امنیت فناوری اطلاعات
در عصر دیجیتال

بخش اول

مقدمه

ظهور فناوری دیجیتال یکی از بارزترین پیشرفتهای فناوری در نیم‌قرن اخیر به شمار می‌آید که در زندگی کنونی بشر بصورت عاملی حیاتی درآمده است.[1] برای بسیاری از ما این نوع فناوری در قالب رایانه‌های دیجیتالی تجلی کرده و به ابزاری لازم برای انجام کارها و رفع نیازهای شخصی تبدیل شده است. در سال ۱۹۵۱ میلادی زمانیکه اولین رایانهٔ دیجیتال تجاری موسوم به UNIVAC I به *سازمان آمار و سرشماری ایالات متحده آمریکا*[2] تحویل داده شد، بسیاری از مردم در مورد رایانه‌ها چیزی نمی‌دانستند و آن رایانه‌ها نیز تنها در تعداد انگشت شماری از دانشگاهها و آزمایشگاههای تحقیقاتی مورد استفاده قرار داشتند. این رایانه‌ها بزرگ، گران و مملو از اشکال بودند. در مقابل، رایانه‌های امروزی اندازه‌ای نسبتاً کوچک دارند، ارزان و قابل اطمینان هستند و می‌توان آنها را در هر کشوری یافت.

به فاصلهٔ کوتاهی پس از رواج رایانه‌ها در دانشگاهها، پروژه‌های تحقیقاتی برای مرتبط ساختن آنها با یکدیگر به نحوی که امکان مبادلهٔ اطلاعات میان آنها بوجود آید آغاز شدند. از میان این پروژه‌ها، پروژهٔ توسعهٔ شبکهٔ ARPANET موفقیت بیشتری کسب کرد و به آن چیزی تبدیل شد که امروز آنرا بعنوان "اینترنت" می‌شناسیم و درحال حاضر بیش از ۳۰۰ میلیون رایانه را در سراسر جهان به هم مرتبط کرده است.

شبکهٔ جهانی وب[3] که توسط *تیم برنرز لی*[4] و *رابرت کایلیو*[5] در *مرکز تحقیقات هسته‌ای اروپا*[6] در اوایل دههٔ ۹۰ میلادی و در شهر ژنو ایجاد شد سرویس قدرتمندی است که از اینترنت برای ایجاد یک سیستم اطلاعاتی جهانی بهره جسته و بهره‌وری و جذابیت اینترنت را به مراتب افزایش داده است. هر چند بسیاری از مردم تفاوتی میان شبکهٔ جهانی وب و اینترنت قائل نیستند، ولی در واقع وب تنها یکی از این *خدمات*[7] (و البته مهمترین آنها) است که اینترنت را به چنین ابزار قدرتمندی برای اطلاع‌رسانی و برقراری ارتباطات تبدیل کرده است.

طی ده سال اخیر اینترنت به یک ابزار مهم ارتباطی میان تمامی اقشار جامعه تبدیل شده و ما برای دسترسی آنی به اطلاعات، ارتباطات اختصاصی، تمامی انواع برنامه‌های کاربردی، تجاری، روابط کاری و نقل و انتقالات مالی به آن وابسته‌ایم. قابلیت اطمینان و دسترسی آسان به اینترنت برای موفقیت پایدار و مداوم کشورهای توسعه‌یافته یک عامل حیاتی بشمار می‌رود و اهمیت آن برای کشورهای درحال توسعه نیز بسرعت رو به افزایش است. آثار استفاده از رایانه‌ها و نتایج حاصله از انقلاب اینترنت از مرز فواید مستقیم آنها فراتر رفته و پیش‌بینی می‌شود که تأثیرات بیشتری نیز در راه باشند.

اول از همه اینکه اینترنت مرزهای جغرافیایی میان کاربران متصل به خود را کمرنگ کرده و روند جهانی‌سازی را با ارائه قابلیتهای رسانه‌های ارتباطی تسهیل نموده و لذا هر کسی مستقل از محل فیزیکی خود قادر به برقراری ارتباط با آن می‌باشد. *موتورهای جستجو*[8] بر روند این تغییر تأثیری مضاعف داشته‌اند؛ چراکه نتایج جستجو بر اساس موضوعات ظاهر می‌شوند و نه بر اساس فاصله‌ای که کاربر با آنها دارد؛ بطوریکه پایگاه وبِ کارخانجات و شرکتهای واقع در کشورهای توسعه‌یافته و درحال توسعه از موقعیت یکسانی برای نظاره‌شدن توسط مراجعین برخوردار هستند.

دومین مسئله این است که اینترنت تأثیری شگرف در فرآیند حذف واسطه‌های تجاری داشته است. بعنوان مثال می‌توان به کاهش چشمگیر نرخ استخدام منشی در کشورهای توسعه‌یافته اشاره‌کرد که دلیل آن این است که نوشتن متن و چاپ و ارسال پیام شخصی برای افراد از طریق تسهیلاتی چون پردازشگر کلمات و پست الکترونیکی آسانتر از دیکته کردن متن برای یک منشی است. به همین ترتیب

1 *Digital Tornado: The Internet and Telecommunications Policy FCC Staff Working Paper on Internet Policy (1997): http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/1997/nrmc7020.html*
2 *U.S. Bureau of Census*
3 *World-Wide Web*
4 *Tim Berners-Lee*
5 *Robert Cailliau*
6 *Center for European Nuclear Research (CERN)*
7 *Services*
8 *Search Engine*

گردشگریِ دسته‌جمعی نیز درحال حاضر رو به انقراض است، چراکه گردشگران می‌توانند بلیطهای هوایی یا قطار و همچنین اتاقهای هتل مورد نظر خود را بصورت *برخط*[9] رزرو کنند و این امر موجب صرفه‌جویی در هزینه و وقت مشتری شده و باعث شده بتوان با کمی دقت روی سفارشات، از یک سفر مفرح لذت برد. پیدایش شرکتهای فروشندهٔ کتاب، موسیقی و محصولات الکترونیکی بصورت برخط موجب تهدید و ضربه به فروشگاههای عرضه‌کنندهٔ اینگونه محصولات شده، اما در عین حال در بسیاری از بخشهای این صنف به گسترده‌تر شدن طیف بازار هدف نیز انجامیده است. از آنجا که حرفه‌ها و صنایع سنتی به وجود خود ادامه می‌دهند، تمایل دارند افراد کمتری به استخدام درآورند و حتی ممکن است بجای ارائه خدمات عمومی به سمت بازارهای تخصصی حرکت کنند. تأثیرات مشهود روند حذف واسطه‌ها که با ظهور این فناوری شروع شد برای مدتی طولانی ادامه خواهد یافت و با اهمیت روزافزون فناوری اطلاعات، صنایع و حرفه‌های بیشتری با آن جایگزین خواهند شد.

سومین پیامد این است که نرخ بهره‌وری حداقل در صنایع وابسته به فناوری اطلاعات با شتابی چشمگیر افزایش خواهد یافت. به کمک پست الکترونیکی امکان ارسال و تبادل اطلاعات در سراسر جهان طی تنها چند ثانیه ممکن شده، بطوریکه مباحث و مذاکرات جهانی را می‌توان بسیار سریعتر از گذشته پیگیری کرد و به نتیجه رساند. امور بازرگانی که تا چندی قبل از طریق پست، تلکس و تلفن انجام می‌شدند اکنون با بکارگیری مفاهیمی نوین در صنعت مخابرات سیار، سریعتر و کارآمدتر به انجام می‌رسند و این مسئله چرخهٔ زمانی انجام فعالیتها را کاهش داده است.

نکتهٔ آخر اینکه ایمن نگاه داشتن محل ذخیرهٔ اطلاعات و خطوط ارتباطی مخابراتی نیز در این محیط جدید الزامی است. صنعت و فناوری امروز به شدت در تکاپوی یافتن راهی برای تضمین امنیت زیرساختهای خود هستند، چراکه دست‌اندرکاران آن دریافته‌اند که بیشتر نقایص امنیتی اینترنت ناشی از وجود سخت‌افزارها و نرم‌افزارهای ناامن در آن می‌باشند. در این محیط ایجاد اطمینان و اعتماد به رایانه، شبکه و داده‌های ذخیره‌شده نسبت به محیطی که در آن روابط کاری بر اساس گفتگوهای رو در رو انجام می‌گیرد کمابیش از اهمیت یکسانی برخوردار است.

این مطلب در مورد کشورهای درحال توسعه نیز واضح است: سازمانهایی که به سطح امنیتی مناسبی در زیرساختهای دیجیتالی خود دست نیافته و از ارسال اطلاعات خویش به نحو مطلوبی محافظت نمی‌کنند شایستهٔ اعتماد نخواهند بود و از کاروان اقتصاد نوین جهانی عقب خواهند ماند.[10]

انقلاب دیجیتال

امروزه فناوری دیجیتال از حیطهٔ رایانه‌ها فراتر رفته است. پیشرفتهای فناوری در صنعت میکروالکترونیک امکان ساخت ابزارهای پیچیدهٔ الکترونیکی در مقیاسهای بسیار کوچک را فراهم آورده بطوریکه اکنون شما می‌توانید تجهیزات ارتباطی و محاسباتی بسیار پیچیده را در جیب خود جای دهید. علاوه بر این بهبود نسبت قیمت به کارآیی برای این نوع فناوری در هر سال چیزی حدود ۳۰٪ است و احتمال برقراری این نسبت تا ده سال آینده نیز بسیار بالاست.[11] انتظار ما این است که این فناوری مورد استقبال گسترده قرار گیرد و عرصه‌های نوینی در تجارت پدید آورد و نقطهٔ شروعی برای آغاز عصر طلایی فناوری دیجیتالی باشد.

تجهیزات تلفنی مدرن امروز کاملاً دیجیتالی هستند و سیستمهای هدفمند رایانه‌ای جایگزین تجهیزات Switching مبتنی بر رلهٔ مکانیکی شده‌اند. از زمان پیدایش دیسک فشرده در اواخر دههٔ ۸۰ میلادی، صدا و موسیقی شکل دیجیتالی به خود گرفته و با پیدایش قالب موسیقی MP3 در اواخر دههٔ ۹۰ میلادی ضبط صدا حتی در محیطهای خانگی نیز کاملاً دیجیتالی شده است. در دنیای عکاسی و فیلمبرداری نیز تصاویر دیجیتالی و دوربینهای دیجیتالی ثبت تصاویر فیلمهای عکاسی گشته‌اند.

---

9 *Online*

10 *Braga, Carlos Prima, Inclusión or Exclusion, UNESCO Courier: http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/1997/nrmc7020.html*

۱۱ *این نرخ پیشرفت فنی یکی از پیامدهای قانون Moor است که بوسیلهٔ Gordon Moor، پدر اینتل در دههٔ ۱۹۶۰ تشریح شده. او می‌گوید طی هر دورهٔ ۲ ساله (که بعداً آنرا به ۱۸ ماه کاهش داد) فناوری به تولیدکنندگان اجازه می‌دهد ریزپردازنده‌هایی با ظرفیت دوبرابر و قیمت یکسان تهیه کنند. این روند طی ۴۰ سال گذشته به همین منوال بوده و انتظار می‌رود که حداقل تا ۱۰ سال دیگر نیز همینطور باشد.*

امروز حتی فیلمهای سینمایی و کارتونها نیز دیجیتالی شده‌اند؛ چراکه بدین شکل هزینه‌های تولید آنها کمتر و کیفیتشان بیشتر است. رفته‌رفته نوارهای ویدئویی جای خود را به فناوری DVD داده‌اند و فیلمهای سینمایی با امکانات دیجیتالی ساخته و تدوین می‌گردند.

