بهره می‌برند. رمزگذاری پیام را تغییر می‌دهد؛ بنابراین برای افراد غیرمجاز بسیار سخت و حتی غیرممکن می‌شود که بتوانند پیام رمزگذاری‌شده را بخوانند (برای جزئیات بیشتر ضمیمهٔ ۱ همین بخش را مطالعه نمایید). نام پروتکل رمزگذاری "*SSL*"[89] است. می‌توانید برای پیامهایی که دریافت می‌کنید از SSL استفاده نمایید. در اکثر مرورگرها تصویر کوچکی از یک قفل وجود دارد که برای انتقال عادی پیام باز است و برای انتقالاتی از نوع SSL به حالت بسته در می‌آید. در اینحالت URL آن صفحه بجای "http" با "https" آغاز می‌شود. درصورتیکه در کشورتان امکان آن وجود داشته باشد، بهتر است همواره از قوی‌ترین روش رمزگذاری استفاده نمایید.

توجه داشته باشید که این قفل مشخص نمی‌کند پیامی که از طرف شما به سرویس‌دهنده ارسال می‌شود برای رمزگذاری از SSL استفاده کرده است یا نه، اما فرض بر این است که اگر صفحهٔ ارسالی رمزگذاری شده باشد، پیام بازگشتی نیز بصورت رمزگذاری‌شده منتقل می‌شود.

SSL تنها زمانی کار می‌کند که مرورگر بداند مخاطب آن کیست. این امر به کمک *گواهی امنیتی*[90] و *امضای دیجیتالی*[91] صورت می‌پذیرد. بطور کلی اگر سرویس‌دهندهٔ وب بخواهد قابل اطمینان باشد باید از یک مرکز معتبر صدور گواهی، گواهی امنیتی تهیه نماید. اگر این مرکز بخواهد

87 *Cache*
88 *Temporary Internet Files*

89 *Secure Socket Layer*
90 *Security Certificate*
91 *Digital Signature*

بدرستی به وظیفهٔ خود عمل نماید باید بررسی کند فردی که درخواست گواهی نموده همان کسی است که خودش ادعای آنرا دارد. سپس این مرکز گواهی را بصورت دیجیتالی امضا می‌کند و مرورگر شما جداولی را برای شناسایی این گواهی‌ها ذخیره می‌نماید.

گاهی اوقات از سوی یک پایگاه وب پیامی دریافت می‌کنید مبنی بر اینکه گواهی دیجیتالی آن *منقضی*[۹۲] شده یا متعلق به مکان دیگری است. حالت اول زمانی است که تاریخ اعتبار گواهی بتازگی به پایان رسیده و پایگاه وب برای تمدید آن باید تشریفات اداری تمدید گواهی را دنبال کند. در حالت دوم نیز معمولاً پایگاه مورد نظر تغییر نام داده و این تغییر در گواهی آن منعکس نشده است. با این وجود اگر خواستار سطح مناسبی از ایمنی هستید در هر دو حالت باید تا زمانیکه مشکل بگونه‌ای رفع شود به ارتباط خود با آن پایگاه خاتمه دهید.

آیا انتقال امن کافی است؟

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

- فقدان اصول اخلاقی در بعضی پایگاههای وب؛
- سوء استفاده از پایگاههای وب شخصی؛
- سوء استفاده از رایانه‌های شخصی.

استثنای اصلی در این موضوع "انتقال بی‌سیم" است که در بخش بعدی بررسی خواهد شد.

سیاستهای حریم خصوصی[۹۳]

بسیاری از پایگاههای وب برای حفاظت از حریم خصوصی افراد، سیاستهای اعلام شده دارند. این سیاستها مشخص می‌کنند که چه نوع اطلاعاتی را می‌توان در پایگاه وب جمع‌آوری نمود، با آن داده‌ها چه کاری را می‌توان یا نمی‌توان انجام داد، و نیز اینکه چگونه باید از این داده‌ها حفاظت کرد. کلیهٔ پایگاههای وبی که اطلاعات فردی یا مالی جمع‌آوری می‌کنند باید از یک سیاست حریم خصوصی مناسب و اعلام‌شده برخوردار باشند.

انتقال بی‌سیم

استفاده از فناوری بی‌سیم در کشورهای درحال توسعه و توسعه‌یافته رو به افزایش است. این فناوری معمولاً کم‌هزینه‌تر از فناوریهای سیمی است، در اماکن خصوصی راحت‌تر و سریعتر نصب می‌شود و اشکالات تنظیمی کمتری دارد. با این وجود فناوری بی‌سیم دارای دو مشکل بالقوه است:

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

در مورد دستهٔ دوم مشکلات، کار زیادی نمی‌توان انجام داد. این موارد از خصوصیات فناوری بی‌سیم و از هزینه‌هایی هستند که برای استفاده از ارتباطات بی‌سیم باید پرداخت شوند. راه مقابله با *دزدی میان راه*[۹۴] نیز استفاده از روشهای مختلف رمزگذاری است (برای جزئیات بیشتر در مورد روشهای رمزگذاری ضمیمهٔ ۱ از همین بخش را مطالعه کنید). اگر سرویس‌دهنده‌ای دارید که از روشهای رمزگذاری پشتیبانی می‌کند حتماً از آن استفاده نمایید (مثل پایگاههای وب مبتنی بر SSL). اگر از پست الکترونیکی مبتنی بر POP استفاده می‌کنید باید گزینهٔ APOP را انتخاب نمایید تا رمزهای عبور قبل از ارسال رمزگذاری شوند. این ویژگی – مستقل از رسانهٔ انتقال – *امنیت پایانه به پایانه*[۹۵] را برآورده می‌کند. اگر سرویس‌دهنده از رمزگذاری استفاده نکند باید از محدودیتهای فناوری آگاه باشید و درصورت لزوم تصمیم بگیرید که از ارتباط چگونه استفاده کنید.

92 *Expired*
93 *Privacy Policy*
94 *Interception*
95 *End-to-End Security*

802.11 یا Wi-Fi

802.11 مجموعه‌ای از استانداردهای درحال توسعهٔ IEEE برای *شبکه‌های محلی بی‌سیم*[۹۶] می‌باشد. 802.11 که معمولاً *Wi-Fi*[۹۷] نامیده می‌شود، بعنوان جایگزین *اترنت سیمی*[۹۸] برای اتصال رایانه‌های خانگی و رایانه‌های کیفی محبوبیت یافته و مزیتش ارزان بودن و سرعت نسبی آن است.

متأسفانه چندین آسیب‌پذیری در اغلب پیاده‌سازیهای Wi-Fi وجود دارد:

- ایستگاههای اصلی، ارتباط ایمن و مطمئنی با یکدیگر ندارند.
- اگر بخواهید ارتباط شبکه‌ای خود را با فرد دیگری به‌اشتراک بگذارید، باید نام شبکهٔ خود (SSID) را از حالت پیش‌فرض تغییر دهید و آنرا طوری تنظیم کنید که نام آن برای افراد غیر مجاز قابل رؤیت نباشد. درصورت انجام اینکار تنها افرادی که SSID را می‌دانند خواهند توانست آن ارتباط شبکه‌ای را ببینند.
- الگوریتم رمزنگاری آن (WEP) ضعیف است و بسادگی می‌تواند شکسته شود. با این وجود در غیاب روشهای بهتر می‌توانید آنرا فعال سازید. به یاد داشته باشید که اگر فردی واقعاً بخواهد انتقال اطلاعات شما (مانند رمز عبور) را بررسی کند استفاده از این روش بسیار آسیب‌پذیر خواهد بود. البته یک روش جدید رمزنگاری (WPA) وجود دارد که کاستیهای WEP را رفع می‌کند و در تجهیزات جدیدتر قابل استفاده می‌باشد. استفاده از این روش در شبکه‌های مبتنی بر Wi-Fi اکیداً توصیه می‌شود.

تلفنهای سیار

تلفنهای سیار (که تلفنهای دستی یا تلفنهای همراه نیز نامیده می‌شوند) به شکل گسترده‌ای برای انتقال صوت بکار می‌روند و گاهی اوقات نیز می‌توانند برای انتقال اطلاعات مورد استفاده قرار گیرند. بسیاری از فناوریهای تلفن سیار می‌توانند مورد استراق سمع و شنود قرار بگیرند و لذا ایمن نمی‌باشند.

خطوط دور برد

ارتباطات طولانی خصوصاً برای مناطق دوردست معمولاً با استفاده از فناوریهای بی‌سیم مهیا می‌شود. این خطوط می‌توانند به چندین کاربر بطور همزمان خدمات ارائه دهند. اگر روش انتقال بصورت مستقیم باشد (با استفاده از آنتنهای بشقابی یا آنتنهای یاگی) استراق سمع بدون تجهیزات خاص دشوار خواهد بود. این ارتباطات درصورت لزوم می‌توانند با استفاده از تجهیزات سخت‌افزاری رمزنگاری بصورت رمزی درآیند.

تلفنهای بی‌سیم حلقهٔ محلی[۹۹]

این فناوری در منازل و ادارات بسیاری از کشورها بکار می‌رود و نصب کم‌هزینه و بی‌نقص خطوط تلفن را میسر می‌سازد و مشکلاتی که تجهیزات زیرساختهای سیمی دارند را ندارد. از طرف دیگر برخلاف سیمهای مسی، تجهیزات بی‌سیم در میانهٔ راه قابل دزدیدن و فروختن نیستند، اما همانند تلفنهای سیمی هنگامیکه یک مودم به این خطوط متصل می‌شود می‌توانند بجای اطلاعات صوتی، سایر انواع اطلاعات را انتقال دهند. فناوری بی‌سیم ممکن است قابل شنود باشد. بسته به موقعیت محلی، قوانین کشوری و مقررات محلی می‌توانید از ISP خود درخواست کنید که رمزگذاری‌شدن ارتباط را بررسی نماید.

سایر مسائل اینترنتی

اشتراک فایل

درصورت وجود بیش از یک رایانه، استفاده از فایلهای اشتراکی یکی از مهمترین و کاربردی‌ترین ابزار موجود در شبکه می‌باشد. در ساده‌ترین حالت، این ویژگی شما را قادر می‌سازد درحالیکه در یک سیستم فعالیت می‌کنید 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 می‌توانند هر دو در یک

96 *Wireless LANs*
97 *Wireless Fidelity*
98 *Wired Ethernet*

99 *Local Loop Wireless Telephones*

اتاق یا هرکدام در یک نیمکرهٔ زمین باشند. اشتراک فایل این امکان را فراهم می‌سازد که در طول مسافرتها بتوانید به فایلهای رایانهٔ خود دسترسی داشته باشید.

یک رایانهٔ منفرد که بعنوان *سرویس‌دهندهٔ فایل*[۱۰۰] عمل می‌کند می‌تواند بعنوان دیسک سخت تعداد زیادی رایانه تلقی گردد. در اینصورت بیشتر فایلهای شما در سرویس‌دهندهٔ فایل قرار می‌گیرند و بنابراین می‌توانید از طریق شبکه به آنها دست یابید.

آسیب‌پذیری واضحی که در اینجا وجود دارد این است که اگر شما بتوانید به فایلهای خود از راه دور دست پیدا کنید، افراد دیگر نیز می‌توانند اینکار را انجام دهند. یک آسیب‌پذیری ضعیفتر این است که اگر فایلها را با دیگران به‌اشتراک بگذارید، در برابر آسیب‌پذیریهایی که ممکن است برای رایانهٔ آنها پیش آید در امان نخواهید بود. مثلاً اگر رایانه‌ای که به فایلهای شما دسترسی داشته توسط یک ویروس آلوده شود، ممکن است فایلهای شما نیز آلوده گردند.

قانون پانزدهم:

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

قانون شانزدهم:

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

قانون هفدهم:

اگر فایلها را با دیگران به اشتراک می‌گذارید مطمئن شوید آنها مسائل امنیتی را جدی می‌گیرند.

قابلیتهای اشتراک فایل و دسترسی از راه دور این امکان را فراهم می‌سازند که برای کنترل دسترسی از نام کاربری و رمزهای عبور استفاده کنید، و نامهای کاربری و رمزهای عبور شما را قادر می‌کنند بتوانید آنچه که یک کاربر انجام می‌دهد (خواندن، نوشتن، ایجاد و پاک نمودن) را کنترل نمایید. بسیاری از سیستمها می‌توانند تمامی اعمال یک کاربر را کنترل نمایند. بعنوان مثال می‌توانید تسهیلات دسترسی از راه دور را بگونه‌ای محدود سازید که به فایلها تنها اجازهٔ خوانده‌شدن بدهد. به عبارت دیگر اگر نیازی به دسترسی نوشتن ندارید باید آنرا غیر فعال کنید.

سیستمهایی که از بعضی قابلیتهای اشتراک فایلها پشتیبانی می‌کنند می‌توانند 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 اختصاصاً برای کارهای چاپی صادر شده، امکان اعمال خرابکارانه را فراهم کنند.

پیامهای فوری

قابلیت ارسال پیام فوری این امکان را فراهم می‌سازد که پیام تایپ‌شده روی یک رایانه همزمان روی رایانه‌های 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 نرم‌افزارهای متفاوتی دارد. در میان آنها می‌توان به MSN Messenger، *IRC*[۱۰۱]، Yahoo Chat، *AIM*[۱۰۲]، و نیز *ICQ*[۱۰۳] اشاره نمود.

