امنیت فناوری اطلاعات و سازمانها

بخش سوم

فصل اول

مقدمه

همانطور که در بخش دوم مشاهده کردیم کاربران می‌توانند برای حفاظت از رایانه‌های خود و داده‌های ذخیره‌شده در آن کارهای زیادی انجام دهند. در سازمانهای کوچک ممکن است شرایط تأمین امنیت ساده باشد و هرکس مسئولیت رایانه‌ها و فایلهای خود را بر عهده داشته باشد. با اینحال برای گروههای بزرگتر مثل سازمانهایی که با *تراکنشهای تجاری*[1] سر و کار دارند یا گروههایی که از داده‌های محرمانهٔ شهروندان یا مشتریان نگهداری می‌کنند، نیاز به ایجاد سیاستها و روالهای رسمی امنیتی بیشتر اهمیت پیدا می‌کند. هنگامیکه مدیران و کارمندان موضوع امنیت فناوری اطلاعات را مد نظر قرار می‌دهند – چه در شرکتهای تجاری، چه در سازمانهای غیرانتفاعی، و چه در مؤسسات دولتی – همواره با مسائل مشابهی مواجه خواهند بود. هر گروه برای داده‌های خود نیاز به سطح معینی از امنیت و روالهای شفاف و ساده برای به‌اجرا درآمدن توسط کارکنان، توانایی ایجاد و حفظ آگاهی از نیازهای مشتریان، و درکی از چگونگی پیاده‌سازی سیاستهای امنیتی در یک محیط عملیاتی دارد. علاوه بر این نیازهای کلی، هر دسته از سازمانها ملاحظات خاص مربوط به اهداف و مأموریت خود را نیز دارند. مدیران برای نیل به اهداف تعیین‌شده باید بر سیاستهای امنیت اطلاعات توجه مؤکد داشته باشند. همچنین درک هزینه‌های پیاده‌سازی سیاستهای امنیتیِ کاراً از اهمیت زیادی برخوردار است. فناوریها و روالهای امنیتی نوعی سرمایه‌گذاری به حساب می‌آیند و باید با توجه به هزینه‌های ضایعات محتمل مورد ارزیابی قرار گیرند. توصیه‌های عملی بخش سوم با درکی از تحلیل سود و زیان – که در یک محیط با منابع محدود بسیار ضروری است – ارائه شده است.

1 *Commercial Transactions*

بعضی شاخصهای آماری امنیت فناوری اطلاعات در سازمانها

تحقیق جهانی امنیت اطلاعات *ارنست و یانگ*[2] در سال ۲۰۰۳ نشان می‌دهد که ۹۰٪ سازمانها معتقدند امنیت اطلاعات برای دستیابی آنها به اهداف کلی‌شان بسیار حائز اهمیت است. ۷۸٪ از سازمانها عنوان کردند که اولین هدفشان از تلاش برای تأمین امنیت اطلاعات کاهش *مخاطرات*[3] می‌باشد. این سازمانها شامل ۱۰۰۰ شرکت ثروتمند می‌شدند که بخشی از منابع خود را برای مبارزه با مسائل امنیتی اختصاص داده بودند. در ادامهٔ این تحقیق:

- بیش از ۳۴٪ از سازمانها اظهار می‌کنند که قدرت کافی برای تشخیص اینکه آیا سیستمهایشان درحال حاضر مورد حمله قرار دارند یا خیر را ندارند.
- بیش از ۳۳٪ اظهار می‌کنند که توانایی ارائه عکس‌العمل مناسب در واکنش به رخدادهای امنیتی را ندارند.
- تنها ۳۴٪ از سازمانها ادعا می‌کنند که حاضر به اطاعت از ضوابط امنیتیِ قابل اجرا می‌باشند.
- ۵۶٪ سازمانها بودجهٔ ناکافی را مانع اصلی تأمین مؤثر امنیت اطلاعات می‌دانند.
- حدود ۶۰٪ از سازمانها اظهار می‌کنند که بازگشت سرمایه را برای امنیت اطلاعاتی بندرت محاسبه می‌کنند یا هرگز محاسبه نمی‌کنند.
- تنها ۲۹٪ سازمانها آموزش و آگاهی کارمندان را بعنوان قسمتی که بیشترین سرمایه‌گذاری برای امنیت اطلاعات را روی آن داشته‌اند ذکر می‌کنند؛ در مقابلِ ۸۳٪ که از فناوری بعنوان اولویت اول سرمایه‌گذاری خود در تأمین امنیت اطلاعات نام می‌برند.
- تنها ۳۵٪ از سازمانها اظهار می‌کنند که برای کارکنان برنامه‌های پیوستهٔ اطلاع‌رسانی و آموزشی دارند.

این آمارها حاکی از این هستند که همهٔ سازمانها – چه کوچک و چه بزرگ – فشارهای مالی و روانی تهدیدهای امنیت فناوری اطلاعات را حس می‌کنند. فصلهای آتی این

2 *Ernest & Young*
3 *Risks*

بخش به اولویتها و نگرانیهای سازمانهای کوچک و متوسط می‌پردازند. در عین حال به یاد داشتن نتایج تحقیق ارنست و یانگ بعنوان یک نماد از چالشهایی که تعدادی از ادارات تجاری با آنها مواجه شده‌اند بنظر مفید می‌آید.

تجارتهای کوچک و متوسط

اگر شما به *تجارتهای کوچک و متوسط* مشغول هستید[۴] اولویتهای اصلی شما قابلیت سودآوری، تداوم تجارت، پایداری، و کیفیت ارائه خدمات به مشتری هستند. سازمانهای کوچک و متوسط بوسیلهٔ قوانین محلی، ناحیه‌ای، یا ملی محدود شده‌اند و بسته به نوع تجارتی که به آن می‌پردازند و محیط تجاری کشوری که در آن فعالیت می‌کنند، ممکن است لازم باشد در مقابل چند مرکز پاسخگو باشند. در این سازمانها روند برقراری امنیت به حفاظت از سازمان و مشتریانش در مقابل فریب و حملات اساسی و پرهزینه علیه خدمات و سیستمها متمرکز خواهد بود. علاوه بر جرم رایانه‌ای و امنیت شبکه، حفاظت از داده‌ها نیز برای سازمانهای کوچک و متوسط حائز اهمیت است و به دو حوزهٔ اصلی تقسیم می‌شود: حفاظت از داده‌های سازمانی در مقابل جاسوسها یا مهاجمین سازمانیافته، و حفاظت از داده‌های مشتری مثل کارت اعتباری و تراکنشهای مالی.[۵]

سازمانهای غیرانتفاعی

در سازمانهای غیرانتفاعی مدیران و کارمندان به تأثیرگذاری روی بازار، همکاری با جوامع و شرکتهای همکار، و بدست آوردن شهرت تأکید دارند. سیستمها ممکن است هزینهٔ زیادی به خود اختصاص دهند و معمولاً بدلیل محدودیتهای بودجه در مؤسسات غیرانتفاعی از کیفیت پایینتری برخوردار باشند. بعلاوه معمولاً کارمندان تجربهٔ کمتری نسبت به کارهای فنی دارند و لذا وقتی می‌خواهند خدمات مداوم به مشتریان ارائه کنند و برای اهداکنندگان کمکهای مالی، ناظرین، و مؤسسات همکار خود یک وجههٔ مثبت از وضعیت و فعالیت مؤسسه به تصویر بکشند ممکن است با مشکلاتی مواجه شوند.

دانشگاهها

همانند سازمانهای غیرانتفاعی، در سیستمهای دانشگاهی نیز مسائلی چون محدودیتهای بودجه‌ای، شبکه‌های هزینه‌بر، و دامنهٔ وسیعی از مهارتهای فنی وجود دارند. دانشگاهها ممکن است با یکسری تهدیدات داخلی روبرو باشند؛ خصوصاً در حالتی که مثلاً دانشجویان برای پر کردن اوقات فراغت خود بخواهند به سیستم تأسیسات دانشگاه نفوذ کنند! علاوه بر این دانشگاهها ممکن است تحت سیاستهای واحدی عمل کنند و همچنین ملزم به اجرای مقررات دولتی باشند. در محیط دانشگاه حفاظت از داده‌های شخصی بسیار حائز اهمیت است، چراکه فایلهای دانشجویان حاوی اطلاعات مهمی از قبیل شماره‌های شناسایی، سوابق پزشکی و اسناد آموزشی است. مهاجمین بالقوه می‌توانند چنین داده‌هایی را بدزدند، تغییر دهند، یا از بین ببرند؛ و با اینکار به اعتبار دانشگاه آسیب جدی وارد نمایند.

سازمانهای دولتی

پیاده‌سازی و استقرار فناوری اطلاعات در سازمانهای دولتی ممکن است بر اساس کارآیی، سهولت استفاده، و قابلیت برقراری ارتباط با سایر بخشها و سازمانها مورد بررسی قرار گیرد. از آنجا که بطور کلی در بافتهای دولتی مسئله سودآوری مطرح نیست، در اینجا نیز مشابه مؤسسات غیرانتفاعی روی بودجه کنترل وجود دارد و باعث می‌شود توانایی سازمان در تهیهٔ جدیدترین سخت‌افزارها و

---

۴ *تعریف سازمانهای کوچک و متوسط از کشوری به کشور دیگر متفاوت است. در بعضی موارد، یک مالک بتنهایی همهٔ جنبه‌های یک تجارت سنتی مثل مزرعه‌داری یا خواربار فروشی را انجام می‌دهد؛ یعنی مالک تنها کارمند آن تجارت می‌باشد. در تجارتهای پیچیده‌تر ممکن است چند صد نفر تنها به محصولات مصرف‌کننده یا محصولات فنی بپردازند. در دنیای توسعه‌یافته، شرکتهایی که با تکیه به فناوری کار خود را آغاز می‌کنند در گروه سازمانهای کوچک و متوسط قرار می‌گیرند، اما ممکن است توسط گروههای سرمایه‌گذاری روی آنها سرمایه‌گذاری شود، بسرعت بزرگ شوند، و یا توسط شرکتهای بزرگ خریداری شوند. بعضی از سازمانهای کوچک و متوسط بسیار موفق، اوراق سهام منتشر می‌کنند و خودشان به شرکتهای بزرگ و عمومی تبدیل می‌شوند.*

۵ *در حالت کلی جاسوسی سازمانیافته در شرکتهای بزرگ یا شرکتهایی که محصولات مبتنی بر فناوری جدید تولید می‌کنند – جایی که در آن نوآوری ارزش زیادی دارد و ممکن است دزدیده شود – یک نگرانی محسوب می‌شود. برای سازمانهایی که به تجارت مشغولند، استراق‌سمع نگرانی جدی‌تری از جاسوسی است، هرچند آثار هر دو مشابه است. بطور خاص هر شرکت باید سوابق حسابداری، اطلاعات کارکنان، و اطلاعات تراکنشهای کارت اعتباری خود را از دستیابی غیرمجاز محافظت کند.*

نرم‌افزارهای امنیتی محدود شود. همزمان دولتها باید بر حفاظت از داده‌ها نیز تمرکز کنند، چراکه پایگاه داده‌هایشان حاوی اطلاعات حساسی در مورد افراد است؛ اطلاعاتی از قبیل اطلاعات فردی و سوابق پزشکی، جنایی، و مالیاتی.

متأسفانه حتی در سازمانهای دولتی کشورهای صنعتی نیز حفاظت داده‌ها دچار مشکل است و از سیستمهای منسوخ، سرمایه‌گذاریهای نامناسب و کارمندان از کار افتاده‌ای که فاقد شایستگیهای لازم در بعد امنیت فناوری اطلاعات هستند رنج می‌برد. همانند شرکتهای تجاری و مؤسسات غیرانتفاعی، دولت نیز باید به تصویر عمومی ایجادشده از خود پس از خبری و رسانه‌ای شدن هر نفوذ یا رخداد دیگر امنیتی اهمیت دهد.

سازمانهای کوچک و متوسط؛ موتورهای رشد و ترقی

UNDP[۶] در گزارش اخیر خود در مورد وضعیت فناوری اطلاعات در کشورهای درحال توسعه به طرح کلی بعضی چالشهایی که افراد و سازمانها در عصر اطلاعات با آن مواجه هستند پرداخت.[۷] بانک جهانی چند سری گزارش در رابطه با توسعه و استقرار فناوری اطلاعات تهیه کرده است.[۸] اگرچه تجربیات فنی سازمانها در جهان صنعتی از بعضی جهات متفاوت هستند (مقیاس، هزینه‌ها، و پایگاه اطلاعات کارکنان)، اما از نقاط قدرت و ضعف آنها در حوزهٔ امنیت فناوری اطلاعات می‌توان درسهای بسیاری گرفت. تعداد مؤسسات بزرگ کمتر است و هرکدام از قابلیتهای ویژه و منابع مالی وسیعتری برخوردارند. به هرحال هنوز میان مدیران ارشد امنیتی بعنوان مسئولان مراکز مخارج، مدیران ارشد مالی بعنوان کنترل‌کنندگان هزینه، و شاخه‌های دیگر سازمان (مدیران ارشد اطلاعات، فروش و بازاریابی، و محصولات) تنشهایی وجود دارد.[۹]

بدون برنامهٔ کلی برای ایجاد یک محیط امن برای فناوری اطلاعات، هر قسمت ممکن است یک راهکار برای برقراری امنیت توسعه دهد که از مأموریتها، اهداف، و مقاصد عملیاتی همان قسمت ناشی شده و ممکن است به همان اندازه که برای یک قسمت مناسب است برای قسمتهای دیگر چندان به کار نیاید. این راهکارهای مختلف ممکن است باعث شوند امنیت در بعضی حوزه‌ها بیش از حد مورد نیاز یا کمتر از حد مورد نیاز تأمین شده باشد؛ درحالیکه وجود نظارت از طرف مدیریت سطوح بالا تضمین خواهد کرد که تجارب امنیتی بگونه‌ای تنظیم می‌شوند که مجموعهٔ سازمان بتواند عملکرد بهتری داشته باشد. سیاستها و پیاده‌سازیهای فنی که جهت راه‌اندازی یک سیستم امنیتیِ کارآ برای سازمان لازم می‌باشند یک بخش ضروری و اساسی اهداف تجاری را تشکیل می‌دهند که در هر سازمان باید به آن بها داد.

سازمانهای کوچک و متوسط منابع کمتری برای راه‌اندازی، ساختار مسطح‌تری برای مدیریت، و اعتماد بیشتری به پایگاه اطلاعات کارکنان دارند. در این سازمانها ممکن است فرآیندهای تجاری از فرآیندهای سازمانهای بزرگ، شفافتر باشند و لذا در چنین ساختاری که در آن این مقدار از اطلاعات شرکت برای همهٔ کارکنان در دسترس است خطرات امنیتیِ ذاتی وجود خواهد داشت. در سازمانهایی که به فناوری توجه خاص ندارند ممکن است سازمان نسبت به یک کارمند یا مشاور که از نظر فنی قویتر از مدیران شرکت است آسیب‌پذیریهایی داشته باشد. در یک شرکت که در لبهٔ فناوری فعالیت می‌کند این خطر وجود دارد که مالکیت نوآوریها و منابع حیاتی آن به اندازهٔ کافی از سرقت یا تخریب مورد محافظت قرار نداشته باشد.

برای مقابله با این مشکلات، همهٔ سازمانهای کوچک و متوسط باید مروری کامل بر مأموریتها، اهداف، صلاحیتها و

---

6 *United Nations Development Program*

۷ *رجوع کنید به گزارش توسعهٔ انسانی سال ۲۰۰۱:*
"Making New Technologies Work for Human Development" (UNDP: NY, 2001)

۸ *برای مشاهدهٔ منابع می‌توانید به پایگاه بانک جهانی و همچنین پروژه‌های تحقیقاتی و نتایج موجود در مؤسسهٔ راهبری فناوری اطلاعات (ITGI) مراجعه کنید:*
http://www.worldbank.com
http://www.itgi.org

۹ *در شرکتهای فنی بزرگتر یا شرکتهای تازه‌کاری که برنامه‌ریزی کرده‌اند که بسرعت رشد کنند، تیم مدیریت از افرادی تشکیل شده که هر یک در یک حوزهٔ تجاری یا فنی متخصص است. این نقشها عبارتند از موارد زیر (ولی به آنها محدود نمی‌شوند): مدیر ارشد اجرایی (CEO)، مدیر ارشد امور مالی (CFO)، مدیر ارشد فناوری (CTO)، مدیر ارشد اطلاعات (CIO)، و بتازگی مدیر ارشد امنیت (CSO). همچنین در یک سازمان معمولی یک سلسله موقعیتهای قائم‌مقامی وجود دارد از قبیل قائم‌مقام بازاریابی، فروش، و توسعهٔ بازرگانی. از آنجا که استفاده از این ساختار رسمی در سازمانهای کوچکتر ضرورتی ندارد (یا امکان آن میسر نیست)، مشاهدهٔ چگونگی تقسیم مسئولیتها در شرکتهای بزرگ و توجه به افزایش اهمیت CSO می‌تواند بسیار مفید باشد.*

سیستمهای اطلاعاتی خود داشته باشند. اگر در حوزه‌هایی فعالیت می‌کنند که ممکن است برای دیگران مخاطرات امنیتی در بر داشته باشد – مثلاً حوزهٔ فناوریهای درحال توسعه – باید تهدیدهای محتمل علیه امنیت مشتریان خود را پیش‌بینی کنند و طرحهایی برای کاهش تأثیر آنها تدوین نمایند. اگر در حوزه‌هایی کار می‌کنند که به هر نحو به امنیت دولت مربوط می‌شود – مثل ارائه محصولات و خدمات ارتباطات مخابراتی – باید متوجه باشند که در چه زمانی و چگونه مسئولیت قانونی پایبندی به احکام دولتی بر عهدهٔ آنهاست. یک *ارائه‌کنندهٔ سرویس اینترنت* (ISP)[10] نمونه‌ای است از شرکتهایی که با هر دو نوع مخاطره مواجه است. با اتصال مشتری به اینترنت، برای داده‌ها و تجهیزات مشتری مخاطرات امنیتی بوجود می‌آید، و با فراهم کردن محتویات دیجیتالی و ابزار ارتباطی، ISP در معرض احکام و مقررات کشوری قرار می‌گیرد. اگر کسی قابلیت تجارت الکترونیکی را نیز به این خدمات بیافزاید، تهدیدات بالقوه و کسب اطمینان از پایبندی به تعهدات، تبدیل به مشکلاتی بسیار عظیم و اساسی می‌شوند.

خطرهای تهدیدات چندگانه

داده‌های آماریِ چند منبع موثق، یک روند صعودی در استفاده از برنامه‌های آلوده برای دستیابی به اهداف جنایی را نشان می‌دهد. در سال ۲۰۰۲ گزارشات متعددی به چنین موضوعاتی مربوط بود: سرقت هویت با استفاده از برنامهٔ آلوده، تغییر شکل پایگاههای وب با انگیزه‌های سیاسی، *حملات توزیع‌شدهٔ تخریب سرویس* (DDoS)[11] علیه اهداف تعیین‌شدهٔ سازمانی، و موارد مشابه دیگر.

بعلاوه، گستردگی *تهدیدات چندوجهی*[12] در اینترنت برای همه مخاطرات جدی بوجود می‌آورد. این مخاطرات به حوزهٔ خاصی تعلق ندارند ولی تمام شبکهٔ جهانی را تهدید می‌کنند. برای مثال کرم Klez با خصوصیاتی به نگارش درآمده که بر اساس آن صاحبنظران معتقدند یا در چین و یا در هنگ‌کنگ نوشته شده است. درحال حاضر کشورهای آسیایی بطور فزاینده‌ای از رایانه‌های متصل به اینترنت بهره‌برداری می‌کنند. متأسفانه بسیاری از این رایانه‌ها بی‌حفاظ هستند و کاربران آنها نیز از اصول اولیهٔ استفادهٔ ایمن از رایانه‌ها ناآگاهند. درنتیجه احتمال می‌رود مناطقی که از رشد فنی بالایی برخوردارند – مثل چین – با پراکنده‌شدن ویروسها، کرمها، تراواها، و تهدیدهای چندوجهی که آمیخته‌ای از همهٔ این عوامل هستند مورد حملهٔ مهاجمین سراسر جهان قرار بگیرند.

ابزارهای نرم‌افزاری حال حاضر یک طیف از حفاظتها را در مقابل برنامهٔ آلوده ایجاد می‌کنند، اما از دفاع کامل در مقابل همهٔ اَشکال حملات، ناتوان هستند. استفاده از یک طرح دفاعی چندلایه، هم از لحاظ فنی و هم از لحاظ انسانی مخاطرهٔ بروز رخدادهای امنیتی بوسیلهٔ برنامهٔ آلوده را به شدت کاهش می‌دهد – هرچند باز هم آنرا از بین نمی‌برد. تهدیدات چندوجهی مثل Code Red، Slammer، Klez، و Bugbear می‌توانند شبکه‌های رایانه‌ای را مورد آزار دائمی قرار دهند. بسیاری از کرمها به خودیِ خود آثار مخرب ندارند اما در سیستم دامهایی نصب می‌کنند که باعث می‌شود دسترسی افرادی که با آن دامها آشنا هستند به شبکه سریع و آسان گردد.

جدای از این مطلب، کرمها از بعضی جهات در ناتوان کردن سیستمها مؤثرتر هستند؛ چراکه قادرند آسیب‌پذیریهای موجود در نرم‌افزارهای رایج – مثل مرورگرهای وب – را مورد بهره‌برداری قرار دهند.

در محیطهای رایانه‌ای که چنین خصوصیاتی در آنها وجود دارد، کاربران باید در مورد مخاطرات موجود و نحوهٔ بروز واکنش مناسب در موقعیتهای انفرادی، اطلاعات خود را افزایش دهند. هنگامیکه استفادهٔ ایمن از رایانه تمرین شود، مخاطرهٔ یک حمله می‌تواند به میزان قابل توجهی کاهش یابد، اما مجدداً تأکید می‌شود که هرگز نمی‌توان آنرا به صفر رساند. از آنجا که تهدید خرابکاری عمدی در سیستمهای رایانه‌ای برای سازمانها بسیار زیاد است، بررسی مخاطرات امنیت انفرادی و تراکنشهای مالی و چالشهای جدید بوجودآمده در بسترهای رایانه‌ایِ بی‌سیم بسیار حائز اهمیت است.

10 *Internet Service Provider*
11 *Distributed Denial of Service Attack*
12 *Blended Threats*

مزایای فناوری اطلاعات و مدیریت آن

علیرغم چالشهای موجود، مدیران و کارآفرینان بخشهای دولتی و خصوصی در کشورهای درحال توسعه به سرمایه‌گذاری روی فناوری نوین اطلاعات و ارتباطات شامل پست الکترونیکی، اینترنت، ارتباطات بی‌سیم، و نرم‌افزارهای تجاری مشغولند تا به انجام کارهای روزمرهٔ خود کمک کرده باشند. مزایای مختلف استفاده از این محصولات و خدمات جدید – مثل کارآیی و صرفه‌جویی در هزینه‌ها – واضح هستند:

۱. ارتباطات تجاری با مشتریان، فروشنده‌ها و شرکتهای همکار بهبود پیدا می‌کند؛

۲. توانایی دسترسی به حجم زیاد اطلاعات با سرعت زیاد و بصورت ارزانقیمت تقویت می‌شود؛

۳. وسیله‌ای برای توسعهٔ قابلیتهای حفاظت از داده‌ها و مدیریتی فراهم می‌گردد که منجر به نگهداری بهتر از اقلام داده برای مدیران مالی، تحلیل بهتر رفتار مشتری برای مدیران بازاریابی و فروش، و ارائه آمار دقیقتر برای مدیران خط تولید می‌شود.

به هرحال همانطور که مشاهده کردیم این اصلاحات بدون مخاطره نیستند و این مسئله چه در مورد سرمایه‌های فیزیکی و چه در مورد سرمایه‌هایی که کمتر به چشم می‌آیند صدق می‌کند. در این بخش، نگرانیهای حوزهٔ امنیت فناوری اطلاعات که شرکتهای بزرگ و کوچک و در کشورهای توسعه‌یافته و درحال توسعه با آن مواجه می‌شوند مورد بررسی قرار می‌گیرد. قسمتهای مختلف این بخش با توجه خاص به کارهایی که باید بوسیلهٔ دوایر اجرایی، مدیران، و کارکنان برای حفاظت از سیستمها، مشتریان، فروشندگان و دیگر افراد ذینفع در شرکت انجام شوند طراحی شده است. *فهرستهای کنترل*[13] و *یادداشتهای روال‌منده*[14] براحتی می‌توانند توسط یک سازمان دولتی یا غیرانتفاعی مورد استفاده قرار بگیرند.

علاوه بر روالها و سیاستهای داخلی، بعضی از سازمانهای کوچک و متوسط ممکن است تصمیم بگیرند تأمین نیازهای امنیتی خود را به منابع خارج از سازمان واگذار کنند. در جهان صنعتی بعضی کارشناسان اظهار می‌کنند که سپردن خدمات غیر کلیدی مثل تأمین امنیت فناوری اطلاعات به منابع خارج از سازمان حداقل تا ده سال آینده برای شرکتها همچنان یک استراتژی خواهد بود. علاوه بر این بعضی سازمانها علاقهٔ خاصی به تأمین نیازهای امنیتی جهانی بویژه نیازهای امنیتی کشورهای درحال توسعه دارند. بعنوان مثال انجمن *کنترل و ممیزی سیستمهای اطلاعات* (ISACA)[15] در ۶۰ کشور همکار تجاری دارد و متن برنامه‌های مختلفی از کشورهای متفاوت را بصورت آزاد ارائه می‌کند.[16] ISACA همچنین یک چارچوب کنترل و رسیدگی برای سازمانها پیشنهاد می‌کند و برای استفاده از منابع خارجی فهرستهای کنترل ارائه می‌نماید.

این سیستمها چه در داخل سازمان تهیه شوند و چه خارج از آن، باز هم توسعه و پشتیبانی از زیرساختها، سیاستها، و روالهای امنیتی برای غالب شرکتها چیزی جز برقراری توازن میان ضابطه‌ها نخواهد بود. مقامات اجرایی، مدیران، و سیاستگذاران باید به مخاطرات اهمیت دهند و با تعریف اهداف رسمی و رشد حداقل سازمان، برای ایجاد توازن میان سرمایه‌گذاری روی امنیت، یک معیار و استاندارد تعیین کنند. وقتی سازمان به سطح مطلوبی از امنیت رسید، مدیریت نباید اهمیت به روز نگهداشتن سیستمها و ممیزیهای منظم طرح امنیتی را فراموش کند. تغییرات رایانه و تجهیزات شبکه، مثلاً از نوعی که به *بسته‌های نرم‌افزاری متن‌باز*[17] منحصر است، به بررسی کامل طرح تفصیلی امنیت نیاز دارد. بطور خلاصه می‌توان گفت که امنیت بیش از آنکه یک علم باشد یک هنر است و برای تضمین تأثیرگذاری موفق آن در سازمانها به

13 *Checklist*
14 *Procedural Notes*

15 *Information System Audit and Control Association (ISACA)*

۱۶ *برای آگاهی از برنامه‌های آیندهٔ این انجمن به پایگاه آن در آدرس زیر مراجعه کنید:*
http://www.isaca.org
این مطالعه باعث شد کشور اروگوئه یک کشور مورد علاقه برای مطالعهٔ خوانندگان این کتاب شود (!):
http://www.isaca.org/ct_case.htm
COBIT (http://www.isaca.org/cobit.htm) یک بستر برای منابع مناسب امنیت الکترونیک جهت استفاده برای مدیران، کاربران، ممیزی امنیت اطلاعات، کنترل، و متخصصین امنیت ارائه کرده است. برقراری تماس با ISACA به شما دید خوبی از فعالیتهای فعلی و آتی انجمن می‌دهد.

17 *Open Source Software Packages*

همفکری و هماهنگی تعداد زیادی از متفکران خـلاق جامعـه نیاز می‌باشد.[۱۸]

۱۸ *بـدلیل افـزایش رخـدادهای امنیتـی در سراسـر جهـان، تعـدادی از شرکتهای مشاوره گزارشاتی در مورد فنـاوری اطلاعـات و تـأثیرات جهانی آن تهیه کرده‌اند. برای مثال می‌توانید به منبـع زیـر مراجعـه کنید:*

Ernst & Young's 2003 Global Information Security Survey: http://www.ey.com/global/download.nsf/US/TSRSGlobal_Information_Security_Survey_2003/$file/TSRS_-_Global_Information_Security_Survey_2003.pdf

فصل دوم
مروری بر روشهای کاهش آثار مخاطرات امنیت الکترونیکی[۱۹]

کلیات

این فصل از کتاب به شناسایی، تعریف، و بحث در مورد یک مجموعه سیاستها و روالهای هشت رکنی و نیز یک زیرساخت کلی جهت تقویت محیط امن الکترونیکی برای بخش خدمات مالی می‌پردازد. این بخش برای سیاستگذارانی که با ارائه‌دهندگان خدمات مالی – بویژه دوایر اجرایی، مدیران ارشد اطلاعات، و مدیران ارشد امنیت – کار می‌کنند تهیه شده است. نکات فنی این بخش برای کسانیکه سیستمهای امنیت الکترونیکی را راهبری می‌کنند، بازرسین بانکها که کارآیی امنیت الکترونیکی را ارزیابی می‌کنند، و کسانیکه با مخاطرات ذاتی و روزمرهٔ تراکنشهای الکترونیکی سر و کار دارند بسیار بکار می‌آید.

امنیت در خدمات مالی الکترونیکی

در چند مقالهٔ جدید، امنیت الکترونیکی بعنوان مسئله‌ای حیاتی در توانمند ساختن *خدمات مالی الکترونیکی*[۲۰] برای پاسخگویی به انتظارات سازمان و مشتریان و ارائه منافع فناوری معرفی شده بود.[۲۱] امنیت الکترونیکی با قلب اقتصاد جدید در تماس است؛ چراکه منافع بالقوهٔ بازارهای جهانیِ جوامع بین‌المللی بسیار حائز اهمیت هستند و استفادهٔ بهینه از این بازارها میسر نمی‌شود مگر با تأمین امنیت در محیط الکترونیکی. به هر ترتیب، روند حرکت اقتصاد جهانی بحث عمیقی دربارهٔ تجارت و سیاستگذاری نوین را می‌طلبد: چگونه باید *حریم خصوصی*[۲۲] را تعریف و از آن محافظت کرد؟، اطمینان و اعتماد در یک محیط دیجیتال چه معنا و مفهومی دارند؟، چگونه می‌توان سطح مناسبی از امنیت را مشخص کرد؟، و نهایتاً اینکه برای سرمایه‌گذاریهای امنیتی، چگونه باید شاخصِ *بازگشت سرمایه* (ROI)[۲۳] را اندازه‌گیری نمود؟

به علت ماهیت همواره متغیرِ فناوری، این کتاب نه‌تنها به جزئیات تمام این موضوعات نمی‌پردازد، بلکه برای بعضی از آنها پاسخهای کلی هم ارائه نمی‌کند. در عوض به مروری سریع بر آنچه تا امروز در دنیای امنیت اتفاق افتاده، شکافهایی که در حوزهٔ امنیت الکترونیکی درحال بوجود آمدن هستند، و ارائه بعضی راهکارهای ممکن برای کم کردن این شکافها می‌پردازد، و همچنین به بعضی فعالیتها که در سراسر جهان برای رفع این نگرانیها انجام می‌شوند اشاره می‌کند.