استانداردهای تلفنهای بی‌سیم درحال حرکت به سمت فناوری دیجیتال هستند و با وجود پروتکلهایی چون GSM، CDMA، TDMA و گونه‌های مختلف آنها بتدریج جایگزین نسل قدیمی استانداردهای فناوری آنالوگ خواهند شد. در کشورهای توسعه‌یافته تلویزیون دیجیتال به صحنه آمده است و دیری نخواهد گذشت که جای استانداردهای پخش برنامه را خواهد گرفت (هرچند که این تغییر کمی کندتر از بقیه خواهد بود؛ چراکه حجم گیرنده‌های خانگی موجود که به استانداردهای قدیمی‌تر وابسته‌اند بسیار وسیع است).

سیستمهای امنیت فیزیکی نیز درحال تبدیل به انواع الکترونیکی خود هستند. در هتلها، آپارتمانها و دفاتر اداری، کلیدهای فیزیکی جای خود را به کارتهای الکترونیکی داده‌اند. دوربینهای تلویزیونی مورد استفاده در سیستمهای نظارتی ساختمانها و تأسیسات نیز اغلب از تجهیزات الکترونیکی استفاده می‌کنند که بجای ارسال سیگنالهای تلویزیونی به یک مانیتور ویدئویی، تصاویر الکترونیکی را به ایستگاههای نظارت دیجیتالی ارسال می‌کنند.[۱۲]

بسیاری از خدماتی که امروزه از آنها استفاده می‌کنیم بدون وجود رایانه، شبکه و فناوری دیجیتال قابل ارائه نخواهند بود. خطوط هوایی نیز بدون سیستمهای رزرو رایانه‌ای و سیستمهای نگهداری و پشتیبانی پرواز قادر به رقابت با هم نیستند. هواپیماها تا اندازهٔ زیادی به حسگرهای الکترونیکی و کنترلهای دیجیتالی وابسته‌اند و بدون آنها نمی‌توانند به خوبی کار کنند. حتی اتومبیلها نیز برای عملکرد مناسب و کمک به عیب‌یابی و نگهداری خود از ریزپردازنده‌ها استفاده می‌کنند. *سیستمهای مکانیابی جهانی* (GPS)[۱۳] نیز به شما این امکان را می‌دهند که بدانید در هر لحظه در چه مکانی روی کرهٔ زمین قرار گرفته‌اید و با داشتن چنین دستگاه نسبتاً ارزانی در کنار رایانه‌ای که حاوی پایگاه داده‌ای از نقشه‌ها باشد قادر به یافتن مسیر حرکت، نقاط مهم، رستورانها، تابلوهای راهنما، خدمات ارائه‌شده در طول مسیر، و در نهایت مقصد مورد نظر خواهید بود.

این دستگاههای دیجیتال با سرعتی باورنکردنی در شبکه قرار می‌گیرند. تلفنهای بی‌سیم قادر به برقراری ارتباط با اینترنت هستند و ابتدا قادر به ارسال صوت و اکنون قادر به مبادلهٔ تصاویر از طریق اینترنت می‌باشند و بزودی دارای قابلیت GPS نیز خواهند شد و به این ترتیب افرادی که در معرض خطر و حادثه قرار گرفته باشند را می‌توان با دقتی زیاد و تنها با یک تلفن مکانیابی کرد. بسیاری از خدماتی که اکنون مورد استفادهٔ ما قرار می‌گیرند – مثل دستگاههای خودپرداز که برای تبادل و نقل و انتقال پول بکار می‌روند – بر اساس اصل "در دسترس بودن شبکه" کار می‌کنند. نقل و انتقالات مالی و اعتباری میان‌بانکی و بین‌المللی وابستگی زیادی به شبکه‌های اعتباری و مالی دارند.[۱۴] امروزه نقل و انتقالات بانکهای الکترونیکی از طریق اینترنت برای افراد میسر است.

توسعهٔ ابزارهای الکترونیکیِ دیجیتال و دستگاههای مرتبط با هم فواید بسیاری دارد؛ ولی نکات منفی نیز در آن قابل مشاهده است. پیدا کردن محل استقرار شما برای افراد آسانتر شده است. دیدن صفحات تبلیغاتی وب، یافتن آنچه که بدنبال خرید آن در مغازه‌ها هستید، و مشاهدهٔ آنچه که درحال تماشا یا خواندن بصورت برخط هستید نیز ساده‌تر از قبل می‌باشد. اگر چنین نظارتی بر منافع شما حاکم باشد قاعدتاً شما از آن باخبر نخواهید شد، اما شاید بخواهید مطمئن شوید که چنین داده‌هایی با کسب اجازه از شما جمع‌آوری می‌شوند و تنها برای اهدافی بکار می‌روند که از

---

۱۲ *این مورد خاص ممکن است مشاغل را به سمت کشورهای درحال توسعه هدایت کند. به محض اینکه تصاویر در قالب دیجیتال درآیند و روی اینترنت قرار داده شوند، می‌توانند به یک سیستم نظارت در هر کجای شبکه فرستاده شوند. بنابر پیش‌بینی‌ها این قابلیت امنیتی که به مهارت خاصی نیاز ندارد می‌تواند در کشورهای درحال توسعه با هزینهٔ کمتر و کیفیت برابر راه‌اندازی شود. این پیشنهاد در با استقبال توسعه‌دهندگان مواجه شد، اما از آنجا که در این نوع واگذاری مرزهای ملی در نوردیده می‌شوند، ممکن است برخی نگرانیهای امنیت فیزیکی به بار بیایند.*

13 Global Positioning System

۱۴ *شبکهٔ تبادل مالی میان بانکها در گذشته از یک شبکهٔ اختصاصی بسیار ایمن که برای همین هدف خاص طراحی شده بود استفاده می‌کرد و به اینترنت نیز متصل نبود. این مسئله با درنظر گرفتن ارزش زیاد آن شبکه و تأثیرات بسیار مخرب و جدی هرگونه نفوذ به آن کاملاً منطقی بنظر می‌رسد.*

آن اطلاع دارید و با آن موافق هستید. بسیاری از مردم برای حریم خصوصی خود اهمیت زیادی قائل هستند و دولتها نیز مایل به حفظ حقوق افراد می‌باشند، گرچه میزان و شدت اجرای قوانین از یک کشور تا کشور دیگر متفاوت است. مسئله اصلی برای دولتها این است که منافع حاصل از فناوریهای نوظهور را تشخیص دهند و در عین حال ارزشها و آزادیهایی که بدون آن فناوریها می‌توان از آنها برخوردار بود را همچنان حفظ کنند. موضوع این است که دولتها باید فناوریهای جدید را درک کرده و تأثیر قابلیتها و امکانات نوین بر آزادیها را ارزیابی نمایند. همچنین دولتها باید گامهای مؤثری بردارند تا مطمئن شوند اگر قوانین و سیاستهای عمومی در این زمینه آزادیهای فعلی را تقویت نمی‌کنند، حداقل یک وفاق جمعی در مورد آنها وجود داشته باشد.

دنیای دیجیتالی معمولاً با عنوان *فضای سایبر*[15] شناخته می‌شود و تعریف آن تمامی رایانه‌ها و ابزارهای دیجیتالی که با شبکه‌های داخلی و خارجی به هم متصل می‌شوند و می‌توانند با یکدیگر ارتباط داشته باشند را در بر می‌گیرد.[16] در فضای سایبر هم مثل فضای فیزیکی می‌توان دربارهٔ ملاقاتها و انجام کارها صحبت کرد، اما باید میان رفتار در فضای سایبر و دنیای حقیقی که در آن زندگی، کار و بازی می‌کنیم تفاوت قائل شد.

گسترش و رواج سریع رایانه‌های شخصی و اینترنت در بخشهای مختلف کشورهای درحال توسعه منافع بسیاری داشته است. با اینحال اینترنت بخودی خود رسانه‌ای نیست که نسبت به رفتار تبهکارانه ایمنی داشته باشد. هزینهٔ عدم توجه کافی به امنیت می‌تواند از دست دادن داده‌های مورد نیاز برای انجام کار یک سازمان بزرگ یا مؤسسهٔ دولتی باشد. اینترنت ماهیتاً از ایمنی لازم برخوردار نیست اما هزینهٔ امن کردن آن نیز در مقایسه با هزینهٔ از دست رفتن داده‌های ارزشمند سازمانها و مؤسسات چندان قابل توجه نمی‌باشد. از دیگر مواردی که می‌تواند بسیار مهم باشد آنست که تأثیر سرقت و وقوع تخلف مالی در یک شرکت تنها محصور به آن شرکت نیست و در کل صنعت کشور تأثیر می‌گذارد.

با گسترش اینترنت و افزایش چشمگیر نگرانیهای ناشی از *حملات سایبر*[17]، تعداد چنین حوادثی نیز رو به افزایش است:

"با وجود اینکه رایانه‌ها نقطهٔ مناسبی برای انجام حملات تروریستی هستند، اما این نکته را نیز باید درنظر داشت که برخی اقدامات خرابکارانه توسط افرادی صورت می‌گیرند که از این راه بدنبال کسب درآمد هستند. *مرکز فوریتهای امنیت رایانه‌ای* (CERT)[18] در سال ۲۰۰۱ میلادی رقمی برابر با ۵۲۶۵۸ رخداد امنیتی اینترنتی را شناسایی کرده که دو برابر تعداد یکسال قبلتر است و نسبت به دو سال پیش از آن چهار برابر می‌باشد."[19]

بحث امنیت رایانه‌ها و شبکه‌ها برای کشورهای درحال توسعه از اهمیت خاصی برخوردار است. اینترنت می‌تواند فواصل را از میان بردارد و دسترسی به مطالب بی‌شماری را فراهم کند. با وجود شبکهٔ جهانی وب، اینترنت قادر خواهد بود از اطلاعات موجود دربارهٔ شرکتها، امکانات، و محصولات کشورهای درحال توسعه استفاده کند و تجارت را در آنها توسعه دهد. علاوه بر این، موتورهای جستجو از نظر جغرافیایی تمایزی میان پایگاههای وب قائل نمی‌شوند؛ و بدین ترتیب تأمین‌کنندگان خدمات و کالاهای اساسی و مواد اولیهٔ کشورهای درحال توسعه روی وب در کنار تأمین‌کنندگان کالاها و خدمات کشورهای توسعه‌یافته قرار می‌گیرند.[20] این امر را گاهی "مرگ فاصله‌ها" می‌نامند؛[21] واژه‌ای که روند جریان اطلاعات در اینترنت را نشان می‌دهد.