ارتباطات اینترنتی از قبیل AOL، MSN، Yahoo، میزبانهای بازیهای اینترنتی و... هریک دارای Messenger و Chat مخصوص به خود هستند. بعضی از آنها با سایرین تبادل اطلاعات می‌کنند و برخی دیگر چنین کاری انجام نمی‌دهند.

بسیاری از سیستمهای ارسال پیام فوری به کاربر اجازه می‌دهند اسمی انتخاب کند که همراه پیامهای ارسالی‌اش 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 IP شناسایی کنند.

---

100 File Server

101 Internet Relay Chat

102 AOL Instant Messenger

۱۰۳ یک علامت اختصاری برای عبارت "I Seek You"

قانون هجدهم:

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

قابلیت ارسال پیام فوری به چند دلیل نقش مفیدی ایفا می‌کند:

- استفاده از آن نسبت به پست الکترونیکی راحت‌تر و سریعتر است و تقریباً هیچ تأخیری ندارد. این مسئله باعث می‌شود گفتگوهای انجام‌شده در آن عملی‌تر از نامه‌های الکترونیکی باشند.
- درحالیکه مشغول انجام کار دیگری هستید پیام در پنجرهٔ کوچکی روی صفحهٔ شما دریافت و ارسال می‌گردد و چندان باعث ایجاد وقفه در سایر کارهایتان نمی‌شود.
- نیازی نیست که آدرس پست الکترونیکی (و هویت) خود را برای سایر شرکت‌کنندگان در گفتگوهای انجام‌شده در پیامهای فوری فاش کنید.

در موارد خاص استفاده از قابلیت ارسال پیام فوری نسبت به نامهٔ الکترونیکی ارجح است. درنظر بعضی افراد استفاده از این سرویس ایمن‌تر نیز هست؛ چراکه پیامها در مکانهای دیگر دیسک کپی نمی‌شوند، درصورتیکه در پست الکترونیکی این اتفاق می‌افتد. به هرحال هنوز به کاربران هشدار داده می‌شود که ممکن است پیامهای فوری آنها ایمن نباشد. مشکل اصلی سیستمهای ارسال پیام این است که بعضی از آنها قابلیت انتقال فایل هم دارند. این موضوع آنها را مانند سایر قابلیتهای اشترک فایل – مثل ضمائم نامه‌های الکترونیکی – دچار مشکل می‌کند. برخی از سیستمهای ارسال پیام فوری اجازهٔ اجرای دستورات از راه دور را نیز می‌دهند و اینکار می‌تواند منجر به وقوع تهاجم گردد.

خدمات فعال غیرضروری

سیستم‌عاملها و برنامه‌های کاربردی بسیار قدرتمند و کاراً هستند. در بیشتر موارد کاربر عادی تمام قابلیتهای موجود در نرم‌افزارها را لازم ندارد. خدماتی که مورد نیاز نیستند باید غیرفعال شوند. متأسفانه بعضی از عرضه‌کنندگان نرم‌افزار تمامی قابلیتهای برنامه‌های خود را فعال می‌کنند و بستگی به کاربر دارد که از آنها استفاده کند یا نکند، و در غالب موارد هم کاربر از وجود این خدمات آگاه نیست. بعنوان مثال برای چندین سال متوالی بعضی از سیستمهای UNIX بگونه‌ای طراحی شده بودند که هر دستگاه مجهز به آنها بتواند بعنوان یک مرکز پست الکترونیکی غیر محدود عمل نماید (البته اگر این قابلیت توسط کاربر غیرفعال نمی‌شد). این مسئله به هرزنامه‌نویس‌ها امکان داد که از این دستگاهها برای توزیع هرزنامه‌ها استفاده کنند، بدون آنکه بسیاری از صاحبان دستگاهها از وجود چنین قابلیتی آگاهی داشته باشد.

قانون نوزدهم:

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

عرضه‌کنندگان نرم‌افزارها بطور فزاینده‌ای درحال آگاه‌شدن از مشکلات هستند. بنابراین علیرغم علاقهٔ آنها به توسعه و عرضهٔ سیستمهایی با توانمندیهای زیاد، برنامه‌های خود را با خدمات فرعی غیرفعال‌شده منتشر می‌کنند؛ و کاربر درصورت نیاز می‌تواند هریک از آنها را فعال سازد. غیرفعال بودن خدماتی که از آنها استفاده خاصی نمی‌شود اهمیت زیادی دارد. چنین خدماتی شامل اشتراک فایلها و چاپگر، سرویس‌دهنده‌های وب، سرویس‌دهنده‌های پست الکترونیکی، سرویس‌دهنده‌های *پروتکل انتقال فایل* (FTP Servers)[۱۰۴]، *سرویس‌دهنده‌های فراخوانی تابع از راه دور* (RPC Servers)[۱۰۵] و غیره می‌باشند.

104 File Transfer Protocol Servers
105 Remote Procedure Call Servers

فصل هفتم
ابزارهایی برای ارتقای امنیت

کلیات

در این فصل بسته‌های نرم‌افزاری امنیتی و روشهای افـزایش امنیت شبکه‌ها و رایانه‌ها مورد بررسی قرار می‌گیرد. منظور از بسته‌های نرم‌افزاری امنیتی همان ویروس‌یابها، دیـواره‌هـای آتش، و ابزارهای دسترسی از راه دور است.

ویروس‌یاب

قانون بیستم:
روی هر رایانهٔ آسیب‌پذیر نسبت به ویـروس بایـد نـرم‌افـزار ضـدویروس نـصب شـود و هـر روز به‌روزرسانی گردد. همچنین دستگاه باید بـصورت دوره‌ای برای یافتن ویروس جستجوی کامل شود.

قانون بیست و یکم:
در مورد رایانه‌هایی که تحت تأثیر ویروسـها قـرار نمی‌گیرنـد (ماننـد سیـستمهای مبتنـی بـر Unix) بایـد اطمینان حاصل شود که نامهٔ الکترونیکـی ارسـالی حاوی ویروس نیست تـا بـه گیرنـده نیـز آسـیبی نرسد.

قانون بیست و دوم:
سیستم‌عاملها و نرم‌افزارهای کاربردی مهم خود را به‌روزرسانی نمایید و به خاطر داشـته باشـید کـه ویروس‌یابها تنها ویروسهای مهاجم بـه فایلهـا را بررسـی مـی‌کننـد؛ درحالیکـه آسـیب‌پـذیری سیستم‌عاملها و برنامه‌های کاربردی ممکن اسـت موجب آسیب دیدن سیستم از ابعاد دیگر شوند.

ویروس‌یابها به روشهای زیر رایانهٔ شما را از ویروسها، کرمهـا و تراواهای شناخته‌شده ایمن می‌سازند:

- هر زمان که به فایلی دسترسی داشـته باشـید یـا آنـرا کپی، ذخیره، منتقل، باز یا بسته نمایید، جلـوی آسـیب رساندن ویروسها به سیستم را می‌گیرند.
- هرگاه یک دیسک خارجی وارد دستگاه خود کنید آنـرا برای یافتن ویروسهای احتمالی بررسی می‌نمایند.
- هر زمان که یک نامهٔ الکترونیکی دریافت شـود، خـود نامه و ضمائم آن برای عاری بودن از هر نوع ویـروس مورد بررسی قرار می‌گیرند.
- هرگاه فـایلی از یـک پایگـاه وب download شـود مورد بررسی قرار می‌گیرد.
- در بیشتر موارد زمانیکه یک صفحهٔ وب و نرم‌افزارهای جاسازی شده در آن به رایانهٔ شما download شـود بررسی می‌گردد.
- با اسـتفاده از ایـن برنامـه‌هـا مـی‌توانیـد یـک فایـل، مجموعه‌ای از فایلها و یا تمامی دیـسکهای موجـود را برای ویروس بررسی نمایید.
- اگر یک ویروس، کرم، یا تراوا شناسایی شود، این ابزار آنرا از بین می‌برد یا اگر نتواند اینکار را انجام دهـد بـه شما اطلاع می‌دهد که این مشکل قابل رفع نیـست؛ و درنتیجه فایل خراب را قرنطینه می‌کند و بدینوسـیله از آسیب دیدن سایر قسمتهای سیـستم فایـل جلـوگیری می‌نماید.

وجـود یـک ویـروس‌یـاب حـاوی *نـشانهای ویـروس*[۱۰۶] به‌روزرسانی شده ("نشان" مشخصهٔ خاصی از یک ویـروس اسـت کـه ویروس‌یاب توسط آن می‌تواند نوع ویروس را تشخیص دهـد)، یکـی از مهمترین قسمتهایی از یک شـبکه اسـت کـه مـی‌توانـد بـه اینترنـت متـصل باشـد. توجـه داشـته باشـید کـه بتـازگی ویروسهایی برای محیط UNIX درحال گسترش هستند، امـا کرمها و تراواها برای این محیط از قبل وجود داشته‌اند.

تا اواخر آگوست ۲۰۰۳ یکـی از ضدویروسـهای دسـتگاههای شخـــصی و Macintosh (ضـــدویروس Norton) تقریبـــاً

106 *Virus Signatures*

می‌توانست ۶۵۰۰۰ ویروس مختلف را شناسایی کند. آگوست ۲۰۰۳ از نظر انتشار نرم‌افزارهای مخرب ماه جالبی بود، چراکه بسیاری از کرمها که در آن ماه منتشر شدند از یک آسیب‌پذیری بسیار حیاتی در سیستم‌عامل Windows بهره‌برداری می‌کردند (Blaster و SoBig از رایجترین آنها بودند). یکماه پیشتر مایکروسافت برای آن وصله‌ای منتشر کرده بود، اما افراد کمی آنرا نصب کرده بودند و به همین دلیل کرمهای جدید توانستند به دستگاههای زیادی آسیب بزنند و به سرعت در آنها پخش شوند؛ بگونه‌ای که شاید در این زمینه رکوردهای جدیدی به ثبت رسیده باشد. در شلوغترین روز آن ماه، ویروس‌یاب Norton حدود ۵۰ نشان جدید ویروس را به فهرست ویروسهای قابل شناسایی خود اضافه نمود. این عدد تا یکماه بعد از آن به حدود ۵۲۰ رسید.

دیوارهٔ آتش

یک دیوارهٔ آتش تمامی فعالیتهای داخل یا خارج از شبکه را بررسی می‌کند و بر اساس مجموعه قوانین موجود در خود به *ترافیک*[۱۰۷] اجازه می‌دهد که از شبکه عبور کند یا آنرا متوقف می‌سازد. دیوارهٔ آتش می‌تواند به شکل یک برنامهٔ روی رایانه نصب شود یا قسمتی از تجهیزات میان رایانه (یا گروهی از رایانه‌ها) و ارتباط شبکه‌ایِ آن باشد. گاهی اوقات دیوارهٔ آتش در بعضی تجهیزات دیگر مانند *مسیریابها*[۱۰۸] قرار داده می‌شود. این نوع دیواره‌های آتش معمولاً رایگان و از پیش نصب‌شده هستند و در بسیاری از سیستم‌عاملها وجود دارند.

قانون بیست و سوم:

تمامی رایانه‌ها باید توسط یک دیوارهٔ آتش محافظت شوند که می‌توان آنرا بصورت نرم‌افزار در هر رایانه نصب نمود یا بصورت یک دیوارهٔ آتش سخت‌افزاری برای تمامی شبکهٔ محلی قرار داد.

با درک این موضوع که دیوارهٔ آتش چه کاری انجام می‌دهد و چگونه می‌توان قوانینی برای کنترل آن تنظیم نمود باید مفهوم پروتکل TCP/IP – مجموعه قوانینی که تمامی پیامهای ارسالی از طریق اینترنت را کنترل می‌کند – را نیز دریابید. اگر با پروتکل TCP/IP آشنا هستید می‌توانید به فصل بعدی مراجعه کنید اما اگر آنرا نمی‌شناسید ابتدا ضمیمهٔ ۲ همین بخش را مطالعه نمایید. توجه داشته باشید حتی درصورتیکه نخواهید این جزئیات را بیاموزید همچنان می‌توانید از دیوارهٔ آتش استفاده کنید. در ادامه تمامی آنچه که لازم است بصورت خلاصه در مورد TCP/IP بدانید ذکر می‌شود:

- دستگاههایی که به اینترنت متصل هستند دارای یک آدرس IP به شکل 12.222.103.43 می‌باشند که همانگونه که می‌بینید متشکل از چهار عدد مجزا است. اینترنت برای پیدا کردن مسیر پیام از این آدرس استفاده می‌کند و هر رایانه با ارائه آدرس مقصد در چنین قالبی مشخص می‌کند که این پیامها باید به کجا ارسال شوند.
- در هر دستگاه برنامه‌های مختلف بوسیله *شمارهٔ پورت*[۱۰۹] شناسایی می‌شوند (مانند شماره تلفنهای داخلی تلفن در شرکتهای بزرگ – تنها یک شماره تلفن عمومی وجود دارد، اما هر اتاق شمارهٔ داخلی مربوط به خود را دارد).
- اطلاعاتی که به رایانه یا از آن فرستاده می‌شوند، *بسته*[۱۱۰] نام دارند.
- از کلمات TCP و UDP در بحث زیر چشم‌پوشی کنید و چندان نگران از دست دادن جزئیات نباشید.