امنیت الکترونیکی چیست؟

بطور کلی امنیت الکترونیکی عبارت است از هر ابزار، فن، یا فرآیندی که برای حفاظت از سرمایه‌های اطلاعاتی یک سیستم مورد استفاده قرار می‌گیرد. امنیت الکترونیکی ارزش یک شبکه را زیاد می‌کند و از زیرساختهای نرم و سخت تشکیل شده است. زیرساختهای نرم عبارتند از سیاستها، فرآیندها، پروتکلها و راهبردهایی که از مورد سوء استفاده قرار گرفتن سیستم و داده‌ها جلوگیری می‌کنند. زیرساختهای سخت نیز متشکل از نرم‌افزار و سخت‌افزار مورد نیاز برای

---

۱۹ *این فصل با کمک یک گزارش که بوسیلهٔ Thomas Glaessner، Tom Kellerman، و Valerie McNevin در سال ۲۰۰۲ برای بانک جهانی تهیه شد به نگارش در آمده است:*
"Electronic Security: Risk Mitigation in Financial Transactions.": http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/SearchGeneral?openform&E-Security/E-Finance&Publications

20 *E-Finance*

۲۱ *برای اطلاعات بیشتر، فعالیتهای Glaessner، Kellerman و McNevin از جمله کتاب زیر را ببینید:*
"Electronic Safety and Soundness: Securing Finance in a Digital Age, Public Policy Issues" (October 2003)

این رساله اوج تلاشهایی است که در سه سال اخیر انجام شده و به ارائه چند مقاله منجر شده است. چند مقالهٔ دیگر از این دسته مقالات عبارتند از:
"Electronic Security: Risk Mitigation in Financial Transactions" (May 2002, June 2002, July 2002),
"Electronic Finance: A New Approach to Financial Sector Development?" (2002),
"Mobile Risk Management: E-Finance in the Wireless Environment" (May 2002)
که همگی در آدرس زیر قابل دسترسی هستند:
http://www.worldbank1.org/finance

22 *Privacy*

23 *Return on Investment*

حفاظت از سیستم و داده‌ها در مقابل تهدیدات امنیتی داخلی و خارجی سازمان می‌باشد. باید توجه داشت که سطح امنیت الکترونیکی هر فعالیت باید متناسب با ارزش آن فعالیت باشد؛ بنابراین امنیت برای تراکنشها و معاملات مهم باید در سطحی بالاتر از تراکنشها و معاملات عادی تأمین شود.

از آنجا که یک فناوری جدید مخاطرات جدیدی نیز بوجود می‌آورد و فناوریها هر روز گسترده‌تر می‌شوند، لذا امنیت الکترونیکی شایستهٔ توجه بیشتری است.

خدمات مالی الکترونیکی عبارت است از بکار بردن وسایل الکترونیکی برای تبادل اطلاعات، انتقال علائم و اسناد اعتباری، و انجام داد و ستد در یک محیط تجاری. خدمات مالی الکترونیکی از چهار جزء پایه‌ای تشکیل می‌شود:

- *انتقال دهنده‌های سرمایه‌های الکترونیکی* (EFTs)[۲۴]؛
- *تبادل داده‌های الکترونیکی* (EDI)[۲۵]؛
- *انتقال منافع الکترونیکی* (EBTs)[۲۶]؛ و
- *تصدیق تجارت الکترونیکی* (ETCs)[۲۷].

اگرچه خدمات مالی الکترونیکی یک فرصت بزرگ جهت گسترش تجارت برای بازارهای درحال توسعه بوجود می‌آورد، اما چند مخاطرهٔ جدی نیز بدنبال دارد. تمام چهار جزء خدمات مالی الکترونیکی مستعد کلاهبرداری، سرقت، اختلاس، و دستکاری هستند. بیشتر جرائم تجاری که در اینترنت رخ می‌دهند تازگی چندانی ندارند – کلاهبرداری، سرقت، جعل هویت، و اخاذی سالهاست که صنایع خدمات مالی را به ستوه آورده‌اند – اما با اینهمه، پیشرفت فناوری همواره باعث بوجود آمدن ابعاد جدیدی می‌گردد و این مسئله می‌تواند عمق و دامنهٔ جرائم را گسترده‌تر کند. فناوری باعث می‌شود جنایتهای بسیار گسترده و پیچیده بتوانند بسرعت و بصورت گمنام انجام شوند. در گذشته سرقت ۵۰،۰۰۰ کارت اعتباری برای جنایتکاران بسیار سازمانیافته ماهها یا حتی سالها زمان می‌برد؛ اما امروز یک مجرم با استفاده از ابزارهای رایگان در پایگاههای وب می‌تواند با نفوذ به پایگاه داده‌های هویت، همان تعداد کارت اعتباری را در تنها چند ثانیه به سرقت ببرد.

بر اساس بررسیهای اخیر تخمین زده می‌شود که ۵۷٪ از حملات نفوذ ایالات متحده در سال گذشته از بخشهای مالی شروع شده بودند. بسیاری از تخلفات نظیر یک مورد جدی که در وزارت خزانه‌داری آمریکا رخ داد ناشی از اشتباه در پیاده‌سازی روندهای ارزیابی مخاطره و بکارگیری نرم‌افزارهای تجاری آماده بدون استفاده از رویکردهای چندلایهٔ امنیتی – مواردی چون سیاستهای کارکنان، راهبردهای ارتباطات، و به‌روزرسانی منظم ابزار فنی مورد استفاده مانند *ویروس‌یابها*[۲۸] و *دیواره‌های آتش*[۲۹] – بودند. نتایج این نفوذهای امنیتی که اخبار آن به رسانه‌ها نیز راه پیدا کرد طیفی شد که یکسوی آن از دست دادن شهرت و اعتبار مالی و سوی دیگر آن تغییر رفتار نهان مشتریان در مقابله با داد و ستد الکترونیکی بود؛ و این همه دلیلی نداشت جز عدم اعتماد مشتریان به واسطه‌های تجارت و خدمات مالی الکترونیکی.

اقتصاد شبکه‌ای، برای ایجاد ثروت و همچنین انجام سرقت و تخریب، فرصتهای متفاوتی ایجاد می‌کند. در بررسی مزایا و معایب این فرآیند، سیاستگذاران و تصمیمگیران باید آگاهی خود را در مورد نقشی که امنیت الکترونیکی در تضمین داد و ستدهای قابل اطمینان تجاری بازی می‌کند افزایش دهند.

صنعت امنیت الکترونیکی درحال رشد و جهانی‌شدن است؛ لذا چالشهای سیاست عمومی را در حوزه‌های سیاست رقابتی، تعارضهای بالقوهٔ منافع و همچنین اعطای گواهی نشان می‌دهد.

در گذشتهٔ نزدیک شرکتهای ارائه‌دهندهٔ خدمات امنیت الکترونیکی عموماً در سه حوزه فعالیت می‌کردند: دسترسی، استفاده، و ارزیابی. علاوه بر اینها، صنعت امروزی شامل شرکتهایی است که خدماتی دیگر نیز در این زمینه ارائه می‌کنند؛ خدماتی از قبیل نظارت و غربال کردن داده، مهاجم‌یابی، دیواره‌های آتش، آزمونهای نفوذپذیری برای بررسی میزان آسیب‌پذیری نرم‌افزارها و سخت‌افزارها،

24 *Electronic Funds Transfers*
25 *Electronic Data Interchange*
26 *Electronic Benefits Transfers*
27 *Electronic Trade Confirmations*

28 *Virus Scanners*
29 *Firewalls*

نرم‌افزارهای رمزگذاری، خدمات تصدیق هویت بوسیلهٔ رمزهای عبور، نشانها، کلیدها و یا معیارهای زیستی؛ که همگی هویت گروهها یا یکپارچگی داده‌ها را تصدیق می‌کنند.

بسیاری از فروشندگان علاوه بر امنیت الکترونیکی حجم قابل توجهی از ارتباطات فی‌مابین عرضه‌کنندگان خدمات مالی الکترونیکی در کشورهای مختلف را نیز برقرار می‌کنند. این شرکتها شامل *شرکتهای میزبان*[۳۰]، ISPها و ارائه‌دهندگان خدمات مالی هستند. شرکتهای مخابرات در بازارهای جدید معمولاً بعنوان ارائه‌کنندگان کلیدی خدمات کوتاه‌موج، ماهواره و تلفن همراه فعالیت دارند. این شرکتها ممکن است خدمات میزبانی، خدمات انتقال پول و در بعضی موارد خدمات زیربنایی امنیت الکترونیکی را نیز فراهم کنند.

مالکیت صنایع امنیت الکترونیکی و امور مالی الکترونیکی باعث طرح سؤالات پیچیده‌ای دربارهٔ سیاست رقابتی و کشمکشهای بالقوه برای کسب منافع می‌شوند. در مورد سیاست رقابتی می‌توان پرسید: آیا نقشهای چندگانهٔ شرکتهای مخابراتی می‌تواند به جلوگیری از رقابت بویژه در بازارهای درحال رشد – که معمولاً برای ارائه این خدمات، متخصصین فنی در اختیار خود دارند – منجر شود؟ و یا اینکه یکپارچگی خدمات ارائه‌شده و سیاستهای شرکت دربارهٔ گزارش دقیق و فوری نفوذهای امنیتی چگونه تضمین می‌شود؟ علاوه بر این، روند واگذاری امور به یک شرکت ثالث، اهمیت اصلاح حوزهٔ مسئولیتها از رأس هرم مسئولیت در صنعتی با چنین مجموعهٔ پیچیده‌ای از فروشندگان را روشن می‌کند. معمولاً در قراردادهای میان مؤسسات مالی و ارائه‌دهندگان خدمات به آنها از قسمتی از هزینهٔ قرارداد خدمات بعنوان ضمانت کارآیی استفاده می‌شود، ولی حتی با این وجود هم از دیدگاه امنیتی به مسئله کارآییِ فعالیت انجام‌شده به اندازهٔ کافی پرداخته نشده است.

در مقررات امنیت الکترونیکیِ صنعت خدمات مالی، منافع عمومی باید مورد توجه قرار گرفته باشد. در امنیت الکترونیکی باید میان حریم خصوصی و مسائلی نظیر هزینه، کیفیت خدمات، و نوآوری به یک توازن معقول رسید و در تدوین ضوابط و سیاستها نیز باید توجه خاصی به این توازن داشت.

صنعت مخابرات بطور سنتی لازمهٔ رفاه، آسایش و سلامت عمومی به حساب می‌آمد و از اینرو یک جزء اصلی ضوابط آن، توسعهٔ خدمات به منظور دسترسی عموم بود. اما درحال حاضر در بسیاری از کشورها دسترسی به خدمات اولیهٔ الکترونیکی نیز یک ضرورت برای زندگی به حساب می‌آید.

از لحاظ تاریخی، صنعت خدمات مالی بر اساس این منطق ضابطه‌مند شده که در نقل و انتقالات منظم کالا و پول، اعتماد و اطمینان از بالاترین میزان اهمیت برخوردار است؛ و با توجه به اینکه مؤسسات مالی نیازمند اعتماد مردم هستند، باید فعالیت خود را سالم، منطقی، و محتاطانه پیش ببرند. با نزدیک‌شدن صنعت مخابرات و بخش خدمات مالی به یکدیگر از طریق اینترنت، اهمیت و ضرورت ایجاد سیاست عمومی و مقررات آگاهانه روز به روز بیشتر می‌شود تا تضمین کند که دولت، شرکتهای تجاری و مردم می‌توانند استفادهٔ خود از خدمات ایمن مالی را ادامه دهند.

در تهیهٔ سیاستهای عمومی به منظور ایجاد یا اصلاح معیارهای امنیت الکترونیکی باید به هشت رکن مهم توجه داشت:

- یک چارچوب قانونی و اجرایی مناسب؛
- تمهیدات فنی و مدیریتی برای تضمین امنیت الکترونیکی سیستمهای پرداخت؛
- نظارت قوی و پیشگیری؛ برای ایجاد انگیزه‌های بهتر در پیاده‌سازی سیستمهای مناسب و لایه‌بندی‌شدهٔ مدیریت خطر؛ از جمله امنیت الکترونیکی برای ارائه‌دهندگان خدمات مالی؛
- چارچوبی که در آن شرکتهای خصوصیِ بیمه بتوانند خود را در مقابل مخاطرات الکترونیکی بیمه کنند و در کنار آن استانداردهای این حوزه را با ایجاد تعهدات مالی بازپرداختها ارتقا دهند؛
- امضاهای دیجیتالی؛
- به‌اشتراک‌گذاری اطلاعات؛
- آموزش شهروندان، کارکنان، و مدیریت دربارهٔ مسائل امنیتی؛ و
- یک ساختار امنیتی لایه‌بندی شده.

30 Hosting Companies

رکن اول:
چارچوب قانونی و اجرایی

کشورهایی که در آنها بانکداری الکترونیکی یا سایر خدمات مالی الکترونیکی (مثل توزیع و داد و ستد اوراق بهادار) انجام می‌شود همزمان با توسعهٔ قوانین، سیاستها و روشها، باید مسائل امنیت الکترونیکی خود را نیز مورد توجه قرار دهند. آنها باید امنیت را برای حفاظت از عملیات الکترونیکی تأمین کنند و قوانین جنایی را برای در بر گرفتن این نوع جرائم اصلاح نمایند.

در فرآیند تدوین سیاست و چارچوب قانونی برای خدمات مالی الکترونیکی باید به موضوعات زیر توجه داشت:

- معاملات الکترونیکی و تجارت الکترونیکی؛
- امنیت سیستمهای پرداخت؛
- حریم خصوصی؛
- جرائم سایبر؛
- مقابله با شستشوی پول؛ و
- زیرساخت اجرایی.

این شش حوزهٔ سیاست، قانون و اجرا در کنار هم باید روابط ابتدایی میان تمامی ذینفعان و سپس تراکنشهایی که در سیستمهای پرداخت جریان می‌یابد را مد نظر قرار دهند. یکی از مهمترین اجزای یک چارچوب قانونی مناسب برای خدمات مالی الکترونیکی شناسایی اعتبار قانونی امضاهای الکترونیکی، تراکنشها، و همچنین سوابق مشتریان می‌باشد. چارچوب قانونی باید راه‌حلهای فنی را ترجیح دهد، برای مشتریان در انجام معاملات الکترونیکی حفاظت بوجود آورد، و قابلیت فعالیت داخلی را ارتقا بخشد.

معاملات الکترونیکی

قانون معاملات الکترونیکی باید عنوان کند که منظور از یک امضا، سابقه یا تراکنش الکترونیکی چیست و با اینکار اعتبار قانونی هر عنصر را مشخص نماید. این سیاستها خصوصاً در تعریف امضای الکترونیکی باید بسیار دقیق باشند. تعاریف تا حد امکان باید خصوصیات فنی داشته باشند تا راه‌حلهای مختلف بتوانند وارد بازار شوند.

امنیت سیستمهای پرداخت

در تهیهٔ سیاست برای امنیت سیستمهای پرداخت باید تمام اجزایی که مستقیماً روی سیستم تأثیرگذار هستند را مد نظر قرار داد. همهٔ این اجزا باید بصورت امن کار کنند تا بتوانند از یکپارچگی و قابلیت اطمینان سیستمها حفاظت نمایند. بعلاوه وجود سیاست در این زمینه باعث می‌شود در تمامی خسارات مالی الکترونیکی و حملات و ضایعات بتوان گزارشات دقیق و ارزشمندی تهیه کرد. صرف وجود سیاست امنیتی به این معنی است که احتمالاً مؤسسهٔ مالی و اداره‌کنندگان آن در مقابل مخاطرات، تدابیر لازم را اندیشیده‌اند.

حریم خصوصی

قانون حریم خصوصی باید حفاظت و کاربرد داده‌ها، حفاظت از مصرف‌کننده و سایر نیازهای مرتبط تجاری را در بر بگیرد و سیاستهای سازمان در مورد بکارگیری اطلاعات را اعلام کند. اتحادیهٔ اروپایی همچنان در حفاظت از حریم خصوصی شهروندانش طبق دستورالعمل حفاظت از داده‌ها (مصوب سال ۱۹۹۵) پیشتاز است. در حالت حداقلی، قانون حریم خصوصی باید اصول استفادهٔ عادلانه از اطلاعات (شامل توجه، انتخاب، دسترسی و حداقل اطلاعات لازم برای تکمیل معامله) را شامل شود.

جرائم سایبر[۳۱]

هر کشور باید در مورد سوء استفاده از شبکه و رایانه که منجر به وارد آمدن خسارتهای جدی به خود شبکه و رایانه و بسیاری آسیبهای دیگر می‌شود قوانینی داشته باشد. قانون همچنین باید ابزار و منابع لازم برای تحقیق و پیگرد و نیز مجازات مرتکبین جرائم سایبر را تعیین کرده باشد. نمونه‌ای از چنین قوانین و دستورالعملهایی را می‌توان در *معاهدهٔ جرائم اینترنتی اروپا*[۳۲] پیدا کرد که در فصل چهارم به تفصیل در مورد آن بحث شده است.[۳۳]

مقابله با شستشوی پول

سیاستها باید روشهای مقابله با شستشوی پول را تعریف کنند و جوامع بین‌المللی را به همکاری در بازرسی، پیگرد و

---

31 *Cyber Crime*

32 *Europe's Convention on Cyber Crime*

۳۳ *انجمن جرائم سایبر شورای اروپا:*
http://conventions.coe.int

مجازات چنین جرائمی تشویق نمایند تا خطر تهدیدات موجود از جانب شستشوی پول که به فناوریهای جدید نیز سرایت کرده را کاهش دهند.

اجرای قانون

شاید بتوان گفت که نیاز به اجرای قوانین امنیت الکترونیکی در مرزهای یک کشور به اندازهٔ وجود چارچوب قانونی آن از اهمیت برخوردار است. مبدأ بسیاری از انواع حملات رایانه‌ای، کشورهایی بوده‌اند که نظام قانونی و اجرایی ضعیفی برای امنیت الکترونیکی داشته‌اند و همین امر ضرورت وجود راهکارهایی برای همکاریهای بین‌المللی را بیش از پیش نمایان می‌کند.

رکن دوم:
امنیت الکترونیکی در سیستمهای پرداخت

سیستمهای پرداخت جزء مهمی از هر سیستم مالی محسوب می‌شوند. سیاستهایی که برای کاهش مخاطرات سیستمهای پرداخت تدوین می‌شوند باید بگونه‌ای برای پنج مورد زیر راه‌حلی ارائه دهند:

۱. تعریف انتقال‌دهندگان پول؛
۲. الزامات گزارش‌دهی؛
۳. ضوابط؛
۴. ضمانتنامه‌ها، جبران خسارات، و مسئولیتها؛ و
۵. نیازهای امنیتی ارائه‌دهندگان خدمات.

تعریف انتقال‌دهندهٔ پول

انتقال‌دهندهٔ پول عبارت است از هر سازمان تجاری که در زمینهٔ انتقال و تبادل ارز و لوازم پولی مشغول فعالیت می‌باشد. معمولاً این سازمانها به "تجارت خدمات پولی" مشغول هستند و بعنوان *دفاتر تسویه خودکار شخص ثالث*[۳۴] فعالیت می‌کنند.[۳۵] در بررسی امنیت سیستم پرداخت الکترونیکی، قانونگذاران باید بدانند که الگویی جدید برای جنبش پولی در محیطهای پیچیدهٔ فناوری اطلاعات بوجود آمده است. حجم قابل توجه پولی که بجای داخل بانکها در اطراف بانکها جریان دارد تأثیر بسزایی بر سیستم پرداخت جهانی، سیاستهای پولی، و پیش‌بینیهای اقتصادی دارد.

الزامات گزارش‌دهی

ناتوانی در تهیهٔ گزارش از وقایع امنیتی بویژه در حوزهٔ خدمات مالی برای کسانیکه بدون انجام بررسی و پیشگیریهای لازم از سیستمهای پرداخت استفاده می‌کنند، احتمال تداوم بیشتر فعالیتهای نامطمئن و نادرست و درنتیجه وارد آمدن خسارات بیشتر را افزایش می‌دهد. یک راهکار می‌تواند این باشد که وظیفهٔ تهیهٔ گزارش از وقایع بر عهدهٔ مأموران اجرایی گذارده شود.[۳۶]

پیشگامان قانونگذاری

قانونگذاران باید به چگونگیِ گسترشِ نظارت و اجرای قانون برای وسایلِ انتقالِ الکترونیکی توجه کنند. اولین دلیلی که بیشترِ مردم برای عدم استفاده از وسایل انتقال الکترونیکی از آن نام می‌برند هراس از تأمین‌نبودن حفاظت کافی برای اطلاعات است. حفاظت صحیح می‌تواند باعث افزایش اطمینان مصرف‌کننده و تقویت نظم بازار شود و درنتیجه زمینه را برای استفادهٔ بیشتر از سیستمهای مالی الکترونیکی فراهم سازد.

ضمانتنامه‌های جبران خسارات

مؤسسات مالی می‌توانند خدمات بعد از فروش و جبران خسارت را برای شرکتهای تجاری که نرم‌افزار و سخت‌افزار تولید می‌کنند الزامی نمایند. همچنین می‌توانند شرکتها را به عرضهٔ محصولاتی ملزم کنند که در مقابل آسیبهای احتمالی ناشی از رخنه‌های امنیتی سخت‌افزاری و نرم‌افزاری مقاوم باشند. سازمانهایی که چنین خدمات یا محصولاتی را برای صنعت خدمات مالی فراهم می‌کنند، استانداردهای حفاظتی مستحکم‌تری را مورد استفاده قرار می‌دهند و خود را ملزم می‌دانند ذکر نمایند که محصولشان برای استفاده در یک بخش خاص پیکربندی نشده و یا مناسب نیست. یکی از راه‌حلها برای این همهٔ این موارد قراردادن یک *یادداشت سلب مسؤلیت*[۳۷] بر نرم‌افزار یا سخت‌افزار است که اظهار

34 Third-Party Automated Clearinghouse

۳۵ *این خدمات ممکن است درخواستهای دریافت و انتقال پول، تبدیل سرمایه، و سایر موارد مشابه را نیز در بر بگیرد.*

۳۶ *خصوصاً مدیران ارشد اطلاعات و مدیران امنیت اطلاعات*

37 Disclaimer Note

می‌دارد این محصول برای ایجاد، انتقال یا ذخیرهٔ اطلاعات غیرمجاز، حساس یا محرمانه نباید بکار رود و در غیراینصورت هیچ مسئولیتی متوجه پدیدآورندهٔ آن نخواهد بود.

استانداردهایی برای ارائه‌دهندگان خدمات

ارائه‌دهندگان خدمات به صنعت خدمات مالی می‌توانند نسبت به تأمین‌کنندگان خدماتی که مستقیماً با این صنعت در ارتباط نیستند، از استاندارد مستحکم‌تری استفاده کنند. بار دیگر تأکید می‌شود که با انجام اینکار هم هنوز راه زیادی تا ایجاد اطمینان و اعتماد وجود دارد.

رکن سوم:
چالشهای نظارت و پیشگیری

علاوه بر کنترل سیستمهای پرداخت و نظارت بر انتقال‌دهندگان پول، ممکن است اصلاح راهبردهای قانونی، نظارت، و پیشگیری، برای تضمین امنیت ارائه‌دهندگان خدمات مالی مفید باشد. این موضوع بویژه برای شرکتهای تجاری که در بانکداری الکترونیکی یا ارائه سایر خدمات مالی اینترنتی فعال هستند مطرح می‌باشد.

نیازهای سرمایه‌ای

راهبردهای جدید *باسل*[۳۸] برای سرمایه – بویژه آنهایی که به تهدیدهای عملیاتی مربوط می‌شوند – به مخاطرهٔ از دست دادن شهرت یا مخاطرات استراتژیک آسیب‌پذیریهای امنیت الکترونیکی نپرداخته‌اند. از اینرو این سؤال مطرح می‌شود که وقتی اطلاعات در مورد رخدادهای امنیتی دقیق نیست و ارزیابی خساراتی که به شهرت وارد می‌شود سخت است، بهترین راه اندازه‌گیری مخاطرات عملیاتی بانکی چیست؟ با توجه به مسئله تعیین سرمایهٔ لازم برای مخاطرات امنیت الکترونیکی، یک روش مؤثر می‌تواند استفاده از یک روند ارزیابی برای شناسایی و ترمیم نفوذهای امنیتیِ الکترونیکی در کنار ایجاد انگیزه‌های بیشتر برای ثبت گزارشات چنین وقایعی باشد.[۳۹] علاوه بر این مقامات می‌توانند ارائه‌دهندگان خدمات مالی را به بیمه کردن خود در بعضی از جوانب مخاطرات الکترونیکی که در چارچوب سیاستگذاریهای موجود درنظر گرفته نشده‌اند (مثل تخریب سرویس یا سرقت هویت) ترغیب یا ملزم نمایند. از آنجا که صنعت بیمهٔ بخش خصوصی در این حوزه فعالتر شده، این روش بیش از پیش عملی بنظر می‌رسد و می‌تواند به سلامت عمومی صنعت بیمه و ساختار آن در بازارهای درحال رشد منجر شود.[۴۰]

مسئولیت

چارچوب حقوقی و قانونی می‌تواند انگیزه‌هایی را برای شرکتهای میزبان، ارائه‌دهندگان خدمات برنامه‌ها، نرم‌افزار، سخت‌افزار و تأمین‌کنندگان امنیت الکترونیکی ایجاد کند تا به صنعت خدمات مالی پاسخگو باشند.

فرآیندهای نظارت و آزمون

کمیتهٔ باسل در *گروه بانکداری الکترونیکی (EGB) مؤسسهٔ نظارت بانکی*[۴۱] برای ارائه پیشنهاد در زمینه افزایش، ایجاد تغییرات یا انجام اصلاحات مورد نیاز در نظارت و ارزیابی جهت تطبیق روالها با فناوریهای جدید شکل گرفت. در سال ۲۰۰۱، EBG اصول مدیریت مخاطره برای بانکداری الکترونیکی را منتشر کرد که شامل اصول خاصی بود که استانداردهایی برای تأیید اعتبار و تصدیق هویت، کنترلهای داخلی، جامعیت امنیت سرمایه‌ها و همچنین جامعیت اطلاعات بانکداری الکترونیکی اعلام می‌کرد. حوزه‌های نظارت و ارزیابی در چند سال آینده تغییر جهت عمده‌ای پیدا می‌کنند. همانطور که صنعت امنیت با معرفی و تکیه بر انبوه رایانه‌های شخصی و اینترنت یک تغییر الگو را تجربه کرد، بنظر می‌رسد نظارت بانکی نیز تغییر مرکز ثقل صنعت خدمات مالی را تجربه خواهد نمود.

هماهنگی سازمانهای درون‌مرزی و برون‌مرزی

یک موضوع کلیدی که اکثر کشورها با آن روبرو هستند نیاز به ارتقای سطح تبادل اطلاعات میان قانونگذاران و دوایر اجرای قانون (نیروهای انتظامی) است. بسیاری از کشورها

---

38 Basel

۳۹ *مراجعه کنید به بند ۶ همین خلاصهٔ اجرایی*

۴۰ *در بسیاری از بازارهای درحال رشد، صنعت بیمه به خودیِ خود ممکن است نیاز داشته باشد که ساختار مجدد بیابد و به یک حالت استوار برسد؛ اما در هر حال می‌توان از این شرایط نیز جلوگیری کرد.*

41 Banking Supervision's Electronic Banking Group

چندین سازمان برای جمع‌آوری اطلاعات مهم دارند، اما معمولاً اطلاعات میان این سازمانها با یکدیگر یا با سازمانهای برون‌مرزی به‌اشتراک گذاشته نمی‌شوند (گاهی اوقات به دلایل حقوقی). موضوع تبادل اطلاعات میان سازمانها در ابعاد ملی و بین‌المللی فراتر از دامنهٔ این کتاب است. در هر صورت از آنجا که دولتها سعی دارند با جرائم موجود در محیط الکترونیکی به مقابله برخیزند، اشتراک اطلاعات و نیز همکاری بین‌المللی در این بحث موضوعاتی کلیدی به حساب می‌آیند.

رکن چهارم: نقش بیمهٔ خصوصی به عنوان یک سیستم نظارت تکمیلی

سازمانهای نظارت‌کننده بر خدمات مالی هنوز درحال تدوین استانداردهای قانونی هستند. به علت مشکلات ذاتی که در مسئله نظارت بر تراکنشهای پیچیدهٔ مبتنی بر زیرساختهای فنیِ متغیر وجود دارد، یافتن راه‌حلهای تکمیلی برای مدیریت مخاطرات از اهمیت زیادی برخوردار است. علیرغم نقایص موجود در اطلاعات لازم برای تخمین آسیبهای ناشی از مخاطرات الکترونیکی، مدتی است که صنعت بیمه در این قسمت نقش ایفا می‌کند. پیش‌بینی می‌شود در چند سال آینده تنها در بازار ایالات متحده، رشد بیمهٔ مسئولیت در تجارت الکترونیکی و گسترهٔ مخاطرات آن سالانه به ۲،۵ میلیارد دلار برسد.

هرچند بیمهٔ مسئولیت در تجارت الکترونیکی و مخاطرات الکترونیکی هنوز در مراحل اولیهٔ توسعه است، اما حاوی مشکلاتی در رابطه با شخص اول و شخص ثالث می‌باشد. تخمین هزینهٔ مخاطرات سایبر باید توسعهٔ بیشتری پیدا کند، ولی برای انجام اینکار، صنعت بیمه باید اطلاعات بیشتری دربارهٔ نفوذهای امنیتی و مخاطرات مرتبط با آنها داشته باشد. بعنوان مثال می‌توان گفت در تجارب ثبت‌شدهٔ کنونیِ این نوع بیمه، به مخاطرات جدیدی که فناوریهای بی‌سیم برای خدمات مالی بوجود آورده‌اند توجه کافی نشده است. ارائه‌کنندگان خدمات بیمه می‌توانند الزام کنند که استانداردهای امنیت الکترونیکی برای فناوری بی‌سیم شناسایی شوند و مورد استفاده قرار گیرند؛ تا پیش از آنکه مجبور به تبعیت از سیاستهای مخاطرات الکترونیکی شوند، این دسته از مخاطرات را کاهش داده باشند.

صنعت بیمهٔ جهانی می‌تواند بعنوان یک نیروی مهم برای تغییر الزامات امنیت الکترونیکی بکار رود. اول اینکه می‌تواند موجب بهبود استانداردهای حداقلی امنیت الکترونیکی در صنعت خدمات مالی شود. برای مثال صنعت جهانی خدمات مالی می‌تواند شرکتها را برای استفاده از امنیت الکترونیکی لایه‌بندی‌شده بعنوان یک پیشنیاز برای تجارت تحریک کند. ثانیاً شرکتهای بیمه می‌توانند از مؤسسات خدمات مالی بخواهند که به فروشندگانی مراجعه نمایند که برای ارائه خدمات امنیت الکترونیکی از استانداردهای تأییدشده و قابل قبول صنعتی بهره می‌برند تا مخاطرات احتمالی را کاهش داده باشند. ثالثاً شرکتهای بیمه می‌توانند قانونگذاران را ترغیب کنند تا مؤسسات خدمات مالی را ملزم نمایند که کیفیت اطلاعات و گزارشها در مورد رخدادها را بگونه‌ای بهبود بخشند که با استفاده از آنها بتوان تحلیل بهتری در مورد مخاطرات الکترونیکی و بازگشت سرمایه انجام داد. سرانجام اینکه صنعت بیمه می‌تواند راه‌حلهایی منتشر کند که در آنها مسائلی چون به‌اشتراک‌گذاری مخاطرات و مسئولیت‌پذیری در قبال نفوذهای امنیتی میان فروشندگان خدمات امنیت الکترونیکی و سایر شرکتهای فعال در این زمینه (مثل شرکتهای میزبان) الزامی شود.