15 *Cyberspace*

۱۶ *"فضای سایبر" اولین بار توسط یک نویسنده به نام William Gibson برای یک دنیای موازی که توسط رایانه‌های سراسر دنیا ساخته شده بود در سال ۱۹۸۴ و در رمان او با عنوان "Neuromancer" بکار رفت. این تعریف می‌تواند در ادبیات مفید باشد، اما معنی آن بتدریج از آنچه Gibson مد نظر داشت تغییر یافته است. برای اطلاعات بیشتر به همین پاورقی در کتاب اصلی و یا منبع زیر مراجعه کنید:*

Intven, et al., Legal and Regulatory Aspects of e-Commerce and the Internet, World Bank Legal Review, vol. 1 2003, at fn 17. (Kluwer)

17 *Cyber Attacks*

18 *Computer Emergency Response Team*

19 *Reuters/USA Today, April 16, 2003*

۲۰ *در حقیقت موتورهای جستجو بر اساس زبان میان پاسخهای یافته‌شده تفاوت می‌گذارند، و لذا در بازار جهانی هر کس باید به زبان بازار هدف خود صحبت کند. همچنین موتورهای جستجو ممکن است آنقدر تحمل نداشته باشند که بخواهند منتظر دریافت پاسخ از پایگاههایی باشند که ارتباطشان کند است. در هرحال شرکتهای تجاری می‌توانند پایگاه خود را در هر کجای دنیا میزبانی کنند و بگونه‌ای محل میزبان خود را برگزینند که اطلاعات به بازارهای هدف نزدیک باشد. بعضی از شرکتها از پایگاههای انعکاسی (mirror sites) استفاده می‌کنند؛ به این معنی که یک*

ولی با اینحال همواره مخاطراتی جدی مانند از دست دادن سوابق، حملات تخریب سرویس، خراب شدن اطلاعات و سایر انواع حملات خصمانه وجود دارد. از دست رفتن تمام یا بخشی از سوابق الکترونیکی می‌تواند یک شرکت را زمینگیر کند. برای کشوری که امنیت فناوری اطلاعات آن ضعیف است این احتمال وجود دارد که منابع حیاتی آن در معرض خطر قرار گیرند و به آنها صدمات جبران ناپذیری وارد شود. عدم توجه کافی به امنیت برای کشورهایی که به روابط خارجی در صنایع خود اهمیت می‌دهند می‌تواند موجب خسارتهای جدی و پیش‌بینی نشده‌ای گردد. نیل به *اهداف توسعهٔ هزاره* (MDG)[۲۲] به توانایی کشورهای درحال توسعه در استفادهٔ مؤثر از فناوری اطلاعات و افزایش بودجهٔ آنها با عضویت دائمی در سازمان تجارت جهانی بستگی دارد.[۲۳] توانایی کسب و تأمین اطلاعات مناسب می‌تواند در تمامی زمینه‌های اقتصادی به کشورهای درحال توسعه کمک کند.

متأسفانه همهٔ ظواهر خوب و بد انسانی را می‌توان در فضای سایبر نیز مشاهده نمود. از آنجا که نسخه‌برداری از مضامین دیجیتالی و ویرایش آنها آسان است، مغالطه و تحریف اطلاعات مثل جعل مستندات اداری و رسمی آسان می‌شود. به دلیل آنکه اینترنت از یک محیط پژوهشی و تعاونی شروع به کار کرد و هدف آن اشتراک آسان اطلاعات بود، ساختار آن باعث تسهیل حمله به رایانه‌ها و سرقت اطلاعات محرمانه می‌گردد.

انگیزهٔ افرادی که در فضای سایبر چنین رفتاری از خود بروز می‌دهند شبیه انگیزه‌هایی است که در دنیای واقعی آنها را به کارهای مشابه وادار می‌کند، اما با یک تفاوت عمده: محیطی که توسط رایانه‌ها و اینترنت بوجود آمده باعث شده در افراد این تمایل بوجود بیاید که بخواهند ثابت کنند که می‌توانند به سیستمها وارد شوند و مشکلاتی بوجود بیاورند. بیشتر مشکلات موجود در فضای سایبر از جانب *خرابکارها*[۲۴] ناشی می‌شود. خرابکارها افرادی هستند که می‌خواهند ثابت کنند می‌توانند از هر سد امنیتی که سر راهشان قرار داشته باشد عبور کنند. اگر بخواهیم چنین رفتاری را در دنیای واقعی مدل کنیم باید فردی مورد اشاره قرار دهیم که می‌خواهد ثابت کند می‌تواند به خانه شما وارد شود و سپس بدون دست زدن به چیزی خارج شود! چنین پدیده‌ای نه‌تنها موجب بروز نوعی احساس عدم اطمینان می‌شود، بلکه این سؤال را نیز پدید می‌آورد که چه چیزی درحال تغییر یافتن یا کم شدن است یا اینکه چه اقداماتی می‌توان برای جلوگیری از نفوذهای بعدی انجام داد. همانطور که چنین رفتاری در دنیای واقعی قابل تحمل نیست، در فضای سایبر هم نمی‌توان این رفتار را تحمل کرد. فنون موجود در این کتاب به شما در حفاظت از خودتان در مقابل چنین رفتارهایی کمک خواهد نمود.

این کتاب و هر آنچه که در فضای سایبر وجود دارد شما را از کسب دانسته‌های جدیدتر دربارهٔ رایانه و اینترنت و افزایش سطح آگاهی و مهارتهایتان بی‌نیاز نمی‌کند. امروزه اینترنت دروازهٔ ورود به دنیای شگفت انگیز اطلاعات و دانسته‌ها است و می‌تواند این اطلاعات را با قیمت بسیار نازل در اختیار عموم قرار دهد. بدین ترتیب می‌توان اطلاعات را بصورت کارآمد و مؤثری به‌اشتراک گذارد. با اینحال برای دستیابی به این هدف لازم است امکانات و رفتارهایی که ممکن است در مقابل آن قرار داشته باشند را بشناسیم. با مفهوم هوشیاری در دنیای واقعی آشنا هستیم. اکنون باید بیاموزیم که چگونه می‌توان در فضای سایبر به هوشیاری (هوشیاری سایبر) رسید. این کتاب برای کمک به شما در انجام این مهم تهیه و تدوین شده است.

امنیت چیست؟

مفهوم امنیت در دنیای واقعی برای بسیاری از ما حیاتی است. در دوران ماقبل تاریخ، امنیت عبارت بود از اصول حفظ بقا؛ نظیر امنیت در برابر حملهٔ دیگران یا حیوانات، و نیز امنیت تأمین غذا.

نسخه از پایگاه را در یک محل متفاوت جغرافیایی میزبانی می‌کنند تا زمان دسترسی مشتری به اطلاعات، حداقل شود.

21 *Cairncross, F., The Death of Distance: How the Communications Revolution will Change our Lives, Harvard Business School Press (1997).*

22 *Millennium Development Goals*

۲۳ *امنیت اطلاعات و اینترنت یکی از سه موضوع اصلی هستند که اجلاس سران جامعهٔ اطلاعاتی در کنفرانس خود در جنوا (دسامبر ۲۰۰۳) روی آن کار کرد و قرار است باز هم در تونس (آوریل ۲۰۰۵) روی آن کار شود. این یک دلیل دیگر برای این واقعیت است که نقش فناوری اطلاعات و ارتباطات در توسعه بتدریج به جایگاه واقعی خود نزدیکتر می‌شود.*

نیازهای دیگر چون امنیت در مقابل حوادث طبیعی یا بیماریها عموماً برای انسانهای ماقبل تاریخ مطرح نبود. با پیشرفت تمدن، محدودهٔ امنیت فراتر رفته و ابعاد وسیعتری مانند در اختیار داشتن مکانی برای آسایش و زندگی بی‌خطر را در بر گرفت و امروزه مفهوم اموال شخصی نیز به تعریف امنیت اضافه شده است.

بیشتر آنچه که ما در دنیای واقعی انجام می‌دهیم با مخاطره همراه است؛ هرچند بسیاری از فعالیتهایمان مخاطرهٔ کمی در پی دارد. مثلاً وقتی به همراه شخصی ناآشنا به سفر می‌رویم و یا به شهر یا کشوری ناآشنا وارد می‌شویم این حقیقت را می‌دانیم که برای امنیت جسمی‌مان تهدیداتی وجود دارد. تهدیدات موجود در اطراف ما وقتی جدی خواهند شد که ما در مکانی حفاظت‌نشده قرار بگیریم و با فردی روبرو شویم که بتواند از موقعیت ما سوء استفاده کند. اگر به اندازهٔ کافی به مخاطرات اطراف خود توجه کنیم موفق خواهیم شد مکانی امن پیدا کنیم یا راه چاره‌ای بیابیم؛ مثلاً همراه کسی شویم که ما را به مکان امنی هدایت کند، یا یک تاکسی بگیریم.

بعضی از کارها مخاطرات روانشناختی یا مالی به همراه دارند ولی مخاطرهٔ جسمی ندارند. وقتی سرمایه‌گذاری می‌کنیم (در هریک از اشکال خرید زمین، سهام یا حتی فعالیت در تجارت و یا کار در بازار) انتظار داریم که این سرمایه هرچه زودتر به ما بازگردد. همانطور که می‌دانیم بعضی از سرمایه‌گذاریها دیر یا زود بازخواهند گشت؛ حال آنکه بعضی از سرمایه‌گذاریها اینگونه نیستند و بعضی از آنها هم به زیان منجر می‌شوند. مثلاً وقتی با شخص جدیدی ارتباط برقرار می‌کنیم امیدواریم که این رابطهٔ جدید برایمان آورده‌ای داشته باشد، هرچند خطر این مسئله که ممکن است این رابطه از فایدهٔ لازم برخوردار نباشد را نیز می‌پذیریم.

در بعضی زمینه‌ها دستیابی به سطحی از امنیت که انتظار آنرا داریم ممکن نیست. مثلاً همیشه مایلیم عمری طولانی و جسمی سالم داشته باشیم؛ ولی آنچه که در معدل آماری طول عمر وجود دارد نشان می‌دهد که این مسئله برای بسیاری از افراد صدق نمی‌کند. بعضی از ما در سنین پائین می‌میریم، تعدادی در طول حیات با بیماریهای مختلف دست و پنجه نرم می‌کنیم، و برخی تا سالیان دراز زنده می‌مانیم و عمری به سلامت روزگار می‌گذرانیم. عدم توانایی خود در تعیین سرنوشت را با بیمه جبران می‌کنیم تا ما را در برابر اثرات منفی مالی، حوادث و بیماریها حفاظت کند.

این مقدمه حقیقتی را دربارهٔ امنیت پیش روی ما قرار می‌دهد: امنیت مطلق چه در زندگی واقعی و چه در فضای سایبر غیرممکن و محال است؛ ولی با اینحال امنیتی که به اندازهٔ کافی مناسب باشد تقریباً در تمامی شرایط محیطی دست‌یافتنی می‌باشد.

راههای گوناگونی برای در اختیار گرفتن مکانیزمهای تقویتیِ افزایش و حفظ امنیت وجود دارد. ما از مکانیزمهای فیزیکی برای تضمین امنیت خود برخوردار هستیم: ساختمانهای بلند و مستحکم و درهای محکم و نفوذناپذیر به همراه قفلها و کلیدهای بی‌شمار. ما می‌توانیم به مرزهای فیزیکی دیگر مثل دیوارها و دیگر موانع جداساز نیز تکیه کنیم. همچنین می‌توانیم روی مناطقی که از طریق آنها احتمال نفوذ می‌رود نور کافی متمرکز کنیم. نهایتاً اینکه درصورت لزوم می‌توان با این فرض که اقدامات نفوذی اولیه موفق باشند از سیستمهای هشداردهنده و محافظهای قویتر برای شناسایی و مقابله با کسانیکه موفق به نفوذ شده‌اند استفاده نمود. مهمتر از همه اینکه می‌توانیم از پشتیبانی قوانین عمومی و جزایی و نیروهای انتظامی نیز درخواست کمک نماییم.