چرا به دیوارهٔ آتش نیاز داریم؟

اگر رایانهٔ شما به شبکهٔ محلی یا اینترنت متصل نیست نیازی به دیوارهٔ آتش ندارید. همینکه به شبکه متصل شوید این احتمال پدید می‌آید که مهاجمین رایانهٔ شما را مورد سوء استفاده قرار دهند. بعنوان مثال:

- اگر از اشتراک فایل، اشتراک چاپگر یا سایر خدمات رایانه‌ای استفاده می‌کنید، رایانهٔ شما روی پورتهای مشخصی به انتظار می‌ایستد (در اصطلاح گفته می‌شود که رایانه آن پورت را "می‌شنود"). اگرچه با انجام اینکار می‌توانید منابع خود را با رایانهٔ دیگری به‌اشتراک

۱۰۷ منظور اطلاعات تبادل شده روی شبکه است
108 Router

109 Port Number
110 Packet

بگذارید، اما ممکن است رایانهٔ دیگری در هر نقطهٔ دنیا نیز بتواند اطلاعات شما را مشاهده نماید.

- اگر بتوانید روی پورتهای اشتراک فایل به انتظار بایستید، ممکن است به دلیل وجود اشکالات، شخصی بتواند برایتان پیام ماهرانه‌ای بفرستد و از آن طریق اعمال مخربی روی رایانهٔ شما انجام دهد. متأسفانه درحال حاضر این نوع حمله بسیار رایج شده است.
- حتی اگر نتوانید روی هیچ پورتی منتظر پیام بمانید رایانه‌های دیگر همچنان می‌توانند پیامهای زیادی برای شما ارسال نمایند. اگرچه می‌توان از تمامی آنها صرفنظر کرد اما پیامها می‌توانند ارتباطات شبکه‌ای شما را مسدود کنند و باعث شوند نتوانید کارهای خود را انجام دهید (در این مورد فقط دیواره‌های آتش سخت‌افزاری می‌توانند به شما کمک نمایند).
- اگر علیرغم تلاشهای بسیار، توسط ویروس، کرم یا تراوا آلوده شدید، ممکن است تمام اطلاعات موجود در رایانه برای نویسندهٔ نرم‌افزار مخرب ارسال شود. این مورد شامل داده‌ها و تمامی آنچه که در رایانهٔ قربانی ثبت شده (از جمله رمزهای عبور) می‌شود.

دیواره‌های آتش چگونه کار می‌کنند؟

دیوارهٔ آتش تمامی بسته‌هایی که به رایانهٔ شما ارسال می‌شود را نظارت و بررسی می‌کند که آیا با قوانین درنظر گرفته شده مغایرت دارد یا خیر. اگر چنین بود راه عبور بسته‌ها مسدود می‌شود. در دیواره‌های آتش نرم‌افزاری و سخت‌افزاری بهتر است قوانین زیر پیاده شوند:

- اجازه ندهید هیچ بسته‌ای از پورتهای 135، 137، 139، و TCP/UDP 445 عبور کند. این پورتها برای سرویس اشتراک فایل و انواع دیگری از خدمات Windows مورد استفاده قرار می‌گیرند. با متوقف ساختن این بسته‌ها اطمینان خواهید یافت که هیچکس از طریق اینترنت نمی‌تواند برای استفاده از این خدمات با رایانهٔ شما ارتباط برقرار کند.
- اجازه ندهید هیچ بسته‌ای از پورتهای 135، 137، 139، و TCP/UDP 445 عبور کند، مگر آنکه آدرس IP مبدأ آن مربوط به یکی از رایانه‌هایی باشد که شما مایلید از خدمات آن استفاده کنید.
- می‌توانید فهرستی از رایانه‌های مورد اطمینانی که به شبکه آسیب نمی‌رسانند را برای دیوارهٔ آتش تعریف کنید تا تنها رایانه‌های مطمئن بتوانند با شما ارتباط برقرار کنند. با انجام اینکار همچنان می‌توانید با سایر رایانه‌ها مانند سرویس‌دهنده‌های وب در اینترنت نیز ارتباط برقرار کنید، اما برای اینکار شما باید آغاز کنندهٔ آن ارتباط باشید.

دیواره‌های آتش نرم‌افزاری منابع موجود در رایانه را بکار می‌گیرند، اما با این مزیت که تنها محتوای اطلاعات (همراه با آدرسها و پورتهای فرستنده یا گیرندهٔ آن) را بررسی نمی‌کنند؛ بلکه می‌توانند بررسی کنند که چه برنامه‌ای پیام را ارسال نموده است. اگر یک برنامهٔ غیرمجاز با رایانهٔ شما ارتباط برقرار کرده باشد، دیوارهٔ آتش قبل از عبور دادن آن می‌تواند از شما کسب اجازه کند. دیوارهٔ آتش سخت‌افزاری نمی‌تواند تشخیص دهد که از کدام برنامه برای ارسال پیام استفاده شده؛ اما از آنجا که یک قسمت از تجهیزات سخت‌افزاری است، سرعت رایانه را پایین نمی‌آورد.

اگر دارای یک دیوارهٔ آتش سخت‌افزاری یا نرم‌افزاری هستید مشابه تمامی تجهیزات امنیتی دیگر باید همیشه آنرا به‌روزرسانی کنید. خرابکاران بسیار خلاق هستند و لذا به‌روز بودن ابزارهایی که برای حفاظت از سیستم خود بکار می‌برید از اهمیت زیادی برخوردار است.

فضاهای آدرس خصوصی[111]

طراحی اینترنت از ابتدا بدینصورت بود که هر رایانه یا دستگاه موجود در آن آدرس مخصوص به خود را داشت و لذا هر رایانه می‌توانست با رایانهٔ دیگر ارتباط برقرار کند. امروزه به دلایل زیادی برقراری ارتباط جهانی در این سطح چندان مطلوب نیست. دو دلیل عمده برای این مسئله وجود دارد:

- گاهی اوقات می‌خواهید مجموعه‌ای از رایانه‌ها را بصورت مجزا از بقیه نگهداری کنید تا نتوانند بطور مستقیم با سایر رایانه‌ها در اینترنت ارتباط داشته

111 *Private Address Spaces*

باشند. این مسئله‌ای است که در مورد رایانه‌های برخی از سازمانهای عمومی و خصوصی وجود دارد.

- از آنجا که آدرسهای IP در محیط اینترنت اختصاص داده می‌شوند ممکن است سازمان شما به تعداد کافی آدرس IP نداشته باشد که بخواهد به همهٔ ماشینها اختصاص دهد. این مسئله اغلب در کشورهای درحال توسعه وجود دارد که در آنها اینترنت ملی چند سال بعد از ایجاد شبکه‌های ارتباطی کشورهای توسعه‌یافته بوجود آمد.

آدرسهای IP مشخصی وجود دارند که در اینترنت مورد استفاده قرار نمی‌گیرند. این آدرسها "فضاهای آدرس خصوصی" نامیده می‌شوند و می‌توانند در دو مورد ذکر شده بکار روند. از آنجا که رایانه‌هایی که از فضاهای آدرس خصوصی استفاده می‌کنند بصورت مستقیم با اینترنت ارتباط برقرار نمی‌کنند به آدرسهای منحصر به فرد نیاز ندارند. اگرچه سازمانهای مختلفی ممکن است از مجموعه آدرسهای مشابهی استفاده کنند، اما هیچیک از آنها نمی‌توانند سایرین را ببینند و لذا این آدرسهای مشابه هیچ مشکلی پدید نمی‌آورند.

دو روش وجود دارد که با استفاده از آنها یک رایانه که آدرس خصوصی دارد می‌تواند با اینترنت ارتباط برقرار کند:

سرویس‌دهنده‌های Proxy[۱۱۲]

سرویس‌دهندهٔ proxy نوع خاصی از دیوارهٔ آتش است. این سرویس‌دهنده دارای یک آدرس در فضای آدرس خصوصی است اما همچنین یک ارتباط و آدرس ثانویه نیز برای اتصال به اینترنت دارد. اگر کاربری بخواهد از یک دستگاه با آدرسی در فضای خصوصی به اینترنت متصل شود، پیام خود را به سرویس‌دهندهٔ proxy ارسال می‌کند و از آن می‌خواهد که پیام را به مقصد مورد نظر در اینترنت برساند. این سرویس‌دهنده درخواست را بعد از فرستادن روی اینترنت نگهداری می‌کند و زمانیکه پاسخ آن بازگشت آنرا به دستگاه درخواست‌کننده بازپس می‌فرستد.

سرویس‌دهنده‌های proxy همچنین می‌توانند برای آدرسهای IP عادی مورد استفاده قرار گیرند. آنها برای کنترل نوع ترافیک عبوری اینترنت یا تسهیل ارتباطات کاربر و شبکه بکار می‌روند. یک سرویس‌دهندهٔ proxy وب یک نسخه از صفحات درخواست‌شده را نگهداری می‌کند و درصورتیکه کاربر دیگری همان صفحه را درخواست کند نسخه‌های نگهداری شده را برای وی ارسال می‌نماید؛ و با اینکار پهنای باند مورد نیاز اینترنت کاهش می‌یابد. این مکانیزم caching نامیده می‌شود.

NAT[۱۱۳]

NAT جایگاهی بین شبکهٔ محلی و اینترنت دارد و مشابه سرویس‌دهندهٔ proxy با اینترنت و شبکهٔ محلی که آدرسهای IP خصوصی در آن بکار می‌رود مرتبط می‌باشد. زمانیکه یک پیام با استفاده از NAT از شبکهٔ محلی به اینترنت ارسال می‌شود، NAT آنرا با استفاده از آدرس IP خود ارسال می‌کند و اینطور وانمود می‌کند که پیام از پورتی فرستاده شده که درحال استفاده نیست، و هنگامیکه پاسخ پیام دریافت می‌شود، به رایانهٔ اصلی در شبکهٔ محلی باز می‌گردد. NAT شبیه سرویس‌دهندهٔ proxy عمل می‌کند، اما برای همهٔ انواع ترافیک (و نه فقط ترافیک web) بکار می‌رود و از مکانیزم caching نیز استفاده نمی‌نماید.

سرویس‌دهنده‌های proxy و NAT هر دو مثل دیواره‌های آتش هستند و از دستگاههایی که در فضاهای آدرس خصوصی قرار دارند در برابر انواع حملات بیرونی محافظت می‌کنند.

ابزارهای دسترسی، مدیریت، و راهبری از راه دور

ابزارهای دسترسی از راه دور[۱۱۴]، *ابزارهای مدیریت از راه دور*[۱۱۵] و *ابزارهای راهبری از راه دور*[۱۱۶] این امکان را فراهم می‌کنند که رایانهٔ خود را از راه دور و از طریق خط تلفن یا

112 *Proxy Servers*

113 *Network Address Translation*
114 *Remote Access Tools*
115 *Remote Management Tools*
116 *Remote Administration Tools*

اینترنت کنترل نمایید. هنگامیکه با این روش به رایانهٔ خود متصل می‌شوید مثل این است که پشت صفحه‌کلید دستگاه خود نشسته‌اید.

قانون بیست و چهارم:
اگر از امکانات دسترسی از راه دور برای کنترل رایانه‌ها استفاده می‌کنید مطمئن شوید که از ایمنی لازم (نامهای کاربری و رمزهای عبور مناسب) برخوردارند، تا مهاجمین نتوانند از این ابزارها علیه شما استفاده کنند.

ابزارهای دسترسی از راه دور کاربردهای مهم بسیاری دارند. از میان آنها می‌توان به موارد زیر اشاره کرد:

- زمانیکه به رایانهٔ ادارهٔ خود دسترسی فیزیکی ندارید این امکان را فراهم می‌کنند که از آن استفاده نمایید. با اینکار می‌توانید به داده‌ها، برنامه‌های کاربردی و خدمات شبکه‌ای محل کارتان دسترسی داشته باشید.
- اجازه می‌دهند رایانهٔ خود را برای معاینه به یک متخصص نشان دهید؛ بدون آنکه وی را به محل کار خود ببرید.
- افراد زیادی خواهند توانست از برنامه‌های کاربردی که تنها بر روی یک دستگاه نصب شده استفاده کنند.
- مسئولین پشتیبانی سیستمها با استفاده از آنها می‌توانند چندین سرویس‌دهنده را به آسانی مدیریت نمایند.

ابزارهای دسترسی از راه دور این امکان را برای مهاجمین نیز فراهم می‌کنند که بتوانند تمامی موارد ذکر شده را انجام دهند. در حقیقت میان ابزارهای دسترسی از راه دور در کاربردهای مذکور (مانند pcAnywhere) و دربهای مخفی تراواها (مثل Back Orifice یا NetBus) تفاوت عملکرد چندانی وجود ندارد.