رکن پنجم: گواهی[۴۲]، استانداردها، و نقش بخشهای عمومی و خصوصی

بخشهای عمومی و خصوصی باید با همکاری یکدیگر برای تدوین استانداردها و هماهنگ‌سازی طرحهای تأیید و اعطای گواهی اقدام کنند. دو عنوان که در این زمینه به آنها می‌پردازیم عبارتند از گواهی‌های ارائه‌دهندگان خدمات امنیت الکترونیکی و گواهی‌های عناصر هر تراکنش.

یک رویکرد ممکن برای تأمین امنیت امور مالی الکترونیکی می‌تواند این باشد که قانونگذاران، فروشندگانی که مستقیماً بر سیستم پرداخت تأثیر دارند را ملزم به کسب مجوز نمایند. یک رویکرد دیگر می‌تواند الزام صنعت به تأیید و اعطای

42 Certification

گواهی به ارائه‌دهندگان خدمات امنیت الکترونیکی باشد. بعنوان مثال اخیراً در صنعت امنیت یک گواهینامه با عنوان "متخصص امنیت" ایجاد شده است. در حقیقت در اثر این اتفاق، با تهیهٔ یک ساختار قابل شناسایی برای مصرف‌کننده، مسؤلیت‌پذیری میان صنعت و متخصصین آن، و تفکیک متخصصینِ تأییدشده از کسانیکه خود را متخصص می‌دانند، این تمام صنعت است که سود می‌برد. این روش همچنین وضعیت حوزهٔ امنیت را به وضعیت یک حوزهٔ حرفه‌ای ارتقا می‌دهد و باعث می‌شود صنعت انگیزهٔ لازم برای تدوین و اعمال استانداردها را داشته باشد.

حوزهٔ بعدی که باید مورد ملاحظه قرار گیرد گواهی‌های عناصر انجام معامله نظیر امضای الکترونیکی است. گواهی می‌تواند ارزش یک معامله را بسته به اینکه چه کسی و چه چیزی آنرا گواهی کرده افزایش دهد. گواهی ممکن است بوسیلهٔ یک سازمان دولتی نظیر ادارهٔ پست یا یک سازمان خصوصی مثل بانک صادر شود. هریک از این موارد، مسائل ساختاری و مدیریتی خاص خود را دارند. در بسیاری از کشورها ممکن است شرکتهای خصوصی برای تهیهٔ زیرساخت اطلاعاتیِ مورد نیاز برای اعطای گواهی بهتر عمل کنند.

عنصر اصلی یک برنامهٔ موفق برای اعطای گواهی این است که ساختارهایی که در مراکز قضایی مختلف وجود دارند باید از خصوصیات یکسانی برای تأیید کلیهٔ تراکنشها استفاده کنند و حدود اختیارات و مسئولیتهای یک تأییدکننده باید در تمام حوزه‌های قضایی یکپارچه و جامع باشد.

اگرچه استفاده از فناوری *زیرساخت کلید عمومی* (PKI)[۴۳] و اعطای گواهی معمولاً بعنوان تنها راههای قابل قبول برای تأمین امنیت درنظر گرفته می‌شوند، لیکن توجه به هزینه‌ها و ساختارهای پیچیده و درهم PKI و ناسازگاریهای حقوقی آن با *مراکز صدور گواهی* (CAs)[۴۴] نیز ضروری است. یک راه‌حل برای اینکه معقول و مناسب باشد باید با درنظر گرفتن مرزهایی چون اعتماد و مسئولیت‌پذیری قابل اجرا باشد و این چندان اهمیتی ندارد که برای انجام آن کدام فناوری مورد استفاده قرار خواهد گرفت.

43 *Public Key Infrastructure*
44 *Certification Authorities*

رکن ششم:
دقت در اطلاعات رخدادهای امنیتی، و همکاری دولت و بخش خصوصی

فقدان اطلاعات دقیق دربارهٔ رخدادهای امنیت الکترونیکی، نتیجهٔ دانش یا انگیزهٔ کم برای تهیه، اندازه‌گیری و به‌اشتراک‌گذاری اطلاعات است. با گسترش تدارکات درون‌مرزی و برون‌مرزی به منظور تسهیل در اشتراک اطلاعات دقیق دربارهٔ حملات تخریب سرویس، سرقت، کلاهبرداری و غیره توسط ارائه‌دهندگان خدمات مالی، امنیت الکترونیکی در سراسر جهان تقویت خواهد شد. به‌اشتراک نگذاشتن اطلاعات نه تنها دانش را در یک سطح معین نگه می‌دارد، بلکه از آن مهمتر می‌تواند توسعهٔ راه‌حلهای بخش خصوصی (شامل بیمه) را نیز محدود نماید. این فقدان اطلاعات ممکن است باعث افزایش هزینهٔ بیمهٔ شرکتها و ارائه‌دهندگان خدمات مالی شود.

در این حوزه همکاریهای گسترده‌تر دولت و بخش خصوصی لازم است. برای مثال *کمیتهٔ راهبری ارزیابی امنیت و مخاطرهٔ BIST*[۴۵] با ایجاد آزمایشگاه امنیت خدمات مالی، موضوعاتی چون امنیت، سلامت و صحت پرداختها ، تجارت الکترونیکی، و فناوریهای مربوطه را مورد بررسی قرار می‌دهد. این آزمایشگاه همچنین تبادل اطلاعات دربارهٔ موضوعات امنیتی صنعت خدمات مالی را تسهیل می‌نماید.

علاوه بر این وجود *اتحاد امنیت اینترنت*[۴۶]، *تیمهای امنیت رخداد و واکنش*[۴۷]، و *مرکز فوریتهای امنیت رایانه‌ای* (CERT)[۴۸] در کشورهای مختلف نشان می‌دهد که همکاری متقابل باعث اشتراک فزایندهٔ اطلاعات میان مجریان قانون و شرکتهای خصوصی ارائه‌کنندهٔ خدمات مالی می‌شود. یک عنصر مشترک در تمام این برنامه‌ها رعایت محرمانگی و اعتماد است: مجریان قانون و مؤسسات آموزشی، هویت منابع اطلاعات دقیق خود را فاش نمی‌کنند. در این حوزه نقش سازمانهای چندجانبه در تسهیل همکاری نیاز به بررسی دارد. بدیهی است که هر چه اقتصاد منسجم‌تر شود، به نحو احسن

45 *BIST's Security and Risk Assessment Steering Committee*
46 *Internet Security Alliance*
47 *Forum of Incident and Response Security Teams*
48 *Computer Emergency Response Team*

انجام‌شدن مسئولیت هر بخش اهمیت بیشتری پیدا می‌کند؛ و این درحالی است که صنعت خدمات مالیِ امروز، در آغاز بعنوان یک سیستم متمرکز شروع به کار کرد و تغییرات فناوری در دهۀ گذشته بود که وابستگیهای درونی این سیستم را گسترش داده و بیشتر کرده است.

رکن هفتم: آموزش و پیشگیری از وقوع رخدادهای امنیت الکترونیکی

تحلیل آماری نشان می‌دهد که در بسیاری از کشورها بیش از ۵۰٪ حملات امنیت الکترونیکی به سازمانها توسط افراد داخل سازمانها صورت می‌گیرد. نیروی کار با تحصیلات کم در مقابل حملات اینترنتی آسیب‌پذیرتر است. برعکس، نیروی کار آموزش‌دیده که از موضوعات امنیتی آگاه است می‌تواند یک لایۀ مؤثر حفاظتی به سیستم بیافزاید.

اقدامات اولیۀ آموزشی باید برای ارائه‌دهندگان خدمات مالی اعم از مدیران و راهبران سیستم – که در سازمانهای مختلف به نظارت و اجرای قانون می‌پردازند – و همچنین برای کاربران اینترنتی خدمات مالی مورد توجه قرار گیرد. اقدامات اولیه شامل موارد زیر می‌شوند:

- ارتقای آگاهی و آموزش افراد بخش مالی در مورد اصول اخلاقی در اینترنت و رفتار مناسب کاربر در سیستمهای شبکه‌ای؛
- تدوین سیاستهای امنیت الکترونیکی در سطح سازمان در مواردی چون رفتار درست و راههای موجود برای گزارش حملات یا رخدادها با هماهنگی کامل با تمام فعالیتهایی که در راستای تکمیل اطلاعات جهانی دربارۀ حملات انجام می‌شوند؛
- افزایش آگاهی مجامع بانکداریِ بازارهای نوین دربارۀ نیاز به *طرحهای واکنش به رخداد*[۴۹] در مواردی که حادثه‌ای رخ می‌دهد؛
- تسهیل همکاری و انتقال دانش میان مجریان قانون، *واحدهای اطلاعات خدمات مالی*[۵۰] و سازمانهای نظارتی در بازارهای توسعه‌یافته و نوین با ابزارهایی نظیر طرحهای تبادل فعال اطلاعات میان کارکنان؛
- طراحی دوره‌های متمرکز برای ممتحنان با کمک *مؤسسه پایداری خدمات مالی*[۵۱] یا دیگر مراکز آموزشی؛
- تدوین یک طرح چندمنظورۀ دانشگاهی برای آموزش متخصصین آیندۀ امنیت الکترونیکی، و بطور همزمان ارتقای سطح دانش کاربران خدمات مالی اینترنتی.

رکن هشتم: امنیت چندلایه

دوازده لایۀ اصلی امنیت وجود دارند که از اجزای بنیادی یک طرح مناسب برای حفظ یکپارچگی داده‌ها و کاهش مخاطرات محیطهای دارای معماری باز به حساب می‌آیند. این سلسلۀ دوازده لایه‌ای توضیح می‌دهد که در هر شرایط کدام مکانیزم امنیت باید مورد استفاده قرار بگیرد؛ و همچنین می‌گوید که امنیت هر شبکه تنها به اندازۀ ضعیفترین عنصر آن شبکه است. جزئیات این طرح دوازده لایه‌ای امنیت در انتهای همین بخش ارائه شده است.

تبصره‌ها

بخش سوم و چهارم کتاب مربوط به محیطهایی است که بسرعت درحال شکل‌گیری می‌باشند و با بکارگیری یک روش ضابطه‌مند تلاش دارند اقتصاد و قانون و فناوری را به تناسب یکدیگر هماهنگ کند. به علت رشد سریع جهانی، امنیت الکترونیکی قالبی مرموز دارد. غالب کشورها از جمله آنها که تجربۀ بیشتری دربارۀ مسائل امنیتی دارند هنوز از دانش اندکی در این زمینه برخوردارند و بازارهای نوین حتی از این هم کمتر می‌دانند. این کتاب توجه بیشتری به آموزه‌های ایالات متحده دارد؛ چراکه محل بوجود آمدن اینترنت بوده و زمان بیشتری برای تجربۀ مزایا و معایب آن داشته، و همچنین استانداردهای اولیه در این زمینه را بوجود آورده است.[۵۲] در تدوین این کتاب به فعالیتها و تجارب

49 *Incident Response Plan*
50 *Financial Intelligence Units*

51 *Financial Stability Institute*
۵۲ *اینترنت از ARPANET بوجود آمد، که در سال ۱۹۶۹ بوسیلۀ سازمان پروژه‌های تحقیقاتی پیشرفته (Advanced*

کشورهای پیشرفتهٔ اقتصادی در اروپا، آسیا و آمریکای جنوبی نیز توجه شده است. بدیهی است که مطالب زیادی را می‌توان دربارهٔ موضوعاتی چون "مشکلات ویژهٔ بازارهای نوین در این عرصه"، و "زمینه‌های حقوقی و موافقتنامه‌های سازمانی لازم برای بهبود امنیت الکترونیکی در سراسر جهان" طرح کرد.

بدون انجام این فعالیها، نیروی بالقوهٔ عظیم شرکتهایی که خود را با تجارت الکترونیکی تطبیق داده‌اند به شدت به خطر می‌افتد؛ چراکه اعتماد و اطمینان کسانیکه در بازار هستند بطور جدی تحت تأثیر قرار می‌گیرد. در فصلهای بعدیِ این بخش موارد زیر دنبال شده‌اند:

الف) روشهایی برای ارزیابی مخاطره و تحلیل زیان؛

ب) راهنمای عملی تدوین سیاستها و روالهای امنیتی که برای یک سازمان مناسب هستند؛

ج) توصیه‌های کلی و ویژه برای مدیران و کارمندان دربارهٔ الگوهای سرآمدی امنیت الکترونیکی؛ و

د) مجموعه‌ای از فهرستهای کنترل، با اظهار نظرهایی از سراسر دنیا در موضوع امنیت در عملیات تجاری، بویژه در رابطه با بخش مالی و کاربردهای تجارت الکترونیکی.

Research Projects Agency) در وزارت دفاع ایالات متحده طراحی شده بود.

فصل سوم
برآورد مخاطره و تحلیل زیان

کلیات

در این فصل *برآورد مخاطره*[۵۳] و *تحلیل زیان*[۵۴] و آسیبهای امنیتی از دیدگاه تجاری بررسی می‌شوند؛ ، منشأ، عملکرد محتمل، و شدت اثرات گستره‌ای از مخاطرات امنیتی بر فعالیتهای روزمره مورد مطالعه قرار می‌گیرند؛ نکات اصلیِ یک سیاست امنیتی صحیح تشریح می‌شوند و اصول اساسی تحلیل زیان هنگام وقوع یک رخداد امنیتی واقعی نیز مورد بررسی قرار می‌گیرند.

توسعهٔ فناوری: مرزهای جدید

کلیهٔ سازمانها – چه کوچک و چه بزرگ – درحال فعالیت در یک محیط جهانی هستند. پیشرفت ارتباطات و شبکه‌های حمل و نقل در قرن گذشته مشتریان و بازارها را به هم نزدیکتر کرده، هزینه‌ها را به حداقل رسانده و باعث شده امروز بتوان محصولات را برای خریداران به تمامی نقاط دنیا ارسال کرد. از دیدگاه بین‌المللی مدیران باید گستره‌ای از مخاطرات را برای مؤسسه‌هایشان درنظر بگیرند. از انتهای دههٔ ۱۹۹۰ به بعد حملات شدید بسیاری در سراسر دنیا صورت پذیرفت (نظیر حمله به مرکز تجارت جهانی در سال ۲۰۰۱). در مقابله با چنین رخدادهایی، نیاز به امنیت فیزیکی کاملاً روشن شد: ضرورت حضور پلیس در اطراف ساختمانها، کنترل ورود به ساختمانها، طراحی سیاستهای صحیح برای تخلیهٔ محیط درصورت وقوع حادثه، و توسعه دادن نقاط تماس مطمئن‌تر با مقامات محلی و کشوری.

در قسمت فنی نیز بصورت متناظر بررسی تهدیدهایی که از داخل و خارج سازمان متوجه تجهیزات رایانه‌ای، برنامه‌های کاربردی، پایگاههای داده، و شبکه‌هایی که گروهها را به هم متصل می‌کنند اغاز شده است. در محیط کار، داده‌های خام نظیر سوابق مشتریان یا اطلاعات کارت اعتباری برای رقبا و تبهکاران رایانه‌ای اهدافی ارزشمند است و به توجه خاص نیاز دارد. علاوه بر این در مؤسسات پیشرفته‌تر *مالکیت معنوی*[۵۵] نظیر اسناد تحقیقات علمی یا فرآیندهای کاریِ منحصر بفرد ارزش زیادی دارند و نیازمند مراقبتهای امنیتیِ ویژه هستند. در دنیایی که روز به روز رقابت در آن شدت می‌گیرد، سرقت داده‌های خام و دارائیهای فکری از طریق رایانه رو به افزایش است. مواردی چون "پشتیبانی پیشگیرانه" که در نگرش کلی و سرمایه‌گذاری مدیریت مورد توجه قرار می‌گیرد، آموزش و هوشیارسازی کارکنان، و ارتباطات شفاف درون سازمان، به کاهش خطرات ناشی از تخلفات امنیت فیزیکی و امنیت سایبر کمک می‌کنند.

خود را بشناسیم

اگرچه طرحها و روالهای مشترکی برای ایمن‌سازی سیستمهای رایانه‌ای و ساختمانها وجود دارد، اما داشتن تصویر کاملی از سازمان و قالب فعالیت آن برای تدوین یک طرح امنیتیِ خوب، لازم است. مجموعهٔ سیاستها و روالهای امنیتی مورد نیازِ شرکتی که در زمینهٔ دفع ضایعات خطرناک یا مواد زیستی فعال است با سیاستها و روالهای مورد نیازِ یک تولیدکنندهٔ لوازم الکترونیکی متفاوت است. برای آغاز فرآیند شناساییِ خطرات بالقوهٔ امنیتی توسط مدیریت، پاسخگویی به پنج سئوال زیر مفید خواهد بود:

۱. اصلی‌ترین محصول یا خدمت سازمان چیست؟ اگر چند پاسخ وجود دارد سعی کنید آنها را اولویت‌بندی نمایید.

۲. منابع اصلی درآمد و رشد سازمان کدامند؟

۳. ساختار سازمان چگونه است؟ بخشهای مختلف و عملکردهای اصلی هریک کدامند؟ این بخشها چگونه فعالیت می‌کنند؛ چگونه با یکدیگر ارتباط برقرار می‌نمایند؛ و چگونه بعنوان یک مجموعهٔ واحد به فعالیت می‌پردازند؟

53 *Risk Evaluation*
54 *Loss Analysis*
55 *Intellectual Property*

۴. کدام اطلاعات برای هر بخش حساستر است و از چه فناوریهایی برای ذخیره و توزیع این اطلاعات در خارج و داخل سازمان استفاده می‌شود؟

۵. مشتریان، شرکا و فروشندگان سازمان چه کسانی هستند و نحوهٔ تعامل آنها با سازمان چگونه است؟

اطلاعات مورد نیاز برای پاسخ دادن به این سؤالات را می‌توان از گفتگو با کارمندان (بخصوص کارکنان بخش فناوری اطلاعات)، مدیران و هیأت مدیره شرکت بدست آورد. ارزیابی نظرات مشتریان و فروشندگان در مورد مسائل دیگر ممکن است منجر به کشف مسائل امنیتی جدید شود. دست آخر اینکه تیمی که به جمع‌آوری اطلاعات می‌پردازد باید با ادبیات گزارشات رسانه‌ها در مورد شرکت آشنا باشد. نظرات عمومی نیز می‌تواند مؤثر باشد؛ بخصوص اگر شرکت در صنعتی بحث‌انگیز یا در جایگاهی حساس فعالیت کند، و یا گزارشاتی در مورد آن بصورت منظم در نشریات ظاهر شده باشد.

دشمن را بشناسیم: تهدیدات داخلی و خارجی

زمانیکه شرکت ساختار و عملکرد خود را ارزیابی کرد، موقعیتی مناسب برای تدوین شرحی از نقاط بالقوهٔ قوت و ضعف امنیتی آن بدست می‌آید. در ابتدا بهتر است روی تهدیدات کلی متمرکز شویم. هنگامیکه این تهدیدات شناسایی شدند، ارزیابی سطح تهدیدات داخلی و خارجی در فعالیتهای مربوط به هرکدام از این تهدیدها امکانپذیر خواهد بود.

تهدیدات کلی هر شرکت یا سازمان رسمی عبارتند از:

تهدیدات فیزیکی

- بلایای طبیعی (آتش‌سوزی، زلزله، طوفانهای شدید و سیل)؛
- دزدی؛
- تخریب؛
- تداخلهای فیزیکی؛
- تخریب شبکه؛ و
- جاسوسی سازمانیافته.

تهدیدات نرم‌افزاری

- نفوذ به دیواره‌های آتش؛
- برافزارها (ویروسها، تراواها، کرمها)؛
- انتشار غیرمجاز یا تخریب داده‌ها؛ و
- جاسوسی سازمانیافته بوسیلهٔ ابزارهای دیجیتالی .

از موضع تهدیدات انسانی، شرکت باید عوامل خرابکار داخلی و خارجی را شناسایی کند. در برخی موارد نقض امنیت داخلی می‌تواند ناشی از خطای انسانی باشد: یک سهل‌انگاری ساده، بی‌توجهی، یا عدم آموزش کافی کارمندان. در حوزه‌های دیگر بخصوص جاسوسی سازمانیافته، می‌توان از *مهندسی اجتماعی*[۵۶] برای دسترسی به تسهیلات و داده‌های سازمانی و محرمانهٔ افراد آگاه داخل شرکت استفاده کرد. مجموعه‌ای مناسب از سیاستها باید توسط بخش امنیت و با همکاری بخش پرسنلی ایجاد شوند تا به کاهش خطرات کمک نمایند. بخشهای امنیتی و پرسنلی همچنین می‌توانند در روالهای استخدام و اخراج کارکنان با یکدیگر همکاری نمایند. اگرچه در برخی موارد نمی‌توان انگیزهٔ شفافی برای اعمال خرابکارانه یافت انگیزه‌های متفاوت اینگونه فعالیتهای مخرب رایانه‌ای نیاز به توضیح مفصل دارند. دسته‌بندی کسانیکه به رایانه‌ها نفوذ می‌کنند چندان امکانپذیر نیست، ولی به هر ترتیب می‌توان در مورد شدت تهدیدها و متناظراً آسیب مورد انتظار هر تهدید بصورت کلی بحث کرد.

نفوذگران تفننی[۵۷] **(نفوذگران تابستانی**[۵۸]**)**، کارمندان یک سازمان هستند که با پروتکلهای شبکه آشنایی دارند. این افراد معمولاً قصد تخریب داده‌ها و دارائیهای شرکت را ندارند، اما از روی کنجکاوی سعی می‌کنند به منابعی که مجاز به استفاده از آنها نیستند دست پیدا کنند. با این وجود شاید کاملاً با ابزارهای نفوذ آشنا نباشند و با استفادهٔ نادرست از ابزارها باعث تخریب سیستمها شوند. علاوه بر این اگر ابزارها از اینترنت download شده باشند ممکن است دارای *درب مخفی*[۵۹] یا *تراوا*[۶۰] باشند که مورد استفاده دیگر مهاجمین قرار می‌گیرند. لذا نفوذ تفننی یک تهدید بزرگ

56 *Social Engineering*
57 *Casual Hackers*
58 *Summertime Hackers*
59 *Backdoor*
60 *Trojan*

محسوب می‌شود و مهمترین دلیل ممنوع بودن آن نیز همین است.

"Script Kiddie"ها معمولاً نفوذگران جوانتر (در سن دبیرستان یا پیش‌دانشگاهی) هستند که مهارتهای رایانه‌ای خوب و اوقات بیکاری زیادی دارند، اما چندان خبره نیستند و برای انجام نفوذ از تکه‌برنامه‌هایی که دیگران تهیه کرده‌اند استفاده می‌کنند. بطور کلی افراد این دسته مانند تبهکاران هدفدار (که در ادامهٔ همین مطلب بررسی شده)، بر روی تخریب متمرکز نمی‌شوند اما تعداد آنها زیاد است و گاهی به صورت تیمی کار می‌کنند و طبیعتاً در این قالب تهدید بزرگتری به حساب می‌آیند. "Script Kiddie"ها نفوذ موفق خود را منتشر و از آن طریق ادعای شهرت می‌کنند. در واقع آنها به بدنامیِ حاصل از حجم زیاد حملات خود افتخار می‌کنند. به علت رواج این تهدید، سازندگان نرم‌افزارهای امنیتی ابزارهای مؤثری را برای جلوگیری از این نوع نفوذ تهیه کرده‌اند. دیواره‌های آتش و *سیستمهای مهاجم‌یاب*[61] برای دفاع در مقابل چنین حملاتی بوجود آمده‌اند.

تبهکاران هدفدار معمولاً مهاجمان خبره‌ای هستند که هدف آنها سرقت اطلاعات، تخریب و از بین بردن داده‌ها، و از کار انداختن سیستمها در خلال یک بازهٔ زمانی می‌باشد. برخلاف نفوذگران تفننی و "script kiddie"ها، هدف آنها واقعاً نفوذ به سیستمها است. آنها در برخی موارد بدنبال اطلاعات ارزشمندی مثل داده‌های مالی (شماره‌های کارت اعتباری و جزئیات حساب بانکی) یا اطلاعات شخصی (شماره‌های شناسایی، سوابق دانشگاهی و فایلهای مشتریان) هستند تا آنها را تغییر دهند یا بگونه‌ای دیگر از آنها بهره ببرند. این دسته از مهاجمان غالباً بخوبی سازماندهی می‌شوند و پیش از انجام حملهٔ اصلی، اطلاعات ارزشمندی راجع به سازمان قربانی جمع‌آوری می‌کنند. خوشبختانه تعداد این نوع مجرمان کمتر از انواع دیگر است، اما جلوگیری از نفوذ آنان بسیار مشکل می‌باشد و درصورت نفوذ موفقیت‌آمیز، ممکن است باعث تخریبهای جدی شوند.

کارمندان و مشاوران می‌توانند بطور عمدی و یا سهوی تهدیدات جدی برای سیستم ایجاد کنند و این بستگی به ماهیت روابط آنها با مدیران و همکارانشان در محیط کار دارد. این افراد به علت سطح دسترسی‌شان در داخل سازمان، از لحاظ امنیتی یک نگرانی جدی محسوب می‌شوند.

در دستهٔ نفوذگران تفننی، برخی از کارکنان به علت خستگی از کار یا جذابیتهای رقابت فنی به سیستم نفوذ می‌کنند. گروهی دیگر بدنبال اطلاعات مربوط به ترفیع و دستمزد همکاران یا داده‌های سازمانی هستند. بعضی دیگر ممکن است برای انجام اقدامات تلافی جویانه علیه سازمان به این عمل دست بزنند؛ یا باعث تهدیدات ناخواسته‌ای شوند که علت آن عدم حفاظت صحیح از سیستم به علت آموزش فنی ناقص یا بی‌دقتی کارکنان باشد.

هریک از این تهدیدات بالقوهٔ انسانی برای سیستمها و اطلاعات امنیتی سطح متفاوتی از مخاطره را به همراه دارند و برای جلوگیری از وقوع آنها به روشهای متفاوتی نیاز است. دیواره‌های آتشِ به‌روز و سیستمهای مهاجم‌یاب ممکن است برای جلوگیری از نفوذگران تفننی یا "script kiddie"ها کفایت کنند. اما در مورد تبهکاران هدفدار، این راهبران هوشیار سیستم و مدیران هستند که باید آنها را شناسایی و متوقف سازند؛ و در این راستا استفاده از سیاستهای کارکنان و توجه مدیریت به خنثی‌سازی حملات احتمالی درون‌سازمانی مفید خواهد بود. اما هیچ طرحی بدون نقص نیست و بسیار اهمیت دارد که سازمان، سابقه و روند این طرحها را با توجه به نفوذهای امنیتی مستمراً بررسی کند. نظارت مستمر بر دورنمای امنیتی، کشف و جلوگیری از نفوذ را ساده‌تر می‌نماید. علاوه بر این، اتخاذ سیاستهای شفاف دربارهٔ آنچه که باید حین و بعد از وقوع حمله انجام شود به کاهش آسیب کمک می‌کند، افراد مسئول را برای رسیدگی به خرابی راهنمایی می‌نماید و امکان ثبت مناسب گزارشات لازم برای مقامات داخل و خارج سازمان را فراهم می‌سازد.

تخمین عملی امنیت: برآورد مخاطره و تحلیل زیان

همانگونه که مشاهده کردیم تخلفات امنیتی ریشه در حملات داخلی و خارجی دارند و به دسترسی غیرمجاز به سیستمها و داده‌ها برای اهداف غیرقانونی و غیراخلاقی منتهی می‌شوند. گامهای ابتدایی ایجاد سیاست امنیتی زمانی برداشته می‌شود که سازمان، یک تخمین امنیتی در مورد فرآیندهای داخلی، اهداف، و آسیب‌پذیریهای موجود داشته باشد. هنگامیکه این

61 *Intrusion Detection Systems (IDSs)*

عناصر تجزیه و تحلیل شدند، یک سیاست امنیتی و نیز طرحی برای روالها می‌تواند توسعه یابد.

این طرح باید حاوی اطلاعاتی دربارهٔ حوزه‌های کلیدی ذیل باشد:

- دانستن زمانی که مورد حمله واقع می‌شوید – از طریق بکارگیری سیستمهای کشف تهاجم و هوشیاری داخلی.
- فراهم ساختن سناریوی بدترین حالت ممکن – تفکر دربارهٔ تأثیرات مضاعفی که نقض امنیت می‌تواند برایتان بدنبال داشته باشد.
- تدوین یک سیاست مکتوب برای ثبت وقایع امنیتی (موسوم به *طرح نفوذ*[۶۲]) – این سند کتبی به تحلیل وقایع منفرد و جلوگیری از حملات موفق در آینده کمک می‌کند.
- استخدام یک متخصص درصورت نیاز – بر مبنای رخدادها یا بر مبنای موافقتنامهٔ مشاورهٔ دوره‌ای. از استخدام نفوذگران خودخوانده (کسانیکه مدعی نفوذگری هستند) اجتناب کنید. مبحث تأمین امنیت از طریق منابع خارجی در ادامه این بخش مطرح می‌شود.[۶۳]
- فراهم نمودن آموزش لازم برای کارکنان فنی و سایر کارمندان – بسیاری از نقصهای امنیتی ناشی از کمبود اطلاعات کافی در مورد روالهای مقابله با مسائل امنیتی هستند. هریک از کارکنان در شرکت باید نحوهٔ پیاده‌سازی روالهای امنیتی را بداند.
- تعیین یک نقطهٔ تماس – این فرد باید در حوزهٔ فناوری اطلاعات متخصص باشد و وقایع مستقیماً به اعضای تیم مدیریت گزارش دهد.
- درک و اولویت‌بندی اهداف – که شامل همه یا برخی از موارد ذیل می‌شود:
  - حفاظت از اطلاعات مشتریان؛
  - پیشگیری از حمله؛
  - اعلام حمله به مدیریت ارشد؛
  - ثبت وقایع؛
  - تهیهٔ *تصاویر آنی*[۶۴] از سیستم؛
  - تماس با *تیم واکنش به رخدادهای امنیت رایانه‌ای*[۶۵]؛
  - شناسایی مهاجم؛
  - شناسایی افراد مسئول در هر مورد؛ و
  - شناسایی فردی که بتوان به وی اطمینان کرد.