ما معمولاً از چندین روش مختلف برای افزایش امنیت خود استفاده می‌کنیم تا درصورتیکه یکی از تدابیر مفید واقع نشد دیگری خلاء آنرا پر کند. اگر یکی از کلیدها به سرقت رفت و قفلِ در از آن پس حفاظ مطمئنی به شمار نمی‌رفت، می‌توان از علائم هشداردهنده برای اعلام خطر نفوذ استفاده کرد. البته تعداد مرزها و عوامل سدکننده به ارزش چیزی که مورد حفاظت قرار می‌گیرد و انتظارات معقولانه‌ای که در زمینهٔ حمله به آن وجود دارد باز می‌گردد.

تمامی این تدابیر و روشهای حفاظتی در فضای سایبر به شکلی دیگر مطرح می‌شوند و ما به آن اندازه که با تدابیر امنیت فیزیکی آشنا هستیم با ماهیت آنها در فضای سایبر آشنا نیستیم، اما لازم است که آنها را درک کنیم و درصورت نیاز به تأمین امنیت در فضای سایبر ، روش کاربرد آنها را بدانیم. هم در دنیای واقعی و و هم در فضای سایبر نیازمند حفاظت و دفاع از سرمایه‌های خود در برابر حملات دیگران و درصورت موفقیت‌آمیز بودن حملات، بازپس‌گیری سرمایه‌های از دست رفته می‌باشیم.

تعاریف و توضیحاتی که در فرهنگهای لغات و واژه‌نامه‌ها برای واژهٔ امنیت وجود دارد به مواردی اشاره دارند که با سلامتی مرتبط هستند، نظیر "کیفیت یا حالتی از اطمینان، آزادی از خطر و رهایی از ترس یا اضطراب". با اینحال هیچیک از این تعاریف نمی‌توانند برای توصیف دقیق امنیت در فضای سایبر بکار روند.

در عوض ما تعریف زیر را پیشنهاد می‌کنیم: هنگامی در فضای سایبر ایمن هستید که دسترسی به منابع اطلاعاتی شما تحت کنترل خودتان باشد، یعنی هیچ کس بدون کسب اجازه از جانب شما قادر به دسترسی به این منابع اطلاعاتی نباشد. این منابع شامل داده‌ها و منابع رایانه‌ای، شبکه‌ای، تراکنشی، پردازشی، و اطلاعاتی می‌باشند. طبیعتاً ممکن است برخی از این منابع از جانب دیگران و برای استفادهٔ شما ارائه شده باشند، مثل *حساب کاربری*[۲۵] در یک رایانهٔ اشتراکی یا دسترسی به اینترنت از طریق یک *ارائه‌کنندهٔ خدمات اینترنتی* (ISP)[۲۶]. از آنجا که این موارد هیچگاه کاملاً ایمن نیستند، تنها تا وقتیکه دستورالعملهای فروشندهٔ خدمات برای استفادهٔ صحیح از آنها را دنبال کنید می‌توانید بر دسترسی مداوم و استفادهٔ مناسب از خدمات اشراف داشته باشید.

مثالی در مورد ماهیت امنیت سایبر در اینجا ارائه می‌شود. برای این منظور به آخرین نقصی که (تا پیش از انتشار این کتاب) در هستهٔ سیستم‌عامل Microsoft Windows یافته شده می‌پردازیم:

"مایکروسافت تقریباً در تمامی نسخه‌های موجود از سیستم‌عاملهای Windows خود یک *آسیب‌پذیری*[۲۷] بسیار مهم را کشف کرد که اولین تأثیر آن می‌تواند از کار افتادن کامل Microsoft Windows Server 2003 باشد. مایکروسافت گفته که این آسیب‌پذیری می‌تواند نفوذگرها را قادر کند که از طریق اینترنت کنترل سیستم‌عامل Windows رایانه‌های قربانیان خود را بدست گرفته، اطلاعات آنها را بدزدند، فایلها را حذف کنند و یا از طریق پست الکترونیکی انتقال دهند. این شرکت به مشتریان خود اطمینان داد که بلافاصله یک *وصله*[۲۸] رایگان برای برطرف ساختن این اشکال روی پایگاه وب مایکروسافت قراردهد ...."

این اشکال که توسط پژوهشگرانی از کشور لهستان کشف شد نسخه‌های رایج Windows در میان کاربران خانگی را نیز تحت تأثیر قرار داد: "این مورد یکی از بدترین آسیب‌پذیریهای Windows است که تا کنون وجود داشته"، این گفتهٔ *مارک مایفرت*[۲۹] مدیر اجرایی *مؤسسهٔ امنیت دیجیتال چشم الکترونیکی*[۳۰] واقع در *آلیسو ویه‌جو*[۳۱] در ایالت کالیفرنیاست که محققان آن نظیر همین آسیب‌پذیری خطرناک را در سه نسخهٔ قبلی Windows کشف کرده‌اند. مایفرت دربارهٔ شرکتهای آسیب‌دیده عنوان کرد: "تا زمانیکه آنها این وصلهٔ نرم‌افزاری را نصب نکنند سیستمهایشان مثل یک تکه پنیر سوئیسی خواهد بود و هرکس می‌تواند براحتی به سرویس‌دهنده‌های آنها وارد شود."

اما همان زمان چهار پژوهشگر لهستانی که با عنوان "Last Stage of Delirium Research Group" شناخته می‌شدند پیدا کرده‌اند که راهی برای عبور از وصله‌های جدید مایکروسافت می‌دانند و این زمانی بود که تنها سه ماه از انتشار این وصله‌ها می‌گذشت. هرچند پژوهشگران لهستانی ابزاری برای اثبات وجود آسیب‌پذیریهای جدی‌تر طراحی کرده و با استفاده از آن به چند رایانه نفوذ کردند، ولی متعهد شدند که هیچ اثری از این آسیب‌پذیریهای جدید در اینترنت بجای نگذارند. بعضی از متخصصان انتظار داشتند که نفوذگران طی چند ماه آینده از این اشکال جدید برای نفوذ به رایانه‌ها استفاده کنند. حتی بدون اعلام این مسئله از سوی آن پژوهشگران، نفوذگران نوعاً قادر به عبور از وصله‌های مایکروسافت هستند."[۳۲]

همانند کاربران و کارمندان درون یک سازمان، ما هیچ کنترلی روی متن برنامه‌هایی نظیر Windows نداریم. می‌دانیم که برای فروشندگان نرم‌افزار بسیار مهم است که برنامه‌هایشان ایمن و عاری از هرگونه خطا باشد، اما زمانی که چنین مشکلاتی بروز می‌کنند با اتخاذ تدابیر و تصمیمات مناسب می‌توانیم نسبت به تهیه و نصب نسخه‌های اصلاحی

25 *User Account*
26 *Internet Service Provider*
27 *Vulnerability*
28 *Patch*

29 *Marc Maiffret*
30 *eEye Digital Security Inc*
31 *Aliso Viejo*
32 *Ted Bridis, Associated Press July 16.2003.*

فروشندگان اقدام کنیم و این تنها روش مقابله‌ای است که در اختیار داریم.

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

از نظر مفهومی میان ماهیت تهدیدات فضای سایبر و تهدیداتی که در دنیای واقعی وجود دارند هیچ تفاوتی نیست، بلکه تفاوت این دو مقوله برخاسته از خصوصیات فضای الکترونیکی و تهدیدات این حوزه است که باعث می‌شود بتوان از بروز آنها جلوگیری کرد و آنها را خنثی، یا شناسایی و رفع نمود.

عناوین *حریم خصوصی*[۳۳] و *محرمانگی*[۳۴] با مسئله امنیت در ارتباط هستند. اطلاعاتی که "خصوصی" بشمار می‌روند تنها زمانی می‌توانند واقعاً خصوصی بمانند که بصورت ایمن ذخیره شده باشند. برای این منظور در دنیای واقعی بگونه‌ای رفتار می‌کنیم که گویی چنین اطلاعاتی وجود خارجی ندارند. این سیاست را *امنیت گمنامی*[۳۵] می‌نامند. به همین ترتیب اطلاعاتی که باید بصورت محرمانه به‌اشتراک گذارده شوند باید برای کسانیکه آنها را به اشتراک گذاشته‌اند بصورت ایمن باقی بمانند. اگر این افراد همیشه در یک مکان نیستند هنگام انتقال این اطلاعات باید سیاستهای امنیتی کافی در مورد آنها اعمال شود.

موقعیتهایی نظیر این مسئله در فضای سایبر نیز وجود دارد، ولی با فرض طبیعت خاص فضای سایبر و ارتباط میان رایانه‌های موجود در آن، امنیت گمنامی یا استفاده از پنهان‌سازی سیاستی ضعیف می‌نماید و باید از آن اجتناب کرد. این کتاب در سطوح مختلف جزئیاتی در مورد مقیاسهای امنیتی مورد نیاز فضای سایبر ارائه می‌نماید.

پیدایش و رشد اینترنت

محیط رایانه‌ای و شبکه‌ایِ اینترنت امروز در ابتدا با هدف پژوهش و آموزش بوجود آمده بود. زمانیکه ARPANET (اینترنت اولیه) برای اولین‌بار ایجاد شد، هدف اصلی آن اشتراک منابع گروههای متعدد پژوهشگران در موقعیتهای جغرافیایی مختلف بود. این گروهها اهداف یکسان داشتند و با هدف به‌اشتراک‌گذاشتن منابع و داده‌ها کار می‌کردند؛ دسترسی به شبکه محدود به اعضای این گروهها می‌شد و لذا در آن زمان نگرانی چندانی در مورد تأمین امنیت اطلاعات وجود نداشت. طراحی شبکه جهانی وب نیز بر همین اساس شکل گرفت تا یک ابزار قوی برای کشف منابع اطلاعاتی و قراردادن آن در اختیار افراد دیگر باشد؛ بدون استفاده از مکانیزمی برای کسب مجوز یا تسهیل سرمایه‌گذاریهای مالی.

فرهنگ به‌اشتراک‌گذاری اطلاعات میان پژوهشگران و دانشگاهیان طی دههٔ ۹۰ توسط ARPANET مطرح شد و هنوز هم نشانه‌هایی از آن دیده می‌شود. بر اساس این فرهنگ، اطلاعات در شبکهٔ جهانی وب تا حد ممکن در دسترس و رایگان است و امکان استفاده از آن برای صدها میلیون نفر از مردم در سرتاسر جهان وجود دارد. این مسئله بسیار مهم است و پاسخی به این سؤال می‌باشد که چرا اینترنت تا امروز به این سطح از رشد رسیده است. جنبهٔ اخلاقی این فرهنگ در گفتگوهای عامیانهٔ مردمی که اینترنت را منبعی بسیار خوب و معتبر توصیف می‌کنند مشاهده می‌شود؛ چراکه قدرت رسانه‌ای اینترنت و اثرات کار با آنرا دیده‌اند. گاهی اوقات در مورد ماهیت اینترنت گفته می‌شود که "اطلاعات در آن تمایل به آزاد بودن دارند".