آشکارگرهای بدافزارها

فرض کنیم شما نرم‌افزار خود را به‌روزرسانی می‌کنید، ویروس و فایلهای دریافتی را مورد بررسی قرار می‌دهید، از نامهای کاربری و رمزهای عبور مستحکم استفاده می‌نمایید و یک دیوارهٔ آتش مناسب را نیز برای محافظت از سیستم خود بکار می‌برید.

حال اگر سؤال شود با تمام این کارها آیا کاملاً ایمن هستید؛ باز هم پاسخِ مثبت از اطمینان صد درصدی برخوردار نیست. همیشه این احتمال وجود دارد که قبل از ارائه راه‌حل برای یک اشکال، شما از همان اشکال آسیب ببینید. همچنین ممکن است هر از چندگاه کاری انجام دهید که نتوان آنرا کاملاً ایمن دانست.

"آشکارگرهای بدافزارها" برنامه‌هایی هستند که برای یافتن برنامه‌های مشکوک – صرفنظر از چگونگی نصب آنها – رایانهٔ شما را مورد بررسی قرار می‌دهند. بعضی مواقع عملکرد آنها با جستجوگرهای ویروس تداخل دارد، زیرا هر دوی آنها نرم‌افزارهای مخرب موجود در دیسک را شناسایی نموده، بررسی می‌کنند که برنامه‌های کلیدی سیستم بصورت مخفیانه تغییر نکرده باشند.

این آشکارگرها plug-inها و add-onهای مرورگرها را بررسی می‌کنند و هرآنچه که به سیستم شما آسیب می‌رساند و یا برخلاف قوانین محرمانگی است را شناسایی می‌نمایند. برخی از این نرم‌افزارها دارای ابزارهایی برای از بین بردن بدافزارهای شناسایی‌شده نیز هستند.

ثبت رخدادها

فایلهای ثبت رخدادها ابزار مناسبی هستند که امنیت رایانهٔ شما را تضمین می‌کنند اما معمولاً زیاد مورد توجه قرار نمی‌گیرند. فایلهای ثبت روی دیسک قرار دارند و برنامه‌ها می‌توانند در آن پیام بنویسند. معمولاً پیام هنگامی نوشته می‌شود که یک اتفاق رخ می‌دهد یا اشکالی بوجود می‌آید.

قانون بیست و پنجم:
قابلیت ثبت رخدادهای توابع سیستم و برنامه‌های کاربردی باید بصورت صحیح فعال باشند.

نمونه‌هایی از وقایعی که می‌توانند ثبت شوند عبارتند از:

- رایانه روشن شد؛
- شخصی وارد سیستم شد؛

- شخصی سعی داشت وارد سیستم شود اما رمز عبور وی اشتباه بود؛
- یک نامهٔ الکترونیکی دریافت شد؛
- یک نامهٔ الکترونیکی می‌خواست فرستاده شود اما ارتباط قطع شد؛
- خطاهای زیادی روی دیسک (یا ارتباط شبکه‌ای) پیش آمد؛
- دیوارهٔ آتش یک ارتباط غیرمجاز را شناسایی و آنرا مسدود کرد؛
- جستجوگر ویروس بطور خودکار مجموعهٔ جدیدی از نشانهای ویروس را download نمود؛
- یک ویروس‌یاب تمامی فایلهای موجود در سیستم را بررسی و یک ویروس را شناسایی کرد.

بسته به برنامه و سیستمی که برنامه روی آن اجرا می‌شود، ممکن است فایلهای ثبت بعد از زیاد شدن حجمشان پاک شوند، یا اینکه هر چند وقت یکبار فایل ثبت جدیدی ایجاد گردد و فایلهای قدیمی‌تر برای بررسیهای بعدی همچنان حفظ شوند (عمدتاً در قسمتی از نام فایلهای ثبت یک تاریخ وجود دارد).

بطور کلی برای هر سیستم و نرم‌افزار کاربردی یک فایل ثبت مجزا وجود دارد. گاهی اوقات می‌توانید این فایل را با یک ویرایشگر متن بخوانید و گاهی نیز برای خواندن و قالب‌بندی فایلها به ابزارهای خاصی نیاز خواهید داشت.

ثبتها بسیار مفید هستند و بطور کلی باید فعال باشند. در عین حال باید مراقب باشید که آنها را برای فعالیتهای روزمره و عادی فعال نکنید؛ زیرا سیستم باید وقت زیادی برای انجام ثبت و بررسی آنها صرف کند و حجمی از دیسک نیز توسط آنها اشغال می‌گردد.

اگر بدانید که اقلام مشروح فایلهای ثبت چه چیزهایی را نشان می‌دهند باید آنها را بطور دوره‌ای مرور کنید تا ببینید آیا اتفاق غیرعادی رخ داده یا خیر. در غیر اینصورت ثبتها باید بگونه‌ای نگهداری شوند که درصورت وقوع اتفاقات غیرطبیعی بتوانند راهنماییهایی برای کشف دقیقتر آنچه که رخ داده باشند.

فصل هشتم
نکات ویژهٔ بسترهای مختلف

رایانه‌های شخصی مبتنی بر Windows

نقاط قوت و نقاط ضعف

سیستم‌عامل Windows پردازندهٔ Intel x86 (یا معادلهای آن) رایجترین سیستم رایانه‌ای است که تاکنون طراحی شده است. قابلیتهای این سیستم‌عامل و نرم‌افزارهای کاربردی آن از دیدگاه یک کاربر بسیار جذاب هستند و تعداد زیادی نرم‌افزار تجاری، نرم‌افزار shareware و نرم‌افزار رایگان برای آن موجود است. اگرچه مشابه هر سیستم دیگر در اینجا هم افراد متخصص به سختی پیدا می‌شوند، اما متخصصین زیادی با سطح دانش قابل قبول برای کار با این سیستمها وجود دارند. همچنین رقبای زیادی در بعد سخت‌افزار با هم رقابت می‌کنند که این خود باعث تنوع محصولات و قیمتهای نسبتاً پایین آنها شده است.

Windows از نظر امنیتی وضعیت چندان جالبی ندارد. *هستهٔ سیستم‌عامل*[۱۱۷] با ملاحظهٔ مسائل امنیتی ارتباطات شبکه‌ای طراحی نشده بود و هرچند در نسخه‌های جدیدتر آن (Windows 2000 و Windows XP و...) به بسیاری از این موارد پرداخته شده، اما هنوز ایمنی لازم وجود ندارد و تغییرات اخیر به کاربرانی که از سیستمهای قدیمی‌تر استفاده می‌کردند کمک اندکی نموده است. تا همین اواخر مایکروسافت توجه زیادی به مقولهٔ امنیت نداشت. البته درحال حاضر این شرایط تغییر کرده‌اند، بویژه آنکه این شرکت توجه خود را به اشکالات موجود در نرم‌افزارهای چندرسانه‌ای و دیگر آسیب‌پذیریهای سیستم‌عاملهای خود معطوف داشته است.

عملکرد توسعه‌یافتهٔ سیستمها و نرم‌افزارها معمولاً باعث بالا رفتن هزینهٔ ایمن‌سازی آنها می‌شود. در بسیاری موارد بمنظور آسان کردن استفادهٔ کاربران تازه‌کار از ابزار، سیستمها دارای چندین زیرسیستم و قابلیتهای بسیار زیادی شده‌اند که آنها را آسیب‌پذیر کرده است. به دلیل کثرت آسیب‌پذیریها و نیز تعدد رایانه‌های مورد استفاده، دهها هزار رایانهٔ شخصی مبتنی بر Windows به اهداف اصلی برنامه‌نویسانی که بدافزارهایی مثل ویروس، کرم و تروا منتشر می‌کردند تبدیل شدند. واسطهای گرافیکی کاربر در Windows بسیار کاربرپسند هستند و هم‌اکنون میلیونها نفر با دانش فنی اندک توانایی استفاده از آنها را دارند. این روش مبتنی بر کاربر وقتی در کنار آسیب‌پذیریهای مذکور قرار می‌گیرد سیستمهای مبتنی بر Windows را مستعد بروز مشکلات امنیتی می‌کند.

چگونه از خود محافظت کنیم

تمامی مطالب این کتاب برای سیستمهای Windows قابل اعمال است و کاربرانی که نگران مسائل امنیتی هستند باید تمام توصیه‌های ارائه‌شده را جدی بگیرند.

انتشار نرم‌افزار

اگر پهنای باند کافی دارید، برای به‌روز نگه‌داشتن سیستم‌عامل خود با آخرین نسخهٔ ServicePackها از پایگاه به‌روزرسانی مایکروسافت[۱۱۸] استفاده کنید. در غیراینصورت وصله‌های امنیتی منتشرشده برای به‌روزرسانی Windows را بکار بگیرید (این وصله‌ها نسبت به Service Packها پهنای باند کمتری اشغال می‌کنند). اگر به‌روزرسانی از طریق پایگاه به‌روزرسانی مایکروسافت برایتان امکانپذیر نیست می‌توانید بسته‌های به‌روزرسانی را از مرکز download مایکروسافت[۱۱۹] دریافت کنید.

شاید ISP شما یا سایر فراهم‌آورندگان خدمات بتوانند به‌روزرسانی‌های منتشرشده را download و روی دیسک فشرده توزیع کنند. اگرچه منابع قابل‌توجهی برای اینکار مورد نیاز است، اما یک ابزار برای مدیریت به‌روزرسانی Windows در قالب خدماتی به نام Software Update Services برای سیستم‌عامل Windows 2000 در پایگاه زیر قابل دسترسی است:

117 *O.S. Kernel*

118 *http://windowsupdate.microsoft.com*
119 *http://www.microsoft.com/downloads*

http://www.microsoft.com/windows2000/windowsupdate/sus/

حسابهای کاربری

در سیستمهای Windows NT، Windows 2000 و Windows XP که از قابلیت *چندکاربری*[۱۲۰] پشتیبانی می‌کنند باید اطمینان حاصل کنید که هیچ حساب کاربری غیر ضروری در آنها ایجاد نشده است. علاوه بر آن مطمئن شوید که تمامی کاربران یک رمز عبور مناسب – بر اساس آنچه که در فصل سوم همین بخش توضیح داده شد – برای خود برگزیده‌اند. به کاربران باید تنها امتیازاتی که مورد نیاز آنها است داده شود. بعنوان مثال حتی اگر تنها یک دستگاه توسط کاربر اصلی خود راهبری شود، این کاربر برای کارهای روزمره و معمولی خود نباید از امتیازات راهبری استفاده کند.

اشتراک فایل

اگر از قابلیتهای اشتراک فایل یا اشتراک خدمات چاپ استفاده نمی‌کنید مطمئن شوید که غیرفعال شده‌اند. مراحل انجام اینکار در Windows Help و پایگاه اطلاع‌رسانی پشتیبانی مایکروسافت قابل دسترس می‌باشد. برای اینکار عبارت زیر را جستجو کنید: "disable file sharing xx" که در آن xx نسخهٔ سیستم‌عامل شما می‌باشد؛ مثلاً XP یا 2000. اگر از اشتراک فایل استفاده می‌کنید مطمئن شوید که هیچ امتیاز غیرضروری در آن فعال نیست.

سیستم فایل[۱۲۱]

سیستمهای فایل FAT و FAT32 که در Windows مورد استفاده قرار می‌گیرند بطور کامل ایمن نیستند؛ بخصوص اگر از اشتراک فایل استفاده کنید. چنانچه دسترسی به فایلها از طریق شبکه انجام می‌شود، درصورت امکان باید از سیستم فایل NTFS استفاده گردد. توجه داشته باشید در مواردی که دستگاه رایانه شما می‌تواند با بیش از یک سیستم‌عامل راه‌اندازی شود یا در شرایطی که لازم است به دیسک سخت یک سیستم‌عامل دیگر دسترسی داشته باشید نمی‌توانید از NTFS استفاده نمایید.

خدمات سیستمی[۱۲۲]

در برخی از سیستمها تمامی قابلیتهای شبکه فعال هستند تا ارتباط میان رایانه‌ها بتواند به آسانی برقرار شود. اگر در شرکت خود شبکه ندارید خدماتی که کاربرد ندارند را غیرفعال نمایید.

دیوارهٔ آتش

یک دیوارهٔ آتش سخت‌افزاری یا نرم‌افزاری روی سیستم خود نصب کنید. نسخه‌های رایگان این نرم‌افزار در دسترس می‌باشد. دیوارهٔ آتش را به‌روز نگهدارید. مطمئن شوید که دیوارهٔ آتش بگونه‌ای تنظیم شده که درصورت وقوع هر اتفاق غیرعادی به شما هشدار می‌دهد.

ضدویروس

یک نرم‌افزار ضدویروس نیز روی دستگاه خود نصب کنید. اگر نتوانستید نسخهٔ رایگان آنرا بیابید باید هزینهٔ نسخهٔ تجاری آنرا بپردازید. برخی از فروشندگان بر به‌روزرسانی روزانهٔ ضدویروسهای خود تأکید دارند و برخی دیگر به‌روزرسانی هفتگی آنها را پیشنهاد می‌کنند. طبیعتاً هرچه نرم‌افزار شما به‌روزتر باشد بهتر می‌تواند از سیستم حفاظت کند.