اگر حادثه‌ای رخ دهد می‌توانید سیاستها و روالهای موجود را مجدداً آزمایش کنید و تا آنجا که بودجه و تدارکات به شما اجازه می‌دهند آنها را تقویت نمایید. در ارزیابی سازمان، مجموعه‌ای از سؤالات وجود دارند که می‌توانند به شما در تعریف نقاط ضعف و قوت طرح امنیتی کمک کنند. یک فهرست نمونه که بر توانایی واکنش مؤثر در مقابل تهاجم تمرکز دارد را در ادامه می‌بینید:

روالهای مواجهه با رخداد، طرحهای ترمیم و سرمایهٔ مورد نیاز:

- آیا روالهایی برای پاسخگویی به رخداد وجود دارند؟
- آیا روالها قابل فهم و به روز هستند؟
- آیا طرحهای لازم برای ترمیم آثار بلایای طبیعی تهیه شده‌اند؟
- آیا سرمایهٔ کافی برای بروز واکنشهای مناسب در مقابل رخداد تخصیص داده شده است؟

روالهای متخصصان امنیتی و مدیریت:

- آیا روالها شامل دستورالعملهایی برای تماس با متخصص امنیتی در تمام طول شبانه‌روز و هر هفت روز هفته هستند؟
- اگر متخصص امنیت در دسترس نباشد، آیا راهی برای مطلع کردن مدیریت از مشکل وجود دارد؟

62 *Break-In Plan*

۶۳ *این توصیه بیشتر در سازمانهای متوسط و بزرگ عملی است و همچنین برای شرکتهایی که برای انجام فعالیتهایشان وابستگی زیادی به فناوری دارند و بازار هدفشان بازار فنی پیشرفته است. در مورد دوم مشتریان بالقوه ممکن است بر اساس وجههٔ فنی شرکت و استحکام فعالیتهای آن نظراتی در مورد شرکت ابراز کنند که باعث جوسازی مثبت یا منفی شود.*

64 *Snapshots*

65 *Computer Security Incident Response Team*

- آیا روشی برای مطلع کردن مدیر ارشد اطلاعات (درصورت وجود) از وقوع حوادث احتمالی تعریف شده است؟
- آیا روالی برای تعیین زمان تماس با افراد خارجی برای درخواست کمک و فردی که باید این تماس را برقرار کند وجود دارد؟

روالهای کارکنان:

- آیا همهٔ کارکنان کلیدی برای بکار بستن روالها آموزش دیده‌اند؟
- آیا کارکنان کلیدی واقعاً در همهٔ جلسات آموزشی حضور پیدا می‌کنند؟
- آیا دلیل انتخاب کارکنان کلیدی، سوابق درخشان آنها بوده است؟
- آیا ارتباطات راهبران سیستم و گروههای امنیتی روان است؟

روالهای منابع فنی:

- آیا دستوراتی برای آغاز کردن یا پایان دادن به برنامه‌های سیستم وجود دارد؟
- آیا دستورات آغاز یا پایان طرح بصورت دوره‌ای بررسی می‌شوند؟
- آیا ابزارهای مورد نیاز برای کشف تهاجم روی سیستم نصب و فعال شده‌اند؟
- آیا *نرم‌افزار شناسایی*[۶۶] که روی شبکه نصب شده می‌تواند حملات ناشناخته را شناسایی کند؟
- آیا می‌توانید با استفاده از ساختار لایه‌بندی‌شده حملاتی که به شبکه می‌شوند را کشف و از وقوع آنها جلوگیری کنید؟
- آیا روی شبکه می‌توان حملات را بسادگی تعقیب کرد؟
- آیا بر اساس ممیزیِ رسمیِ امنیت، کلیهٔ سیستمها دارای کنترل امنیتی کافی هستند؟

مراحل برآورد مخاطره

اولین گام برای ارتقای امنیت سیستم شما پاسخگویی به این سئوالات اساسی است:

۱. سعی در حفظ چه چیزی دارم و این مسئله چقدر برای من ارزش دارد؟
۲. در مقابل چه چیزهایی نیاز به حفاظت دارم؟
۳. حاضرم چقدر زمان، تلاش و سرمایه برای تأمین حفاظت مناسب اختصاص دهم؟

این سؤالات، اساسِ فرآیندی به نام *ارزیابی مخاطره*[۶۷] را شکل می‌دهند. ارزیابی مخاطره بخش بسیار مهمی از فرآیند امنیت رایانه است. اگر شما ندانید که برای چه و در مقابل چه چیزی حفاظت را اعمال می‌کنید، نخواهید توانست گامهای آنرا تدوین نمایید. وقتی خطرات را شناختید، می‌توانید سیاستها و فنونی که برای اجرای طرحهای کاهش مخاطره نیاز دارید را طراحی کنید. بعنوان مثال اگر خطر قطع برق وجود دارد و این امر برای شما مهم است، باید این خطر را با استفاده از *UPS*[۶۸] کاهش دهید.

ارزیابی مخاطره شامل سه مرحلهٔ کلیدی است:

۱. شناسایی دارائیها و ارزش آنها
۲. شناسایی تهدیدات
۳. محاسبهٔ مخاطرات

روشهای بسیاری برای انجام این فرآیند وجود دارد. یک روش که تاکنون بسیار موفق بوده، ایجاد مجموعه‌ای از کارگاههای آموزشیِ درون‌سازمانی است. در این روش شما باید از کاربران آگاه بخشهای مختلف، مدیران میانی و مدیران اجرایی سازمان خود دعوت بعمل آورید؛ و طی جلساتی فهرستی از دارائیها و تهدیدات را تهیه نمایید. این فرآیند نه‌تنها به شما کمک می‌کند که فهرست کاملتری تهیه کنید، بلکه آگاهی حضار از مسائل امنیتی را نیز بالاتر می‌برد.

یک رویکرد آماری بسیار پیچیده‌تر از آن است که بخواهد برای حفاظت از رایانهٔ خانگی یا یک شرکت بسیار کوچک مورد استفاده قرار گیرد. به همین ترتیب روالهایی که در اینجا مطرح می‌شوند برای حفاظت از شرکتهای بزرگ، سازمانهای

66 *Detection Software*

67 *Risk Assessment*
68 *Uninterruptible Power Supply*

دولتی، و دانشگاههای مهم کافی نیستند. در چنین مواردی، بسیاری از سازمانها از مؤسسات مشاوره‌ای که متخصص ارزیابی مخاطره هستند استفاده می‌کنند، و برخی دیگر نرم-افزارهای تخصصیِ ارزیابی را بکار می‌برند.

شناسایی دارائیها

فهرستی از اقلامی که به حفاظت نیاز دارند تهیه کنید. این فهرست باید بر اساس *طرح کسب و کار*[۶۹] و دانش عرفی شما تنظیم شود. این فرآیند نیازمند آگاهی از قوانین کاربردی، درک کامل تسهیلات، و علم به گسترهٔ پوشش بیمهٔ شما است. اقلام تحت حفاظت می‌توانند ملموس (مثل دیسک‌گردانها، صفحات نمایش، کابلهای شبکه، تجهیزات پشتیبان‌گیری، و کتابچه‌های راهنما) و یا غیرملموس (مثل دسترسی به رایانه، رمز عبور اصلی، توانایی ادامهٔ پردازش، فهرست مشتریان، وجههٔ عمومی، و اعتبار در صنعت) باشند. این فهرست باید هر چیزی که برای شما ارزشمند است را در بر بگیرد. برای تشخیص ارزشمند بودن هر مورد، درنظر بگیرید که درصورت تخریب یا فقدان آن، چه هزینه‌های زمانی و پولی برای تعمیر یا جایگزینی آن به شما تحمیل می‌شود. برخی از مواردیکه بطور حتم باید در فهرست ارزیابی شما قرار بگیرند عبارتند از:

موارد ملموس:

- رایانه‌ها؛
- داده‌های اختصاصی؛
- نسخه‌های پشتیبان و بایگانی؛
- دستورالعملها، راهنماها و کتابها؛
- نسخه‌های چاپی؛
- وسایل توزیع نرم‌افزارهای تجاری؛
- وسایل ارتباطی و کابل‌کشی‌ها؛
- سوابق کارکنان؛ و
- اسناد حسابرسی‌شده.

موارد غیرملموس:

- امنیت و سلامت کارکنان؛
- حریم خصوصی کاربران؛
- رمزهای عبور کارکنان؛
- وجههٔ عمومی و اعتبار سازمان؛
- حسن نیت مشتریان؛
- در دسترس بودنّ پردازش؛ و
- اطلاعات مربوط به پیکربندی.

شما باید بجای توجه صرف به جنبه‌های رایانه‌ای، نگرشی وسیعتر به اقلام فوق و سایر موارد مربوطه داشته باشید. اگر شما نگران این موضوع هستید که کسی بتواند گزارشات مالی شما را مطالعه کند، شیوهٔ دسترسی آن فرد به این اطلاعات (چه از طریق نسخه‌های کاغذی چه از طریق پست الکترونیکی و چه از طریق دسترسی مستقیم به نسخه‌های پشتیبان) از اهمیت خاصی برخوردار نیست و کلیهٔ راهها برای انجام چنین کاری باید مسدود شده باشند.

شناسایی تهدیدات

مرحلهٔ بعدی تعیین فهرستی از تهدیدات موجود برای دارایی شما می‌باشد. برخی از تهدیدات محیطی هستند و شامل آتش‌سوزی، زلزله، انفجار و سیل می‌شوند. این فهرستها باید شامل موارد بسیار نادر اما ممکن هم باشند؛ مثل بروز نقص کلی در ساختمان یا پیداشدن مواد آتشزا در دیوارهای اتاق رایانه که ممکن است شما را برای مدتی نه‌چندان کوتاه وادار به تخلیهٔ اتاق نماید. سایر تهدیدات از کارکنان و افراد خارج سازمان نشأت می‌گیرند. در اینجا مثالهایی برای این دسته از تهدیدات ذکر شده‌اند:

- بیماری افراد کلیدی؛
- بیماری همزمان بسیاری از کارکنان (نظیر بیماریهای مسری مثل آنفولانزا)؛
- از دست دادن پرسنل کلیدی (مرگ، بازنشستگی، پایان یافتن دورهٔ کاری)؛
- از دست دادن خدمات تلفن یا شبکه؛
- قطع خدمات شهری (تلفن، برق، آب) برای مدتی کوتاه؛
- قطع خدمات شهری برای مدت طولانی؛
- صاعقه؛
- سیل؛
- سرقت دیسکها یا نوارها؛
- سرقت رایانهٔ کیفی یک فرد کلیدی؛
- سرقت رایانهٔ خانگی یک فرد کلیدی؛
- ورود یک ویروس به سیستمها؛
- ورشکستگی فروشندگان یا شرکتهای ارائه‌دهندهٔ خدمات کلیدی طرف قرارداد با شما؛

69 *Business Plan*

- اشکالات سخت‌افزاری؛
- اشکالات نرم‌افزاری؛
- خرابکاری کارمندان؛
- خرابکاری پرسنل شخص ثالث (مثلاً کارمند بخش پشتیبانی فروشندگان)؛
- اغتشاش کارکنان؛
- مهاجمینی که بصورت تصادفی به ماشینهای شما دسترسی پیدا می‌کنند؛
- کاربرانی که روی اینترنت اطلاعات سازمانی تحریک‌کننده یا انحصاری می‌فرستند؛ و
- جاسوسهای سازمانیافتهٔ تجاری.

محاسبهٔ مخاطرات

ارزیابی مخاطرات نباید تنها یکبار انجام شود و پس از آن فراموش گردد، بلکه باید همواره و بصورت دوره‌ای – حداقل یکبار در سال یا هر زمان که تغییرات عمده‌ای در کارکنان، سیستمها یا محیط عملیاتی صورت می‌پذیرد – آنرا انجام دهید.[۷۰] علاوه بر این هنگامیکه تغییر جدی در ساختار یا عملیات رخ می‌دهد مجدداً باید تهدیدات را مورد ارزیابی قرار داد. لذا اگر شما سازماندهی مجدد می‌کنید، به ساختمان جدید می‌روید، فروشندگان طرف قرارداد خود را تغییر می‌دهید و یا تغییر جدی دیگری را ایجاد می‌نمایید، باید مجدداً تهدیدات و آسیبهای بالقوه را ارزیابی نمایید.

تحلیل زیان

تعیین هزینهٔ خسارتها ممکن است بسیار سخت باشد. یک شیوهٔ سادهٔ محاسبه این است که تنها هزینهٔ تعمیر یا تعویض تجهیزات و محصولات را محاسبه کنیم. یک شیوهٔ پیچیده‌ترِ احتساب هزینه‌های عدم ارائه خدمات، آموزش مجدد، روالهای اضافه‌شدهٔ ناشی از آسیب، از دست رفتن اعتبار شرکت، و حتی خسارتهای واردشده به مشتریان شرکت است. بطور کلی افزودن عوامل جانبی به محاسبهٔ هزینه باعث زحمت بیشتری می‌شود ولی دقت تخمین را بالا می‌برد. در اکثر موارد نیازی به تعیین دقیق ارزش و هزینهٔ هر مخاطره نیست و در حالت عادی اختصاص یک بازه یا محدودهٔ هزینه برای هر تهدید کفایت می‌کند. برخی از اقلام آسیب‌دیده را می‌توان در دستهٔ اقلام غیرقابل تعمیر و جایگزینی یا جبران‌ناپذیر قرار داد؛ مثل پاک شدن کامل پایگاه دادهٔ حسابها، یا مرگ یک کارمند کلیدی. شاید بخواهید هزینهٔ این خسارتها را با مقیاسها ظریفتری مورد بررسی قرار دهید؛ مثلاً برای هریک از موارد ذیل هزینهٔ جداگانه‌ای درنظر بگیرید:

- در دسترس نبودن در کوتاه‌مدت (کمتر از ۷ تا ۱۰ روز)؛
- در دسترس نبودن در میان‌مدت (۱ الی ۲ هفته)؛
- در دسترس نبودن در درازمدت (بیش از ۲ هفته)؛
- زیان یا تخریب دائمی؛
- زیان یا تخریب تصادفی؛
- زیان یا تخریب تعمدی؛
- افشای غیرمجاز اطلاعات درون سازمان؛
- افشای غیرمجاز اطلاعات به منابع خارجی؛
- افشای غیرمجاز و کامل اطلاعات برای همهٔ منابع خارج از سازمان، رقبا و مطبوعات؛ و
- هزینهٔ جایگزینی یا ترمیم.

احتمال زیان

پس از اینکه تهدیدات را شناسایی کردید باید احتمال رخداد هر اتفاق را تخمین بزنید. تخمین سالانهٔ این تهدیدات از ساده‌ترین روشها است. تعیین کمیت یک مخاطره کار بسیار دشواری است. شما می‌توانید از طریق شرکتهای دیگر (مثل شرکت بیمه) این برآوردها را بدست آورید. اگر واقعه برای چند بار متوالی رخ داده باشد، بر اساس سوابق نیز می‌توان آنرا تخمین زد. سازمانهای صنعتی معمولاً آمارهایی جمع‌آوری و گزارشاتی منتشر می‌کنند. شما نیز می‌توانید حدسیات خود را بر اساس تجربیات گذشته به واقعیت نزدیکتر کنید. بعنوان مثال:

---

۷۰ *تغییرات در کارکنان می‌تواند استخدام و بازنشستگی تعداد زیادی از افراد باشد، یا بازنشستگی یکی از کسانیکه در طرح امنیت سازمان فعالیت داشته است. تغییرات در سیستمها می‌تواند نصب چند سیستم جدید باشد. اگر ۱۰۰ رایانه دارید و با رعایت اصول ایمنی ۱ رایانه به سیستم اضافه می‌کنید، ارزیابی مجدد مخاطرات ضروری نیست، اما اگر مثلاً ۱۰ رایانه دارید و ۱۰ رایانهٔ دیگر اضافه می‌کنید، این توسعه ممکن است یک جنبهٔ کاملاً جدید در سازمان شما بوجود بیاورد. تغییرات دیگر سیستمها می‌توانند شامل راه‌اندازی شبکه‌های جدید داخلی و خارجی، ارتقای سیستمها، یا ایجاد تغییرات در بستر عملیات رایانه‌ای باشند. تغییرات در سازمان نیز معمولاً عبارتند از رشد سریع، برقراری ارتباط با فروشندگان یا مشتریان خارجی، و نیز شرکتهای بازاریابی که ممکن است شما را در بازارهای محلی و جهانی بیشتر جا بیاندازند.*

- شرکت برق بر اساس تجربهٔ سال گذشتهٔ خود برآوردی از احتمال قطع برق در خلال سال آینده دارد. مقامات مسئول نیز می‌توانند مخاطرهٔ قطع برق برای چند ثانیه، چند دقیقه، و یا چند ساعت محاسبه نمایند.
- سوابق پرسنلی می‌تواند در تخمین احتمال استعفای یک کارمند کلیدی بخش رایانه به شما کمک کند.
- خوشبینانه‌ترین حدسیات در مورد تکرار تجربیات گذشته می‌توانند برای تخمین احتمال کشف اشکالات جدی در نرم‌افزارهای شما در خلال سال آینده مورد استفاده قرار گیرند.

اگر انتظار دارید حادثه‌ای بیش از یکبار در سال رخ دهد، تعداد دفعات وقوع آنرا در طول یکسال ثبت کنید. مثلاً اگر وقوع زلزله را در هر ۱۰۰ سال یکبار پیش‌بینی کنید، طبق آنچه گفته شد در فهرست شما می‌شود ۱٪؛ اگر اما انتظار داشته باشید طی ماه آینده سه اشکال جدی در سرویس‌دهندهٔ Microsoft IIS کشف شود، خواهد شد ۳۶۰۰٪.

هزینهٔ پیشگیری

سرانجام باید هزینهٔ پیشگیری از وقوع هر نوع مخاطره را محاسبه کنید. بعنوان مثال هزینهٔ قطعِ برقِ لحظه‌ای احتمالاً عبارت خواهد بود از هزینهٔ زمان بیکاری پرسنل و راه‌اندازی مجدد رایانه‌ها؛ اما هزینهٔ پیشگیری از آن برابر هزینهٔ خرید و نصب یک سیستم UPS می‌باشد.

هزینه‌ها باید در طول عمر مورد انتظار، با استفاده از رویکردی مناسب مستهلک شوند. بدست آوردن این هزینه‌ها می‌تواند هزینه‌ها و اعتبارات دیگری را مشخص کند که آنها نیز باید مد نظر قرار گیرند. مثلاً نصب یک سیستم اطفاء حریقِ بهتر می‌تواند حق بیمهٔ آتش‌سوزی را کاهش دهد و به علت استهلاک سرمایه برای شما مزیت مالیاتی ایجاد کند؛ اما صرف پول برای سیستم اطفاء حریق به این معناست که آن پول دیگر برای سایر اهداف نظیر آموزش کارکنان یا حتی سرمایه‌گذاری در دسترس نیست.

جمعبندی نتایج

در بخش نتیجه‌گیری باید یک جدول چند ستونی از دارائیها، مخاطرات و زیانهای احتمالی طراحی کنید. برای هر زیان باید احتمال، خسارت پیش‌بینی‌شده و مقدار پول مورد نیاز برای پیشگیری از وقوع آنرا بدانید. اگر خیلی دقیق هستید می‌توانید احتمال نامناسب بودن تمهیدات دفاعی را نیز محاسبه کنید. اکنون فرآیند تصمیم‌گیری در مورد بکار گرفتن یا نگرفتن هر مکانیزم دفاعی کاملاً روشن است. کافیست شما ضرر مورد انتظار هر مخاطره را در احتمال وقوع آن ضرب کنید تا برای هر تهدید یک کمیت بدست آید. این ارقام را به ترتیب نزولی مرتب نمایید و کمیت متناظر هر تهدید را با هزینهٔ پیشگیری آن مقایسه نمایید.

نتیجهٔ این مقایسه فهرستی است اولویت‌بندی شده از آنچه که باید انجام شود. این فهرست ممکن است در ابتدا کمی تعجب‌آور باشد. توجه کنید که هدف شما باید جلوگیری از زیانهای پرهزینه و محتمل و توجه کمتر به موارد نادر و کم‌هزینه باشد. در بسیاری از محیطها احتمال وقوع مواردی نظیر آتش‌سوزی و از دست دادن پرسنل کلیدی بسیار بیش از مورد نفوذ قرار گرفتن شبکه می‌باشد؛ اما با کمال تعجب این نفوذهای شبکه‌ای هستند که توجه مدیران و درنتیجه قسمت عمده‌ای از بودجه را به خود جلب می‌کنند. این عملکرد از لحاظ هزینه اثربخش نیست و بالاترین سطح اطمینان را برای کل سیستم فراهم نمی‌کند. برای تجسم اقداماتی که باید انجام دهید، آنچه برای پیشگیری و ترمیم هر رخداد جمع‌آوری کرده‌اید را بر مبنای اولویت، طبقه‌بندی نمایید. برای انجام اینکار هزینهٔ ترمیم را به میانگین زیان مورد انتظار اضافه کنید و آنرا در احتمال وقوع رخداد ضرب نمایید. آنگاه نتایج حاصله را با هزینهٔ سالانهٔ پیشگیری مقایسه کنید. اگر هزینه‌ها کمتر از هزینهٔ مورد انتظار مخاطره است توصیه می‌شود که درصورت وجود منابع مالی کافی استراتژی پیشگیری را در پیش بگیرید؛ اما اگر هزینهٔ پیشگیری بیش از هزینهٔ آسیبها و ترمیمِ بعد از وقوع رخداد است، تا پیش از وقوع حادثه هیچ اقدامی نکنید.

فصل چهارم
برنامه‌ریزی برای نیازهای امنیتی

کلیات

این فصل به سیاستها و روالهای مربوط به پیشگیری و دفاع مؤثر در مقابل تهدیداتی که در فصل قبل در مورد آنها بحث شد می‌پردازد و جزئیات فرآیند برنامه‌ریزی را شرح می‌دهد.

سیاستگذاری و راه‌حلهای فنی برای تأمین موفقیت‌آمیز امنیت

اساساً امنیت رایانه‌ای مجموعه‌ای از راه‌حلهای فنی برای مشکلات غیرفنی است. زمان، پول و تلاش زیادی را می‌توان برای ایمن کردن رایانه صرف کرد، اما هرگز نمی‌توان از نگرانی در مورد پاک‌شدن تصادفی داده‌ها یا تخریب عمدی اطلاعات راحت شد. با درنظر گرفتن مجموعهٔ شرایط – اشکالات نرم‌افزاری، حوادث، اشتباهات، بداقبالی، آب و هوای بد یا یک مهاجم مجهز و با انگیزه – مشاهده می‌شود که هر رایانه ممکن است مورد سوء استفاده قرار بگیرد، از فعالیت بیافتد، یا حتی کاملاً منهدم شود.

وظیفهٔ متخصصین امنیتی کمک به سازمان در تصمیم‌گیری در مورد زمان و هزینه‌ای است که می‌خواهد برای مسئله امنیت اختصاص دهد. بخش دیگر اینکار حصول اطمینان از وجود سیاستها، خط‌مشی‌ها و روالهای مناسب در سازمان است تا بودجهٔ امنیتی بصورت صحیح هزینه شود. در نهایت افراد حرفه‌ای باید سیستم را بررسی کنند تا از پیاده‌سازی صحیح کنترلهای مناسب در راستای برآورده‌شدن اهداف اطمینان یابند. بنابراین امنیت عملی بیش از اینکه مسئله‌ای فنی باشد، مسئله‌ای مدیریتی است. درنتیجه امنیت باید یکی از اولویتهای مدیریت سازمان باشد. حتی در مؤسسات بسیار کوچک که بودجهٔ قابل توجهی برای امنیت صرف نمی‌شود، مدیریت باید مسائل اصلی امنیتی را درک کند و اصول اولیهٔ امنیت را برای حفاظت از دارائیها به اجرا درآورد.

برنامه‌ریزی امنیتی را می‌توان به پنج مرحلهٔ مجزا تقسیم کرد:

۱. برنامه‌ریزی برای تعیین نیازهای امنیتی
۲. ارزیابی مخاطره و انتخاب بهترین شیوه‌ها
۳. ایجاد سیاستهایی برای انعکاس نیازها
۴. پیاده‌سازی امنیت
۵. بررسی و واکنش به وقایع

دو اصل اساسی وجود دارند که در برنامه‌ریزی اثربخش سیاست و امنیت تأثیر ضمنی می‌گذارند:

در سازمانها آگاهی از امنیت و سیاست امنیتی باید از بالا به پائین گسترش یابد. نگرانیها و آگاهی کاربران از مسائل امنیتی حائز اهمیت است؛ اما آنها نمی‌توانند در گسترهٔ سازمان یک فرهنگ مؤثر امنیتی ایجاد و آنرا حفظ نمایند. در عوض این مدیران سازمان هستند که باید به امنیت بعنوان موضوعی مهم بنگرند و ضوابط و مقررات آنرا نظیر سایر افراد بپذیرند و اجرا نمایند.

امنیت مؤثر رایانه به معنای حفاظت از اطلاعات می‌باشد. اگرچه حفاظت از منابع دیگر هم مهم است اما ضررهای ناشی از تخریب سایر منابع بسیار راحت‌تر از ضررهای وارده به اطلاعات قابل تشخیص و جبران هستند. کلیهٔ طرحها، سیاستها و روالها باید منعکس‌کنندهٔ نیاز به حفاظت از اطلاعات در هر قالب ممکن باشند. اطلاعات انحصاری اگر به چاپ برسند یا به یک دفتر فکس شوند ارزش خود را از دست نمی‌دهند. اطلاعات محرمانهٔ مشتریان نیز اگر بجای ارسال از طریق پست الکترونیکی، با استفاده از تلفن گزارش شدند همچنان از ارزش زیادی برخوردارند. خلاصه اینکه اطلاعات باید مورد محافظت قرار بگیرد، مستقل از اینکه در چه قالبی باشد.

انواع مختلف و تعاریف متفاوتی از امنیت رایانه‌ای وجود دارد. این کتاب بجای ارائه یک تعریف رسمی، توجه بیشتری به رویکرد عملی دارد و در مورد انواع حفاظتهایی که باید مورد ملاحظه قرار گیرند به بحث پرداخته است.

دسته‌بندی ملاحظات امنیتی

در این تعریف گسترده، گونه‌های مختلفی از امنیت وجود دارند که راهبران و کاربران باید به آنها توجه کنند:[۷۱]

محرمانگی[۷۲]
حفاظت از اطلاعات در مقابل خواندەشدن یا نسخه‌برداری توسط اشخاصی که از جانب مالک آن اطلاعات مجوز دسترسی به آنرا ندارند. این گونهٔ امنیت نه‌تنها حفاظت کلی از اطلاعات را در بر می‌گیرد، بلکه حفاظت از داده‌های منفرد که ممکن است به خودیِ خود آسیبی در پی نداشته باشند ولی از طریق تعدادی از آنها بتوان به اطلاعات محرمانه پی برد را نیز شامل می‌شود.

یکپارچگی و صحت (تمامیت)[۷۳]
محافظت از اطلاعات (منجمله برنامه‌ها) در مقابل هرگونه حذف و تغییر بدون اجازهٔ مالک آن اطلاعات. اطلاعاتی که باید مورد محافظت قرار گیرد شامل سوابق حسابداری، نسخه‌های پشتیبان، زمانهای ایجاد فایل و اسناد می‌شود.

در دسترس بودن[۷۴]
حفاظت از برنامه‌های خدماتی بگونه‌ای که بدون تصدیق اعتبار تنزل پیدا نکنند و تخریب نشوند. اگر هنگامیکه یک کاربرِ مجاز به اطلاعات نیاز دارد سیستم و داده‌ها در دسترس نباشند، نتیجه می‌تواند به اندازهٔ زمانی که اطلاعات از روی سیستم حذف شده‌اند ناخوشایند باشد.

ثبات و سازگاری (پایداری)[۷۵]
حصول اطمینان از اینکه سیستم بگونه‌ای که مورد انتظار کاربران است رفتار می‌کند. اگر نرم‌افزار یا سخت‌افزار ناگهان بگونه‌ای بسیار متفاوت از قبل عمل کند – خصوصاً بعد از یک ارتقا یا رفع اشکال – مشکلات زیادی ممکن است رخ دهد. تصور کنید اگر فرمان "ls" بطور تصادفی حذف شود هنگام فهرست‌گیری از فایلها چه اتفاقی می‌افتد! این گونهٔ امنیت را می‌توان اطمینان از صحت داده‌ها و نرم‌افزارهایی که مورد استفاده قرار دارند نامید.

کنترل
ضابطه‌مند کردن دسترسی به سیستم. اگر افراد (یا نرم‌افزارهای) ناشناخته و غیرمجاز در سیستم شما وجود داشته باشند می‌توانند دردسرهای زیادی بیافرینند و شما راجع به چگونگی ورود آنها، آنچه که ممکن است انجام داده باشند، و افراد دیگری که احتمالاً به سیستم شما دسترسی داشته‌اند احساس نگرانی می‌کنید. جبران چنین مشکلاتی می‌تواند بسیار وقتگیر و پرهزینه باشد. شاید مجبور شوید سیستم خود را از ابتدا نصب و راه‌اندازی کنید و تازه متوجه شوید که تغییر مهمی رخ نداده – حتی اگر واقعاً هیچ اتفاقی نیافتاده باشد.

بازبینی
به همان میزان که نگران دسترسی افراد غیرمجاز به سیستم هستید، باید به امکان وقوع اشتباهات یا انجام اعمال بدخواهانه توسط کاربران مجاز نیز توجه کنید. در چنین شرایطی باید آنچه که انجام شده، فرد انجام‌دهنده و تأثیرات آنرا مشخص نمایید. تنها راه مطمئن برای دستیابی به این نتایج، داشتن سوابق و ثبتهای تخریب‌نشدنی از فعالیتها در سیستم است که می‌تواند افراد و عملکرد آنها را شناسایی کند. در برخی از نرم‌افزارهای بسیار حساس، شیوهٔ بازبینی ممکن است آنقدر گسترده باشد که بتواند بعد از تنظیم وضعیت سیستم به یک حالت جدید، اجازهٔ بازگشت به وضعیت اولیه را نیز بدهد.

اگرچه کلیهٔ این وجوه امنیتی اهمیت دارند، اما سازمانهای مختلف به هریک با درجهٔ اهمیت متفاوتی می‌نگرند. این اختلاف بدلیل این است که هر سازمان ملاحظات امنیتی خاص خود را دارد و باید اولویتها و سیاستهای خود را بر حسب آن ملاحظات تعیین کند. بعنوان مثال:

محیط بانکداری
در چنین محیطی، یکپارچگی، کنترل، و بازبینی، از اصول بسیار مهم و حیاتی هستند؛ و محرمانگی و در دسترس بودن در درجهٔ بعدی قرار دارند.

محیط نظامی
در یک سیستم دفاعی ملی که حاوی اطلاعات طبقه‌بندی‌شده است، محرمانگی در اولین درجهٔ اهمیت قرار

---

۷۱ *مراجعه کنید به رویکرد COBIT در راهبردهای امنیتی:*
http://www.isaca.org/cobit.htm
72 *Confidentiality*
73 *Integrity*
74 *Availability*
75 *Consistency*

دارد و در دسترس بودن در درجهٔ آخر. در برخی از محیطهای بسیار طبقه‌بندی شده ممکن است مقامات رسمی ترجیح دهند که یک ساختمان را منفجر کنند تا اجازه نداده باشند اطلاعات بدست مهاجمین بیافتد.

محیط دانشگاهی

در چنین محیطی، یکپارچگی و در دسترس بودن اطلاعات مهمترین نیازمندیها هستند. حصول اطمینان از در دسترس بودن اطلاعات در زمانیکه دانشجویان به آنها نیاز دارند به مراتب مهمتر از این است که راهبران بتوانند زمان استفادهٔ دانشجویان از حسابهای کاربری خود را تشخیص دهند.

اگر یک راهبر امنیت هستید باید نیازهای محیط عملیاتی و کاربران را بشناسید و سپس بر مبنای آن روالهای خود را تعریف کنید. ناگفته پیداست که مطالب مشروح در این کتاب لزوماً برای تمامی محیطها مناسب نیستند.