یک توجیه دیگر برای آسیب‌پذیریهای حال حاضر اینترنت آن است که نسل اول اینترنت بر اساس اعتماد متقابل ایجاد شده بود و کاربران آشکارا برای کار با یکدیگر به هم اعتماد می‌کردند. با گسترش وسیع اینترنت و به عضویت درآمدن افراد بیشتر با علایق و اهداف مختلف در آن، اعتماد متقابل معنای خود را از دست داد. درحال حاضر یکی از مباحث عمده در اینترنت توسعهٔ مفهوم نوین اعتماد متقابل است

33 *Privacy*
34 *Confidentiality*
35 *Security By Obscurity*

بگونه‌ای که مؤثر، واقع‌گرایانه، و بسادگی قابل پیاده‌سازی باشد.

اینترنت با سیستمهای ارتباطی قبل از خود چندین تفاوت اساسی دارد که هر کدام از اهمیت خاصی برخوردارند. بعضی از این تفاوتها هنگامیکه اینترنت را با *شبکهٔ تلفن عمومی سوئیچ شده* (PSTN)[۳۶] که روزانه در سراسر دنیا استفاده می‌شود مقایسه کنیم بهتر درک می‌شوند.

اینترنت براساس مدلی از انتقال اطلاعات کار می‌کند که Packet Switching نام دارد. هر زمان که اطلاعات از طریق اینترنت عبور می‌کند به چندین بستهٔ داده شکسته می‌شود. این بسته‌ها رمزگذاری شده و هر کدام بصورت مستقل در شبکه ارسال و پس از دریافت در مقصد مجدداً سرهم‌بندی می‌شوند (مسیر ارسال آنها می‌تواند متفاوت باشد). این روش انتقال در نقطهٔ مقابل Circuit Switching – که PSTN از آن استفاده می‌کند – قرار دارد. در این روش به هر مکالمهٔ تلفنی یک مدار واحد اختصاص داده می‌شود و لذا در آن حجم صدای انتقال یافته در هر لحظه مهم نیست.

اینترنت رسانه‌ای نادان است، چراکه تمام آنچه که می‌داند این است که باید یک بسته را از یک مبدأ متصل به شبکه به یک مقصد متصل به شبکه برساند. تمامی *خدمات اینترنتی*[۳۷] در انتها و در لبه‌ها به رایانه‌هایی می‌رسند که متصل به شبکه هستند. در عوض در PSTN اساس کار شبکه "هوشمندی" است و ابزار کاربر در نقاط انتهایی کاربرد اندکی برای صحبت‌کردن یا گوش‌دادن دارند.

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

اینترنت باز است و می‌توان آنرا بعنوان شبکه‌ای از شبکه‌ها درنظر گرفت که هر شبکه‌ای که به خانواده‌ای از پروتکل *TCP/IP*[۳۸] تعلق داشته باشد می‌تواند به آن متصل شود و بخشی از آن محسوب گردد. استانداردهایی که مجموعهٔ این پروتکلها را تعریف می‌کنند توسط *IETF*[۳۹] ارائه می‌شوند و معمولاً بدنهٔ فنی غیررسمی آنها بر اساس شایسته‌سالاری فنی و پیاده‌سازی استانداردهای توافقی تدوین می‌گردد.

اینترنت غیرمتمرکز است و در آن هیچ سیستم مرکزی ارتباطی وجود ندارد و همینکه شما از پروتکلهای اصلی آن نظیر TCP/IP پیروی کنید می‌توانید رایانه یا شبکه خود را به اینترنت متصل نمایید.

اینترنت در همه‌جا رایج است و موانع ورود به آن اندک هستند. مقدار *پهنای باند*[۴۰] (سرعتی که می‌توانید داده‌ها را با آن انتقال دهید) نیز به ظرفیت حمل سیمهای مسی، اتصالات فیبری یا کانالهای ماهواره‌ای واقع در مسیر انتقال بستگی دارد. در شاهراه آن طیفهای الکترومغناطیسی کمیاب وجود ندارند. هرجا که از طیف رادیویی استفاده گردد – مانند *شبکه‌های محلی بی‌سیم* (WLANs)[۴۱] که معمولاً با عنوان Wi-Fi از آنها نام برده می‌شود – قوانین و پروتکلهای مرتبط یک محیط اشتراکی را پدید می‌آورند که دسترسی را ساده می‌کند.

اینترنت برای کاربران متوسط واقع در بخشهایی از دنیا که مکالمات تلفنی محلی در آنها رایگان است نسبتاً ارزان تمام می‌شود. قیمت دسترسی به اینترنت از طریق خطوط تلفن و کافی‌نت و دیگر نقاط دسترسی عمومی در این کشورها بسیار اندک است و درنتیجه دسترسی به اینترنت برای درصد زیادی از مردم جهان بسیار ساده‌تر می‌باشد.

اینترنت مانع موجود میان مؤلف و ناشر را از بین برده است؛ شما می‌توانید یک ناشر باشید و روی رایانهٔ خود خدمات شبکه‌ای ایجاد کنید و برای اینکار تنها کافیست رایانهٔ شما همواره به اینترنت وصل باشد. همچنین می‌توانید دربارهٔ خدماتی که ارائه می‌دهید تصمیم‌گیری کنید و هر کس دیگری نیز درصورت اتصال به اینترنت و کسب اجازه از

36 *Public Switched Telephone Network*
37 *Internet Services*
38 *Transmission Control Protocol/Internet Protocol*
39 *Internet Engineering Task Force*
40 *Bandwidth*
41 *Wireless Local Area Networks*

جانب شما می‌تواند به رایانهٔ شما وصل شده و از آن خدمات استفاده نماید. اینترنت توسط کاربران قابل کنترل و شنود است، اما در بسیاری از کشورها شما می‌توانید انتخاب کنید که پیامها و سایر داده‌های ارسالیتان برای مقابله با شنود رمزگذاری شوند یا خیر.

بعلاوه غربال کردن پیامها تحت کنترل شما می‌باشد، هرچند که می‌توانید از یک منبع خارجی درخواست کنید اینکار را برای شما انجام دهد – مثلاً از ISP خود بخواهید که پیامهای نامطلوب را براساس ضوابطی که خودتان تدوین می‌کنید غربال نماید.

اینترنت یک رسانهٔ تعاملی است؛ می‌توانید به آسانی و با سرعت چندین پایگاه وب را مشاهده کنید، یا از افراد بسیاری پیامهای الکترونیکی دریافت و یا به آنها پیام ارسال نمایید. از آنجا که زمان انتظار برای خدمات برخط بستگی به میزان پهنای باند خط ارتباطی شما دارد، ممکن است دریافت پاسخ از این خدمات کمی طول بکشد.

اینترنت می‌تواند آسیب‌پذیر باشد؛ چراکه در ابتدا اساس آن بر ارائه خدمات به گروههای همکار و نسبتاً مشابه مردم قرار داشت و بجای استفاده از مکانیزمهای تصدیق هویت مطمئن، در آن به همه اعتماد می‌شد. این کتاب آسیب‌پذیریهای اینترنت را به شما شناسانده و مجموعه‌ای از الگوهای سرآمدی امنیتی را برای کمک به شما در کاهش آسیب‌پذیری ارائه می‌کند.

بر اساس مشخصه‌های فوق تاکنون باید در ذهن خود تصویری از اینترنت داشته باشید که در آن هر نوع فعالیت مجاز است و چیزی در آن محدودیت ندارد و تحت کنترل نیست. این فضای باز بخوبی ریشه‌های پژوهشی و دانشگاهی اینترنت را نشان می‌دهد و فواید آنرا برای تمامی اقشار جامعه می‌نمایاند. اینترنت با هدف برقراری امنیت طراحی نشده، بلکه برای افزایش ثمرات فعالیتهای مشترک بوجود آمده است. این میزان آزادی عمل فرصتهایی برای افراد ایجاد می‌کند که بتوانند از شبکه‌ها سوء استفاده کنند و به دیگران آسیبهای جدی وارد نمایند. ما ابتدا باید ماهیت این نوع سوء استفاده‌ها را درک کرده و سپس شبکه‌های خود را در مقابل آنها امن کنیم.

موضوعات مطرح در حوزهٔ امنیت اطلاعات

مفاهیم رایانه، شبکه و امنیت داده‌ها در فضای سایبر همانند دنیای واقعی هستند، ولی مکانیزمهای پیاده‌سازی روالهای مرتبط با آنها متفاوت است. مثلاً برای استفاده از حسابهای کاربری که اجازهٔ دسترسی به اطلاعات یا خدمات را فراهم می‌آورند، به جای کلیدهای فیزیکی یا الکترونیکی، دارای *شناسهٔ کاربری*[42] و *رمز عبور*[43] هستیم و بجای استفاده از پاکتهای دربسته برای انتقال اطلاعات می‌توانیم دادهٔ انتقالی را به نحوی رمزگذاری کنیم که توسط افراد ناشناس، غیرقابل خواندن باشد.

در مقایسهٔ دنیای واقعی با فضای سایبر می‌توانیم تخلفات مشابهی را در مورد قابلیت اطمینان و محرمانگی ببینیم. در هر دوی آنها ممکن است آدرسهای نادرست و یا امضاهای جعلی وجود داشته باشد. در هر دو فضا امکان ارائه اطلاعات غلط یا گمراه‌کننده نیز وجود خواهد داشت. همچنین امکان به اشتباه انداختن اشخاص با اطلاعات – چه بصورت تصادفی و چه از روی عمد – وجود دارد که باعث می‌شود نتوان تعیین کرد که چه اطلاعاتی مهم و قابل تأیید هستند.[44] دست آخر اینکه در هر دو فضا امکان دسترسی غیرمجاز به اطلاعات محرمانه و استفاده از آنها برای مقاصد غیرقانونی نیز وجود دارد.

اما با همهٔ این شباهتها سه تفاوت عمده میان این دو فضا مشاهده می‌شود:

اول: هر نوع نقض امنیت در فضای سایبر می‌تواند بسیار سریع اتفاق بیافتد؛ یعنی تا زمانیکه بخواهید آگاه شوید چه اتفاقی برای سرمایه‌های شما افتاده، ممکن است دیگر برای جلوگیری از وارد آمدن خسارت بسیار دیر شده باشد. البته تمامی حملات سریع اتفاق نمی‌افتند؛ بلکه بعضی از آنها در هنگام وقوع قابل مشاهده‌اند و برای به نتیجه رسیدن زمان

---

42 *Username*

43 *Password*

۴۴ *کاپیتان کشتی معروف تایتانیک از رادیوی اولیه برای برقراری تماس از کشتی با ساحل استفاده می‌کرد. منشی رادیو که اولین سفر دریایی خود را تجربه می‌کرد آنقدر پیامهای شخصی دریافت می‌نمود که یک پیام مهم – هشدار در مورد یک کوه یخی بزرگ در مسیر حرکت کشتی – بعنوان یک پیام مهم و شایستهٔ پیگیری شناسایی نشد. نتیجه این بود که کشتی با کوه یخی برخورد کرد و چند ساعت بعد غرق شد.*

زیادی می‌برند. درسی که از این مطلب گرفته می‌شود آن است که تدابیر امنیتی و بازدارنده باید از استیلای کافی برای تشخیص نقض حریم امنیتی در حین وقوع جرم یا پس از آن برخوردار باشند.