آشکارگرهای بدافزارها

برنامه‌هایی وجود دارند که سیستم را برای انواع نرم‌افزارهای مخرب جستجو می‌کنند، مثل:

Pest Patrol
(*http://www.pestpatrol.com*)

Lavasoft
(*http://lavasoftusa.com/software/adawareplus/*)

SpybotSD
(*http://www.safer-networking.org*)

همگی برنامه‌های فوق رایگان هستند و انواع مختلف نرم‌افزارهای مخرب روی سیستم را شناسایی می‌نمایند.

120 Multi-User
121 File System

122 System Services

بررسی خلاصهٔ امنیتی

اگر شما یک کاربر غیرفنی هستید و هیچ سازمانی برای کمک به شما وجود ندارد می‌توانید به پیشنهادات Microsoft برای کاربران خانگی نگاهی بیاندازید:

http://www.microsoft.com/security/home
http://www.microsoft.com/protect/

اگر متخصص فناوری اطلاعات هستید می‌توانید از این پایگاه اطلاع‌رسانی استفاده کنید:

http://www.microsoft.com/technet/security

اگر سیستم جدیدی دارید می‌توانید *MBSA*[۱۲۳] را که برای ارائه خدمات پشتیبانی به سیستمهای Windows 2000 و Windows XP طراحی شده روی آن نصب و راه‌اندازی کنید.

رایانه‌های Macintosh

نقاط قوت و نقاط ضعف

رایانه‌های Apple Macintosh و سیستم‌عامل آنها کمتر از Windows رایانهٔ شخصی پذیرای مشکلات امنیتی هستند. بعلاوه از آنجا که تعداد کاربران دستگاههای Mac نسبت به رایانه‌های شخصی کمتر است مهاجمان علاقهٔ کمتری به خرابکاری در آنها نشان می‌دهند. شاید بزرگترین آسیب‌پذیری آنها این است که کاربران Mac تصور می‌کنند همیشه ایمن هستند و هیچگاه مورد آزار و اذیت کسی قرار نخواهند گرفت. سیستمهای MacOS که پیش از MacOS X بوجود آمدند سیستم‌عامل مناسبتری داشتند. MacOS X بر اساس FreeBSD UNIX است و باید با دید یک سیستم UNIX خاص که با ملاحظات امنیتی مناسب طراحی شده به آن نگاه کرد (این مورد در بخش بعدی که در مورد UNIX است بررسی شده). در هستهٔ مرکزی MacOS X خدمات سیستمی متعددی تعبیه شده اما همهٔ آنها غیرفعال هستند.

چگونه از خود محافظت کنیم

انتشار نرم‌افزار

اطمینان حاصل کنید که از تمامی وصله‌ها برای حفاظت از سیستم استفاده کرده‌اید. به پایگاه اطلاع‌رسانی http://www.apple.com بروید و روی گزینهٔ Support کلیک کنید. مشابه سیستمهای Windows، اینجا هم این احتمال وجود دارد که سیستم اصلاح‌نشدهٔ شما بعد از تنها چند ساعت یا چند روز مورد نفوذ قرار بگیرد؛ خصوصاً اگر روی آن یک ارتباط دائمی شبکه داشته باشید.

حسابهای کاربری

مطمئن شوید تمامی حسابهای کابری که مورد نیاز نیستند غیرفعال یا حذف شده‌اند. خصوصاً بررسی کنید که حساب کاربری guest بدون داشتن رمز عبور فعال نباشد. امتیازات راهبری را برای حسابهایی که از آنها زیاد استفاده می‌کنید محدود سازید و از حساب کاربری راهبر برای کارهای روزمره که بدون امتیاز راهبری قابل انجام هستند استفاده نکنید.

اشتراک فایل

اگر از این قابلیت استفاده نمی‌کنید آنرا غیرفعال سازید. در غیراینصورت مطمئن شوید که امتیازات تعیین‌شده در حداقل سطح ممکن قرار دارند.

خدمات

خدماتی که مورد نیاز نیستند را غیرفعال سازید. اگر آنها را بطور موقتی فعال می‌کنید یادتان باشد که پس از اتمام کار مجدداً همگی را غیرفعال نمایید.

نرم‌افزارهای کاربردی جدید

نرم‌افزارهای کاربردی جدید مرتبط با شبکه (خصوصاً آنهایی که برای UNIX طراحی شده‌اند) ممکن است در سیستمهایی که قبل از MacOS Xها طراحی شده‌اند آسیب‌پذیر باشند. اگر چنین نرم‌افزاری نصب کرده‌اید مراقب این موضوع باشید.

123 *Microsoft Baseline Security Analyzer*

دیوارهٔ آتش

یک دیوارهٔ آتش سخت‌افزاری یا نرم‌افزاری روی سیستم خود نصب کنید و آنرا به‌روز نگهدارید. مطمئن شوید که دیوارهٔ آتش بگونه‌ای تنظیم شده‌است که درصورت وقوع هر اتفاق غیرعادی به شما هشدار می‌دهد.

ضدویروس

یک نرم‌افزار ضدویروس نیز روی دستگاه خود نصب کنید. اگر نتوانستید نسخهٔ رایگان آنرا بیابید باید هزینهٔ نسخهٔ تجاری آنرا بپردازید. برخی از فروشندگان بر به‌روزرسانی روزانهٔ ضدویروسهای خود تأکید دارند و برخی دیگر به‌روزرسانی هفتگی آنها را پیشنهاد می‌کنند. طبیعتاً هرچه نرم‌افزار شما به‌روزتر باشد بهتر می‌تواند از سیستم حفاظت کند.

UNIX، Linux، و سیستمهای مشابه

نقاط قوت و نقاط ضعف

سیستمهای Unix از ابتدای پیدایش در محیطهای علوم رایانه‌ای و فیزیکی بعنوان *ایستگاه کاری*[۱۲۴] و سرویس‌دهنده (هم برای خدمات سیستمی و هم برای محاسبات چندکاربری) بکار می‌رفتند و طی دههٔ گذشته از سیستمهای Windows و Macintosh – که در محیطهای دیگر ایستگاه‌های کاری *تک‌کاربره*[۱۲۵] بودند – تا حدودی پیشی گرفتند. با محبوبیت رو به افزایش Linux این پدیده گسترش یافت؛ زیرا از یک سو این سیستم بسیار جالب و جذاب بود و از سوی دیگر برخلاف Windows متن برنامهٔ آن بصورت رایگان در اختیار عموم قرار گرفت. این موضوع در کشورهای درحال توسعه بیش از کشورهای توسعه‌یافته در کانون توجه‌ها واقع شد؛ چراکه هزینهٔ تهیهٔ نرم‌افزار در کشورهای درحال توسعه در مقایسه با متوسط سطح درآمد افراد بسیار بالاتر می‌باشد. از نقاط قوت UNIX می‌توان به انعطاف‌پذیری آن و نیز نرم‌افزارهایی که توسط کاربران و شرکتها طی این سالها برای آن تولید شده‌اند اشاره کرد.

متأسفانه قدرت و انعطاف‌پذیری UNIX با کاربرپسند بودن (از دید یک کاربر تازه‌کار) همراه نشد. درنتیجه زمانی که این سیستمها برای کاربران غیر متخصص UNIX بعنوان ایستگاه کاری بکار می‌روند، وجود کارمندان قوی برای پشتیبانی سیستمها لازم می‌شود. در هر حال پایه و اساس این سیستم هنوز پیچیده است و برای یک کاربر بی‌تجربه و تازه‌کار احتمال زیادی وجود دارد که راههای ورود را برای یک خرابکاری امنیتی باز گذارد. اگرچه سیستمهای UNIX نسبتاً عاری از ویروس هستند ولی پذیرای آخرین کرمها و تروجانهای منتشر شده می‌باشند، و لذا این موارد هنوز جزء مشکلات بالقوه آنها محسوب می‌شوند.

چگونه از خود محافظت کنیم

تمامی عناوینی که در ۷ فصل گذشته ذکر شدند در مورد سیستمهای UNIX، Linux و سیستمهای مشابه آنها نیز صادق هستند و درصورتیکه بخواهید رایانهٔ خود را واجد امنیت نسبی کنید باید به این موارد بپردازید. این بخش روی ایستگاههای کاری تک‌کاربره متمرکز است. افرادی که مسئول سرویس‌دهنده‌ها هستند باید بخش پنجم این کتاب را مطالعه کنند.

انواع مختلف UNIX

به دلیل وجود سیستم‌عاملهای مختلف شبیه UNIX، بسیاری از فروشندگان *مکانیزمهای از پیش نصب شدهٔ امنیتی*[۱۲۶] مخصوص به خود را دارند. بنابراین بسیار مهم است که راهنمای عملی آن نگارش از Unix که از آن استفاده می‌کنید را مطالعه نمایید. نام چندین کتاب، پایگاه اطلاع‌رسانی، و گروه پست الکترونیکی مفید که به امنیت Unix اختصاص دارند در بخش ضمائم کتاب آمده است.

انتشار نرم‌افزار

نرم‌افزار حتماً باید به‌روز گرددو تمامی وصله‌های امنیتی سریعاً روی آن نصب شوند. جزئیات اینکه بستهٔ به‌روزرسانی را از کجا باید تهیه کرد و چگونه آنرا اعمال نمود در سیستمهای مختلف متفاوت است.

124 *Workstation*
125 *Single-User*
126 *Pre-Installed Security Mechanisms*

حسابهای کاربری

کاربر ریشه[۱۲۷] (uid 0) بالاترین سطح دسترسی را دارد و معمولاً می‌تواند تمامی ابعاد سیستم را تغییر دهد. بر همین اساس حفاظت از حساب کاربری ریشه و فرآیندهایی که اجرای آنها توسط این حساب کاربری امکانپذیر است از مهمترین ابعاد امنیت UNIX بشمار می‌رود. از بکارگیری حساب کاربری ریشه در فعالیتهای روزمره خودداری کنید و برای اطمینان بیشتر امکان ورود به سیستم را با استفاده از حساب کاربری ریشه غیرفعال سازید. هنگامیکه باید از این حساب کاربری استفاده کنید از دستور ***superuser*** (su یا نمونه‌های دیگر مانند sudo) استفاده کنید تا حساب کاربری مورد استفاده را به حساب کاربری ریشه تبدیل نمایید.

اگر روی سیستم بیش از یک کاربر دارید از *فهرستهای کنترل دسترسی*[۱۲۸] استفاده کنید تا بتوانید دسترسیهای کاربران را محدود نمایید.

هرجا که امکان آن وجود دارد با یک حساب کاربری غیر از حساب کاربری ریشه از خدمات شبکه‌ای استفاده کنید.

هیچگاه با حساب کاربری ریشه، نرم‌افزار جدید را باز و یا کامپایل نکنید. معمولاً نرم‌افزارها در محیطی که با ***chroot*** وارد آن می‌شوید کامپایل می‌شوند تا از شما در برابر انواع مختلف تروا‌ها محافظت نمایند.

نصب دیسکهایی که از راه دور مورد استفاده قرار می‌گیرند

اگر برای دسترسی به دیسک از راه دور از روشهای مختلف دسترسی از راه دور استفاده می‌کنید (با استفاده از رایانه‌های شخصی و یا سیستمهای UNIX) برای اینکار رمزهای عبور مناسبی تعیین و درصورت امکان دسترسی به فایلهایی که نرم‌افزارها به آنها نیازمندند را تنها به همان اندازهٔ مورد نیاز محدود نمایید.

خدمات سیستمی

بسیاری از دستگاههای UNIX دارای خدمات سیستمی گسترده‌ای هستند، مثل سرویس‌دهندهٔ FTP، سرویس‌دهندهٔ وب و سرویس‌دهندهٔ پست الکترونیکی. در بسیاری موارد این خدمات بصورت پیش‌فرض فعال هستند. تمامی خدمات مبتنی بر شبکه که مورد استفاده قرار نمی‌گیرند را غیرفعال سازید. بعضی مردم تصور می‌کنند چون این خدمات وجود دارند باید از آنها استفاده نمود – حتی اگر تخصص فنی برای مدیریت امنیت آنرا نداشته باشند. این اشتباه بزرگی است و این خدمات نباید بدون دلیل قانع‌کننده و پشتیبانی فنی کافی در ایستگاههای کاری کاربران راه‌اندازی شده باشند.

بسیاری از خدمات شبکه‌ای با استفاده از فرمان ***inetd*** یا ***xinetd*** شروع به فعالیت می‌کنند. فایلهای پیکربندی که توسط این daemon مورد استفاده قرار گرفته‌اند را بررسی کنید و هریک از خدماتی که لازم ندارید را غیرفعال نمایید. خدمات شبکه‌ای دیگر که هنگام راه‌اندازی سیستم شروع به فعالیت می‌کنند در فایلهایی در مسیر /etc/init.d یا /etc/rc*.d و یا /etc/rc و /etc/rc.local قرار گرفته‌اند. به خدماتی که ممکن است اطلاعات سیستم یا کاربر آنرا در اختیار دیگران قرار دهند – مثل ***fingerd*** – توجه ویژه داشته باشید.