اعتماد

متخصصین امنیت معمولاً سیستمهای رایانه‌ای را با عناوین "امن" و "ناامن" خطاب نمی‌کنند؛ بلکه کلمهٔ "اعتماد" را برای توضیح سطح اطمینان مورد انتظار از یک سیستم رایانه‌ای بکار می‌برند. دلیل این مسئله این است که امنیت مطلق هیچگاه نمی‌تواند بدست آید. تنها می‌توانیم با ایجاد اعتماد کافی در پیکربندی کلی و تضمین استفاده از آن برای برنامه‌های مورد نظر به امنیت مطلق نزدیک شویم. ایجاد اعتماد کافی در سیستمهای رایانه‌ای مستلزم تفکر و برنامه‌ریزی دقیق است. تصمیمات عملیاتی و درصورت امکان سیاستهای کلی باید بر اساس ارزیابی مخاطره اتخاذ گردند و برای این منظور استفاده از توصیه‌های تخصصی بسیار حائز اهمیت است:

اگر شما در یک شرکت، دانشگاه یا سازمان دولتی بزرگتر کار می‌کنید، پیشنهاد می‌کنیم که با بخشهای ممیزی داخلی یا مدیریت مخاطرهٔ شرکت برای دریافت کمکهای لازم ارتباط برقرار نمایید (آنها ممکن است از طرحها و سیاستهایی استفاده کنند که لازم باشد از آنها مطلع شوید). همچنین می‌توانید با مراجعه به منابع معرفی‌شده در بخش ضمائم، در خصوص این موضوع مطالب بیشتری بیاموزید. ممکن است بخواهید از یک مؤسسهٔ مشاور طلب همکاری کنید. بعنوان مثال بسیاری از شرکتهای حسابداری و ممیزی دارای تیمهای متشکل از متخصصین هستند که می‌توانند امنیت نصبهای رایانه را ارزیابی کنند.

اگر شما با یک شرکت کوچکتر همکاری می‌کنید یا با رایانه‌های شخصی سر و کار دارید، ممکن است دارای بخش تخصصی امنیت نباشید. در اینحالت پیشنهاد می‌شود بخش دوم کتاب را به دقت مطالعه نمایید. ممکن است تصور کنید که این کتاب بیش از میزان احتیاج شما وارد جزئیات شده، اما اطلاعات موجود در این فصول به شما در تنظیم اولویتهایتان کمک شایانی خواهد کرد.

تحلیل سود و زیان و الگوهای سرآمدی

بعد از اتمام ارزیابی مخاطره، فهرستی طولانی از مخاطرات را پیش روی خود دارید – بسیار بیش از مقداری که بتوانید به همهٔ آنها بپردازید یا با تمام آنها مقابله کنید. چون زمان و پول محدود هستند، اکنون شما به یک روش درجه‌بندی برای این مخاطرات نیاز دارید تا بتوانید تصمیم بگیرید که می‌خواهید آثار و احتمال کدام مخاطرات را از طریق ابزارهای فنی کاهش دهید، در مقابل کدامها از بیمه استفاده کنید، و وقوع چه مواردی را صرفاً بپذیرید. بطور سنتی تصمیم‌گیری در مورد اینکه با کدام مخاطره باید مقابله کرد و کدامیک را باید پذیرفت با استفاده از یک تحلیل سود و زیان – تخصیص هزینه به هر زیان احتمالی؛ تعیین هزینهٔ مقابله با آن، تعیین احتمال وقوع هر مخاطره، و سپس تعیین اینکه آیا هزینهٔ مقابله با آن از مزایای پیشگیری بیشتر است یا نه – انجام می‌شود.

ارزیابی مخاطره و تحلیل سود و زیان اعداد زیادی بوجود می‌آورند که باعث می‌شود فرآیند کاملاً علمی و منطقی بنظر بیاید، اما در عمل جمع‌آوری و کنار هم قراردادن این اعداد ممکن است بسیار وقتگیر و پرهزینه باشد و نتیجهٔ حاصله نیز تنها اعداد غیردقیق هستند. ارزیابی مخاطره به توانایی اندازه‌گیری استفادهٔ مورد انتظار از یک دارائی، تخمین احتمال مخاطره برای آن دارائی، شناسایی عواملی که احتمال وقوع مخاطرات را بیشتر می‌کنند، و محاسبه تأثیر بالقوهٔ هر انتخاب – شاخصهایی که بدست آوردن آنها بسیار دشوار است – بستگی دارد. چگونه مخاطرهٔ یک مهاجم را که خواهد توانست امتیازات راهبری سیستم شما را بدست گیرد محاسبه

می‌کنید؟ آیا این مخاطره با گذشت زمان و کشف آسیبهای جدید افزایش می‌یابد، یا با گذشت زمان و اصلاح آسیبها کاهش می‌یابد؟ آیا سیستمی که بخوبی مورد مراقبت قرار دارد با گذشت زمان ایمن‌تر می‌شود یا ناامن‌تر؟ و چگونه خسارتهای تقریبی یک نفوذ موفق را محاسبه می‌کنید؟ متأسفانه مطالعات علمی و آماری اندکی در مورد این مسائل انجام شده است. افراد بیشماری فکر می‌کنند که پاسخ این سؤالات را می‌دانند؛ اما محققان نشان داده‌اند که بیشتر افراد بر اساس تجربهٔ شخصی قادر به تخمین صحیح مخاطرات و احتمال وقوع آنها نیستند.

به علت مشکلات ذاتی روش ارزیابی مخاطره، در سالهای اخیر رویکرد دیگری برای برقراری امنیت رایانه بوجود آمده که *الگوهای سرآمدی*[۷۶] یا *مراقبت دقیق*[۷۷] نام دارد. این رویکرد شامل مجموعه‌ای از پیشنهادات، روالها و سیاستهایی است که بطور معمول در جوامع محققان امنیتی تائیدشده که سازمانها را به سطح قابل قبولی از امنیت عمومی می‌رساند و مخاطرات را با هزینهٔ معقولی کاهش می‌دهد. می‌توانید الگوهای سرآمدی را "بدیهیات پیاده‌سازی منطقی تدابیر امنیتی" بدانید.

استفاده از الگوهای سرآمدی هم مشکلات خود را دارد. بزرگترین مشکل این است که هیچ مجموعه‌ای از الگوهای سرآمدی وجود ندارد که برای تمام محیطها و کاربران مناسب باشد. الگوهای سرآمدی برای یک پایگاه وب که اطلاعات مالی را مدیریت می‌کند ممکن است شباهتهایی به الگوهای سرآمدی پایگاه وب یک خبرنامهٔ اجتماعی داشته باشد؛ اما به احتمال زیاد پایگاه وب حاوی اطلاعات مالی، نیاز به اقدامات امنیتی بیشتری خواهد داشت.

دنبال کردن الگوهای سرآمدی نمی‌تواند تضمین کند که سیستم شما با مشکل امنیتی روبرو نخواهد شد. در غالب الگوهای سرآمدی، بخش امنیت سازمان باید اینترنت را برای اخبار حملات جدید و download کردن وصله‌های ارائه‌شده توسط فروشندگان محصولات نرم‌افزاری بررسی نماید. اما حتی اگر شما از این ساختار نیز پیروی کنید، مهاجمان همچنان ممکن است برای تسخیر سیستم رایانه‌ای شما از شیوهای نادانستهٔ تازه و منتشرنشده استفاده کنند. حال اگر اطلاعات شما از اخبار جدید کم باشد و یا شخصی که مسئول بررسی فهرستهای پست الکترونیکی است در سفر باشد، مهاجم از شما پیشی خواهد گرفت.

این تفکر که دهها هزار سازمان می‌توانند یا باید الگوهای سرآمدی موجود را برای امنیت رایانه‌هایشان پیاده‌سازی کنند مشکل آفرین است، چراکه الگوهای سرآمدی موجود برای تمامی سازمانها مناسب و به‌صرفه نیستند.

بسیاری از سازمانهایی که مدعی هستند از الگوهای سرآمدی پیروی می‌کنند در حقیقت از حداقل استانداردها برای امنیت دستگاههای خود استفاده می‌نمایند؛ و در عمل، الگوهای سرآمدی و یا بعبارتی راهکارهای بهینه هم خود واقعاً بهینه نیستند!

توصیهٔ ما ترکیبی از دو رویکرد ارزیابی مخاطره و الگوهای سرآمدی است. با شروع از بدنهٔ یک مجموعه از الگوهای سرآمدی، یک طراح آگاه باید مخاطرات را ارزیابی کند، و برای هر حالت خاص سیستم یک راه‌حل معقول ارائه نماید. برای مثال سرویس‌دهنده‌ها باید روی دستگاههای مجزا قرار داشته باشند و از طریق سیستم‌عامل و نرم‌افزارهایی پیکربندی شوند که حداقل قابلیتهای امنیتی روی آنها فعال است. متصدیان باید در خصوص تغییرات آگاه باشند، با وصله‌ها خود را به روز نگهدارند، و منتظر حوادث غیرمنتظره باشند. انجام صحیح این موارد نیاز به درک عمیقی از چگونگی عملکرد سیستم و دلایل عملکرد ناصحیح آن دارد. این رویکردی است که در بخشهای بعدی این کتاب دنبال می‌شود.

76 *Best Practices*
77 *Due Care*

فصل پنجم
پیشگیری و سیاست امنیت سازمانی

کلیات

این فصل بطور کامل به تشریح سطوح مختلف سیاست امنیتی می‌پردازد؛ که در آن هر کارمند سازمان در امنیت رایانه‌ها، شبکه‌ها و اطلاعات نقشی برای ایفا کردن دارد. فهرستهای کنترل مدیریتی که در این قسمت مورد اشاره قرار گرفته‌اند را می‌توانید در فصول انتهایی همین بخش از کتاب بیابید.

امنیت در یک سازمان درحال فعالیت

امنیت رایگان نیست. هر چقدر که معیارهای امنیتی شما گسترده‌تر شوند، به همان میزان هزینهٔ آنها بالاتر خواهد رفت. استفاده از سیستمهایی که از امنیت بالاتری بهره می‌برند معمولاً دشوارتر است. همچنین امنیت ممکن است از جانب کاربران قدرتمند – که می‌خواهند فعالیتهای سخت و بعضاً خطرناکی انجام دهند اما غالباً مجاز به انجام آن نیستند و در قبال پیامدهای آن نیز پاسخگو نمی‌باشند – مورد تهدید واقع شود. بعضی از این کاربران ممکن است در سازمان از قدرت سیاسی بهره‌مند باشند. از طرف دیگر، بعضی از سازمانها ممکن است احساس کنند که تأمین امنیت سازمان در یک سطح مناسب بسیار پرخرج می‌باشد و به همین دلیل بدون صرف وقت برای ارزیابی هزینه‌های واقعی این خطرات و بدون توجه به ملاحظات امنیتی فعالیت خود را ادامه دهند. در انتهای بخش سوم مجموعه‌ای از فهرستهای کنترل ارائه شده‌اند که گامهای لازم برای حصول اطمینان از تأمین حداکثر ایمنی در سطوح مختلف را با توجه به محدودیتهای زمانی، پرسنلی و مالی تشریح می‌کنند.

پس از اتمام ارزیابی مخاطره و تحلیل سود و زیان، شما باید مدیریت سازمان را متقاعد کنید که طبق برنامه عمل نمایند. در حالت عادی برای اینکار یک سیاست تدوین می‌شود که باید رسماً مورد تبعیت قرار گیرد. معمولاً انجام این فرآیند یک پیکار دشوار است. هدف از انجام ارزیابی مخاطره و تحلیل سود و زیان اولویت‌بندی اقدامات و نحوهٔ صرف هزینه‌های امنیتی شما است. اگر برنامهٔ تجاری شما طوری باشد که طبق آن نباید در طول سال مخاطرهٔ بیمه‌نشده‌ای داشته باشید که هزینهٔ آن از یک مقدار مشخص بالاتر باشد، می‌توانید از ارزیابی مخاطره استفاده کنید تا متوجه شوید برای رسیدن به این هدف باید چه هزینه‌هایی را متحمل شوید. این ارزیابی همچنین می‌تواند شما را راهنمایی کند که کدام گام را اول و کدام گام را دوم بردارید، و چه کارهایی را به سالهای بعد موکول کنید. یک فایدهٔ دیگر ارزیابی مخاطره این است که مدیریت شرکت متقاعد می‌شود که شما برای برقراری امنیت نیاز به منابع بیشتری دارید.

غالب مدیران دربارهٔ رایانه‌ها اطلاعات مختصری دارند، ولی ارزیابی مخاطره و تحلیل سود و زیان را درک می‌کنند. اگر بتوانید نشان دهید که سازمان درحال حاضر با مخاطره‌ای مواجه است که می‌تواند باعث هزینه‌های سالانهٔ زیادی شود (برای این منظور مجموع خسارتها و هزینهٔ تعمیرات همهٔ آنچه هم‌اکنون مورد استفاده قرار دارد را محاسبه کنید)، آنگاه ممکن است این برآورد مدیریت را متقاعد کند که برای اجتناب از وقوع مخاطرات، روی منابع و کارکنان سرمایه‌گذاری بیشتری نمایند.

از طرف دیگر اگر با سخنان مبهمی مثل "احتمال زیادی وجود دارد که بعد از اعلامیهٔ بعدی CERT/CC روی اینترنت نفوذهای متعددی رخ دهد" به مدیریت مراجعه کنید، بسیار بعید است که نتیجه‌ای جز یک نگرانی بسیار ملایم (آن هم تنها در بعضی موارد) به بار بیاید!

نقش سیاستهای امنیتی

سیاست امنیتی به تعریف سرمایه‌های سازمان کمک می‌کند و نیز گامهایی که لازم است برای حفاظت از این سرمایه‌ها برداشته شود را مشخص می‌نماید.

سیاستهای امنیتی را به چند روش متفاوت می‌توان تدوین کرد. می‌توانید یک سیاست کلی بسیار سادهٔ چند صفحه‌ای بنویسید که بیشتر احتمالات را درنظر گرفته باشد. همچنین می‌توانید برای هریک از دارائیهای مختلف یک سیاست

خاص تدوین کنید؛ مثل سیاست پست‌الکترونیکی، سیاست داده‌های کارکنان و سیاست اطلاعات حسابهای کاربری. سومین رویکردی که بسیاری از شرکتها از آن بهره جسته‌اند و برای تمامی شرکتها با اندازه‌های مختلف قابل اجرا است داشتن سیاستها، استانداردها و خط‌مشی‌های ساده و مختصر است که با الگوهای سرآمدی بهبود یافته‌اند. در ادامه، رویکرد آخر را بطور خلاصه تشریح خواهیم کرد و منابع بیشتر در این رابطه نیز در بخش مراجع معرفی شده‌اند.

سیاست سه نقش عمده ایفا می‌کند. اول مشخص می‌کند از چه چیزی حفاظت می‌شود و چرا؛ دوم اینکه مسئولیت مربوط به تأمین این حفاظت را مشخص می‌نماید؛ و سوم اینکه زمینه‌ای برای تفسیر و حل درگیریهایی که ممکن است در آینده بوجود بیاید ارائه می‌دهد. آنچه که در سیاست نباید بیاید عبارت است از فهرست تهدیدها، ماشین‌آلات و افراد (با نامهایشان). سیاست باید کلی باشد و در طول زمان بندرت دچار تغییر شود.

استانداردها

از استانداردها برای معرفی راهکارهای موفقیت‌آمیز امنیت در یک سازمان استفاده می‌شود و در عبارتهای آن معمولاً از فعل "باید" استفاده می‌گردد. استانداردها عموماً مستقل از بسترهای مختلف فنی تهیه می‌شوند و حداقل یک معیار برای تعیین اینکه آیا رعایت شده‌اند یا نه را معرفی می‌نمایند. استانداردها برای پشتیبانی از سیاست پدید آمده‌اند و در طول زمان به آهستگی تغییر می‌کنند. استانداردها ممکن است دربرگیرندهٔ مطالبی باشند مانند اینکه استخدامهای جدید باید چگونه انجام شوند، از نسخهٔ پشتیبان باید تا چه مدتی نگهداری بعمل آید، و اینکه سیستمهای UPS چگونه مورد آزمایش قرار می‌گیرند.

بعنوان مثال یک استاندارد در مورد نسخه‌های پشتیبان را درنظر بگیرید. ممکن است در آن اینگونه آمده باشد:

> پشتیبانها باید از تمام داده‌های اینترنتی و نرم‌افزاری و بر اساس یک برنامهٔ منظم زمانی تهیه شوند. در هیچ صورتی عملیات عادی پشتیبان‌گیری نباید کمتر از یکبار در هر هفتاد و دو ساعت انجام شود. همهٔ پشتیبانها باید حداقل برای یک دورهٔ شش ماهه حفظ شوند؛ و از اولین پشتیبان ماههای ژانویه و ژوئن هر سال در یک محل امن در خارج از سازمان برای همیشه مراقبت به عمل می‌آید. حداقل یک هفته در میان باید یک پشتیبان کامل از کل سیستم تهیه شود. همهٔ رسانه‌های پشتیبان‌گیری باید در نوع خود واجد استانداردهای پذیرفته‌شدهٔ صنعتی باشند تا حداقل بعد از پنج سال باقی‌ماندن در یک انبارِ بدون مراقب، اطلاعات روی آنها باز هم قابل بازیابی باشد.

این استاندارد نام هیچ مکانیزم پشتیبان‌گیری یا بستهٔ نرم‌افزاری خاص را ذکر نمی‌کند؛ هرچند آن چیزی که باید ذخیره شود و اینکه برای چه مدت باید ذخیره گردد و چند وقت یکبار باید اینکار انجام گیرد را بوضوح عنوان می‌نماید.

یک استاندارد معقول برای تصدیق هویت را درنظر بگیرید:

> در یک رایانهٔ چندکاربره هر حساب کاربری باید تنها یک کاربر مجاز برای استفاده داشته باشد. آن کاربر باید هویت خود را با استفاده از یک نشانهٔ تأییدکننده برای سیستم اثبات نماید. اثبات هویت برای رایانه را می‌توان بوسیلهٔ یک *نشان تصدیق هویت*[78]، یک *کارت هوشمند*[79]، یک رمز عبور یکبار مصرف، یا یک *معیار زیستی*[80] تأییدشده صورت داد. در هیچ دستگاه رایانه‌ای که تاکنون به شبکه وصل شده، قابل حمل به خارج از شرکت بوده، یا بیرون از دفتر خصوصی مورد استفاده قرارگرفته، نباید از رمزهای عبور تکرارشدنی بعنوان مکانیزم اصلی تصدیق هویت استفاده کرد.

راهبردها

راهبردها (خط‌مشی‌ها) اسنادی هستند که معمولاً در آنها فعل "بهتر است" بکار می‌رود. هدف راهبردها تفسیر استانداردها برای یک محیط خاص- یک محیط نرم‌افزاری یا یک محیط فیزیکی – می‌باشد. برخلاف استانداردها، راهبردها درصورت نیاز تغییر می‌کنند. این اجزای سیاست، همانطور که از نامشان پیداست، معمولاً مثل استانداردهای کارایی مورد استفاده قرار نمی‌گیرند، بلکه بصورت راههایی که به انجام کار کمک می‌کنند بکار می‌روند.

ذیلاً یک نمونه راهبرد در مورد نسخه‌های پشتیان آمده است:

78 *Authentication Token*
79 *Smart Card*
80 *Biometic*

پشتیبانها در ماشینهای مبتنی بر یونیکس باید با استفاده از برنامهٔ "dump" تهیه شوند. تهیهٔ پشتیبان از سیستمهایی که در ۲۴ ساعت شبانه‌روز از آنها استفاده نمی‌شود باید در طول شب و در حالت تک‌کاربره انجام شود. تهیهٔ پشتیبان از سیستمهایی که ۲۴ ساعته درحال فعالیت هستند باید در زمان نزدیکترین تغییر شیفت کاری به نیمه‌شب صورت بگیرد (زمانی که بار کاری سیستم از همیشه کمتر است). تمام نسخه‌های پشتیبان بلافاصله پس از نوشته شدن باید مجدداً خوانده شوند تا صحت اطلاعات نوشته‌شده به تأیید برسد.

در اولین پشتیبان‌گیری ماههای ژانویه و ژوئن، *پشتیبان سطح صفر*[۸۱] تهیه می‌شود. پشتیبان‌گیری سطح ۳ باید در اول و پانزدهم هر ماه صورت بگیرد. پشتیبان‌گیری سطح ۵ باید شبهای هر دوشنبه و پنج‌شنبه انجام شود، مگر اینکه پشتیان سطح صفر یا ۳ در همانروز انجام شده باشد. پشتیبان سطح ۷ باید یک شب در میان تهیه شود، مگر در ایام تعطیلات.

راهبر سیستم در هر هفته یک فایل را بصورت تصادفی از یک پشتیبان که در همان هفته تهیه شده انتخاب می‌کند تا کارمند بخش پشتیبان‌گیری برای کسب اطمینان از عملکرد صحیح روالهای تهیهٔ نسخهٔ پشتیبان، آن فایل را از روی پشتیبانها بازیابی کند.

راهبردها برای معماریهای خاص و دستگاههای ویژه تهیه می‌شوند؛ و نسبت به استانداردها در بازه‌های کوتاهتری تغییر می‌کنند تا بتوانند شرایط متغیر را بصورت صحیح منعکس کنند.

نکات کلیدی در تدوین یک سیاست کارآ

نقش سیاست (و استانداردها و راهبردهای مربوطه) کمک به حفاظت از مواردی است که رویهمرفته برای شما مهم تلقی می‌شوند. در بیشتر موارد لزومی ندارد سیاستی که بکار می‌رود ویژه و پیچیده باشد. گاهی اوقات یک قانون ساده برای تمام سیاست محیط شما کافی است، مانند مثال زیر:

استفاده و حفاظت از این سیستم وظیفهٔ همه می‌باشد. تنها کارهایی انجام دهید که مایلید دیگران هم آنرا انجام دهند. به حریم خصوصی کاربران دیگر احترام بگذارید. چنانچه با مشکلی روبرو شدید سعی کنید آنرا یا خودتان رفع کنید و یا سریعاً گزارش نمایید. به قوانین مربوط به کاربرد سیستم احترام بگذارید. مسئولیت کارهای خود را بپذیرید و همیشه خود را معرفی کنید. از کارتان لذت ببرید.

گاهی اوقات نیز لازم است یک سیاست رسمی‌تر که توسط یک متخصص رسمی و چند مشاور امنیتی بازبینی شده را برای حفاظت از دارائیهایتان بکار برید. سیاست هر سازمان با سازمان دیگر تفاوت دارد؛ چراکه همواره برای هر سازمان ملاحظات خاصی وجود دارد که لازم است بطور مجزا در سیاستهای تدوین‌شده مورد اشاره قرار گیرند.

تخصیص یک مسئول

هر جزء اطلاعات و تجهیزات که باید مورد محافظت قرار گیرد باید یک مسئول معین داشته باشد. "مسئول" کسی است که در قبال نسخه‌برداری، از بین رفتن، پشتیبان‌گیری و سایر جنبه‌های حفاظت از اطلاعات مسئولیت دارد. او همچنین یکی از کسانی است که مجاز است به اطلاعات دسترسی داشته باشد.

مشکل امنیت در بسیاری از سازمانها این است که اطلاعات مهمی وجود دارد که مسئول مشخصی ندارد. درنتیجه کاربران نمی‌دانند چه کسی دربارهٔ ذخیره‌سازی اطلاعات تصمیم می‌گیرد یا چه کسی ضوابط دسترسی به اطلاعات را تدوین می‌نماید. بعضی اوقات اطلاعات (و همچنین تجهیزات) بدون اینکه کسی متوجه شود برای مدتی طولانی ناپدید می‌شوند؛ چراکه کسی مسئول آنها نیست که شرایط را کنترل کند.

مثبت باشید

افراد به جملات مثبت و اثباتی بهتر از جملات منفی و عبارات نفی‌کننده واکنش نشان می‌دهند. بجای تهیه لیستهای طویل از عبارتهای "اینکار را انجام ندهید"، ببینید که چگونه می‌توانید همان ضوابط را بصورت مثبت جمله‌بندی نمایید. سیاست خلاصهٔ قبلی را می‌توان بصورت مجموعه‌ای از "نبایدها" مطابق زیر تهیه کرد؛ اما ببینید که همان

81 *Level 0 dump*

عبارتهای قبلی چقدر راحت‌تر خوانده می‌شدند:

> این وظیفهٔ شماست که اجازه ندهید از سیستم استفادهٔ نادرست بشود. کارهایی که دوست ندارید دیگران انجام دهند را انجام ندهید. حریم خصوصی دیگران را خدشه‌دار نکنید. اگر مشکلی پیدا کردید و نتوانستید آنرا برطرف کنید، مشکل را مخفی نگه ندارید. قوانین مربوط به استفاده از سیستم را نقض ننمایید. سعی نکنید مسئولیت کارهای خود را به گردن دیگران بیندازید؛ و هویت خود را نیز پنهان ننمایید. امیدواریم اوقات بدی نداشته باشید!

وقتی سیاستها را می‌نویسید، همواره رفتار کاربران را در ذهن خود داشته باشید. آنها دچار اشتباه می‌شوند و از نکات، تعبیرِ نادرست می‌کنند. سیاست شما نباید طوری باشد که درصورت اشتباه کاربران، آنان را مستحق هر مجازاتی بداند.

از این گذشته درنظر بگیرید که سیستمهای اطلاعاتی ممکن است شامل داده‌هایی در مورد کاربران باشند و کاربران بخواهند تا حدودی آن اطلاعات را خصوصی نگهدارند. این اطلاعات خصوصی می‌تواند شامل نامه‌های الکترونیکی، سوابق شخصی و ارزشیابیهای شغلی باشد. پس این اطلاعات نیز باید مورد محافظت قرار گیرند؛ هرچند شاید نتوانید خصوصی ماندن آنها را تضمین کنید. خلاصهٔ مطلب اینکه از نیازها و احساسات کاربران غافل نشوید.

بر آموزش و آگاهی تمرکز کنید

می‌توانید استانداردها را در برنامهٔ آموزش و بازآموزی کلیهٔ کاربران قرار دهید. هر کاربر باید آگاهی اولیه‌ای در مورد امنیت داشته باشد، و سپس آن مطالب باید در یک برنامه و قالب مشخص برای وی یادآوری شوند (حتی اگر برنامهٔ یادآوری تنها شامل ارائه نسخه‌ای از این کتاب به کارکنان باشد!). احتمال گرفتارشدن کاربران آموزش‌دیده در ترفندها و خصوصاً حملات مهندسی اجتماعی کمتر است. همچنین اگر کاربران بدانند که هریک از معیارهای امنیتی چرا مورد استفاده قرار گرفته‌اند، در آنصورت احتمال بیشتری وجود خواهد داشت که از آنها احساس رضایت کنند و هریک را بدرستی اجرا نمایند.

یک بخش حیاتی هر سیستمِ امنیت، اعطای زمان و فراهم کردن پشتیبانی برای تحصیل و آموزش بیشتر کارکنان است. همواره ابزارهای نو، تهدیدات جدید، روشهای نوین، و اطلاعات تازه برای یادگیری وجود دارد. اگر کارمندان هفته‌ای ۶۰ ساعت صرف یافتن ویروسهای خیالی رایانه‌های شخصی و تهیهٔ نسخه‌های پشتیبان کنند، بازهم به اندازهٔ کارمندانی که سالانه تنها به مدت چند هفته تحت آموزش قرار می‌گیرند کارآیی ندارند. از این گذشته اگر به آنها فرصت ترقی و یادگیری در طول مدت کار داده شود و اجازه داشته باشند بجای نصب نرم‌افزارها و پشتیبان‌گیری، عصر هر روز و تعطیلات آخر هفته را با خانواده‌هایشان سپری کنند، از کارهایشان خرسندتر و راضی‌تر خواهند بود.

اختیارات را متناسب با مسئولیتها توزیع کنید. یک اصل در راهبری امنیت می‌گوید:

اگر مسئولیتی در رابطه با امنیت دارید ولی اختیاری برای قانونگذاری و تنبیه متخلفین به شما داده نشده است، هنگام وقوع یک مشکل بزرگ این شما هستید که سرزنش می‌شوید.

هر چند اصل بالا در بیشتر موارد برقرار است، اما مسئولیت واقعی متوجه کسی است که اختیارات را متناسب با مسئولیتها توزیع نکرده است.

این بخش شامل فهرستهای کنترل مدیران و کارکنانی است که مسئولیت امنیت با آنها است. در این بخش به عوامل مهم طرح امنیت هر سازمان شامل ارتباطات، آگاهی، آموزش و سرمایه‌گذاری مناسب برای حمایت از طرح می‌پردازیم.

مطمئن شوید که محیط امنیتی خود را می‌شناسید

هنگامیکه سیاست خود را تدوین می‌نمایید، باید اطمینان حاصل کنید که انواع مختلف سیستمها، شبکه‌ها، کارکنان و رسانه‌های ذخیره‌سازی موجود در محیط امنیتی خود را می‌شناسید و همهٔ آنها را درنظر گرفته‌اید. این شناخت، آنچه باعث نگرانی شماست را تعریف می‌کند. وقتی سیاستها را تدوین می‌کنید، باید اطمینان حاصل کنید که تمام آنچه که در محیط شماست و یا می‌تواند به محیط شما وارد شود و با منابع اطلاعاتی شما تعامل داشته باشد را از قلم نیانداخته‌اید. بسیاری از سازمانها در سالهای گذشته محیط امنیت فناوری اطلاعات خود را با همان مرزهای بوجودآمده بوسیلهٔ دیوارها و نرده‌ها تعریف می‌کردند؛ اما امروزه محیطهای سازمانی

بندرت اینقدر ایستا هستند.

هنگام تدوین سیاستهای خود باید نکاتی مثل موارد زیر را درنظر بگیرید:

- هنگامیکه از موقعیت فیزیکی خود دور هستید می‌توانید برای دستیابی به اطلاعات از رایانه‌های قابل حمل و PDAها استفاده کنید. این وسایل می‌توانند اطلاعات حساسی مثل آدرسهای IP، شماره‌های تلفن و رمزهای عبور را در خود ذخیره کنند. این سیستمها باید دارای امنیت حداقلی باشند؛ مثلاً با استفاده از رمزگذاری و یا حداقل نشانهایی برای برقراری امنیت فیزیکی. کاربران باید در رابطه با خطرات دزدی و استراق‌سمع آگاه و آموزش‌دیده باشند.

- شبکه‌های بی‌سیم که در ساختمانها مورد استفاده قرار می‌گیرند یا به تجهیزات سایت متصل می‌شوند، می‌توانند با استفاده از آنتنهای جهتدار یا پارک کردن یک ماشین خارج از ساختمان و استفاده از یک رایانهٔ کیفی در داخل ماشین مورد استفادهٔ افراد بیرونی قرار بگیرند. شبکه‌های بی‌سیم باید طوری پیکربندی و حفاظت شوند که اطلاعات حساس آنها در خارج از سایت قابل شناسایی نباشند و از ورود قطعه‌برنامه‌های مخرب مهاجمین به آنها جلوگیری گردد.

- رایانه‌هایی که توسط کارکنان سازمان در منازل مورد استفاده قرار می‌گیرند ممکن است در معرض خطر نفوذ، دزدی، و ورود قطعه‌برنامه‌های مخرب باشند و همچنین ممکن است برخلاف سیاستهای سازمان مورد استفاده قرار گیرند (مثلاً برای راه‌اندازی یک تجارت مستقل و یا میزبانی یک سرویس‌دهندهٔ وب با محتویات سؤال برانگیز). سیاست باید مشخص کند که این رایانه‌ها چگونه باید مورد استفاده، حفاظت و بازبینی قرار گیرند.

- رسانهٔ ذخیره‌سازی معمولاً قابل حمل و فشرده است. اگر کسی یک نسخه از سوابق مالی شرکت را برای استفاده در یک سایت راه دور روی دیسک فشرده یا DVD بریزد، درصورت دزدیده یا جابجا شدن آن رسانه چه اتفاقی خواهد افتاد؟ سیاستها باید مشخص کنند که چه کسی می‌تواند یک رسانه را به بیرون از محوطه ببرد، با چه روشهایی باید از این اطلاعات محافظت کرد (که این امر شامل رمزگذاری هم می‌شود) و اگر آن رسانه دزدیده یا گم شود چه اقداماتی باید انجام داد. همچنین لازم است بطور مشروح بیان شود رسانه‌ای که قبلاً مورد استفاده قرار گرفته چگونه باید از بین برود تا احتمال خطرهای ناشی از افشای اطلاعات روی آن کاهش یابد.