به گزارشهای زیر دربارهٔ کرم Slammer که در اوایل سال ۲۰۰۳ میلادی باعث خرابی شدید در کار اینترنت شد توجه کنید. در اثر فعالیتهای این کرم، کشورهای زیادی از تمامی پنج قارهٔ جهان آلوده شدند و بخش عمدهٔ خرابیها نصیب کشورهای درحال توسعه شد:

Slammer (که گاهی اوقات Sapphire نیز نامیده می‌شود) سریعترین کرم رایانه‌ای است که در طول حیات رایانه‌ها منتشر شده. با شروع گسترش آن در سراسر اینترنت، بیش از ۹۰٪ *میزبانهای*[45] آسیب‌پذیر در عرض ۱۰ دقیقه آلوده شدند و این امر موجب اختلال در انجام داد و ستدهای مالی و امور حمل و نقل مؤسسات دولتی شد و جایی برای عکس‌العمل انسانی باقی نگذاشت...

Slammer قبل از ساعت ۵:۳۰ *UTC*[46] روز شنبه ۲۵ ژانویه ۲۰۰۳ میلادی با بهره‌برداری از یک *آسیب‌پذیری سرریزی بافر*[47] با نفوذ به رایانه‌های متصل به اینترنت که نرم‌افزار Microsoft SQL Server یا Microsoft SQL Desktop Engine (MSDE) 2000 را اجرا می‌کردند نفوذ کرد و به آرامی اقدام به آلوده ساختن تمامی رایانه‌های میزبان نمود. *دیوید لیچفیلد*[48] در جولای سال ۲۰۰۲ میلادی این آسیب‌پذیری را کشف کرد و مایکروسافت نیز قبل از انتشار کرم Slammer وصله‌ای برای اصلاح آن منتشر کرده بود.[49]

طبق گزارشهای رسمی کرم مذکور با استفاده از این آسیب‌پذیری حداقل ۷۵ هزار رایانهٔ میزبان را آلوده کرد – که البته تعداد واقعی بسیار بیش از این میزان است – و موجب اختلال شدید در کار اینترنت و بروز نتایج پیش‌بینی‌نشده‌ای چون لغو پروازهای هوایی، اختلال در انتخابات، و بروز اشکال در کار دستگاههای خودپرداز شد.[50]

دوم: لازم نیست شما در یک محل بصورت فیزیکی حضور داشته باشید تا بتوانید امنیت فضای سایبر را خدشه‌دار کنید. این بدان معناست که مثلاً یک نفر در اروپا می‌تواند امنیت رایانه‌های یک هدف در هند را به آسانیِ کسی که در هند تنها به اندازه عرض یک خیابان با آن هدف فاصله دارد خدشه‌دار نماید. تهدید امنیتی در فضای سایبر می‌تواند از هر جای شبکه شروع شود و به سمت هدفی معلوم و مشخص جهت‌گیری کند؛ و هدف نیز می‌تواند بصورت تصادفی انتخاب شده باشد. این تهدیدات خطرناک باعث می‌شوند که ما نحوهٔ تفکر خود در مورد امنیت را تغییر دهیم. می‌توان گفت این هیچ ارزشی ندارد که در آیین‌نامهٔ حق تکثیر Digital Millennium طراحی نرم‌افزارهای قفل‌شکن غیرقانونی اعلام شود؛ چراکه درحال حاضر کمیته‌های ملی و جهانی حق تکثیر در این موضوع و سایر موارد مرتبط به حفاظت از داده‌ها، هنوز مشغول تدوین راهکارهای اجرایی هستند.[51]

سوم: فضای سایبر محیطی قدرتمند اما پیچیده را بوجود آورده که در آن نقش تأمین امنیت بر عهدهٔ چند بازیگر است. مثلاً اگر شما یکی از کاربران یک ISP باشید، راههای مختلفی برای حفاظت از خود و رایانه شخصی‌تان پیشِ‌رو دارید؛ هرچند نمی‌توانید سیاستهای امنیتی ISP مورد استفادهٔ خود یا نحوهٔ پیاده‌سازی آنرا کنترل کنید. همچنین نمی‌توانید نرم‌افزارهای مشتریان خود را تحت کنترل داشته باشید؛ حتی اگر در ارتباط نزدیک با سیستمهای آنها باشید. پس باید یک استراتژی حفاظتی برای سرمایه‌هایتان اتخاذ کنید، چراکه

45 *Hosts*
46 *Universal Time Coordinated*
47 *Buffer Overflow Vulnerability*
48 *David Litchfield*
49 *http://www.microsoft.com/security/slammer.asp*

50 *Moore, Paxson, Savage, Shannon, Staniford and Weaver,"Inside the Slammer Worm,"IEEE Security and Privacy,Vol.1,No.4,July/August 2003, pp.33-39.*

۵۱ *برای دستیابی به نظرات جدید در مورد این سند می‌توانید به مراجع زیر مراجعه کنید:*
U.S. Copyright Office Digital Millennium Copyright Act Study: http://www.copyright.gov/reports/studies/dmca/dmca_study.html
DMCA: http://www.copyright.gov/legislation/hr2281.pdf

می‌دانید برقراری ارتباط با دنیای بیرون باعث می‌شود نتوانید تمام آسیب‌پذیریهای شبکه را خنثی نمایید.

مخاطرات محتمل در فضای سایبر چیستند؟ اگر هیچ ملاحظهٔ امنیتی را مد نظر قرار نداده باشید بعضی نتایجی که ممکن است به بار بیایند عبارتند از:

تخریب اطلاعات – داده‌های ذخیره‌شده روی رایانهٔ شما ممکن است حذف شوند. البته معمولاً امکان بازیابی آنها وجود دارد، اما فرآیندی زمان‌بر و احتمالاً ناقص خواهد بود. اگر یک مؤسسهٔ دولتی باشید ممکن است فعالیتهایتان حین این دوره دچار اختلال شود.

سرقت اطلاعات و نقض حریم خصوصی – ممکن است از سرقت اطلاعات بلافاصله یا با تأخیر مطلع شوید و این مسئله از اینکه متوجه شوید چه کسی داده‌های شما را در اختیار گرفته، چه اطلاعاتی در اختیار اوست، یا با آنها چه کارهایی انجام خواهد داد کاملاً مجزاست. اگر حجم وسیعی از اطلاعات شخصی شما به سرقت رفته باشد به احتمال زیاد سارق اطلاعات کلیدی شما را در اختیار دارد و همین امر می‌تواند نتایجی نامعلوم و تا اندازه‌ای خطرناک در پی داشته باشد.

نقض یکپارچگی اطلاعات – اطلاعات موجود در رایانه ممکن است بدون اطلاع شما تغییر کنند و دستکاری شوند. بر اساس نوع اطلاعاتی که نگهداری می‌کنید نتایج این دستکاری می‌تواند مقطعی یا درازمدت باشد. اگر این داده‌ها شامل سوابق مالی، اطلاعات مشتریان، وضعیت سفارشات یا پرونده‌های کارمندان باشند، پیامدهای نقض یکپارچگی آنها ممکن است بسیار پرهزینه و زیانبار باشد.

نقض انسجام شبکه از طریق سایر سیستمها و شبکه‌ها – هرچند در این مورد به طور مستقیم مورد حمله قرار نگرفته‌اید، ولی ممکن است رایانه‌های دیگری که به آنها دسترسی داشته‌اید مورد حمله قرار گیرند و این مسئله روی شما نیز تأثیرگذار باشد. در اینصورت اگر مثلاً یک مؤسسهٔ مالی و اعتباری باشید حین دورهٔ بازیابی اطلاعات قادر به تکمیل تراکنشهای مالی خود نخواهید بود.

ثبت کلیدها – نرم‌افزارهای پنهانی می‌توانند روی رایانهٔ شما نصب شوند که فشرده‌شدن دکمه‌های صفحه‌کلید توسط شما را ثبت کرده و آنها را به رایانه‌ای دیگر ارسال نمایند. این مسئله می‌تواند دسترسی به منابع خارجی نظیر دسترسی به یک *سرویس‌دهندهٔ وب*[52] محافظت‌شده، دسترسی به یک سرویس‌دهندهٔ پست الکترونیکی، نقل و انتقالات مالی، و یا دریافت اطلاعات محرمانه را دچار اشکال کند. در اینحالت سارق می‌تواند *نشانهای تصدیق هویت*[53]، شمارهٔ کارت اعتباری، و رمزهای عبور شما را بدست آورد و در آینده برای منافع شخصی خود مورد استفاده قرار دهد.

منع دسترسی[54] – ممکن است شما از دسترسی به اطلاعات خود محروم شوید، حتی اگر آن اطلاعات پاک نشده باشند. مثلاً امکان دارد اطلاعات شما در قالبهای رمزگذاری‌شده‌ای ظاهر شوند و تنها مهاجم کلید رمزگشایی آنها را در اختیار داشته باشد.

هزینهٔ ترمیم موفقیت‌آمیز از هر یک از این حملات قابل ملاحظه است و بازیابی در برخی موارد ناممکن بنظر می‌آید. اگر شما مدیر یک رسانهٔ تبلیغاتی باشید که به منابع داده‌ای الکترونیکی خود وابستگی شدید دارد، یک حملهٔ مخرب می‌تواند موجب ورشکستگی مؤسسه شما گردد. توجه داشته باشید که کرم Slammer سیستمهایی را آلوده می‌کرد که وصلهٔ ارائه‌شده توسط مایکروسافت روی آنها نصب نشده بود.

یکی از نفوذهای امنیتی که بیش از یکسال فعالیت موفقیت‌آمیز داشت روشهای نوینی را به تصویر کشید که با آنها می‌توان امنیت را در فضای سایبر خدشه‌دار کرد:

" آسوشیتد پرس (نیویورک) – برای بیش از یکسال، *جوجو جیانگ*[55] بدون اطلاعِ افرادی که از *پایانه‌های*[56] اینترنتی در *فروشگاههای کینکو*[57] در نیویورک استفاده می‌کردند، آنچه که آنها تایپ می‌کردند را ثبت می‌کرد. جیانگ بصورت مخفیانه نرم‌افزاری را در حداقل چهارده فروشگاه کینکو نصب کرده بود که می‌توانست فشردن

52 *Web Server*
53 *Authentication Tokens*
54 *Denial of Access*
55 *Juju Jiang*
56 *Terminals*
57 *Kinko's Stores*

کلیدهای افراد را ثبت نماید. این نرم افزار در طول فعالیت یکسالهٔ خود بیش از ۴۵۰ شناسهٔ کاربری و رمز عبور ثبت کرده و از آنها برای دسترسی و حتی بازکردن حسابهای بانکی برخط استفاده می‌نمود.