اگر سرویس ***FTP*** *ناشناس*[۱۲۹] را راه‌اندازی نموده‌اید حتماً آنرا به‌روزرسانی نمایید. هرگز فایل /etc/passwd را در محیط FTP تبادل نکنید. اطمینان یابید حسابهای کاربری root، uucp، bin و دیگر حسابهایی که در اختیار کاربر خاصی قرار ندارند در فایل /etc/ftpusers – که شامل فهرست کاربرانی است که نمی‌توانند از FTP استفاده کنند – وجود داشته باشند. مراقب *مجوز دسترسی به شاخه‌ها*[۱۳۰] و *مالکیت*[۱۳۱] آنها در محیط FTP باشید. از انجام download توسط مسیرهای ورودی و انجام

127 *Root User*
128 *Access Control List*

129 *Anonymous FTP*
130 *Directory Permission*
131 *Ownership*

upload بوسیله مسیرهای خروجی جلوگیری نمایید، و بالاخره بطور منظم ثبتهای سرویس FTP خود را مورد بررسی قرار دهید.

دیوارهٔ آتش

هر سیستم UNIX باید *دیوارهٔ آتش مبتنی بر میزبان*[۱۳۲] مخصوص خود را برای *تصفیهٔ بسته‌ها*[۱۳۳] راه‌اندازی نماید. از مستندات فروشنده استفاده کنید تا تشخیص دهید که آیا سیستم شما دارای دیوارهٔ آتش است یا خیر، و اگر هست چگونه می‌توان از آن برای این منظور استفاده نمود. معمولاً ابزارهای پیکربندی دیوارهٔ آتش شامل ipfw، ipchains و iptables هستند. این دیواره‌های آتش باید بگونه‌ای پیکربندی شوند که بطور پیش‌فرض راه عبور تمامی بسته‌ها را مسدود کنند و تنها به آنهایی مجوز عبور دهند که مقصد آنها خدماتی است که شما خواسته‌اید.

حسابهای کاربری پیش‌فرض

بسیاری از سیستمهای Unix دارای چندین حساب کاربری پیش‌فرض هستند که برای فرآیندهای جداگانه یا مجوز مالکیت فایلها مانند bin، daemon و uucp و غیره مورد استفاده قرار می‌گیرند. اطمینان حاصل کنید که تمامی رمزهای عبور رمزگذاری‌شدهٔ حسابهای کاربری مذکور با علامت "*" شروع می‌شوند و بنابراین با هیچ رمز عبوری نمی‌توان به این حسابهای کاربری دسترسی پیدا کرد. همینکه حساب کاربری ریشه یک رمز عبور معتبر داشته باشد کفایت می‌کند؛ و لازم نیست کسی بتواند وارد حسابهای کاربری دیگر گردد (اگرچه درصورت لزوم حساب کاربری ریشه می‌تواند با استفاده از دستور su دسترسی به حسابهای دیگر را فراهم کند).

آشکارگرهای بدافزارها

ابزارهای زیادی برای شناساندن نرم‌افزارهای مخرب به راهبر Unix وجود دارند. یکی از قدیمی‌ترین آنها Tripwire است که تحقیق می‌کند نرم‌افزارهای مهم سیستم و دیگر فایلهای حیاتی بطور مخفیانه تغییر داده شده‌اند یا خیر.

---

132 Host-Based Firewall
133 Packet-Filtering

ضمیمهٔ ۱
آشنایی با کدگذاری و رمزگذاری

کدگذاری[۱۳۴] و *رمزگذاری*[۱۳۵] فنونی هستند که رشته‌های حروف را به قالب و شکل دیگری تبدیل می‌کنند. کدگذاری در دنیای رایانه تغییر شکلی است که ظاهر پیام را تغییر می‌دهد، بطوریکه نتیجهٔ آن معیارهای خاصی را برآورده سازد؛ و رمزگذاری نیز نوعی تغییر شکل است که برای مخفی کردن محتویات پیام بکار می‌رود.

کدگذاری

کدگذاری قالب موضوع را تغییر می‌دهد تا برخی از معیارهای مورد نظر را برآورده سازد. این فرآیند برگشت‌پذیر است؛ بگونه‌ای که قالب کدگذاری شده بعداً می‌تواند *کدگشایی*[۱۳۶] شود تا به شکل اصلی خود تبدیل گردد.

فرآیند کدگذاری

فرض کنید می‌خواهید پیامی ارسال کنید که بصورت یک جملهٔ عادی انگلیسی است:

Security is important.

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

برای این منظور از یکسری قوانین ساده استفاده می‌کنیم:

بجای A عدد ۰۱ را قرار می‌دهیم؛
بجای B عدد ۰۲ را قرار می‌دهیم؛
بجای C عدد ۰۳ را قرار می‌دهیم؛
بجای D عدد ۰۴ را قرار می‌دهیم؛
...
بجای X عدد ۲۴ را قرار می‌دهیم؛
بجای Y عدد ۲۵ را قرار می‌دهیم؛
بجای Z عدد ۲۶ را قرار می‌دهیم؛
بجای فاصله عدد ۲۷ را قرار می‌دهیم؛
بجای نقطه نیز عدد ۲۸ را قرار می‌دهیم.

جملهٔ اصلی را درنظر بگیرید و هر حرف را با کد تعیین شده، جایگزین نمایید.

۱۹ را بجای S قرار دهید؛
۰۵ را بجای E قرار دهید؛
۰۳ را بجای C قرار دهید؛ و ...

حالا می‌توانیم رشته را اینگونه ارسال کنیم:

19050321180920252709192709131615182001142028

اگر میان ارقام فاصله قرار دهیم خواناتر هم می‌شود:

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

هنگامیکه پیام دریافت شد، دریافت‌کننده آنرا به حالت اول باز می‌گرداند:

S جایگزین ۱۹ می‌شود؛
E جایگزین ۰۵ می‌شود؛
C جایگزین ۰۳ می‌شود، و اینکار آنقدر ادامه می‌یابد تا جملهٔ اصلی بدست آید.

کاربردهای کدگذاری

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

اما بسیاری از زبانها تعداد حروفشان بیشتر از زبان انگلیسی است. از طرف دیگر برنامه‌ها، فایلهای پردازش کلمه، عکسها و انواع دیگر فایلها از بایتهای ۸ بیتی تشکیل شده‌اند و

134 *Encoding*
135 *Encryption*
136 *Decoding*

مجموعاً ۲۵۶ حرف منحصر به فرد را می‌سازند، و هیچیک نمی‌توانند توسط نامهٔ الکترونیکی ارسال گردند.

برای حل این مشکل مفهوم *ضمائم*[۱۳۷] بوجود آمد، که در آن فایلی که همراه نامهٔ الکترونیکی ارسال می‌شود ابتدا کدگذاری می‌گردد تا محتوای آن به شکل حروف استاندارد ASCII در آید. این فرآیند مشابه همان فرآیندی است که که طی آن توانستیم آن جمله را تنها با استفاده از اعداد کدگذاری کنیم. مشابه مثال قبلی، در اینجا نیز پیام کدگذاری‌شده از اصل پیام طولانی‌تر است؛ اما می‌تواند بدون ایجاد اشکال خاصی انتقال یابد و هنگامیکه دریافت شد کدگشایی گردد و به شکل اصلی خود درآید.

Unicode

Unicode نوعی روش کدگذاری برای تمامی حروفی است که در زبانهای رایج مورد استفاده قرار می‌گیرند و رایانه‌ها می‌توانند بطور یکسان آنها را بکار برند. جزئیات بیشتر که در کنسرسیوم Unicode (*http://www.unicode.org*) مورد توافق قرار گرفته در ادامه به شکل خلاصه ذکر شده است:

اساساً رایانه‌ها با اعداد و ارقام سر و کار دارند. آنها حروف الفبا و دیگر علامتها را با اختصاص دادن یک عدد به هریک از آنها ذخیره می‌کنند. پیش از پیدایش Unicode صدها سیستم کدگذاری مختلف برای این تبدیلات وجود داشت، اما هیچکدام از آنها به اندازهٔ کافی حروف و علات را پشتیبانی نمی‌کردند؛ و مثلاً اتحادیهٔ اروپایی به تنهایی نیاز به چندین کدگذاری مختلف داشت تا تمامی زبانهای اروپایی را پوشش دهد. حتی در مورد یک زبان منحصر به فرد مانند انگلیسی نیز یک کدگذاری واحد برای تمامی حروف، علائم و علامتهای دستوری و فنی کافی نبود.

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

Unicode برای هریک از حروف، شمارهٔ مجزایی اختصاص می‌دهد. اهمیتی ندارد که چه بستر، برنامه یا زبانی مورد استفاده باشد. استاندارد Unicode با رهبری شرکتهایی چون Apple، HP، IBM، JustSystem، Microsoft، Oracle، SAP، Sun، Sybase، Unisys و... نهایی شده، و در تمام بسترها یک استاندارد ثابت است.

رمزگذاری

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

سه روش رمزگذاری مختلف وجود دارد:

- *رمزگذاری متقارن*[۱۳۸]
- *رمزگذاری کلید عمومی*[۱۳۹]
- *رمزگذاری یکطرفه یا استفاده از Hash*[۱۴۰]

رمزگذاری متقارن

به زبان ساده، رمزگذاری متقارن مشابه کدگذاری است که حروف اصلی متن همگی در آن تغییر ظاهری می‌یابند. یکی از ساده‌ترین الگوریتمهای رمزگذاری این است که هر حرف را با حرف بعدی آن جایگزین کنیم. بنابراین در این روش:

B بجای A قرار می‌گیرد؛
C بجای B قرار می‌گیرد؛
D بجای C قرار می‌گیرد؛
.....
Y بجای X قرار می‌گیرد؛
Z بجای Y قرار می‌گیرد؛
A بجای Z قرار می‌گیرد (در پایان حروف الفبا، دوباره به حرف اول بازگشته‌ایم).

اگر از این الگوریتم استفاده کنیم، مثال ذکر شده تبدیل می‌شود به (فاصله و نقطه را درنظر نگیرید):

TFDVSJUZ JT JNQPSUBOU.

137 *Attachments*

138 *Symmetric Encryption*
139 *Public Key Encryption*
140 *One-way Hash Encryption*

اکنون این پیام تغییر کرده است. دریافت‌کننده آنرا برمی‌گرداند و هر حرف را با حرف قبلی خود جایگزین می‌کند و بدین ترتیب جملهٔ اصلی بدست می‌آید.

بجای آنکه هر حرف را یک واحد انتقال دهیم، می‌توانیم آنها را چند واحد منتقل کنیم. تا زمانیکه دریافت‌کننده مقدار این انتقال را بداند می‌تواند پیام را رمزگشایی نماید.

تعداد تغییر مکان یک حرف را *کلید رمزگذاری*[۱۴۱] می‌گویند. از این عدد هم برای رمزگذاری پیام استفاده می‌شود و هم برای رمزگشایی آن. جولیوس سزار از این روش برای ارسال پیامهای محرمانه و سری خود استفاده می‌نمود (او کلید رمزگذاری و رمزگشایی خود را برابر عدد ۳ انتخاب کرده بود).

با استفاده از این الگوریتم ساده اگر پیام شما دزدیده شود و سارق متوجه روح کلی رمزگذاری بشود، ممکن است با حدس زدن بتواند محتوای آنرا بفهمد. درصورتیکه الگوریتم پیچیده‌تر از آن باشد که با اعمال چند جابجایی بتوان آنرا پیدا کرد آنگاه رمزگشایی بسیار مشکلتر خواهد شد. تا مدتی پیش الگوریتمهای رمزگذاری متعددی از این روش ساده انتقال استفاده می‌کردند.

امروزه برای رمزگذاری بجای انتقال حروف از فرمولهای ریاضی استفاده می‌شود. البته هنوز هم از کلید استفاده می‌کنیم و این کلید بخشی از آن فرمول برای انجام رمزگذاری است. اگر بخواهید پیامی را رمزگشایی کنید حتماً باید از یک کلید استفاده نمایید. البته اگر کلید مخصوص را نداشته باشید می‌توانید کلیدهای دیگر را امتحان کنید تا به جواب برسید. درصورتیکه کلید محدود به شماره‌های ۱ تا ۱۰ باشد، عملیات حدس زدن زیاد طول نمی‌کشد. اما اگر مثلاً میان اعداد ۱ تا ۱۰۰ باشد ممکن است کمی بیشتر زمان ببرد. امروزه کلیدها معمولاً اعداد دودویی ۱۲۸ بیتی هستند. این رقم تقریباً برابر با:

۳۴۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰

انتخاب مختلف است که حدس زدن صحیح کلید را تقریباً غیر ممکن می‌کند.

رمزگذاری متقارن هنگامی مورد استفاده قرار می‌گیرد که فرستنده و دریافت‌کننده بتوانند از یک کلید مشابه استفاده کنند (در اینصورت آنها باید در مورد یک کلید مشخص به توافق رسیده باشند). از این روش درصورتی برای رمزگذاری پیام استفاده می‌شود که بخواهید اطلاعاتی را از جایی به جای دیگر انتقال دهید، مثلاً انتقال از طریق ارتباطات بی‌سیم؛ و یا اینکه بخواهید اطلاعات موجود روی یک دیسک را بگونه‌ای رمزگذاری کنید که دیگران نتوانند آنرا بخوانند. در موارد اخیر اگر کلید مفقود شود اطلاعات شما نیز مطمئناً از دست رفته‌اند.