و سعی کنید برای پرسشهای زیر پاسخهای مناسبی داشته باشید:

- کدام سیاستها به کسانی می‌پردازند که PDAها و رایانه‌های کیفی خود را برای ملاقاتها و یا صرفاً در بازدیدها به محل کار می‌آورند؟ ضوابط اتصال آنها به شبکه‌ها، خطوط تلفن، چاپگرها و سایر ابزارهای محل کار چیستند؟

- چه ملاحظاتی برای حمل رایانه‌ها یا تجهیزات ذخیرهٔ اطلاعات به خارج از محل کار (مثلاً برای تعمیرات) اتخاذ شده است؟ اگر روی دیسکها اطلاعات حساس وجود داشته باشد چه خواهد شد؟ در مورد تجهیزات اجاره‌ای که مجدداً به صاحبانشان عودت داده می‌شوند چه راهبردی اتخاذ شده است؟

- اگر شرکای تجاری یا پیمانکاران به وسایل شما دسترسی داشته باشند – خواه در محل کار شما یا محل کار خودشان – چه کسی از اطلاعات حفاظت خواهد کرد؟ چگونه از اختلاط ناخواستهٔ داده‌های حساس خود با داده‌های آنها جلوگیری می‌کنید؟

- چه سیاستهایی به اطلاعاتی که تحت گواهی "اسرار تجاری" برای سازمان شما فرستاده شده‌اند می‌پردازند؟ چه کسی مسئول حفاظت از اطلاعات است و کجا می‌توان از آن اطلاعات نگهداری کرد؟

- چه سیاستهایی بر تجهیزات غیررایانه‌ای پردازش اطلاعات حاکم هستند؟ بعنوان مثال چه سیاستهایی برای استفاده از چاپگرها، دستگاههای کپی و ماشینهای دورنگار تدوین شده‌اند؟ (توجه داشته باشید که اطلاعات حساسِ کاغذی نسبت به اطلاعات حساس رایانه‌ای از اهمیت یکسانی برخوردار است)

فکر کردن به همهٔ این مسائل قبل از وقوع هر مشکلی کمک می‌کند که بتوان از وقوع آن مشکل جلوگیری کرد. تهیهٔ عبارتهای بامعنی در سیاست امنیتی به همه کمک می‌کند نگرانیها را بفهمند و مکانیزمهای صحیح پیشگیری را بکار بندند.

برای مسائل امنیتی یک رویکرد پایه اتخاذ کنید

ابتدا ببینید که می‌خواهید طبق کدام الگوی زیر عمل کنید: "هرچه صراحتاً ممنوع اعلام نشده باشد مجاز است" یا "هرچه صراحتاً مجاز دانسته نشده باشد ممنوع است". سپس ببینید موارد دیگر را چگونه می‌خواهید تعریف کنید. ممکن است مورد اول با یک محیط تقریباً باز سازگار باشد، مثل یک دانشگاه؛ درحالیکه مورد دوم بیشتر برای یک مؤسسهٔ تجاری مناسب است، مانند یک بانک.

دفاع در عمق

وقتی برای سیاست و روشهای مقابلهٔ خود برنامه‌ریزی می‌کنید، در یک لایه متوقف نشوید و برای دفاع در برابر تهدیدات مختلف، چند سطح حفاظتی همپوشان و مستقل بنا نمائید. سپس نظارت و بازبینی را نیز به آن مجموعه بیافزایید تا مطئمن شوید که اجرای سیاستهای اتخاذشده، در عمل نیز واقعاً جواب می‌دهد. احتمال گریز یک مهاجم از تنها یک مجموعهٔ دفاعی بسیار بیشتر از احتمال گریزش از مثلاً سه مرحلهٔ دفاعی بعلاوهٔ یک سیستم اخطار می‌باشد.[۸۲]

ضمانت اجرایی، و بازبینی‌های امنیتی

تدوین سیاست به تنهایی کافی نیست، بلکه باید مرتباً بررسی شود که آیا سیاست اتخاذ شده بصورت صحیح اعمال می‌شود یا نه، و اگر اعمال می‌شود آیا کافی و صحیح است یا خیر. واژهٔ *ممیزی*[۸۳] بار معنایی جدیدی پیدا کرده و درحال حاضر حداقل در معانی ممیزی مالی، دنباله‌های ردگیری (با استفاده از فایلهای ثبت)، بازبینی امنیتی یک سیستم، و بازبینی رعایت سیاست بکار می‌رود.

یک ممیزیِ *رعایت سیاست*[۸۴] عبارت است از اقداماتی که انجام می‌شود تا مشخص گردد آیا استانداردهای ذکرشده در سیاست رعایت می‌شوند یا نه، و اگر نمی‌شوند دلیل آن چیست. استانداردها معمولاً معیارها و روشهایی برای سنجیده‌شدن خود نیز بدست می‌دهند که می‌تواند توسط یک ممیز برای اندازه‌گیری رعایت‌شدن یا نشدن آن استاندارد مورد استفاده قرار گیرد. اگر استانداردها رعایت نشده باشند، این امر می‌تواند نتیجهٔ هر ترکیبی از موارد زیر باشد:

- کوتاهی کارکنان؛
- آموزش ناکافی و فقدان مهارتهای لازم؛
- کار زیاد؛
- نقص امکانات؛
- نداشتن انگیزهٔ لازم؛
- کمبود وسایل کافی؛
- منابع ناکافی یا نامناسب؛
- تعمیرات و پشتیبانی ناکافی؛
- کاربرد یا بارگذاری بیش از حد؛
- نارسائیهای سازمانی؛
- بی‌مسئولیتی؛
- تداخل مسئولیتها؛
- تقسیم کار نامشخص، ناهماهنگ و گیج‌کننده؛
- نارسائیهای سیاست؛
- مخاطرات پیش‌بینی نشده؛
- سیاستهای ناقص یا از قلم افتاده؛
- سیاستهای متداخل؛ و
- ناسازگاری سیاست و محیط.

نکتهٔ کلیدی در فهرست بالا این است که مشکلات سیاست را نمی‌توان ناشی از خطای کاربران یا راهبران دانست. حتی آموزش ناکافی یا اضافه‌کار بیش از حد عموماً در اختیار راهبران نیست. بنابراین یک ممیزیِ رعایت نباید بعنوان یک فرآیند نامطلوب دیده شود؛ بلکه باید به آن بصورت یک تلاش همگانی برای تشخیص مشکلات، یافتن و تخصیص مجدد منابع، پالایش سیاستها و استانداردها، و افزایش آگاهی در زمینهٔ نیازهای امنیتی نگریست. مشابه همهٔ قسمتهای

۸۲ *مراجعه کنید به منبع زیر، نوشتهٔ Tom Kellermann:*
"The 12 Layer Matrix: Building a Cyber-Fortress (2003)": http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/SearchGeneral?openform&E-Security/E-Finance&Tools

83 Audit

84 Compliance Audit Policy

دیگر امنیت، اینجا نیز رویکرد گروهی در اکثر قریب به اتفاق شرایط مؤثرترین رویکرد است. اگر مسئله بطور صحیح مدیریت شود، کارکنان می‌توانند به امنیت مطلوب دست یابند. نکتهٔ کلیدی این است که به آنها در انجام کارهایشان کمک کنیم، نه اینکه خود را در طرف دیگر میز و در مقابلشان قرار دهیم.

اشکلات امنیت مبتنی بر جهل مهاجم

در مکانیزمهای سنتیِ امنیت که عمدتاً از سازمان اطلاعات ارتش نشأت می‌گرفت یک مفهوم با عنوان "نیاز به دانستن" وجود داشت. اطلاعات تقسیم‌بندی می‌شد و به هر کس آنقدر از آن تخصیص می‌یافت که بتواند با آن به وظایفش عمل کند. در محیطهایی که قسمتهای خاصی از اطلاعات از حساسیت برخوردارند یا *امنیت استنباطی*[۸۵] باید برقرار باشد، این سیاست از معنای خاصی برخوردار است. اگر سه قطعهٔ اطلاعاتی در کنار هم بتوانند یک نتیجهٔ مخرب به بار بیاورند ولی هیچکس به بیش از دو قطعه از آن اطلاعات دسترسی نداشته باشد آنگاه می‌توان گفت که امنیت تضمین شده است.

در یک محیط عملیات رایانه‌ای بکار گرفتن مفهوم "نیاز به دانستن" معمولاً مناسب نیست. این مسئله بویژه در شرایطی صدق می‌کند که شما امنیت خود را بر این مبنا قرار داده باشید که یک مسئله فنی برای مهاجمان نادانسته باشد. اتکا به جهل مهاجمین می‌تواند به ایمنی شما خدشه وارد کند.

محیطی را درنظر بگیرید که در آن مدیریت تصمیم می‌گیرد کتابچه‌های راهنما را از دسترس کاربران دور نگه دارد تا اجازه ندهد در مورد فرامین و گزینه‌هایی که ممکن است با آنها بتوان به سیستم خدشه وارد کرد مطلبی بیاموزند. در چنین شرایطی مدیران ممکن است بر این باور باشند که بدینوسیله امنیت خود را افزایش داده‌اند، اما در واقع اینطور نیست. یک مهاجم مصمم می‌تواند این اسناد را جای دیگری پیدا کند – از طریق کاربران یا ادارات دیگر. مقادیر فراوانی از این اسناد در فاصله‌ای کمتر از نزدیکترین کتابفروشی به هر اداره موجود هستند! مدیریت نمی‌تواند همهٔ راههای یادگیری در مورد سیستم را ببندد. ضمن اینکه کاربران محلی به این دلیل که نمی‌توانند اسناد را ببینند و در مورد گزینه‌های کارآتر مطلب بیاموزند، ممکن است از دستگاهها بهرهٔ بسیار کمی ببرند. همچنین ممکن است انگیزهٔ ایشان تضعیف شود، چراکه پیام ضمنی مدیریت با انجام اینکار این است که "ما به شما اعتماد کامل نداریم که یک کاربر مسئولیت‌شناس باشید". از این گذشته در چنین شرایطی اگر کسی به سوء استفاده از فرامین و ویژگیهای سیستم بپردازد، ممکن است مدیریت توانایی کافی برای شناخت و مبارزه با مشکل را نداشته باشد؛ و اگر مسئله‌ای برای یک یا دو نفر از کاربران که مجاز به دسترسی به اسناد بوده‌اند رخ دهد، دیگر کسی با تجربه یا اطلاعات لازم وجود ندارد که در مواقع بروز مشکلات همیاری کند.

محرمانه نگهداشتن اشکالات یا قابلیتها برای ایجاد حفاظت در مقابل آنها نیز یک رویکرد ضعیف امنیتی است. نویسندگان نرم‌افزار معمولاً در برنامه‌هایشان درب مخفی قرار می‌دهند که به آنها اجازه می‌دهد بدون ارائه رمز عبور، امتیازات دسترسی بدست بیاورند. گاهی نیز اشکالات سیستم با عوارض عمیق امنیتی همچنان باقی می‌مانند، چراکه مدیر تصور می‌کند کسی از آنها اطلاع ندارد. مشکل این رویکردها این است که احتمال زیادی وجود دارد که مشکلات و ویژگیهای موجود در برنامه بصورت تصادفی و یا بوسیلهٔ یک نفوذگر مصمم کشف شوند. مخفی نگهداشتن اشکالات و ویژگیها به این معنی است که مورد مشاهده قرار نمی‌گیرند و طبیعتاً اصلاح‌نشده باقی می‌مانند. لذا پس از آنکه کشف شدند، وجود مشکل باعث می‌شود تمام سیستمهای مشابه نسبت به حملهٔ افرادی که مشکل را کشف کرده‌اند آسیب‌پذیر باشند.

ارزش مخفی نگهداشتن الگوریتمها – مثلاً یک الگوریتم انحصاری رمزگذاری – نیز قابل بحث است. تا زمانیکه یک متخصص *رمزنگاری*[۸۶] نباشید نمی‌توانید قدرت الگوریتم را تشخیص دهید. نتیجه ممکن است مکانیزمی باشد که دارای نقایص جدی است. الگوریتمی که مخفی نگهداشته می‌شود طبیعتاً توسط دیگران مورد بررسی قرار نمی‌گیرد و لذا هر کسی که اشکالی در آن بیابد خواهد توانست بدون اطلاع شما به داده‌هایتان دسترسی پیدا کند.

بطور مشابه محرمانه نگهداشتن متن برنامهٔ سیستم‌عامل یا

85 *Inferential Security*

86 *Cryptography*

برنامه‌های کاربردی نیز هیچ تضمینی برای تأمین امنیت بوجود نمی‌آورد. کسانیکه تصمیم گرفته باشند به سیستم شما وارد شوند هر از چندگاه حفره‌های امنیتی را پیدا می‌کنند؛ مستقل از اینکه متن برنامه را در اختیار داشته باشند یا نداشته باشند.[۸۷] اما بدون دسترسی به متن برنامه، کاربران نمی‌توانند آنرا بطور مدون بررسی کنند تا مشکلات آنرا بیابند؛ و لذا هرچند ممکن است با مخفی نگهداشتن متن برنامه مزیت کوچکی بوجود بیاید، اما امنیت نباید به این مخفی‌بودن وابستگی داشته باشد.

نگرش به مقولهٔ امنیت یک نکتهٔ کلیدی است. درصورت خدشه‌دار شدن محرمانگی آندسته از اقدامات دفاعی که بر مبنای مخفی‌کاری استوارند همگی ارزش خود را از دست خواهند داد. حتی بدتر از آن اینکه تداوم محرمانگی باعث جلوگیری یا محدود شدن بازبینی و نظارت بر برنامه می‌شود و ممکن است هرگز نتوان فهمید که آیا این محرمانگی خدشه‌دار شده است یا خیر. بوسیلهٔ الگوریتمها و مکانیزمهایی که ذاتاً مستحکم هستند می‌توان امنیت بیشتری برقرار کرد، حتی اگر مهاجم از آنها آگاهی داشته باشد. این حقیقت که شما از مکانیزمهای مستحکمی استفاده می‌کنید که همه از آن آگاهی دارند ممکن است مهاجم را ناامید کند و باعث شود جای دیگری غیر از سیستمهای شما بدنبال هیجان ناشی از نفوذ باشد. اگر پولهایتان را در یک کشوی قفل‌دار پنهان کنید امنیت آن بیشتر از زمانی است که کسی نداند از پولهایتان در یک قوطی سس مایونز در یخچال نگهداری می‌کنید!

افشای مسئولانه

مقصود از ایرادی که به "امنیت مبتنی بر جهل مهاجم" وارد شد این نیست که بگوییم بلافاصله بعد از اینکه حفره‌های امنیتی را پیدا کردید آنرا بطور گسترده به اطلاع عموم برسانید. میان مخفی‌کاری و احتیاط تفاوتهای عمده وجود دارد. اگر در یک نرم‌افزار توزیع‌شده یا پرمصرف حفرهٔ امنیتی کشف کردید باید بدون سر و صدا و هرچه سریعتر آنرا به توسعه‌دهندهٔ آن نرم‌افزار اطلاع دهید. همچنین توصیه می‌کنیم که آنرا به اطلاع یکی از مؤسسات FIRST (که در ضمیمهٔ ۴ در مورد آنها توضیح داده شده) نیز برسانید. این مؤسسات می‌توانند به توسعه‌دهندگان کمک کنند تا برای حفره‌های امنیتی کشف‌شده وصله‌هایی تهیه نمایند و مطمئن شوند که وصله‌ها توزیع شده و بطور صحیح مورد استفاده قرار گرفته‌اند.

اگر حفرهٔ امنیتی یک نرم‌افزار را در بوق و کرنا کنید، تمام افرادی را که از آن نرم‌افزار استفاده می‌کنند و نمی‌توانند اشکالات آنرا رفع کنند دچار مشکل کرده‌اید. در محیط Unix بسیاری از کاربران عادت کرده‌اند که برای اصلاح اشکالات یک برنامه، در متن آن ایجاد تغییرات کنند.

متأسفانه همه از چنین قابلیتی برخوردار نیستند و بسیاری از مصرف‌کنندگان باید هفته‌ها یا ماهها صبر کنند تا نرم‌افزار به‌روزرسانی‌شده توسط فروشندهٔ مربوطه منتشر شود. بعضی ادارات ممکن است – بدلیل اینکه جز روشن کردن رایانه و کار با نرم‌افزار مورد نیاز کار دیگری با رایانه نمی‌کنند و یا نرم‌افزارشان بر اساس تنظیمات موجود گواهی دریافت کرده و لذا نمی‌توانند پیکربندی آنرا تغییر دهند – حتی قادر به ارتقای نرم‌افزار خود هم نباشند. ممکن است بعضی سیستمها توسط افرادی راهبری شوند که مهارت لازم برای اعمال وصله‌ها را نداشته باشند، و از سایر سیستمها هم استفادهٔ فعال نشود و یا خارج از حیطهٔ پشتیبانی سازمان باشند. همیشه مسئولانه عمل کنید. بهتر است یک وصله را بدون توضیح در مورد زیربنای آسیب‌پذیری مربوطه میان کارکنان توزیع کنیم، تا اینکه بخواهیم به مهاجمان جزئیاتی در مورد روشهای نفوذ به سیستمهای وصله‌نشده ارائه نماییم.

ما موارد زیادی دیده‌ایم که در آن فردی متخصص یک اشکال مهم امنیتی را در یک گروه پست الکترونیکی بسیار عمومی گزارش کرده است. اگرچه هدف این شخص دریافت یک اصلاح سریع از جانب فروشندگان بوده، ولی نتیجهٔ کار موجی از تهاجمات به سیستمهایی شده که راهبران آنها به مطالب آن گروه پستی دسترسی نداشته و یا قادر به اعمال اصلاح ارائه‌شده نبوده‌اند.

اگر هنوز وصله‌ای برای آسیب‌پذیریهای اخیر سیستم شما وجود نداشته باشد، ارسال جزئیات آنها به یک گروه پستی نه‌تنها بسیاری پایگاههای دیگر را به مخاطره خواهد انداخت،

---

۸۷ *تا زمانی که شما همهٔ قسمتهای یک نرم‌افزار را بوسیلهٔ خود و در ایستگاه کاری خودتان توسعه ندهید، افراد مختلفی ممکن است به متن برنامه دسترسی پیدا کرده باشند و این احتمال وجود دارد که متن برنامه تصادفاً یا تعمداً افشا شود.*

بلکه اگر یک نفوذگر از آن اشکال برای نفوذ به سایتهای دیگر استفاده کند، ممکن است در رابطه با خسارتهای وارده علیه شما نیز اقدامات قانونی صورت بگیرد.[۸۸] اگر شما نگران امنیت خود هستید متوجه باشید که جزئی از یک جامعه می‌باشید. در جامعه باید بدنبال تقویت امنیت دیگران هم بود و به یاد داشت که ممکن است روزی هم ما به کمک دیگران نیاز پیدا کنیم.

جمع‌بندی بحث پیشگیری و سیاست

کلید ارزیابی مخاطرهٔ موفق، تشخیص همهٔ تهدیدات ممکن علیه سیستم و دفاع در برابر حملاتی است که از نظر شما احتمال وقوع بیشتری دارند.

اینکه انسان ضعیفترین حلقهٔ امنیتی است به این معنا نیست که باید حفاظت از نقاط ضعف دیگر را به فراموشی سپرد. انسان غیرقابل پیش‌بینی است اما سوء استفاده از یک مودم که رمز عبور ندارد بسیار ساده‌تر از متقاعد کردن یک کارمند کلیدی به دریافت رشوه است. بنابراین هرجا که امکان آن وجود داشته باشد باید از مکانیزمهای تدافعیِ مبتنی بر فناوری استفاده کنیم و امنیت کارکنان خود را با آموزش کاربران و کارکنان بهبود بخشیم. علاوه بر این به دفاع در عمق تکیه می‌کنیم: مراحل چندگانهٔ دفاعی مثل پشتیبانها را بکار می‌بریم تا درصورت ناموفق بودن یک لایه در تأمین دفاع لازم، دچار زیانهای اساسی نشویم. بعنوان مثال یک سیستم جایگزین UPS می‌خریم؛ یا هرچند روی در ساختمان یک قفل مستحکم وجود دارد، قفل جداگانه‌ای روی در ورودی اتاق رایانه قرار می‌دهیم. حقیقت این است که مهاجم می‌تواند بر این ترکیبها نیز غلبه کند، ولی ما هزینهٔ انجام اینکار را برای او بالا می‌بریم؛ آنقدر بالا که شاید بتوانیم او را قانع کنیم که عبور از موانع سیستم ما به دردسرهایی که دارد نمی‌ارزد. در حالت حداقلی می‌توانید امیدوار باشید که آنقدر سرعت مهاجم را کاهش داده باشید که پیش از اینکه دارائیهای مهم از دچار مشکل شوند، سیستمهای نظارت و هشدار، شما را از جریان نفوذ آگاه کنند.

با توجه به این محدودیتها شما باید با اولویتهایی که از قبل روی آنها کاملاً فکر کرده‌اید به سراغ امنیت رایانه‌ای بروید؛ چراکه نمی‌توانید در مقابل تمام تهدیدات ممکن، حفاظت بوجود آورید. گاهی اوقات بجای جلوگیری از وقوع یک مشکل باید اجازه دهید آن مشکل رخ دهد و سپس به رفع آثار آن اقدام کنید. برای مثال در مواجهه با یک قطعی برق ممکن است شرایط طوری باشد که اگر بگذارید سیستمها خاموش و راه‌اندازی مجدد شوند برایتان بسیار ارزانتر از خریداری یک سیستم UPS تمام شود.

موارد دیگری هستند که ممکن است شما در مورد دفاع در مقابل آنها ایدهٔ خاصی نداشته باشید (مثل تهاجم یک بیگانه از فضا)؛ یا به آن سبب که بسیار غیر محتمل هستند، دفاع در مقابلشان بسیار سخت باشد (مثل وقوع یک انفجار هسته‌ای در ۲۰۰ متری مرکز اطلاعات شما) یا بسیار فاجعه‌آمیزتر از آن باشند که بتوان با آنها مقابله کرد (مثل اینکه مدیر شما تصمیم بگیرد که تمام ماشینهای یونیکس را تبدیل به یک سیستم‌عامل معروفتر نماید!). کلید رمز مدیریت خوب، دانستن چیزهایی است که در مورد آنها نگرانی دارید و نیز اینکه هریک از این مسائل تا چه اندازه نگران‌کننده هستند.

تصمیم‌گیری در مورد آنچه که می‌خواهید از آن حفاظت کنید و هزینه‌هایی که ممکن است برای جلوگیری از تلفات آن بدهید را در مقابل هزینه‌های ترمیم ضررهای ناشی از یک رخداد قرار دهید. آنگاه با توجه به این جدول و بر اساس یک فهرست اولویت‌بندی‌شده از اکثر قریب به اتفاق نیازهای حیاتی، تصمیم خود را در مورد فعالیتها و معیارهای امنیتی بگیرید. اطمینان حاصل کنید که در این تحلیل علاوه بر رایانه‌ها، تجهیزات و سرمایه‌های دیگر را نیز درنظر گرفته‌اید؛ و فراموش نکنید که نوارهای پشتیبان، اتصالات شبکه، پایانه‌ها، و مدارک شما همه اجزایی از سیستم هستند و هریک می‌توانند خسارتهایی را به کل سیستم وارد آورند. سلامت کارکنان، ساختمان شرکت، و اعتبار و وجههٔ عمومی آن نیز بسیار حائز اهمیت هستند و باید در محاسبات طرحهای امنیتی درنظر گرفته شوند.

---

۸۸ *هرچند ما هنوز وقوع چنین موردی را ندیده‌ایم، اما وکیلان متعددی به ما گفته‌اند که انتظار دارند موکلانشان انجام چنین کاری را از آنها بخواهند.*

فصل ششم
امنیت کارکنان

کلیات

این فصل بطور خلاصه آندسته از مسائل امنیتی را بررسی می‌کند که از داخل سازمان نشأت می‌گیرند. مسائل امنیتی کارکنان از استخدام و اخراج گرفته تا آموزش و آگاهی آنان نقشی حیاتی در عملکرد پیشگیرانه و دفاعی سازمان دارند.

مخاطرات نشأت‌گرفته از کارکنان؛ تهدیدی پنهان برای سازمان

چند فقره از رخدادهای خبرسازی که طی چند سال اخیر توسط کارکنان سازمانها اتفاق افتاده را درنظر بگیرید:

- *نیک لیسون*[89] یک تاجر سرمایه‌گذار در بانک *بارینگز*[90] شعبهٔ سنگاپور، و *توشیهاید ایگوچی*[91] از دفتر نیویورک بانک *دایوا*[92] هر دو اقدام به سرمایه‌گذاریهای پر مخاطره‌ای کردند که منجر به از دست دادن مقادیر قابل توجهی از سرمایهٔ بانکهایشان شد؛ اما آنها بجای پذیرش شکست، سوابق حسابهای رایانه‌ای را دستکاری کردند و عملاً با انجام اینکار پولِ باز هم بیشتری را برای جبران ضررهای قبلی وارد این قمار نمودند؛ و سرانجام نیز بعد از وارد آوردن بیش از یک میلیارد دلار زیان به هریک از این دو بانک مورد شناسایی قرار گرفتند. در نتیجهٔ این اقدامات بانک بارینگز مجبور به اعلام ورشکستگی شد و بانک دایوا نیز مجوز انجام فعالیت اقتصادی در ایالات متحده را برای همیشه از دست داد.

- در ایالات متحده بعضی سازمانها و افراد علیرغم در اختیار داشتن تأییدیه‌های معتبرِ امنیتی از CIA، FBI و ارتش، اطلاعات طبقه‌بندی شده‌ای را در اختیار روسیه و اسرائیل قرار می‌دادند (مثل *آلدریچ ایمز*[93]، *جاناتان پولارد*[94]، *رابرت هانسون*[95] و *رابرت واکر*[96]). این افراد علیرغم وجود کنترلهای متعدد امنیتی قادر به انجام فعالیتهای مخرب جاسوسی – بعضاً تا بیش از یک دهه – بوده‌اند.
- *جان داچ*[97] رئیس CIA در زمان ریاست جمهوری بیل کلینتون، اطلاعات محرمانهٔ دولتی را از سازمان به خانه‌اش می‌برد و در آنجا در رایانه‌هایی ذخیره می‌کرد که برای کاربری "طبقه‌بندی نشده" پیکربندی شده بودند. درحالیکه اطلاعات طبقه‌بندی‌شده در رایانه‌ها قرار داشتند، از آنها برای دستیابی به پایگاههای وب مبتذل و غیر اخلاقی هم استفاده می‌شد – پایگاههایی که ممکن بود هم از آسیب‌پذیریهای عمومی و منتشرشده و هم از آسیب‌پذیریهای جدید و افشانشده برای حمله به سیستمهای مراجعه‌کننده استفاده کنند. علیرغم اینکه در این مورد مقررات و قوانین متعددی توسط داچ زیر پا گذاشته شده بود، هیچ اقدام عملی علیه او انجام نشد و در آخرین روز ریاست جمهوری کلینتون نیز مورد عفو وی قرار گرفت.

اگر شما این موارد و سایر قانون‌شکنیها و تخلفات رایانه‌ای را طی چند دههٔ اخیر بررسی کنید، یک ویژگی مشترک در آنها می‌بینید: همهٔ آنها توسط افراد بوقوع پیوسته‌اند. عوامل نفوذ، افراد بوده‌اند؛ ویروسهای رایانه‌ای را افراد نوشته بودند؛ و رمزهای عبور را نیز افراد دزدیده بودند.

امنیت کارکنان" عبارت است از همهٔ مواردیکه مربوط به کارکنان می‌شود: استخدام، آموزش، کنترل رفتار، و گاهی نیز اخراج. آمار نشان می‌دهد که مهمترین دستهٔ مرتکبین جرائمِ سنگین رایانه‌ای کسانی هستند که یا از دسترسی قانونی به داده‌ها برخوردارند و یا در گذشتهٔ نزدیک از آن برخوردار

89 Nick Leeson
90 Barings Bank
91 Toshihide Iguchi
92 Daiwa

93 Aldrich Ames
94 Janathon Pollard
95 Robert Hanson
96 Robert Walker
97 John Deutch

بوده‌اند. بعضی مطالعات نشان می‌دهد که بیش از ۸۰٪ رخدادها توسط چنین افرادی رخ می‌دهد. بنابراین قسمت مهمی از یک طرح امنیتی خوب عبارت است از ادارهٔ کارکنان با دسترسیهای طبقه‌بندی‌شده.

افراد به دو صورت در بروز مشکلات امنیت رایانه‌ای تأثیر دارند. بعضی از آنها با دنبال نکردن روالهای امنیتی، به فراموشی سپردن ملاحظات امنیتی، و مطلع نبودن از نتایج کارهایی که انجام می‌دهند، سهواً به وقوع رخدادهای امنیتی کمک می‌کنند. بعضی دیگر نیز آگاهانه کنترلها و روالها را زیر پا می‌گذارند تا به وقوع یک رخداد کمک کرده باشند یا خود بتنهایی باعث وقوع آن شوند. همانطور که قبلاً اشاره کردیم در بیشتر موارد افرادی که بصورت آگاهانه در مشکلات امنیتی شما نقش دارند کسانی هستند که کارمند خودتان می‌باشند (یا تا همین اواخر بوده‌اند): افرادی که از کنترلها مطلعند و می‌دانند چه اطلاعاتی با چه ارزشی ممکن است در کدام قسمت وجود داشته باشد.

شما در طول مدتی که مثلاً یک سیستم Unix را راهبری می‌کنید ممکن است با افرادی از هر دو گروه مواجه شوید. کنترلها و مکانیزمهای مربوط به امنیت کارکنان بسیار متعدد و گوناگون هستند و بحث و بررسی تمامی آنها به یک کتاب کامل نیاز دارد؛ بنابراین ما تنها به خلاصه‌ای از مهمترینِ آنها می‌پردازیم. تدوین سیاست برای کارکنان نمی‌تواند از وقوع نفوذهای امنیتی جلوگیری کند، اما آندسته از تهدیدات امنیتی که از جانب کارمندان خودتان متوجه شرکت شماست را کاهش می‌دهد.

امنیت در فرآیند استخدام

بررسی پیشینه‌ها

هنگامیکه کارکنان جدید را استخدام می‌کنید پیشینهٔ آنها را بررسی نمایید. ممکن است از متقاضیان خواسته باشید که فرمهای استخدامی را پر کنند، اما بعد از آن چه؟ حداقل کار این است که تمامی منابعی که هر متقاضی برای شناساندن خود معرفی کرده را بررسی کنید تا بتوانید به گذشتهٔ او – از جمله دلایل ترک کارهای قبلی‌اش – پی ببرید. فراموش نکنید که در بررسی سوابق، تاریخ استخدامها و ترک کارهای قبلی و همچنین بازه‌های خالی میان آنها را به دقت مورد کنکاش قرار دهید. همچنین لازم است اعتبار هر گواهینامه و مدرک تحصیلی را بسنجید؛ زیرا تاکنون بسیار پیش آمده که افرادی در مورد مدارک تحصیلی خود از دانشگاههای معتبر سخن رانده‌اند، درحالیکه آن دانشگاهها هیچ سابقه‌ای در اختیار نداشتند که نشان دهد حتی یک واحد درسی توسط آن افراد بصورت کامل گذرانده شده است! بعضی افراد نیز ممکن است مدارکی ارئه کنند که مربوط به دانشگاههایی باشد که تنها اندکی بزرگتر از یک دفتر پستی هستند! توجه داشته باشید از کسی که برای به استخدام در آمدن در یک شغل به دروغ متوسل می‌شود نمی‌توان در مشاغل حساس استفاده کرد.