این پرونده که در اوایل این ماه پس از دستگیری جیانگ منجر به تعیین مجازات برای وی شد خطرهای استفاده از پایانه‌های عمومی اینترنت در کافی‌نت‌ها، کتابخانه‌ها، فرودگاهها و دیگر مؤسسات را آشکار می‌سازد. *نیل مهتا*[58] مهندس پژوهش در مؤسسهٔ *سیستمهای ایمن اینترنتی*[59] هشدار می‌دهد که "هنگام استفاده از هر یک از پایانه‌های عمومی از دانشِ عرفی خود بهره بگیرید. برای بسیاری از ارتباطات روزمره نظیر اتصال به وب ممکن است با مشکلی مواجه نشوید اما برای انجام هر کاری که ممکن است حساسیت ایجاد کند ابتدا کمی فکر کنید". جیانگ زمانی دستگیر شد که مطابق سوابق موجود در دادگاه از یکی از رمزهای عبور مسروقه برای دسترسی به رایانه‌ای مجهز به نرم افزار GoToMyPC استفاده کرده بود. این نرم افزار به افراد امکان می‌دهد که از راه دور و از هر مکانی به رایانهٔ خود دسترسی پیدا کنند. شخصی که برنامهٔ GoToMyPC روی رایانهٔ وی نصب شده بود در زمان وقوع جرم در خانه بود و ناگهان متوجه شد مکان‌نمای رایانهٔ او روی صفحه شروع به حرکت کرد و فایلها خود به خود باز شدند. سپس دید که یک حساب بانکی باز و نام او در یک سرویس خرید اینترنتی درج شد. جیانگ که منتظر صدور حکم دادگاه است، نهایتاً در چهاردهم فوریه ۲۰۰۱ به نصب کردن نرم‌افزار مخفی ثبت‌کنندهٔ کلید در فروشگاههای کینکو اعتراف کرد.[60]

این کتاب راهنمایی دربارهٔ امنیت کاربران هم در محیط خانه و هم در محیط تجاری می‌باشد و لذا حاوی اطلاعات وسیعی دربارهٔ موضوعات امنیتی مانند مخاطرات، نتایج حملات، روشهای حفاظت از رایانه‌ها، شبکه‌ها و داده‌ها، و نیز سیاستهایی است که باید قبل از پیاده‌سازیِ استراتژیِ امنیتیِ مؤثر مورد بررسی قرار گیرند. هدف نهایی این کتاب دور ساختن کاربران از منابع ارائه‌شده در محیطهای دیجیتالی جدید نیست، بلکه قدرت بخشیدن به کاربران برای لذت بردن از این دنیای نوین به روشی ایمن و مطمئن است. در یک کلام می‌توان گفت هدف از انتشار این کتاب توسعهٔ درک واقع‌گرایانه و عمیق از ماهیت مشکلات امنیتی موجود به منظور کاهش آسیب‌پذیریها و افزایش نقاط قوت فناوری اطلاعات و ارتباطات می‌باشد.

انگیزهٔ خرابکاران امنیتی چیست؟

در زندگی واقعی انگیزه‌های زیادی برای انجام تخلفات جنایی علیه یک شخص یا سازمان وجود دارد. یکی از دلایل عمده، انتقامگیری فرد خرابکار از شخصی که فکر می‌کند به او آسیبی رسانده، و یا بدست‌آوردن پول است.

نظیر همین تخلفات نیز در فضای سایبر وجود دارد، اما تخلف در این فضا از جنس دیگری است. فضای سایبر برای گروهی از افراد – که عموماً "خرابکار" نامیده می‌شوند و قادرند وارد حسابهای کاربری افراد شوند و یا بعنوان تفریح و سرگرمی به افراد دیگر آسیب برسانند – یک محیط چالش برانگیز است. بعبارت دیگر، آنها قدرت نفوذ به حسابهای کاربری، پایگاههای داده و تجهیزات شبکه‌ای را یک افتخار برای خود می‌دانند. مشابه این رفتار در دنیای واقعی بسیار نادر است.

خرابکارها معمولاً فعالیتهای خود را "جنایات بدون قربانی" به حساب می‌آورند. استدلال آنها این است که وقتی یک حساب کاربری یا پایگاه داده مورد نفوذ قرار می‌گیرد ولی چیزی تغییر نمی‌یابد و دزدیده نمی‌شود چه آسیبی به کسی وارد شده است؟ در واقع این افراد به تأثیرات حقوقی و پیامدهای اینکار توجه نمی‌کنند و به احساس ناامنی قربانیانشان که ناشی از انجام این فعالیتها می‌شود نیز اهمیتی نمی‌دهند. مشابه این رفتار در دنیای واقعی مثل این است که فردی وارد خانهٔ شما شود و هر زمان که بخواهد نیز بتواند اینکار را تکرار کند. مسلماً این مسئله برای شما غیرقابل تحمل خواهد بود.

متأسفانه اینترنت به ناقضان امنیت کمک زیادی می‌کند. برخی از خرابکارها دارای ابزارهای نفوذ هستند که به نفوذگران تازه‌کار هم امکان بهره‌برداری موفقیت‌آمیز از برخی آسیب‌پذیریها را می‌دهد. چنین ابزارهایی معمولاً به گروههای خبری Usenet که بسیار مشهور هستند فرستاده می‌شوند و افراد مختلف می‌توانند ابزار را از آنجا پیدا کرده و مورد

58 *Neel Mehta*
59 *Internet Security Systems*
60 *Associated Press Bulletin, July 23, 2003*

استفاده قرار دهند. از آنجا که بسیاری از این ابزارها ممکن است بدون خطر باشند، هرگز کسی مطمئن نیست آثار استفاده از هریک از آنها دقیقاً چیست. علاوه بر آن این امکان وجود دارد که با انجام تغییراتی در بعضی از این ابزارِ به‌اصطلاح بی‌خطر بتوان به رایانه‌ها و حسابهای کاربری که از طریق آنها مورد دسترسی قرار گرفته‌اند آسیب وارد کرد. در ادامه، یک نمونه از این موارد ذکر شده است:

> سند CA-203-18 مرکز فوریتهای امنیت رایانه‌ای آخرین حفرهٔ Windows را مستند کرده، و CNet نیز گزارش داده که با بهره‌برداری از این آسیب‌پذیری برای نفوذ به Windows راه برای ظهور برق‌آسا و حملهٔ شدید یک کرم دیگر هموار می‌شود:
>
> پژوهشگران امنیتی هشدار داده‌اند که یک گروه از نفوذگران برنامه‌ای منتشر کرده‌اند که برای سوء استفاده از یک اشکال عمدهٔ Windows طراحی شده و راه را برای انجام یک حملهٔ بزرگ تا اواخر هفتهٔ جاری باز می‌کند. این هشدار روز جمعه اعلام شد؛ بعد از آنکه نفوذگران چینی گروه امنیتی X Focus متن برنامه‌ای را برای چندین مرکز امنیتی دنیا منتشر کردند که با طراحی ماهرانه به رایانه‌های دارای سیستم‌عامل Windows نفوذ می‌کرد.
>
> برنامهٔ گروه X Focus از اشکال موجود در سیستم‌عامل مایکروسافت بهره‌برداری می‌کند و به نفوذگران امکان نفوذ به سیستم از راه دور را می‌دهد. این اشکال توسط چند نفر از متخصصین بعنوان بزرگترین اشکالی که تا کنون در Windows یافت شده معرفی شده است.[۶۱]

حملات روزافزونی که توسط افراد نسبتاً غیرحرفه‌ای انجام می‌شوند نیز ماجرایی طولانی و دنباله‌دار است.

البته تمامی نقض حریمهای امنیتی مختص رایانه‌ها و اینترنت نیستند. دستگاههای خودپرداز نیز تا کنون برای سرقت اطلاعات محرمانه مورد استفاده قرار گرفته‌اند. در یک مورد (در *ایالت کانکتیکات*[۶۲] ایالات متحده) سارقین اقدام به نصب دستگاهی شبیه دستگاه خودپرداز در یک مرکز خرید کردند. هنگامیکه مردم برای گرفتن پول از این ماشین کارت و شمارهٔ رمز خود را وارد می‌کردند، این دستگاه جعلی با ذخیرهٔ رمزهای عبور دسترسیهای غیرمجاز بعدی به این حسابها را بسیار ساده می‌کرد، اما چون اتصالی با مراکز واقعی اعتباری نداشت قادر به تکمیل عملیات مالی نبود. در یک مورد دیگر سارقین از دستگاههای خودپرداز به نحوی استفاده کردند که امکان انتقال پول هم وجود داشته باشد، اما مدتی بعد و با استفاده از اطلاعات ثبت‌شده اقدام به سرقت می‌نمودند.

اگرچه بیشتر جرائمِ قابلِ مشاهده در دنیای سایبر توسط افراد انجام می‌شود، ولی سازمانها و مؤسسات نیز قادر به سوء استفاده از خصوصیات این فضا برای رسیدن به اهداف سازمانی خود هستند. جرائم سازماندهی‌شده ممکن است دستکاری در شبکهٔ اینترنت برای رسیدن به نتایج مطلوب آنها باشد، اما می‌تواند باعث ارتکاب جرم علیه دیگران نیز بشود. ممکن است برخی سازمانها علاقه داشته باشند که نتیجهٔ یک نظرسنجی یا حتی انتخابات را دستکاری کنند تا به نتایج مطلوب خود برسند. برخی از مؤسسات درحال حاضر روی این مسئله سرمایه‌گذاری زیادی انجام داده‌اند و ممکن است بتوانند تا مدتها آنرا همچنان با قوت ادامه دهند.

واضح است که منافع بالقوهٔ موجود در عصر نوین دیجیتال بیشمار هستند. بسیار حائز اهمیت است که با ایمن‌سازی محیط فیزیکی، زیرساختها، رایانه‌ها، خطوط ارتباطی و منابع اطلاعاتیِ خود از این منافع حفاظت کنیم. اولین گام در انجام این مهم رسیدن به سطح شناخت کافی و صحیح از فناوری است که می‌تواند در اتخاذ تصمیمات عاقلانه دربارهٔ چگونگیِ رسیدن به سطح مطلوبی از امنیت به ما کمک کند. بسیاری از ما در این زمینه چندین نقش را بر عهده داریم: ممکن است بعنوان یک کاربر عادی از این منابع استفاده کنیم، در قبال سیستمهای دیجیتال و خدمات موجود در یک سازمان مسئولیت داشته باشیم، و یا به همکاری با دولت در اجرای سیاستهای حمایتی از امنیت علاقه‌مند باشیم.

همهٔ ما در هریک از این نقشها در قبال تحقق سطح مطلوبی از امنیت مسئول هستیم. متأسفانه امنیت در یک محیط پیچیده معمولاً به اندازهٔ امنیت ضعیفترین جزءِ آن محیط استحکام دارد؛ از اینرو باید مطمئن شویم که اجزای محیطی که روی آن کنترل داریم آنقدر قوی هستند که ضعیفترینِ

61 CNet News.com ,July 25,2003
62 Connecticut State

آنها هم از توانایی دفاع در برابر تهدیدات موجود برخوردار است.

اهمیت امنیت برای سازمانهای کوچک و متوسط در کشورهای درحال توسعه

با اینکه امنیت برای همه حائز اهمیت است، اما برای سازمانهای کوچک و متوسط کشورهای درحال توسعه اهمیت ویژه‌ای دارد. نتایج حاصل از ورود به بازار جهانی با کمک فناوری اطلاعات و ارتباطات بسیار مطلوب است، ولی مخاطرات انجام اینکار بصورت ناامن نیز بسیار اساسی است.

در بسیاری از اصناف تجاری، عملیات دستی به مدیریت با استفاده از رایانه‌ها تغییر یافته است. از رایانه‌های مستقل می‌توان در بسیاری از عرصه‌های اقتصادی کشورهای توسعه‌یافته برای مدت‌زمانی مشخص استفاده کرد. با معرفی منابع رایانه‌ای جدید، مدیران به سمت و سوی کسب دانش و اطلاعات دربارهٔ موضوعات کاربردی چون *پشتیبان‌گیری*[۶۳]، نگهداری شبکه، به‌روزرسانی نرم‌افزارها و *ممیزی* (بازبینی)[۶۴] رایانه‌ای در حرکت هستند. کسب موفقیت در همگیِ موارد فوق مستلزم آشنایی با رایانه، شبکه، و مفاهیم امنیت اطلاعات است.