رمزگذاری کلید عمومی

این نوع رمزگذاری مشابه رمزگذاری متقارن است، اما با یک تفاوت عمده: بجای یک کلید، در آن دو کلید وجود دارد. درواقع در اینجا کلیدی که برای رمزگذاری پیام استفاده می‌گردد متفاوت از کلیدی است که برای رمزگشایی پیامِ رمزگذاری‌شده بکار می‌رود. معمولاً کلید اول عمومی است و همه مجازند از آن اطلاع داشته باشند. اگر شما بخواهید برای شخصی یک پیام خصوصی ارسال کنید باید از کلید عمومی وی – که خود او آنرا برای رمزگذاری در اختیار همه قرار داده – استفاده نمایید. برای رمزگشایی پیام، نیاز به کلید خصوصی وی می‌باشد که متفاوت از کلید عمومی است و این کلید را نباید به هیچوجه در اختیار دیگران قرار داد. با این توضیحات مشخص است که اگر پیام شما با استفاده از این مکانیزم برای کسی ارسال شود، هیچ شخص دیگری بجز گیرندهٔ حقیقی نمی‌تواند آنرا بخواند.

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

کلیدهای عمومی و خصوصی می‌توانند عکس آنچه گفته شد نیز استفاده شوند. در اینحالت شما پیام را با کلید خصوصی خود رمزگذاری می‌کنید و هر کسی که کلید عمومی شما را داشته باشد می‌تواند آنرا رمزگشایی نماید. در اینصورت آنچه به اثبات می‌رسد این است که مطمئناً فرستندهٔ پیام کسی نیست جز شما.

141 Encryption Key

رمزگذاری یکطرفه با استفاده از *درهم‌سازی*[۱۴۲]

می‌توانید این روش را مشابه رمزگذاری کلید عمومی بدانید در حالتی که در آن هیچکس کلید خصوصی ندارد. بنابراین مطالب می‌توانند رمزگذاری شوند، اما نمی‌توانند رمزگشایی گردند؛ و تفاوت آن با رمزگذاری کلید عمومی در این است که پیام رمزشده معمولاً حداکثر طول مشخصی دارد. یکی از رایجترین الگوریتمهای رمزگذاری یکطرفه با استفاده از درهم‌سازی، الگوریتمی بنام *MD5*[۱۴۳] است. خروجی الگوریتم MD5، همیشه ۱۲۸ بیت (۱۶ بایت) می‌باشد. اگر یک کد درهم‌سازی‌شده برای دو پیام متفاوت ایجاد کنید احتمال اینکه خروجی دو کد درهم‌سازی‌شده مشابه یکدیگر باشند تقریباً صفر خواهد بود.

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

تضمین جامعیت

شما می‌توانید یک سند طولانی یا یک برنامه را برگزینید، کد MD5 را برای آن محاسبه و آنرا در محلی امن ذخیره نمایید. مدتی بعد می‌توانید به اسناد خود مراجعه و دوباره روی آن همین عملیات را اعمال کنید. طبیعتاً چنانچه کد جدید متمایز از کد قبلی بود متوجه می‌شوید که برنامه یا سند تغییر کرده است. معمولاً یک تغییر بسیار جزئی در یک فایل بزرگ هم باعث ایجاد تغییرات زیادی در کد MD5 مربوطه می‌شود.

ذخیرهٔ رمز عبور

در بسیاری از سیستمها هنگامیکه کاربر از کلمه‌ای بعنوان رمز عبور استفاده می‌کند، این کلمه با استفاده از الگوریتم MD5 (یا یک الگوریتم مشابه) رمزگذاری می‌شود و نسخهٔ رمزگذاری‌شده ذخیره می‌گردد. بار بعد که کاربر سعی می‌کند وارد سیستم شود، آنچه که وارد می‌کند مجدداً رمزگذاری می‌شود و با آنچه که در دیسک ذخیره شده بود مقایسه می‌گردد؛ و درصورت یکسان بودن آنها مشخص می‌شود که رمز عبور صحیح بوده است. البته اگر کاربر رمز عبور را فراموش کند رمزگشاییِ آنچه که روی دیسک ذخیره شده امکانپذیر نیست و باید یک رمز عبور جدید انتخاب گردد. از این روش برای این منظور استفاده می‌شود که اصل رمز عبور هیچگاه نتواند در قالب اصلی خود به نمایش درآید.

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

امضای دیجیتالی[۱۴۴]

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

۱. پیام را می‌نویسد و از MD5 برای ایجاد کد درهم‌سازی‌شده استفاده می‌کند.
۲. با استفاده از کلید خصوصی خود، کد درهم‌سازی‌شده را رمزگذاری می‌کند.
۳. با استفاده از کلید عمومی شما متن پیام را رمزگذاری می‌نماید.
۴. پیام و کد درهم‌سازی رمزگذاری‌شده را ارسال می‌کند.
۵. شما پیام را دریافت می‌کنید.
۶. با استفاده از کلید عمومی وی کد درهم‌سازی را رمزگشایی می‌نمایید، که نتیجه آن بدست آمدن کد درهم‌سازی اصلی است.

142 *Hash*
143 *Message Digest 5*
144 *Digital Signature*

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

۸. برای متن پیام ارسالی، با استفاده از MD5 کد درهم‌سازی را محاسبه می‌نمایید.

۹. اگر دو کد درهم‌سازی بدست آمده یکسان بودند اطمینان می‌یابید متن ارسالی تغییر نکرده‌است و فرستنده نیز همان شخصی است که انتظار آنرا داشتید.

گواهی‌های دیجیتالی[۱۴۵] که بوسیله مرورگرهای وب برای تصدیق هویت ایمن مورد استفاده قرار می‌گیرند نیز بر اساس فنون امضای دیجیتالی (مشابه مثال فوق) کار می‌کنند.

145 *Digital Certificates*

ضمیمهٔ ۲
TCP/IP

پروتکل TCP/IP مجموعه‌ای از قوانین است که تمام پیامهای ارسالی در اینترنت را کنترل می‌کند. اگرچه نیازی نیست که کاربران عادی برای استفاده از اینترنت دربارهٔ TCP/IP اطلاع داشته باشند، اما باید دربارهٔ پیکربندی دیواره‌های آتش و تهدیدات اینترنتی مطالبی بدانند. در ادامه شرح ساده‌ای از عملکرد TCP/IP ذکر شده است. اگر با این مفاهیم آشنا هستید می‌توانید از خواندن این قسمت صرفنظر کنید.

آدرس‌دهی اینترنتی

هر ابزار در اینترنت دارای یک آدرس IP می‌باشد. این آدرس بطور کلی آن ابزار را بصورت منحصر به فرد معرفی می‌کند؛ همانطور که آدرس پستی در تمام دنیا آدرس خانهٔ شما را نشان می‌دهد. آدرسهای موجود در نسخهٔ جاری TCP/IP (که به نام IPv4 شناخته می‌شود) اعداد ۳۲ بیتی دودویی هستند. یعنی تعداد آدرسهای ممکن، ۴۲۹۴۹۶۷۲۹۶=$۲^{۳۲}$ می‌باشد. برای نمایش و بخاطر سپردن ساده‌تر آنها، اعداد ۳۲ بیتی دودویی به ۴ بخش ۸ بیتی تقسیم‌بندی شده‌اند. چون ۲۵۶=$۲^{۸}$ است، هر بخش ۸ بیتی می‌تواند یکی از اعداد ۰ تا ۲۵۵ باشد. این ۴ شماره معمولاً بدنبال هم می‌آیند و با یک نقطه از یکدیگر تفکیک می‌شوند. بنابراین کوچکترین آدرس اینترنتی 0.0.0.0 و بزرگترین آن 255.255.255.255 است. نمونهٔ یک آدرس IP به شکل 24.200.195.15 می‌باشد. در اینترنت ابزاری بنام *مسیریاب*[۱۴۶] وجود دارد که مسیر هر آدرس IP را نگهداری می‌کند و می‌داند که برای دست‌یافتن به هر آدرس باید کدام مسیر را برگزید.

146 *Router*

خدمات نام دامنه[۱۴۷]

چون به خاطر سپردن رشته‌های طولانی اعداد سخت است بسیاری از رایانه‌ها در اینترنت با حروف الفبا (که *نام میزبان*[۱۴۸] نامیده می‌شوند) نامگذاری شده‌اند. نمونهٔ آن www.infodev.org است. هنگامیکه این نام را در مرورگر وب وارد کنید رایانه پیامی را به یک سرویس خاص بنام DNS ارسال می‌کند. DNS می‌تواند حروف الفبا را به شماره تبدیل نماید (در این مثال شماره مورد نظر 192.86.99.121 است). همچنین DNS به سرویس‌دهندهٔ وب اجازه می‌دهد که در مکانهای مختلف جابجا شود؛ چون دامنهٔ مربوطه آدرس جدید را به DNS اطلاع می‌دهد و لذا کاربران همچنان می‌توانند از همان نام میزبان استفاده نمایند.

IP: پروتکل اینترنت[۱۴۹]

هنگامیکه داده‌ها از طریق اینترنت ارسال می‌شوند به شکل مجموعه‌ای از حروف و نشانه در می‌آیند که به آنها *بسته*[۱۵۰] یا *datagram* گفته می‌شود. IP در TCP/IP به معنای "پروتکل اینترنت" است و مشخص می‌کند که قالب داخلی این بسته‌ها باید چگونه باشد. بستهٔ IP شامل چندین بخش اطلاعاتی است که در میان آن موارد زیر به چشم می‌خورند:

- اندازهٔ بسته؛
- آدرس IP گیرنده؛
- آدرس IP محلی که بسته از آنجا ارسال می‌شود؛ و
- نوع بسته.

هنگامیکه یک بسته از رایانهٔ شما ارسال می‌شود به نزدیکترین مسیریاب فرستاده می‌شود و آن نیز سعی می‌کند بسته را در طول مسیر به مسیریاب بعدی ارسال کند و این کار ادامه می‌یابد تا بسته به مقصد خود برسد. اگر مشکلی بوجود آید یا تراکم بسته‌ها زیاد باشد بسته نمی‌تواند ارسال شود و در میان راه متوقف خواهد شد. به همین دلیل به IP *پروتکل غیرقابل اطمینان*[۱۵۱] می‌گویند. اگرچه طبق تئوری

147 *Domain Name Services*
148 *Hostname*
149 *Internet Protocol*
150 *Packet*
151 *Unreliable Protocol*

IP قابل‌اطمینان نیست، اما در بیشتر موارد تمامی بسته‌های ارسالی را به مقصد می‌رساند.

انواع مختلفی از بسته‌ها وجود دارند که می‌توانند ارسال شوند اما در اینجا تنها به دو نوع از آنها اشاره می‌کنیم: TCP و UDP.

TCP: پروتکل کنترل انتقال[۱۵۲]

TCP پروتکلی است که در بیشتر پیامها بکار می‌رود و شامل وب (HTTP)، *پروتکل انتقال فایل* (FTP)[۱۵۳] و نامهٔ الکترونیکی می‌باشد. علاوه بر دادهٔ ارسال‌شده، بسته‌های TCP شامل موارد زیر هم می‌باشند:

- ۱۶ بیت *شمارهٔ پورت ارسالی*؛[۱۵۴]
- ۱۶ بیت *شمارهٔ پورت دریافتی*؛[۱۵۵]
- *اطلاعات ترتیبی*[۱۵۶] بسته‌ها؛ و
- *اطلاعات تصدیقی*.[۱۵۷]

از آنجا که هر رایانه فقط یک آدرس IP دارد از شماره پورت برای نمایش برنامه‌ای که در رایانه پیام را ارسال و یا دریافت می‌کند استفاده می‌شود. این قابلیتی است که امکان می‌دهد روی رایانه چندین مرورگر وب باز باشد و بتوان بوسیلهٔ آنها صفحات درخواستی را مشاهده نمود. برای اینکه یک برنامه پیام TCP را دریافت کند باید روی پورت صحیحی منتظر پیام بماند. معمولاً برای هر نرم‌افزار کاربردی خاص، یک پورت مشخص وجود دارد. بعنوان مثال پورت سرویس‌دهندهٔ وب همیشه پورت شمارهٔ ۸۰ است. هنگامیکه یک پنجرهٔ مرورگر را باز می‌کنید تقریباً بطور تصادفی یک پورت را برای خود انتخاب می‌کند (طبق قرارداد، بزرگتر از ۱۰۲۳) و این همان پورتی است که باید روی آن منتظر پیام ایستاد.