تحقیقات متمرکز

در برخی موارد ممکن است بخواهید تحقیقات جدی‌تری در رابطه با شخصیت و پیشینهٔ متقاضیان داشته باشید. با توجه به سطح شغلی که قرار است متقاضی در آن قرار گیرد و دسترسیهایی که قرار است به سیستمها و داده‌های حساس داشته باشد شاید بخواهید:

- از کمک یک سازمان ویژهٔ انجام تحقیقات برای بررسی پیشینهٔ افراد استفاده کنید؛
- از متقاضیان سند عدم سوء پیشینهٔ جنایی بخواهید؛
- سوابق اعتباری متقاضیان را بررسی کنید تا ببینید آیا بدهی‌های شخصی بزرگی داشته‌اند که از پس آن بر نیامده باشند یا خیر. اگر موردی پیدا کردید دربارهٔ آن با خود متقاضی گفتگو کنید. افرادی که مقروض هستند نباید از کار کردن محروم شوند؛ چون در اینصورت هیچگاه قدرت بازپرداخت بدهی‌هایشان را پیدا نخواهند کرد. البته نباید از نظر دور داشت که احتمال بروز رفتار نادرست کاری از کارکنانی‌که تحت فشارهای اقتصادی هستند بیشتر است.
- بعمل آوردن آزمون دروغ‌سنجی از متقاضی را (اگر قانون به شما اجازه می‌دهد) از نظر دور ندارید. گرچه آزمونهای دروغ‌سنجی همیشه دقیق نیستند، اما اگر موقعیت شغلی حساسی را برای متقاضی درنظر گرفته‌اید می‌توانند مفید باشند.
- از متقاضی بخواهید که برای کار در شغل مربوطه یک ضمانتنامه بیاورد. بطور کلی انجام تمامی این مراحل

برای استخدام همهٔ کارمندان توصیه نمی‌شود، اما در مورد کارمندانی که قرار است در پستهایی کار کنند که در آنها به سطح بالایی از اعتماد نیاز است و شاغلین نیز از دسترسیهای ویژه برخوردار می‌شوند – مثل جذب و یا اخراج کارکنان – باید بررسیهای بیشتری بعمل آورید. پیشنهاد می‌کنیم به متقاضی اطلاع دهید که می‌خواهید چنین بررسیهایی را انجام دهید و برای اینکار رضایت او را نیز جلب کنید. انجام اینکار هرچند ضروری نیست ولی باعث می‌شود که انجام بررسیها راحت‌تر شود و متقاضی متوجه باشد که شما در استخدام وی محتاط و جدی هستید. گاهی اوقات برای انجام این تحقیقات به اجازهٔ صریح متقاضی نیاز دارید.

بررسیهای مجدد و دوره‌ای

زمانی که آزمونهای خود را انجام داده و متقاضی را استخدام کردید باید بعضی از بررسیها را بصورت دوره‌ای مجدداً انجام دهید. پس از آن باید نتایج بررسیهای فعلی و قبلی را با هم مقایسه کنید تا به تغییرات بوجود آمده پی ببرید. بعضی تغییرات ممکن است نیاز به بررسیهای عمیقتری داشته باشند.

بعنوان مثال اگر کارمندی داشته باشید که مسئول سیستم حسابداری شما – از جمله تهیهٔ چکهای رایانه‌ای برای بستانکاران – باشد، شاید لازم باشد اعتبار موجود در حسابهای بانکی او را نیز در بازه‌های کوتاه زمانی بررسی کنید. اگر بررسی و تحقیق مجدد شما هر دو سال یکبار انجام شود و دریابید که رفتار یکی از کارمندان خارج از معیارهای تعیین‌شده است، علی‌القاعده تصمیم خواهید گرفت که در آن مورد تحقیقات بیشتری بعمل بیاورید.

آموزش اولیه

نگرانیهای امنیتی شما در مورد یک کارمند نباید پس از استخدام او متوقف شود. هر کاربر رایانه حتماً باید در مورد سیاستهای امنیتی، آموزشهای زیربنایی ببیند. این آموزش در حالت حداقلی باید شامل روالهای مناسب انتخاب و استفاده از رمز عبور، دسترسی فیزیکی به رایانه‌ها و شبکه‌ها (اینکه چه کسی مجاز است به تجهیزات متصل شود و چگونه)، روالهای تهیه و نگهداری از نسخهٔ پشتیبان، سیاستهای برقراری تماس رایانه‌ای با شرکت (از طریق تلفن)، و سیاستهای افشای اطلاعات پشت تلفن باشد. مقامات اجرایی نباید بدلیل موقعیتشان از این موارد مستثنی شوند – آنها هم اگر نه بیشتر، حداقل به اندازهٔ کارکنان دیگر در معرض انتخاب رمز عبور ضعیف و سایر اشتباهات هستند. آنها نیز باید پایبندی خود به مسائل امنیتی را نشان دهند، چراکه آگاهی امنیتی در سازمانها از بالا به پائین جریان می‌یابد و نه بالعکس.

آموزش باید شامل اسناد نوشتاری و یک نسخه از سیاستهای کاربرد رایانه شود و مباحثی چون کاربرد درست و نادرست رایانه‌ها و شبکه‌ها، استفادهٔ شخصی از تجهیزات رایانه‌ای (در خلال و بعد از اتمام ساعات کار)، سیاستهای مالکیت و کاربرد پست الکترونیکی، و سیاستهای مربوط به ورود و خروج نرم‌افزارها و داده‌ها را در بر گیرد. مجازاتهای نقض مقررات نیز باید هنگام آموزش شرح داده شوند.

همهٔ کاربران باید فرمهایی مبنی بر آگاهی از این اطلاعات و پذیرفتن محدودیتهای آن امضا کنند. این فرمها باید سالها نگهداری شوند تا اگر بعدها این سؤال مطرح شد که آیا به کارمند در مورد آنچه که سازمان در قبال وی مجاز به انجام آن است آگاهی قبلی داده شده یا خیر، بتوان یک مدرک اثبات‌کننده ارائه کرد.

آموزش و آگاهی مداوم

کاربران لازم است بطور متناوب اطلاعات تازه‌ای در رابطه با امنیت و استفادهٔ صحیح از رایانه دریافت کنند. این بازآموزی برای کاربران فرصت مناسبی جهت یادآوری تهدیدهای موجود و پیامدهای آنها بوجود می‌آورد و یک فضای مباحثه‌ای برای تبادل نظر و در میان گذاشتن نگرانیها ایجاد می‌کند.

لازم است به کارمندان فرصت مناسبی برای آموزشهای جاری و آتی بدهید؛ مثل تشویق به حضور در کنفرانسها و سمینارهای حرفه‌ای، اشتراک در نشریه‌های ادواری حرفه‌ای و تجاری، و دستیابی به کتابهای مرجع و سایر موارد آموزشی. باید به کارمندان زمان کافی برای استفاده از کتب و انگیزه‌های لازم برای یادگیری مهارتهای مورد نیاز داده شود.

در کنار آموزش دوره‌ای ممکن است مایل باشید از روشهای متنوع‌تری برای تداوم این روند بهره گیرید – مثلاً نصب پوسترها یا اعلامیه‌هایی در مورد الگوهای سرآمدی، اعلام شعارهای روزانه و هفتگی، نامگذاری یک روز به عنوان "روز

امنیت"، و یا برگزاری نشستها و سمینارهای مختلف به منظور جلوگیری از کمرنگ شدن اهمیت موضوعِ امنیت در منظر عمومی.

البته اندازه و طبیعت سازمان، سطح تهدیدات و ضررهای احتمالی، و نهایتاً تعداد و رفتار کارکنان همه و همه از مواردی هستند که هنگام تنظیم طرحها باید درنظر گرفته شوند. هزینه‌های فعالیتهای آگاهی‌بخش نیز باید از قبل درنظر گرفته و در بودجهٔ سازمان آمده باشند.

بررسی و کنترل کارآیی

کارآیی کارمندان شما باید بصورت دوره‌ای بررسی شود. بطور خاص، در قبال رشد حرفه‌ای و عملکردهای موفق باید به کارمندان امتیاز و پاداش تعلق بگیرد. در عین حال مشکلات باید بصورتی سازنده شناسایی و حل شوند. شما باید کارمندان خود را به افزایش تواناییها و درک بیشتر تشویق کنید.

شما همچنین باید از بوجود آمدن شرایطی که در آنها کارکنان احساسهای مخربی چون خستگی مفرط از کار زیاد، بی‌احترامی، و یا بی‌توجهی پیدا می‌کنند جلوگیری نمایید. بوجود آمدن چنین محیطی در اداره ممکن است منجر به بی‌توجهی کارکنان به منافع سازمان شود. همچنین ممکن است کارکنان برای قرار گرفتن در فرصتهای مناسبتر شغلی سازمان شما را ترک کنند؛ یا بدتر از آن ممکن است برای انتقامگیری در بعضی فعالیتهای آشوبگرانه علیه شما همکاری نمایند. اضافه‌کاری باید بعنوان یک استثنا – و نه یک روال – باشد و به تمام کارمندان – خصوصاً آنهایی که در پستهای حساس هستند – باید تعطیلات و اوقات فراغت کافی داده شود. اضافه‌کاری به شدت کارمندان را خسته می‌کند و خستگی نیز باعث می‌شود که ضریب خطای آنها بالا رود، متوجه اشکالات نشوند یا از آنها چشم‌پوشی کنند، و همچنین از نظر عاطفی آسیب ببینند. در اینصورت در زندگی خصوصی آنها نیز فشارهای عصبی بوجود خواهد آمد، چراکه خانواده‌ها و عزیزانشان هم می‌خواهند گهگاه در طول روز آنها را ببینند. برای کارمندانی که بیش از اندازه تحت فشار و خسته باشند احتمال بیشتری وجود دارد که آزرده‌خاطر شوند و بدیهی است که این مسئله در بهبود امنیت هیچ کمکی نخواهد کرد.

بطور کلی علائم فشارهای روانی زیاد، مسائل شخصی و سایر انواع مشکلات کارکنانی که از امتیازات دسترسی نسبتاً بالا برخوردارند را باید کنترل کرد. تشخیص این مشکلات و درصورت امکان کمک به رفع آنها حداقلِ انسانیت است. انجام اینکار همچنین راهی برای حفاظت از منابع پر ارزش سازمان – خود کارکنان و نیز منابعی که به آنها دسترسی دارند – می‌باشد.

بازبینی دسترسیها

اطمینان حاصل کنید که امکان بازبینیِ دسترسیها به ابزار و اطلاعات وجود دارد. علاوه بر این مطمئن شوید هرکس که از هر نوع دسترسی برخوردار است از وجود این بازبینی‌ها اطلاع دارد. بسیاری از موارد سوء استفاده از رایانه‌ها به این دلیل صورت می‌گیرد که نفوذگر احساس می‌کند کسی متوجه کارهای او نخواهد شد. اگر یک تبهکار بداند که فعالیتهایش به ثبت می‌رسد ممکن از انجام کارهای مخرب خود صرفنظر کند. منظور از بازبینی تنها بازبینی ثبتهای رایانه‌ای نیست؛ بلکه گزارشات ورود و خروج افراد از ساختمان، سوابق استفادهٔ افراد از قفلهای الکترونیکی، و همچنین نوارهای تلویزیون مدار بسته، همگی می‌توانند مورد بازبینی قرار گیرند تا زمینه برای مسئولیت‌پذیری بیشتر مهیا شود.

با تمام این احوال باید مراقب آثار کنترلها پنهانی هم بود. افراد از اینکه به آنها اعتماد نشود و بطور مخفیانه تحت نظر باشند احساس ناخرسندی می‌کنند؛ و اگر بفهمند که تحت نظر قرار دارند ممکن است عصبانی شوند و حتی عملکردی افراطی از خود بروز دهند. بعنوان مثال در بعضی از دادسراها دیده‌شده که قانون کار و قراردادهای استخدامی توانسته باعث روبرو شدن کارفرما با دادرسیهای سنگین مدنی شود.

اگر نظارت بسیار دقیق باشد صرف مطلع کردن کارمندان از اینکه تحت نظر هستند کافی نیست. بعضی مطالعات نشان داده که کارمندان وقتی تحت نظارت شدید قرار داشته باشند کارایی کمتر و رفتار نامناسبتری خواهند داشت. مثلاً اگر شما بخواهید زمان مکالمهٔ تلفنی کارکنان، هر پایگاه وب که از آن بازدید می‌کنند، و یا اینکه هر چند وقت یکبار به استراحت می‌پردازند را تحت نظارت خود داشته باشید، آنگاه این مسئله کاملاً صحت خواهد داشت. بهترین سیاستها آنهایی هستند که با نظر مساعد و تشریک مساعی کارمندان تدوین شوند و کارکنان بخش منابع انسانی هم (اگر چنین بخشی داشته باشید) هنگام تدوین آن حضور داشته باشند.

حداقل دسترسی و تفکیک وظایف

اصول دسترسی حداقلی و تفکیک وظایف را به دقت درنظر داشته باشید. این اصول در طول زمان کارآیی خود را ثابت کرده‌اند و هرگاه در عملیات شما قابل اجرا باشند باید مورد استفاده قرار گیرند.

حداقل دسترسی

این اصل می‌گوید کمترین دسترسی لازم برای انجام کارها را به هر فرد بدهید. این دسترسیِ محدودشده، هم شامل دسترسی منطقی است (دسترسی به حسابهای کاربری، شبکه‌ها، برنامه‌ها) و هم دسترسی فیزیکی (دسترسی به رایانه‌ها، نوارهای پشتیبان و سایر تجهیزات جانبی). اگر هر کاربر روی همهٔ سیستمها حساب کاربری و به تمام منابع دسترسی فیزیکی داشته باشد، آنگاه تمام کاربران از نظر میزان تهدید تقریباً یکسان خواهند بود.

تفکیک وظایف

این اصل بر این مبنا استوار است که شما باید با دقت وظایف افراد را از هم جدا کنید. در اینصورت کسانیکه عهده‌دار نظارت بر استفادهٔ نادرست هستند خود هم نخواهند توانست از سیستمها استفادهٔ نادرست کنند. بنابراین واگذار کردن همهٔ فعالیتهای امنیتی و مسئولیتهای نظارتی به تنها یکنفر کار خطرناکی است. این مسئله می‌تواند منجر به این شود که آن شخص از سیاستهای امنیتی سرپیچی کند و مرتکب کارهای ممنوعه شود؛ و این درحالی است که هیچکس جز خود او گزارشات بازبینی مربوط به این کارها را نمی‌خواند و لذا نافرمانی وی بصورت مخفی باقی می‌ماند و به احتمال زیاد در طول زمان باز هم تکرار می‌شود.

وابستگی به کارمندان کلیدی را محدود کنید

هیچکس در یک سازمان نباید غیرقابل جایگزینی باشد چراکه هیچ انسانی جاودانه و همیشگی نیست. اگر بقای یک سازمان وابسته به عملکرد روزانهٔ یک کارمند کلیدی باشد، بدون شک آن سازمان با مخاطره مواجه است. برای برقراری امنیت، سازمانها باید برای مواقعی چون بیماری یا اخراج ناگهانی افراد کلیدی سیاستها و طرحهای مکتوبی داشته باشند و در عمل نیز از آن طرحها بهره گیرند.

در یک مورد که گزارش آن بدست ما رسیده، یک شرکت با حدود ۱۰۰ کارمند بیش از ۱۰ سال وقت صرف تدوین سیستم حسابداری گمرکی خود و واردات سفارشات نمود. این سیستم با یک زبان برنامه‌نویسی که به سادگی قابل خواندن نبود تهیه شد و شرکتی که آنرا تهیه کرده بود پس از مدت کوتاهی کار تجارت را کنار گذاشت. در آن شرکت تنها دو نفر به نحوهٔ کار این سیستم آشنا بودند: مدیر *سیستمهای اطلاعات مدیریت* (MIS)[۹۸] و نیز برنامه‌نویسِ او. این دو نفر مسئول ایجاد تغییرات در برنامه‌های سیستم حسابداری، آماده‌سازی گزارشات سالانه، تعمیر تجهیزات ازکارافتادهٔ رایانه، و حتی تهیهٔ نسخه‌های پشتیبان (که خارج از محوطهٔ اداری شرکت و در دفتر مدیر MIS ذخیره می‌شد) بودند.

اگر مدیر MIS و برنامه‌نویسِ او یک روز در راه دچار یک تصادف مرگبار می‌شدند چه اتفاقی می‌افتاد؟ اگر به مدیر MIS شغلی مناسبتر با حقوق چندبرابر پیشنهاد می‌شد چه اتفاقی رخ می‌داد؟ اگر برنامه‌نویس بخاطر نیاز شرکت به نگهداری او در پست خود نمی‌توانست ارتقای سازمانی پیدا کند و نسبت به کار در سازمان دلسرد و عصبانی می‌شد چطور؟

اینکه پرسنل اصلی غیرقابل جایگزینی شوند یکی از معایب و هزینه‌های جدی سیستمهای رایانه‌ای محسوب می‌شود – و مدیریت ارشد سازمان بندرت به این هزینه‌ها توجه کافی نشان می‌دهد. این مسئله یکی دیگر از دلایل بکارگیری نرم‌افزارهای حاضر و آماده و استفاده از سیاستها و روالهای نوشتاری – بطوریکه یک فرد تازه‌وارد بتواند براحتی جایگزین نفر قبلی شود – را روشن می‌کند.

غیبت و ترک شغل

گاهی اوقات افراد با میل و ارادهٔ شخصی خود (مثل پیشنهادهای بهتر شغلی) و گاهی بصورت غیرداوطلبانه (مثل وقوع مرگ یا آسیبهای فیزیکی) یک کار را ترک می‌کنند. در بازه‌های کوتاهتر زمانی نیز به هر حال افراد به مسافرت می‌روند و یا بدلایل خانوادگی و شخصی ممکن است برای چند روز از اداره غیبت کنند. در هریک از این موارد باید مجموعه‌ای از اقدامات و روالها برای گردش کار در شرایط غیبت یا ترک شغل تعریف شده باشد. این مجموعه می‌تواند شامل مراحلی چون تعلیق حسابها (البته نه در مورد غیبت)، تخصیص کارهای فرد به کارکنان دیگر، تغییر رمزهای عبور حساس، بررسی

98 *Management Information Systems*

صندوقهای پست صوتی؛ و یا قطع دسترسیها به تمام این سیستمها باشد.

در برخی محیطها ممکن است انجام این کارها تأثیرات گسترده‌ای داشته باشد. مثلاً ممکن است در یک دانشگاه، دانشجویان فارغ‌التحصیل اجازه داشته باشند تا ماهها یا سالها بعد از فارغ‌التحصیلی همچنان از حسابهای کاربری خود (مثلاً برای ارتباط با اساتید) استفاده کنند. در ادارات نیز اگر یکی از کارمندان در سفر باشد یا به خاطر بیماری غیبت کرده باشد (البته به مدت چند روز)، حسابهای او نباید مسدود و رمزهای عبورش نباید تغییر کنند.

در بسیاری مواقع ترک شغل بسیار ناگهانی و غیرمنتظره است. در این شرایط ممکن است فردی در محل کارِ کارمندی که ترک شغل کرده حاضر شود تا از تعویض قفلها اطمینان حاصل کند و یک مأمور امنیتی نیز با جعبه‌ای حاوی وسایل شخصی وی که داخل کشوی میز کارش بوده‌اند به بدرقهٔ او برود. حساب کاربری او قبلاً حذف شده، تمامی رمزهای عبور سیستم تغییر کرده‌اند، و تلفنهای دفتر وی نیز دیگر وصل نیستند. این شکل *مدیریت جدائی*[99] در صنایع خدمات مالی بسیار معمول است و بخشی از مشاغل سازمان بشمار می‌رود. کارکنان این بخش معمولاً کارمندانی هستند که از روی میل خودشان و بر حسب قراردادهایی استخدام شده‌اند که در آنها ذکر شده که ممکن است مسئول انجام چنین اقداماتی شوند. تحت هر شرایطی از دانش عرفی خود استفاده کنید. شما باید دقیقاً تعیین کنید که سیاست دسترسی باید چه باشد و آنرا بوضوح برای کارمندان و افراد مسئول در پیاده‌سازی آن سیاستها بیان کنید.

ملاحظات امنیتی در رابطه با سایر کارکنان

افراد دیگری که به سیستم شما دسترسی دارند ممکن است همواره منافع و نگرانیهای شما را درنظر نداشته باشند یا به خسارتهایی که ممکن است به شما وارد شود بی‌توجهی نشان دهند. گزارشات زیادی در مورد وقوع چنین اتفاقاتی در محیطهای خانوادگی وجود دارد: همبازیهای کودکان که ویروسهایی را وارد سیستمهای رایانه‌ای کرده‌اند و یا افراد متأهلی که برای جمع‌آوری مدارک و آگاه شدن از خیانت همسراشان در پیوند زناشویی، دیسکها را مورد وارسی قرار داده‌اند. در محیطهای تجاری نیز گزارشاتی در مورد نظافتچی‌ها و کارمندان موقت دفتری وجود دارد که حین خرابکاری یا جاسوسی در رایانه‌های شرکت دستگیر شده‌اند.

شما نمی‌توانید پدر و مادر خود را انتخاب کنید اما می‌توانید در تعیین اینکه چه کسی حق دسترسی به رایانه‌های شرکت شما دارد تأثیرگذار باشید. بازدیدکنندگان، کارکنان بخش تعمیرات، پیمانکاران، فروشندگان، و سایر افراد همگی ممکن است به دفتر کار و سیستم شما دسترسی موقتی یا نیمه‌دائمی داشته باشند. ببینید همهٔ مواردی که تاکنون مورد بحث قرار داده‌ایم چگونه می‌توانند در مورد این افراد صدق کنند. در پایان از یاد نبرید که هیچکس از بیرون اداره نباید به تجهیزات رایانه‌ای و شبکه‌ای شما دسترسی فیزیکیِ نامحدود داشته باشد.

افرادی که سوابق کاری آنها هر از چندگاه باید مورد بررسی قرار گیرد عبارتند از:

- متصدیان و راهبران سیستم؛
- کارمندان و پیمانکاران موقت که به سیستم دسترسی دارند؛
- پرسنل تعمیرات و نظافت؛
- نگهبانان امنیتی؛
- نامه‌رسانها و پرسنل بخش تدارکات که به سیستمها دسترسی معمولی یا بدون نظارت دارند؛
- مشاوران؛
- حسابرسان، ممیزها، و سایر پرسنل بخش مالی.

تمامی کارکنانی که به سیستم دسترسی دارند باید در مورد امنیت و پیشگیری از خسارتها آموزشهای لازم را ببینند و مطالب آموزشی بصورت دوره‌ای برایشان تکرار شود. پرسنل همچنین باید در جریان روالهای واکنش به رخدادها و نیز جریمه‌های نقض مقررات امنیتی قرار داشته باشند.

تهدیداتی که از جانب خانوادهٔ خودتان متوجه شما است را از یاد نبرید. خواه در منزل از یک سیستم مشترک برای تمام اعضای خانواده استفاده کنید و خواه کودکانتان را گهگاه برای بازدید به اداره ببرید، این مسئله حائز اهمیت است که آنها بدانند رایانه‌ای که شما با آن کار می‌کنید وسیله‌ای برای بازی نیست. آنها باید یاد بگیرند که به دستگاهها و وسایل حساس

99 *Separation Management*

تجاری دست نزنند. برای این منظور استفاده از محافظهای نمایشگر مجهز به رمزهای عبور، اقدام پیشگیرانهٔ مناسبی محسوب می‌شود. علاوه بر این به اعضای خانوادهٔ خود بیاموزید که لزومی ندارد در رابطه با محیط کار و تجارت رایانه‌ای شما با کسی صحبت کنند.

فصل هفتم
برونسپاری امنیت[۱۰۰]

کلیات

استفاده از منابع بیرونی برای مدیران بنگاههای اقتصادیِ عمومی، خصوصی و غیرانتفاعی که نگران توانمندی واکنش سازمان خود به تهدیدهای امنیتی هستند گزینهٔ مناسبی است، ولی انتخاب شرکتی که اینکار را انجام دهد باید به دقت صورت گیرد و کارآیی آن نیز باید بصورت منظم کنترل شود. در این فصل برخی از مزایا و معایب برونسپاری امنیت ذکر شده و یک دسته سؤالات که پیش از نهایی کردن مذاکرات با شرکای جدید بخش امنیت باید به آنها پاسخ داد نیز عنوان شدهاند.

برونسپاری؛ جایگزینی برای ورود ناخواستهٔ سازمان به عرصههای جدید

بعد از مطالعهٔ همهٔ مطالب فصلهای گذشته شاید به این نتیجه رسیده باشید که تمامی سیاستها و طرحها در وضعیت خوبی هستند؛ یا اینکه هنوز کارهایی وجود دارند که بخواهید انجام دهید؛ یا ممکن است از حجم کل کار ترسیده باشید. اگر جزء دسته آخر هستید این تصور را نکنید که انجامشدن آن فعالیت برای شرکت شما امکانناپذیر است. راههای دیگری هم برای تدوین سیاستها و طرحها و تأمین امنیت در ادارهٔ شما وجود دارد: استفاده از منابع، مشاوران و پیمانکاران خارج از شرکت. حتی اگر شما یک تجارت انفرادی کوچک در منزل یا شرکتی کوچک که وابسته به فناوری اطلاعات و ارتباطات است داشته باشید میتوانید از منافع تقسیم تجارب تخصصی استفاده کنید: عقد قرارداد همکاری با آندسته از شرکتهای امنیتی که میتوانند یک گروه آموزشدیده و باتجربه که به هیچ ادارهای وابسته نیستند را استخدام کنند و تواناییهایشان را با مشتریان متقاضی تقسیم نمایند و مهارتهای خود را در اختیار آنها قرار دهند.

از طرف دیگر اگر شما مهارتهای بالایی در فناوری اطلاعات داشته باشید میتوانید شرکتی تأسیس کنید و توانائیهای خود را در اختیار کسانی قرار دهید که به این خدمات نیاز دارند. در این قبیل شرکتها تواناییهای شغلی مهمی پیدا میشود؛ چراکه در سطح دنیا به اندازهٔ کافی متخصص امنیت اطلاعات وجود ندارد که بتواند جوابگوی تمامی نیازهای صنایع و دولتها در سراسر جهان باشد[۱۰۱]. لذا در پاسخگویی به نیازهای امنیت اطلاعات در غرب، یک انفجار در بکارگیری خدمات مشاوران و منابع خارجی برای کمک به سازمانهای با اندازههای مختلف صورت گرفته است. مشابه حالتی که برای بسیاری دیگر از خدمات قابل واگذاری به منابع خارج از سازمان وجود دارد، اینجا نیز برخی از شرکتها درجهیک و ممتاز هستند، برخی در زمینهٔ کار خود از تخصص بالایی برخوردارند، و برخی دیگر نیز ضعیف عمل میکنند. متأسفانه وضعیت این شاخه بگونهای است که نمیتوان با یک نگاه ضعف پیشنهاداتی که توسط افراد تازهکار تهیه شدهاند را تشخیص داد.

اگر به این دلیل که سازمان شما بخشی مخصوص تهیهٔ برنامههای امنیتی ندارد هنوز نتوانستهاید سیاستها و طرحهای ترمیم از سوانح و واکنش به رخدادهای خود را تدوین کنید، توصیهٔ ما این است که برای اینکار از منابع خارج سازمانی کمک بگیرید. چند سازمان بینالمللی وجود دارند که به کشورهای درحال توسعه در زمینههای مرتبط با فناوری اطلاعات کمک میکنند. اگر چنین تخصصی در دسترس باشد، میتواند هم برای پشتیبانی کوتاهمدت و هم برای پیریزی توانمندیهای بلندمدتتر (آموزش و کسب آگاهی) بسیار ارزشمند باشد.

تدوین طرح اجرایی

اولین قدم این است که تشخیص دهید باید از چه خدماتی استفاده کنید:

---

۱۰۰ واگذاری امنیت به منابع خارج از سازمان (Outsourcing)

۱۰۱ یکی از نتایج کمبود متخصص آموزشدیدهٔ امنیت، کمبود کارکنان و منابع پشتیبانی تحصیلات امنیت اطلاعات در مراکز آموزشی و دانشگاهها است. دولتها و صنایع ادعا میکنند که این حوزه از اهمیت زیادی برخوردار است، اما در تخصیص منابعی برای کمک به ساختهشدن این حوزه به شدت شکست خوردهاند.

آیا بخش امنیت را بعنوان بخشی از سازمان خود و با کارمندان خود راه‌اندازی می‌کنید؟

اگر چنین باشد شاید فقط به مشاورانی نیاز داشته باشید که برای اطمینان از فراموش نشدن یک مسئله مهم، عملیات شما را بررسی کنند.

شاید خودتان برای اینکار کارشناسانی داشته باشید ولی نگران زمان کم یا توانایی واکنش مناسب آنها به یک بحران باشید.

پس می‌توانید برای جلب همکاریِ یک شرکت به بازار بروید تا چند پیمانکار را برای همکاری (تمام وقت و یا پاره وقت) به ادارهٔ شما بفرستد. همچنین ممکن است بخواهید از خدمات *شرکتهای نظارت و واکنش از راه دور*[۱۰۲] استفاده کنید تا تنها بر امنیت شما نظارت کنند و درصورت بروز اشکال به شما کمک نمایند.

شاید نتوانید یک کارمند تمام وقت بکار بگیرید یا نیازی به چنین کسی نداشته باشید. در اینصورت ممکن است عقد قرارداد با یک شرکت مشاوره و نظارت که در این زمینه خدمات کامل ارائه می‌کند نیازتان را برآورده کند و نیز مقرون به صرفه‌تر باشد.

نکتهٔ کلیدی در هریک از موارد فوق این است که بدانید نیازهایتان چیست و هریک از آن خدمات به کدام نیازهایتان پاسخ می‌دهند. این مسئله همیشه ساده نیست، چراکه تا وقتی تجربهٔ مسائل امنیتی را پیدا نکرده و محیط اطراف خود را خوب نشناخته باشید، نیازهای واقعی خود را نمی‌دانید.

انتخاب فروشنده

موفقیت شما در برونسپاری امور امنیتی به شرکتهای ثالث تا حد زیادی به سازمانها یا افرادی بستگی دارد که آنها را برای اینکار انتخاب کرده‌اید.

یک راهنما بگیرید و روی معرفها پافشاری کنید

به علت تنوع زیاد شرکتهای مشاوره، یکی از بهترین روشهای انتخاب شرکت مورد نظرتان، پرسیدن از یک سازمان آشنا و مشابه سازمان خودتان می‌باشد. متأسفانه همیشه پیدا کردن یک معرف خوب امکانپذیر نیست. بسیاری از سازمانها، یا شرکتهای مشاوره‌ای خود را در یک نمایشگاه تجاری پیدا کرده‌اند، یا اولین بار در مقالات خبری از آنها مطالبی خوانده‌اند، و یا پس از یک تماس سادهٔ تلفنی و از طریق یک واسطه تصمیم به استفاده از خدمات آنان گرفته‌اند.