با معرفی ارتباطات شبکه‌ای و امکان ورود به عرصهٔ تجارت الکترونیکی، فرآیندهای سیستم و فرآیندهای مدیریت باید از دو دیدگاه متفاوت نظاره شوند. سیستمهای مستقل عموماً محصول‌محور یا فرآیندمحور هستند (مثل انبارداری، سفارشات یا فرآیندهایی نظیر تولید، ثبت در دفاتر عمومی، و حسابهای پرداختنی و دریافتنی)، اما سیستمهای موفق تجارت الکترونیکی برخط به روش دیگری سازماندهی می‌شوند. در این سیستمها برای کسب موفقیت لازم است که طراحی مشتری‌مدار باشد و سیستم به تعقیب رفتار مشتری در فرآیندهای جستجو و ارزیابی محصولات، ارائه سفارش، تکمیل تراکنشهای مالی و ردگیری محصول ارسال‌شده بپردازد. در این سیستمها نگرانی در مورد محصولات و فرآیندها همچنان مهم است، اما در مقابلِ نیاز به تعقیب رفتار مشتری در پایگاه وب و انجام هر معامله‌ای که مشتری آنرا درخواست می‌کند در اولویت بعدی قرار می‌گیرد. این طراحی مجدد برای دستیابی به موفقیت ضروری است، اما به یک راهکار جایگزین برای مدیریت درخواستهای خرید مشتری نیاز دارد؛ روشی که اگر بدون توجه کافی پیاده‌سازی شود ممکن است راه را برای روشهای جدید نفوذهای امنیتی باز بگذارد.

سازمانهای کوچک و متوسط باید آگاه باشند که اصلاح نگرش سیستمهای تجاری برای بکارگیری اینترنت، مخاطرات جدیدی برای آنها به همراه دارد. یکی از این خطرات از همه جدیدتر است: احتمال به سرقت رفتن و در معرض فروش قرار گرفتن سرمایه‌های موجود در شرکت. در عصری که کالاها و خدمات فروخته‌شده را محصولات اطلاعاتی تشکیل می‌دهند، احتمال توزیع و تهیهٔ غیرقانونی آنها بصورت رایگان و یا در بازار سیاه وجود دارد که در اینحالت منافع اینکار به سارقان می‌رسد، و نه به شرکتی که اطلاعات را تولید کرده است.

بارزترین نمونهٔ نسخه‌برداری غیرقانونی که امروزه می‌توان مشاهده کرد در صنعت موسیقی رواج دارد که به توزیع محصولات مسروقه و غالباً هم در قالب دیسک فشرده منجر شده است. درحال حاضر حفاظت از سرمایه‌های دیجیتالی مسئله‌ای حل‌نشده می‌باشد، هرچند برای حل آن اقدامات زیادی صورت گرفته است. دیرزمانی است که از محصولات اطلاعاتی دیجیتالی نسخه‌برداریهای نسبتاً کاملی انجام می‌شود، چراکه نسخه‌برداری از آنها آسان بوده و حین فروش لزومی ندارد که به دنبال نسخه اصلی آن بود. فناوری مورد استفاده در صنعت موسیقی را می‌توان در شرایط و محیطهای دیگر نیز مورد استفاده قرار داد، به این معنی که فوت و فنهای تجاری یا دیگر اطلاعات محرمانه را نیز می‌توان با روشهایی تهیه و منتشر نمود که موجب تخریب شدید آن تجارت و صنعت گردد. سرمایه‌های با ارزش نیاز به حفاظت کافی و مناسب دارند. البته این سطح از امنیت می‌تواند برقرار شود، اما مخاطرات و روشهای کار برای شرکتی که در قالب تجارت الکترونیکی کار می‌کند با مخاطرات و روشهای کار در شرکتی که بصورت سنتی به تجارت می‌پردازد متفاوت است.

بسوی مفهوم نوینی از قابلیت اطمینان

محیط دیجیتالی جدید از ما می‌خواهد که در تعریف خود از قابلیت اطمینان بازنگری کنیم. در دنیای واقعی از معیارهای گسترده‌ای برای تصمیمگیری دربارهٔ میزان اطمینان به یک

63 *Backup*
64 *Audit*

شخص، یک فرآیند، یا یک سازمان استفاده می‌کنیم؛ مثلاً از تطابق مشاهدات فعلی با تجربیات و دانسته‌های قبلی‌مان استفاده می‌نماییم. حین تبادل اطلاعات در فضای سایبر بیشترِ شاخصهای غیر شفاهی ارتباطات از دست می‌روند. هنگامیکه یک نامهٔ الکترونیکی دریافت می‌کنیم یا صفحهٔ وبی را می‌خوانیم، نمی‌توانیم همیشه بگوئیم که اگر اطلاعات دقیق بود و اگر آنها را بررسی می‌کردیم مشخص می‌شد که صحیح نیستند. همچنین نمی‌دانیم که خطاهای واقع‌شده نتیجه سهل‌انگاری هستند یا تلاشهایی تعمدی برای فریب دادن ما. در غیاب اطلاعات حتی دیگر نمی‌دانیم که آیا نویسندهٔ یک پیام همان شخصی است که خودش ادعای آنرا دارد یا خیر.

مسلم است که فریبکاری در جهان واقعی نیز رخ می دهد، ولی معمولاً تعیین حقیقت در شرایطی که افراد بصورت فیزیکی و مکانها بصورت واقعی وجود دارند ساده‌تر است.

خوشبختانه از طریق *مراکز صدور گواهی*[۶۵] به این بعد از امنیت دنیای سایبر کمک زیادی شده است. این مراکز برای شناسایی افراد و سازمانها به طور رسمی گواهی صادر می‌کنند. این مفهوم در دنیای واقعی نیز وجود دارد: اگر گذرنامهٔ ملی داشته باشید یعنی دولت یک کشور هویت شما را تأیید کرده و لذا گذرنامه نشانه‌ای خواهد بود که می‌توانید برای تصدیق هویت خود از آن استفاده کنید. بطور مشابه اگر گواهینامهٔ وسیلهٔ نقلیهٔ موتوری داشته باشید به این معنی است که یک سازمان ملی یا ناحیه‌ایِ دولت برای شما مجوزی صادر کرده که هم هویت شما را تأیید می‌کند و هم جواز رانندگی با یک وسیلهٔ نقلیه را به شما می‌دهد. شرکتهایی که خدمات کارت اعتباری می‌دهند نیز از طریق صدور کارتهای اعتباری شما را تأیید می‌نمایند. کارفرما یا آموزشگاه شما هم ممکن است از طریق یک کارت شناسایی شما را تأیید کند و آن کارت ممکن است دسترسی شما را به سرویسهای خاصی که مخصوص کارمندان یا دانشجویان یک حوزهٔ خاص هستند برقرار نماید.

واضح است که تعداد مراکز صدور گواهی در دنیای واقعی اندک هستند. بطور کلی هریک از این مراکز از تأیید شما هدف خاصی را درنظر می‌گیرند. جامعیت تأیید هویت از یک مرکز تا مرکز دیگر متفاوت است؛ برخی از آنها ممکن است به اثبات کامل هویت شما نیاز داشته باشند، درحالیکه سایرین ممکن است آنچه که بیان می‌کنید را بپذیرند.

مراکز صدور گواهی در دنیای سایبر این مشخصات را به اشتراک می‌گذارند. سطوح متعدد تأیید هویت برای درجات مختلف اطمینان ایجاد می‌شود و هریک از این گواهیها تنها در سطح خود معتبر می‌باشند. لذاست که هرچند ممکن است بنظر برسد که وجود یک مرکز صدور گواهی برای دستیابی به تمامی اهداف مورد نظر کافی است؛ اما چندین مرکز صدور گواهی در دنیای مجازی وجود دارد. علاوه بر این با استفاده از *گواهی الکترونیکی*[۶۶]، این گواهیها می‌توانند بصورت الکترونیکی امضا شوند و این اطمینان را ایجاد کنند که گواهی منتقل شده صحیح و حقیقی است. این سیستمهای صدور گواهی از روشهای تجربی و شهودی که در دنیای واقعی مورد استفاده قرار می‌گیرند مستحکم‌تر هستند. در دنیای دیجیتالی برای برقراری اعتماد لازم جهت پشتیبانی از انجام تراکنشهای تجاری و نقل و انتقالات مالی در شبکه‌های الکترونیکی، لازم است که روشهای مستحکم‌تر مورد استفاده قرار گیرند.

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

65 *Certification Authorities*

66 *Electronic Certification*

جمع‌بندی

فناوری دیجیتالی ابزارهای جدید و مهیجی را فراهم می‌کند که هریک می‌توانند نقش بسزایی در آموزش، بهداشت، رفاه، تجارت و سایر بخشهای جامعهٔ مدنی داشته باشند.

تمام افراد و کشورها از فناوری اطلاعات بهره می‌جویند، اما این فناوری برای کشورهای درحال توسعه جاذبهٔ خاصی دارد و می‌تواند جا افتادن آنها در جامعهٔ اقتصادَ جهانی را تسریع کند. این فناوری هنوز در آغاز راه خود است ولی بسرعت درحال پیشرفت می‌باشد. متأسفانه همانند سایر پیشرفتهای فناوری، اینترنت نیز می‌تواند هم برای اهداف مشروع و هم برای اهداف نامشروع مورد استفاده قرار گیرد. همانطور که مشاهده کردیم در دنیای سایبر مجرمان و خرابکارانی وجود دارند که از اینترنت برای حمله به کاربران منفرد و سازمانی استفاده می‌کنند.

مفهوم "ایمنی سایبر" یک مفهوم مهم است. مثالهای این فصل، میزان وقایع گزارش‌شده به CERT، و رخدادهای جدیدی که روزانه در مطبوعات گزارش می‌شوند همگی نشان می‌دهند که چرا آگاهی از موضوعات امنیتی حائز اهمیت است و چرا باید گامهایی برای تضمین پشتیبانی از رایانه‌های شخصی، داده‌ها و تجارت برداشت.

این کتاب حاوی مجموعه‌ای از الگوهای سرآمدی در زمینهٔ امنیت است که در اجرای سیاستها و روشهایی که به موقعیت خاص شما مربوط هستند کمک می‌کنند. علاوه بر آن مراجع چاپی و الکترونیکی فراوانی که در بر دارنده ابعاد خاص امنیت فناوری اطلاعات هستند و همچنین سازمانهایی که به شکل تخصصی بر روی موضوعات امنیت فناوری اطلاعات تمرکز دارند را معرفی می‌کند. تمامی این منابع برای افراد و سازمانهایی که در پی گسترش آگاهی خود از امنیت در جهان شبکه‌ای می‌باشند مفید خواهند بود.

این شرایط در کشورهای درحال توسعه از اهمیت خاصی برخوردار است. سرمایه‌گذاری مستقیم خارجی و اعتماد و قابلیت اطمینان در این کشورها بستگی به سطح امنیت و پیاده‌سازی موفقیت‌آمیز فناوری و زیرساختهای آن دارد. دولتها، سازمانها و کاربران منفرد همگی نقش بسزایی در تأمین امنیت سرمایه‌های اطلاعاتی و الکترونیکی کشورها ایفا می‌کنند. شناخت تهدیدات بسیار سودمند است؛ و عملکرد مناسب بر اساس چنین شناختی می‌تواند یک محیط قابل اطمینان ایجاد کند و باعث شود ساکنان کرهٔ زمین تا سرحد امکان فواید عصر نوین دیجیتال را حس کنند.