از آنجا که طول بسته‌های IP محدود است و اطلاعاتی که توسط برنامه‌های کاربردی منتقل می‌شوند ممکن است بسیار بیشتر از آن باشد، اطلاعات باید به قسمتهای کوچکتری تقسیم گردند. هر قسمت در قالب بستهٔ TCP مربوط به خود فرستاده می‌شود. فرستادن ترتیبی اطلاعات سبب می‌شود که برنامهٔ دریافتی این قسمتها را با ترتیبی صحیح مجدداً گردآوری نماید. اما به دلایل متعدد ممکن است بعضی از بسته‌ها سریعتر از بسته‌های دیگر به مقصد برسند و این بدان معنی است که بسته‌ها باید بتوانند خارج از ترتیبی که فرستاده شده‌اند دریافت شوند. از سوی دیگر از آنجا که طبق تئوری ماهیت IP قابل اطمینان نیست ممکن است بعضی از بسته‌ها هرگز به مقصد نرسند. در این مورد برنامهٔ دریافتی متوجه می‌شود که یک شکاف میان ترتیب دریافت بسته‌ها رخ داده است و می‌تواند درخواست کند که بستهٔ گم شده مجدداً ارسال شود.

هنگامیکه فرستنده یک بستهٔ TCP بفرستد، این انتظار می‌رود که برنامهٔ دریافت‌کننده با بازپس فرستادن اطلاعات تصدیقی مخصوص، دریافت آنرا تصدیق کند. اگر پیام تصدیق یک بسته در بازهٔ زمانی مشخص‌شده‌ای باز نگردد، بسته مجدداً ارسال خواهد شد. به دلیل وجود اعداد ترتیبی و تصدیقی بسته‌ها، TCP یک *پروتکل قابل اعتماد*[۱۵۸] است و هنگامیکه از آن استفاده می‌شود نرم‌افزار کاربردی، کاربر می‌تواند مطمئن باشد که درصورت وقوع اشتباه و یا خطا در انتقال یا دریافت اطلاعات، نرم‌افزار در جریان آن قرار خواهد گرفت.

UDP: پروتکل datagram کاربر[۱۵۹]

UDP قالب ساده‌ای است که برای انتقال اطلاعات مورد استفاده قرار می‌گیرد. هر بستهٔ UDP علاوه بر داده‌ها دارای اطلاعات دیگری شامل موارد زیر نیز هست:

- ۱۶ بیت شمارهٔ پورت ارسالی؛ و
- ۱۶ بیت شمارهٔ پورت دریافتی.

در اینجا نیز مانند TCP، به دلیل استفاده از شماره‌های پورت ممکن است برنامه‌های مختلفی بتوانند بطور موازی رشته‌های UDP را دریافت و ارسال نمایند. همچنین مانند دریافت پیام در TCP، برنامه باید روی پورت صحیحی منتظر دریافت پیام بماند. در UDP هیچ شرط مشخصی برای ترتیب‌بندی و تصدیق بسته‌ها وجود ندارد، لذا این

152 *Transmission Control Protocol*
153. *File Transfer Protocol*
154 *Sending Port Number*
155 *Receiving Port Number*
156 *Sequencing Information*
157 *Acknowledgement Information*
158 *Reliable Protocol*
159 *User Datagram Protocol*

پروتکل نیز همانند IP نامطمئن است و پیامها در آن ممکن است گم شوند. UDP در مواردی استفاده می‌شود که گم شدن تعدادی از پیامها اهمیت چندانی نداشته باشد و یا راه ساده‌ای برای بازیابی پیامهای گمشده موجود باشد. اما از مزایای این پروتکل می‌توان به این نکته اشاره کرد که چون هیچ تصدیق و ترتیب‌بندی خاصی در UDP وجود ندارد این پروتکل منابع بسیار کمتری از سیستم را بکار می‌گیرد.

ضمیمهٔ ۳
واژه‌نامهٔ اصطلاحات فنی

تعاریف اصطلاحات در حوزهٔ متون امنیتی

پست الکترونیکی[۱۶۰]

معادل رایانه‌ای پست نامه‌ها. آدرسهای الکترونیکی می‌توانند از طریق اینترنت، نامه ارسال یا دریافت کنند. از دیدگاه اینترنتی تمامی نامه‌های الکترونیکی از متون قابل چاپ (کاراکترهای غیرکنترلی ASCII) تشکیل شده‌اند.

تخریب سرویس[۱۶۱]

حملهٔ تخریب سرویس زمانی اتفاق می‌افتد که رایانه متصل به اینترنت توسط پیامهای بسیار زیاد و غیر حقیقی بمباران شود؛ بطوریکه تمامی وقت خود را صرف پاسخ دادن به این پیامها نماید و مجالی برای عبور ترافیک کاربر واقعی باقی نماند.

ثبت‌کننده‌های کلید[۱۶۲]

برنامه‌ای که هرآنچه از طریق صفحه‌کلید تایپ می‌شود را ثبت می‌کند. داده‌ها می‌توانند روی دیسک نوشته و یا از طریق اینترنت برای شخص دیگری ارسال گردند. اگر ثبت‌کننده‌های صفحه‌کلید روی رایانه‌ای نصب شده باشند، هرآنچه که وارد رایانه گردد – مثل نام کاربری و رمز عبور – ثبت می‌شود؛ دقیقاً مشابه حالتی که شما نام کاربری و رمز عبور خود را وارد می‌کنید و شخصی بالای سرتان ایستاده است!

درب مخفی[۱۶۳]

روشی برای گذر از ورود عادی و ایمن به سیستم و بدست‌آوردن کنترل یک رایانه بدون کسب اجازه از صاحب آن است. اگر درب مخفی روی یک رایانهٔ متصل به شبکه نصب شود ممکن است هر شخصی در اینترنت بتواند بدون اطلاع و رضایت مالک رایانه به آن وارد شود و کنترل آنرا بدست گیرد.

دیوارهٔ آتش[۱۶۴]

دیوارهٔ آتش می‌تواند تبادل غیرمنتظره و غیرمجاز اطلاعات میان شما و دنیای خارج از آنرا مسدود کند. دیواره‌های آتش دو نوع هستند: دیوارهٔ آتش می‌تواند نرم‌افزاری باشد که روی رایانهٔ شما اجرا می‌شود یا قطعهٔ سخت‌افزاری مجزایی باشد که به آنچه در شبکه دریافت و ارسال می‌شود نظاره می‌کند.

رمزگذاری[۱۶۵]

روشی برای مخفی کردن محتوای اطلاعات که باعث می‌گردد اطلاعات براحتی قابل خواندن نباشند، مگر برای کسی که قرار است آن اطلاعات را دریافت کند. در رمزگذاری یک "کلید" وجود دارد که بر اساس یکسری قوانین بوجود آمده است و برای تغییر ظاهری اطلاعات مورد استفاده قرار می‌گیرد. این اطلاعات زمانی می‌تواند خوانده شود که رمزگشایی شده باشد و برای رمزگشایی آن لازم است فرد دریافت‌کننده، هم کلید و هم روش استفاده از آنرا بداند.

سرریزی بافر[۱۶۶]

یک اشکال نرم‌افزاری است و هنگامی اتفاق می‌افتد که یک برنامه داده‌های خود را به فضایی در حافظه منتقل می‌کند که در آن جای کافی برای داده‌ها وجود ندارد. در اینحالت برنامه ممکن است داده‌های قبلی را از حافظه بیرون بیاندازد و سعی داشته باشد فضایی را برای داده‌های جدید مهیا سازد.

---

160 Email
161 Denial of Service
162 Keyloggers

163 Backdoor
164 Firewall
165 Encryption
166 Buffer Overflow

از بین رفتن این داده‌ها می‌تواند باعث ایجاد مشکلات زیادی گردد و معمولاً یکپارچگی و امنیت برنامه را خدشه‌دار می‌کند. با بررسی فضای کافی حافظه قبل از انتقال اطلاعات به آن می‌توان از وقوع این مسئله جلوگیری کرد.

سرقت هویت[۱۶۷]

سرقت هویت زمانی اتفاق می‌افتد که شخص اطلاعات کافی در مورد شما جمع‌آوری کرده باشد و با آن اطلاعات بتواند خود را بجای شما جا بزند (مثلاً در بانکها، فروشگاهها، یا سازمانهای دولتی).

ضمیمه[۱۶۸]

ضمیمه قسمتی از نامهٔ الکترونیکی است که با استفاده از آن می‌توان انواع فایلها مثل فایلهای متن و تصویر را انتقال داد. تمامی فایلهای غیر متنی برای ارسال باید بصورت قابل چاپ (متن‌ساده) درآیند. تمامی آنچه که در رایانه ذخیره می‌شود ترکیبی از ارقام ۰ و ۱ است. به زبان ساده‌تر کدگذاری این صفرها و یک‌ها را با تبدیل به متون ساده، قابل ارسال می‌کند.

نام کاربری و رمز عبور[۱۶۹]

نام کاربری و رمز عبور محرمانه که کاربر را برای یک سیستم رایانه‌ای و یا پایگاه وب شناسایی و تصدیق هویت می‌کند.

نرم‌افزارهای متن‌باز[۱۷۰]

نرم‌افزارهایی که متن برنامهٔ آنها در اختیار عموم است و همه می‌توانند آزادانه آنها را اصلاح کنند و تغییر دهند. به دلیل در دسترس بودن متن برنامه، افراد می‌توانند نحوهٔ عملکرد آنرا ببینند و به دلخواه خود تغییر دهند. معمولاً نویسندگان برنامه‌های متن‌باز سایر برنامه‌نویسان را تشویق به مشارکت در توسعه و گسترش قابلیتهای این برنامه‌ها می‌نمایند. برنامه‌های متن‌باز همچنین شامل نرم‌افزارهای رایگان هم هستند، و بسیاری از برنامه‌های متن باز – چه آنهایی که رایگان هستند و چه آنهایی که برای فروش می‌باشند – قابلیتهایی دارند که مشابه نرم‌افزارهای انحصاری است و ممکن است هزینهٔ بالایی داشته باشد. گاهی اوقات برنامه‌های متن‌باز تحت موافقتنامه‌ها و مجوزهای خاص بصورت غیر رایگان در قسمتهایی از برنامه‌های تجاری استفاده می‌شوند.

برای اطلاعات بیشتر در این زمینه می‌توانید به پایگاههای زیر مراجعه نمایید:

http://www.fsf.org
http://www.opensource.org

نسخهٔ پشتیبان[۱۷۱]

فرآیند نسخه‌برداری از فایلهای یک رایانه به محلهای دیگر در همان رایانه و یا روی ابزارهای جانبی که ممکن است مستقل از آن رایانه باشند. نسخه‌های پشتیبان باعث می‌شوند بتوانید داده‌هایی که به هر دلیلی از بین رفته‌اند (مثلاً بطور تصادفی پاک شده‌اند، آسیب فیزیکی دیده‌اند، و یا مورد سرقت قرار گرفته‌اند) را بازیابی نمایید.

هرزنامه[۱۷۲]

تبلیغات و دیگر نامه‌های الکترونیکی که بدون اینکه شما خواسته باشید برای شما ارسال می‌شوند.

ویروس[۱۷۳]

اصطلاح "ویروس" معنای خاصی دارد که در بخشهای آتی بیشتر مورد بحث و بررسی قرار می‌گیرد. درحال حاضر ویروس به مجموعهٔ همهٔ برنامه‌هایی اطلاق می‌گردد که در رایانهٔ شما ظاهر می‌شوند و ممکن است به رایانه‌های دیگر نیز سرایت کنند و به آنها آسیبهای جدی وارد نمایند.

167 Identity Theft
168 Attachment
169 Username & Password
170 Open-Source Software
171 Backup
172 Spam
173 Virus

Cookie

فایلی است که هنگام درخواست یک پایگاه وب از راه دور، روی دیسک سخت نوشته و یا از روی آن خوانده می‌شود. پایگاه وب درخواست می‌کند که فایل روی رایانهٔ مورد نظر نوشته شود تا بعدها هم بتواند آنرا بخواند. مثلاً اگر پایگاه وبی از شما نام کاربری درخواست کند می‌تواند این اطلاعات را روی دیسک شما ذخیره نماید. هنگامیکه شما مجدداً به آن پایگاه مراجعه می‌کنید، این پایگاه cookie قبلی را می‌خواند و متوجه می‌شود که نام کاربری شما چه بوده است.

Daemon

برنامهٔ کوچکی که روی رایانهٔ شما همیشه درحال اجرا است و منتظر می‌ماند تا از آن بخواهید کاری را برای شما انجام دهد. چنین درخواستی معمولاً از طریق یک شبکه و بوسیلهٔ کاربر راه دور انجام می‌شود.

HTML

HTML یک کلمهٔ اختصاری برای عبارت **H**yper **T**ext **M**arkup **L**anguage است. این زبان مجموعه دستورالعملهایی است که مرورگر وب یا برنامه‌های پست الکترونیکی با استفاده از آنها می‌توانند متون و تصاویر را نمایش دهند و یا عملیات دیگری به انجام رسانند. نمونه‌ای از دستورالعملهای این زبان چنین است:

This sentence is <<Start Bold>> very <<End Bold>> short.

در جملات فوق کلمات داخل علامت <<>> نشاندهندهٔ عملی است که باید انجام شود. در نتیجهٔ دستورالعملهای فوق جمله‌ای به شکل زیر به نمایش در می‌آید:

This sentence is **very** short.

URL[۱۷۴]

یک آدرس عمومی برای اشاره به یک مقصد در اینترنت. بعنوان مثال *http://www.infodev.org/* یا *mailto: info@worldbank.org*

174 *Universal Resource Locator*