بدیهی است که یک شرکت ثالث امنیتی در جایگاهی قرار دارد که می‌تواند خسارتهای سنگینی به سازمان شما وارد آورد. حتی اگر یک شرکت تأمین امنیت بیرونی بسیار امانتدار و شایسته باشد، چنانچه شما در انجام کاری به آنها اعتماد کنید و آن کار بصورت نامطلوب انجام شود ممکن است تا ماهها بعد که پیامدهای آن آشکار شوند – زمانیکه شاید رابطهٔ شما با آن شرکت پایان یافته باشد – متوجه آن اشکال نشوید.

به همین دلیل وقتی یک شرکت را برای همکاری درنظر می‌گیرید باید:

معرفها را بررسی کنید

بدنبال معرفهای حرفه‌ای بگردید که شخص یا سازمانی را بکار گرفته‌اند که خدماتی مشابه آنچه شما بدنبال آن هستید را ارائه می‌کند.

افراد را بررسی کنید

اگر افراد خاصی برای انجام کارتان به شما معرفی شده‌اند، با روشهایی که در ادامهٔ همین مبحث و در بخش "افراد" شرح می‌دهیم آنها را ارزیابی کنید. در مورد شرکتهای بزرگ مشاوره‌ای که اسامی افراد درگیر در پروژهٔ شما را تا پرداخت قسط اول هزینهٔ قرارداد در اختیارتان قرار نمی‌دهند محتاطانه عمل کنید.

پایداری و تداوم فعالیت شرکت را در نظر بگیرید

اگر شما برای انجام یک پروژهٔ بلندمدت قرارداد بسته‌اید باید اطمینان حاصل کنید که شرکت طرف قرارداد در تمام مدت طولِ قرارداد وجود خواهد داشت. منظور از این نکته این نیست که شما نباید با استفاده از خدمات شرکتهای تازه‌تأسیس موافقت کنید، بلکه باید مطمئن شوید که سازمان مربوطه واجد مدیریت و پشتوانهٔ مالی لازم برای انجام تعهداتش می‌باشد. از شرکتهای مشاوره‌ای که دارای نرخهای پائین هستند اجتناب کنید؛ چراکه اگر نتوانند با فروش خدماتی که شما از آنها می‌خرید هزینه‌های خود را تأمین کنند، آنگاه سعی خواهند کرد از جای دیگر این پول را بدست

102 Remote Monitoring and Response Firm

آورند و لذا خدمات هرچند سطح بالای آنها در جای دیگر و شاید حتی تجارت دیگری متمرکز خواهد شد.

مراقب فریبکاریها باشید

در مورد *قراردادهای همه‌جانبه*[۱۰۳] که در آن یک شرکت به تنهایی همهٔ سیاستها را تهیه نموده و برای پیاده‌سازی سیاستها، خدمات و سخت‌افزار لازم را نیز می‌فروشد مراقب باشید. ما گزارشاتی دریافت کرده‌ایم که در آن نیازهای سیاست امنیتی و نیازهای طرح امنیتی به طرز مشکوکی برای همهٔ مشتریان بسیار مشابه یکدیگر بوده و در همگی از سخت‌افزار پایه و راه‌حلهای مشاوره‌ایِ نسبتاً مشابهی استفاده شده بود. اگر شما شرکتی را انتخاب کنید که شما را محدود به ارتباط انحصاری بلندمدت با خود نکند، آنگاه احتمال بیشتری وجود خواهد داشت که سیاستهای تدوین‌شده توسط آن سازمان مطابق نیازهای واقعی شما باشد و نه مطابق وسایلی که آنها به فروش می‌رسانند.

گستردگی تجارب را درنظر بگیرید

شما باید حتی‌الامکان از انتخاب شرکتهایی که عمدهٔ تجربه آنها مربوط یک نوع مشتری یا یک بستر نرم‌افزاری خاص است محتاطانه عمل کنید، مگر آنکه نیازهای سازمان شما دقیقاً با سازمانهایی که شرکت مزبور به آنها ارائه خدمات می‌دهد مطابقت داشته باشد. بعنوان مثال یک شرکت مشاوره‌ای که اساساً خدمات امنیتی شخص ثالث را به ادارات پلیس ارائه می‌دهد که از سیستم Microsoft Windows استفاده می‌کنند ممکن است برای یک شرکت دارویی که ترکیبی از Windows و Unix را بکار گرفته انتخاب مناسبی نباشد. گسترهٔ تجارب شرکت مشاوره‌ای ممکن است آنقدر فراگیر نباشد که بتواند خدمات سیاستی مناسبی برای پاسخگویی به نیازهای محیط کاری شما ارائه دهد. این نکته به این معنی نیست که افراد با سوابق کاری در یک حوزهٔ خاص نمی‌توانند دورنمای مناسبی برای شما فراهم کنند؛ اما شما باید محتاط باشید و ببینید که آیا شواهد روشنی برای تأیید این موضوع وجود دارند یا خیر.

کارکنان این شرکتها حداقل باید با مسائل زیر آشنایی داشته باشند:

- قانون کار و آندسته از مسائل مدیریتی که شرایطی را پیش بینی می‌کنند که در آنها افراد داخلی بر علیه کارفرمایشان اقدام قانونی می‌کنند؛
- قوانین جرائم رایانه‌ای ملی و محلی؛
- محصولات، فناوریها و محدودیتهای رمزنگاری؛
- ویروسها، کرمهای رایانه‌ای، سایر نرم‌افزارهای مخرب، و همچنین *نرم‌افزارهای پوینده*[۱۰۴]؛
- اصول TCP/IP در *شبکه‌های خصوصیِ مجازی* (VPNs)[۱۰۵] و دیواره‌های آتش؛
- آموزش و آگاهی عمومی، راهنماها و خدمات؛
- واکنش به رخدادها و پیگردهای قانونی؛
- امنیت سخت‌افزاری و نرم‌افزاری؛ و
- الگوهای سرآمدی، روشهای رسمی ارزیابی مخاطره، و مسائل مربوط به امور بیمه.

هر شرکت خدمات مشاوره‌ای که بخواهد سیاستهای خوبی برای سازمانهای طرف قرارداد تهیه کند باید پرسنلی داشته باشد که طالب گفتگو دربارهٔ مباحث مختلف که در این کتاب و بویژه در این فصل به آن می‌پردازیم باشند. اگر آنها آماده و یا قادر به بحث در مورد این عناوین نباشند ممکن است انتخاب مناسبی برای ارائه خدمات نباشند.

اگر در مورد این شرکتها نگرانی خاصی دارید کافیست از آنها بخواهید که سیاستها یا روالهایی که برای یک مشتری دیگر تهیه کرده‌اند را در اختیار شما قرار دهند. برخی از شرکتها چنین سندی را بعد از حذف اسم و مشخصات مشتری به شما ارائه می‌دهند. سایر شرکتها ممکن است مشتریهایی داشته باشند که خودشان خواسته باشند در فهرست "مشتریان مرجع" قرار گیرند. بعضی شرکتها ممکن است پیش از ارائه هر اطلاعاتی از شما بخواهند موافقتنامه‌ای دال بر سری نگهداشتن اسناد امضا کنید. از خدمات شرکتهایی که اسم و اسناد مشتریان خود را بدون مجوز آنها در اختیار شما و دیگران قرار می‌دهند استفاده نکنید؛ چون طبیعتاً در اینصورت اطلاعات را شما نیز بدون مجوز در اختیار مشتریان بعدی خود قرار خواهند داد. نکتهٔ آخر اینکه اگر از کارشناسان خارج

103 *"All in One" Contracts*

104 *Scanning Software*
105 *Virtual Private Networks*

از سازمان یا یک کشور دیگر کمک گرفتید، فراموش نکنید که یکی از شرایط قرارداد باید این باشد که آنها به توسعهٔ ظرفیت محلی سازمان و درصورت امکان کشور شما کمک کنند.

این کاملاً طبیعی است که طی دوره‌های گذار در کشورهای درحال توسعه شرکتها از کمک کارشناسان خارجی استفاده کنند. در حالت ایده‌آل می‌توانید از این روابط برای انتقال دانش و فناوری و افزایش استعدادهای بومی و درصورت امکان افزایش آگاهی کارشناسان ملی استفاده کنید.

معیارهای شایستگی برای کارکنان امنیت فناوری اطلاعات

مهمتر از همه باید در فکر افرادی باشید که خدمات سیاستگذاری امنیتی و پیاده‌سازی آنرا به شما ارائه می‌دهند. بر خلاف سایر خدمات مشاوره‌ای، در خصوص مشاورینی که برای مسائل امنیتی به استخدام در آمده‌اند باید بسیار محتاطانه رفتار کنید؛ چراکه بکارگیری نیروی خارجی برای تأمین امنیت معمولاً بدان معناست که سطوحی از دسترسی به سیستم و اطلاعات خود را در اختیار آنها قرار می‌دهید.

همانگونه که قبلاً اشاره کردیم در اطراف ما کارشناسان ماهرِ زیادی وجود ندارند. این بدان معنا است که گاهی اوقات شما باید افرادی را بکار گیرید که اطلاعات آنها به اندازه‌ای که می‌خواهید جامع نیست، ولی به هرحال از عهدهٔ کارتان بر می‌آیند. در مورد کسانیکه در زمینهٔ تخصص خود ادعاهای دروغین می‌کنند یا آنها که تخصصشان به آنچه بدان نیاز دارید نامربوط است مراقب باشید. بهتر است از خدمات فرد یا شرکتی استفاده کنید که خود اعتراف می‌کنند "در خلال کار، یادگیری هم خواهند داشت" (و احتمالاً به همین دلیل وجه کمتری دریافت می‌کنند)، تا اینکه فردی استخدام کنید که تلاش می‌کند نقایص کار خود را پنهان کند.

بازارهای امروزی امنیت در کشورهای توسعه‌یافته از افرادی که در زمینهٔ ایمن کردن بسترهای Windows در سطوح مختلف تخصص دارند اشباع شده است، اما کارشناسان بسترهای دیگر از جمله Unix کمتر هستند. از کتابها می‌توان اطلاعات زیادی در مورد امنیت آموخت، اما تنها مطالعهٔ کتاب کافی نیست. در حوزه‌هایی که در مورد آنها نگرانی دارید بدنبال معیارهای شایستگی کارمندان باشید؛ بخصوص:

گواهینامه‌ها

از متقاضیان گواهینامه بخواهید و از اعتبار گواهینامه‌هایی که ارائه می‌کنند اطمینان حاصل کنید. برخی از گواهینامه‌ها قابل خرید هستند و فرد برای دریافت آنها کافیست در یکسری از سمینارهای اینترنتی یا کلاسهای آموزشی شرکت کند، مطالب تئوری را برای چند ساعت به خاطر بسپارد، و سؤالات تستی را پاسخ دهد. این گواهینامه‌ها چندان ارزشمند نیستند. گواهینامه‌های دیگری وجود دارند که نیازمند تجارب عملی و تخصص عمیقتر می‌باشند.

گواهینامه هنوز یک بحث درحال تکامل است و لذا از اشاره به نمونه‌های فعلی آن اکراه داریم، اما بعنوان مثال می‌توان به گواهینامهٔ CISSP[۱۰۶] اشاره کرد که هرچند همهٔ آن چیزی نیست که ممکن است بخواهیم، اما یک مدرک معتبر برای تأیید سطحی معین از تجربه و تخصص در زمینهٔ امنیت است.[۱۰۷]

تحصیلات

سوابق تحصیلی را بررسی کنید. برخی افراد مهارت بالای رایانه‌ای خود را در نتیجهٔ مطالعه و تجربهٔ شخصی بدست آورده‌اند و برخی دیگر دربارهٔ علوم و مهندسی رایانه مدارک تحصیلی و دانشکده‌ای دارند؛ اما باور جهانی این است که سطح مهارت مهمتر از مدارک است. همانگونه که در بخش کارکنان اشاره کردیم بررسی کنید که آیا ادعاهای متقاضیان با مدارکشان مطابقت دارد یا خیر. سازمان امنیت ملی ایالات متحده در زمینهٔ امنیت اطلاعات تعداد محدودی مؤسسهٔ آموزشی را بعنوان "قطبهای آموزشی" معرفی کرده است. طبق آن فهرست طرحهای پیشروی مؤسسهٔ infosec در ژوئن ۲۰۰۲ در دانشگاههای *جرج میسون*[۱۰۸]، *جیمز مدیسون*[۱۰۹]، ایالت *ایداهو*[۱۱۰]، ایالت *آیوا*[۱۱۱]، آموزشگاه کارشناسی ارشد

---

۱۰۶ *مراجعه کنید به پورتال وب CISSP در:*
http://www.cissps.com/

۱۰۷ *گواهی‌های زیر در آدرس www.isaca.org را نیز ببینید:*
CISA (Certified Information Security Auditor)
CISM (Certified Information Security Manager)

108 George Mason University
109 James Medison University
110 Idaho
111 Iowa

وابسته به نیروی دریایی، *دانشگاه پوردو*[۱۱۲]، دانشگاه *کالیفرنیا در دیویس*[۱۱۳]، و دانشگاه ایداهو ارائه شدند. در اطراف جهان مراکز مقدماتی فراوانی در زمینهٔ فناوری اطلاعات وجود دارند. منابع محلی خود از جمله دانشگاهها را بررسی کنید تا مراکز مشابهی که ممکن است در آنجا مستقر باشند را بیابید. علاوه بر آن می‌توانید یکی از سازمانهایی که در بخش ضمائم کتاب ارائه شده‌اند را انتخاب نمائید.

شهرت

اگر کسی یک قطعه‌برنامهٔ پرکاربرد نوشته باشد یا در یک موضوع امنیتی مثل ویروس یا رمزنگاری کتابی تألیف کرده باشد بدان معنا نیست که با مقولهٔ امنیت بطور کامل آشناست. برخی از نویسندگان سابقهٔ زیادی در دامنهٔ وسیعی از مسائل امنیتی دارند، اما برخی دیگر تنها نویسندگان یا برنامه‌نویسان خوبی هستند. آگاه باشید که شهرت زیاد لزوماً به معنای شایستگی برای مشاوره نمی‌باشد.

بیمه و تعهدنامه

از افرادی که می‌خواهید برای شما کار کنند بپرسید که آیا بیمه هستند و تعهد سپرده‌اند یا خیر. اینکار نشان می‌دهد که شرکت آنها به شایستگی و رفتار افراد اهمیت می‌دهد. اینکار تضمین نمی‌کند که آن سازمان واجد شایستگیهای لازم باشد، اما به نوعی اطمینان می‌دهد که کارکنان آن سوء پیشینهٔ جنایی ندارند.

رابطه‌ها

از افراد بپرسید که در کدام سازمانهای محلی، ملی و بین‌المللی (ACM، ASIS، CSI، IEEE، و UNISEX) عضو هستند و آیا ارتباط مطلوبی با آنها دارند یا خیر. این سازمانها برای اعضای خود مطالب آموزشی و فرصتهای پیشرفت تخصصی مهیا می‌سازند و بسیاری از آنها نیز برای رفتار حرفه‌ای استاندارد منتشر می‌کنند. اگر سوژهٔ شما تنها مدعی سابقهٔ عضویت در گروههایی مثل " The 133t Hax0r Guild" است شاید بهتر باشد جای دیگری بدنبال یک کارشناس امنیت بگردید!

نفوذگران اصلاح شده

توصیه می‌شود از کار با افراد و سازمانهایی که ادعا می‌کنند نفوذگران اصلاح شده را بعنوان مشاوران امنیت بکار گرفته‌اند خودداری کنید.[۱۱۴] اگرچه گاهی اوقات افرادی که در ارتکاب جرائم رایانه‌ای درگیر هستند می‌توانند تبدیل به عضو مفیدی از جامعه شوند، اما نباید بلافاصله به کسانی که مرتکب جرائم شده‌اند یا سوء سابقه دارند خوش‌بین شد. در این زمینه نکات زیر قابل اشاره‌اند:

۱. بنظر نمی‌رسد کسانیکه در گذشتهٔ خود سابقهٔ خدشه‌دار کردن قانون، مالکیت شخصی، و حقوق خصوصی افراد را دارند انتخاب خوبی برای حفاظت از دارائی و حریم خصوصی مشتریان و حراست از منابع حیاتی باشند. آیا شما حاضرید از یک مجرم سابقه‌دار برای طراحی سیستم نظارت و هشدار سازمان خود استفاده کنید؟ آیا حاضرید یک تبهکار اصلاح شده را برای ادارهٔ مرکز مراقبتهای ویژهٔ شرکت بکار گیرید؟ این موارد تنها پیش‌بینیهای بد نیستند؛ بلکه هریک درصورت بروز اشکال می‌توانند پای شما را به دادگاهها و محاکم مدنی باز کنند – به هر حال این شما بوده‌اید که علیرغم آگاهی از سابقهٔ آنان تصمیم به استخدامشان گرفته‌اید.

۲. به همین صورت باید در مورد افرادی که هنگام انجام مصاحبه با شما از ارائه اسم واقعی خود امتناع می‌ورزند مراقبت به خرج دهید. شاید آنها واقعاً در ورود به بدنهٔ یک سازمان با استفاده از یک تماس تلفنی خبره باشند! اما یکی از ابتدائی‌ترین دلایلی که می‌توان برای استفادهٔ افراد از اسامی مستعار برشمرد این است که نمی‌خواهند در قبال کارهایشان مسئولیتی بر عهده داشته باشند. اگر یک نام مستعار بدنام شد بسیار آسانتر می‌توان آنرا عوض کرد تا اینکه کسی بخواهد نام قانونی خود را تغییر دهد و یا سابقهٔ آنرا اصلاح کند.

112 Purdue University
113 The University of California at Davis

۱۱۴ *آمارهای مربوط به شرکتهای ایالات متحده که نفوذگران اصلاح-شده را بکار گرفته بودند در "تحقیق جرم و امنیت رایانه‌ای" سال ۲۰۰۳ CSI/FBI آمده است:*
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

۳. دست آخر اینکه بسیاری از نفوذگران امروزی چندان هم به مباحث امنیتی وارد نیستند. آنها هم در روش و هم در شیوهٔ کار بیشتر مانند تبهکاران جنایی عمل می‌کنند تا برنامه‌نویسان و معماران رایانه‌ای. این کیفیت پائین سیستم‌عاملهای امروزی، فقدان روند امنیت در برنامه‌ریزیها، و در دسترس بودن گستردهٔ ابزارهای نفوذ خودکار است که باعث شده دست‌یازی و حمله به سیستمهای رایانه‌ای بسادگی میسر باشد. همانطور که یکنفر با سابقهٔ پرش با اتومبیل لزوماً یک رانندهٔ ماهر ماشین مسابقه یا یک طراح خبرهٔ موتور اتومبیل نیست، کسی که می‌داند چگونه از ابزارهای نفوذ بهره‌برداری کند و حملات تخریب سرویس را انجام دهد نیز ممکن است در فهم خود از امنیت مورد نیاز برای ایمن نگهداشتن سیستمها دچار مشکلات بنیادین باشد.

خدمات نظارت

اگر وضعیت عمومی پایدار باشد استفاده از خدمات نظارت و کنترل سرمایه‌گذاری خوبی محسوب می‌شود. خدمات رایجی که بصورت روزمره ارائه می‌شوند عبارتند از راهبری محل کار پیمانکاران، نظارت بر امنیت محل کار و خارج از آن، واکنش به رخداد و پیگرد قانونی (درصورت درخواست) و پشتیبانی از یک سایت جایگزین برای استفاده در وقت خرابی سایت اصلی. اما علاوه بر نگرانی در خصوص افرادی که خدمات مشاوره‌ای ارائه می‌دهند باید مراقب سخت‌افزارها و نرم‌افزارهای مورد استفادهٔ آنها هم باشید.

بسیاری از شرکتهای خدمات نظارتی و واکنش به رخداد، سخت‌افزارها و نرم‌افزارهایی دارند که می‌خواهند روی شبکهٔ شما نصب کنند. آنها از اینکار برای جمع‌آوری اطلاعات لازم جهت بازبینی و تغییر تنظیمات امنیتی سیستم استفاده می‌نمایند. باید با این فناوری برخورد محتاطانه داشته باشید؛ چراکه در موقعیتی مجاز و درون دایرهٔ امنیتی شما قرار گرفته است:

۱. مطمئن شوید که از عملکرد اجزای مختلف شبکه و تجهیزات آن توضیحات کامل و کتبی دریافت می‌کنید. همچنین اطمینان حاصل کنید که متوجه می‌شوید آن اجزا چگونه کار می‌کنند و هریک چه کاری انجام می‌دهند.

۲. در مورد خرابیهای تجهیزات از کسی که مسئولیت آن جزء بر عهدهٔ او است گزارش کتبی دریافت کنید. اگر سخت‌افزار یا نرم‌افزاری که روی سیستم نصب شده داده‌های شما را به دنیای خارج از سازمان بفرستد یا در پرکاربردترین ساعات روز بصورت غیرمنتظره سیستمهای شما را از کار بیاندازد، نباید ناگهان متوجه شوید طبق توافقی که با فروشنده داشته‌اید هیچ مسئولیتی متوجه او نیست!

۳. خاطرجمع شوید که در توسعه، آزمایش و استقرار آن فناوری که به سیستمهای شما افزوده می‌شود مراقبت دقیق انجام شده است؛ بویژه اگر طراحی منحصر به فردی داشته باشد. بطور خاص، با توجه به سوابق کیفی و مسائل امنیتی نرم‌افزارهای شرکت مایکروسافت، پیشنهاد می‌کنیم برای استفاده از خدمات هر شرکتی که تصمیم گرفته فناوری امنیت خود را بر مبنای محصولات مایکروسافت قرار دهد دقت لازم را بعمل آورید؛ چراکه آن شرکت باید همواره معایب یافت‌شدهٔ جدید را در بیشتر محصولات رایجِ خود رفع کند و در عین حال سازگاری آن محصولات با نسخه‌های قبلی را نیز حفظ نماید.

۴. اینکه فناوری شرکت مورد نظر واقعاً به جلوگیری از بروز مشکلات کمک می‌کند یا بعد از وقوع مشکل پی به وجود آن می‌برد را به دقت مورد بررسی قرار دهید.

کلام آخر پیرامون منابع خارج از سازمان

استفاده از کارشناسان بیرونی راه خوبی برای تأمین حفاظتهای لازم می‌باشد. مهارتهایی که برای تدوین سیاستها، نظارت بر سیستمهای مهاجم‌یاب و دیواره‌های آتش، و آماده‌سازی و اجرای برنامهٔ ترمیم از سوانح لازم است بعضاً بسیار تخصصی و نامتعارف هستند و ممکن است در میان کارمندان فعلی سازمان وجود نداشته باشند. انجام صحیح همین کارهاست که در تداوم یک تجارت یا خاتمهٔ آن به علت بروز عیب و نقصهای مختلف، تعیین‌کننده است.

در عین حال حوزهٔ مشاورهٔ امنیت با خطر روبرو است؛ چراکه پدیده‌ای جدید است و بخوبی درک نمی‌شود. افراد شارلاتان،

حقه‌باز، بی‌تجربه و تازه‌کار همیشه وجود دارنـد و در بـسیاری موارد نمی‌توان آنها را از افراد قابل اعتماد و حرفـه‌ای کـه در این زمینه کـار مـی‌کننـد تمیـز داد. البتـه گذشـت زمـان بـه تشخیص مسائل کمک می‌کند، اما انتخـاب صـحیح در گـام اول به مقداری تلاش و سرمایه نیاز دارد.

یک راه که برای بهره‌برداری شما از رشد این حوزه پیـشنهاد می‌شود دوری جـستن از انعقـاد قراردادهـای طـولانی مـدت است؛ مگر آنکه تأمین‌کنندهٔ خدمات امنیتی شما بـسیار مـورد اطمینان باشد و همواره خود را بـه‌روز نگـه دارد. چـشم‌انـداز مشاورهٔ امنیت در چند سال آینده مستعد تغییرات زیاد است، و اگر در هر زمان بتوانید گزینه‌های مختلفی کـه همـراه بـا آن تغییرات بوجود می‌آیند را انتخاب کنیـد منـافع خودتـان بهتـر تأمین خواهد شد.

سرانجام علیرغم اینکه شما بـرای دریافـت خـدماتی قـرارداد بسته‌اید که در قبال استفادهٔ نادرست از سیستمهایتان بر آنهـا نظارت کند، امـا هوشـیاری و مراقبـت خـود را نیـز از دسـت ندهید: تا آنجا که ممکن است مراقـب باشـید و سیـستمهای خود را قویتر کنید. همچنانکه تهدیدات پیچیده‌تـر مـی‌شـوند، مدافعین و کسانیکه مستعد قربانی‌شدن هستند نیز باید ترقـی و پیشرفت نمایند.

فصل هشتم
قانون‌نویسی، تدوین آیین‌نامه‌های دولتی، و سیاستهای حریم خصوصی

کلیات

در این فصل مروری خواهیم داشت بر نحوهٔ تدوین سیاستهای عمومیِ تجاری برای مؤسسات غیرانتفاعی و دولتی در دنیای متصل به شبکه. مثالهایی خواهیم دید از قانون‌نویسی برای حفاظت شهروندان، مشتریان و کودکان از سرقت هویت، کلاهبرداری و مطالب غیراخلاقی. در بخش چهارم بحث عمیقتری دربارهٔ مسائل قانونی *فضای سایبر*[۱۱۵] مطرح شده است. در این فصل تأکید ما بیشتر روی مسئولیت سازمانی در فضای عمومی است.

روابط تجارت و مشتری در دنیای دیجیتالی

بازرگانان اینترنتی اطلاعات زیادی از مشتریان خود بدست می‌آورند. یک پایگاه فروش اینترنتی می‌داند شما درحال بررسی کدام محصول هستید؛ کدام محصول را به کارت خرید خود می‌افزایید اما پس از مدتی حذف می‌کنید؛ و کدام محصول را نهایتاً بصورت اینترنتی می‌خرید. بازرگانان اینترنتی همچنین می‌دانند هنگام خرید در خانه هستید و یا سرِ کار، و اگر بخواهند می‌توانند از باقیماندهٔ اعتبار کارت خرید شما نیز مطلع شوند. علاوه بر آن برخلاف دنیای غیراینترنتی، یک بازرگان اینترنتی می‌تواند میان سابقهٔ خرید و عادتهای گردش شما در اینترنت نیز ارتباط برقرار کند و با برقراری چنین روابطی میان داده‌های مختلف طیف وسیعی از مشتریان، به یکسری الگوهای ارزشمند رفتاری پی ببرد.

ISPها قادرند از این هم بیشتر در مورد مشتری خود اطلاعات کسب کنند؛ چراکه هرآنچه کاربرِ اینترنت می‌بیند باید ابتدا از رایانهٔ ISPها بگذرد. ISPها همچنین می‌توانند پایگاههای وبِ مورد استفادهٔ کاربران خود و حتی مقالاتی که مورد مطالعه قرار داده‌اند را تشخیص دهند. آنها حتی می‌توانند نامه‌های الکترونیکیِ افراد را بر حسب کلمات کلیدی بکاررفته در متن آنها تحلیل نمایند. با ردگیری و تحلیل این اطلاعات، یک ISP می‌تواند بگوید که مثلاً آیا کاربرانش به سفر با قایق علاقمند هستند یا به سفر با اتومبیل؛ به مد اهمیت می‌دهند یا خیر؛ و آیا نسبت به درمان بیماری خاصی علاقه نشان می‌دهند یا نه.

سیاستهای حریم خصوصی

سازمانها و شرکتهای اینترنتی که به تجارت می‌پردازند در رابطه با جمع‌آوری اطلاعاتی که امکان تشخیص هویت و شناسایی کاربر را بوجود می‌آورد باید از چه استانداردهایی تبعیت کنند؟

در ایالات متحده حقوق مصرف‌کننده برای بار اول در *قانون گزارش اعتبار بازار*[۱۱۶] (مصوب سال ۱۹۷۰) صراحتاً مورد اشاره قرار گرفت. این قانون حقوق اساسی مصرف‌کنندگان را به رسمیت می‌شناخت؛ حقوقی چون حق ملاحظهٔ گزارشهای اعتباری هر مصرف‌کننده توسط خود او، حق اطلاع از اینکه چه کسانی گزارشات مربوط به وی را می‌بینند، حق الزام سازمانهای تهیه‌کنندهٔ گزارشات به تحقیق در مورد اشتباهات کشف‌شده توسط مصرف‌کنندگان، و حق الزام سازمانها به اضافه‌کردن یک اظهاریه از طرف مشتریان به گزارشهای مورد مناقشه. در سال ۱۹۷۳ – در دوره‌ای که داده‌های شخصی بیش از پیش روی رایانه‌ها قرار داشتند – برای احقاق حقوق مصرف‌کننده، *آیین‌نامهٔ راهکارهای اطلاعات بازار*[۱۱۷] ابلاغ شد.

آیین‌نامهٔ راهکارهای اطلاعات بازار[۱۱۸]

آیین‌نامهٔ راهکارهای اطلاعات بازار بر پنج اصل استوار است:

- هیچ سیستمِ نگهداریِ سوابقِ داده‌های شخصی نباید بصورت مخفی وجود داشته باشد.

115 Cyberspace

116 Fair Credit Reporting Act
117 Code of Fair Information Practices
۱۱۸ منبع: وزارت بهداشت، آموزش و رفاه ایالات متحده

- باید راهی وجود داشته باشد که هر کس بتواند اطلاع پیدا کند که چه اطلاعات شخصی از وی ثبت می‌شود و از آن اطلاعات چگونه استفاده خواهد شد.
- باید راهی برای افراد وجود داشته باشد که بتوانند از بکار رفتن اطلاعات شخصی خود در اهدافی غیر از آنچه که به آنها اعلام شده جلوگیری کنند.
- برای خود فرد باید راهی برای اصلاح اطلاعاتی از او که باعث شناسایی وی می‌شوند وجود داشته باشد.
- هر سازمانی که آندسته از سوابق داده‌های شخصی را تهیه، نگهداری، استفاده و پخش می‌کند که باعث شناسایی افراد می‌شوند باید قابلیت اطمینان داده‌ها در کاربرد مورد نظر را تضمین نماید و از مورد سوء استفاده قرار گرفتن داده‌ها جلوگیری کند.

کنگرهٔ ایالات متحده به تصویب قوانینی که کاربرد اطلاعات شخصی را ضابطه‌مند می‌کرد ادامه داد. با گذشت زمان، سوابق بانکی، سوابق تلفن، سوابق اینترنت، سوابق مشترکینِ تلویزیون کابلی، سوابق بهداشتی، سوابق تحصیلی و حتی سوابق اجارهٔ نوارهای ویدئویی همه و همه تحت پوشش قانون کنگره‌ایِ ایالات متحده درآمدند. با اینحال هر جزء قانون حفاظتهای متفاوتی ایجاد می‌کند و توسط بخش متفاوتی از نیروهای دولتی اعمال می‌شود. برخی جرائم مثل جرائمی که در *آیین‌نامهٔ حریم خصوصی مشترکین تلفن و دورنگار*[۱۱۹] می‌گنجد، بدون شکایت شاکی خصوصی قابل پیگرد نبودند. اما در اروپا مسائل طور دیگری بود. بر پایهٔ تجربهٔ جنگ دوم جهانی که در آن بسیاری از اطلاعات شخصی توسط نازیها مورد سوء استفاده قرار گرفت، بیشتر دوَل اروپایی ترجیح دادند از مؤسسات خاصی برای ضابطه‌مند کردن جمع‌آوری و استفاده از اطلاعات شخصی استفاده کنند. اروپاییان ایده‌های مطرح در آیین‌نامهٔ راهکارهای اطلاعات بازار را به یک نظامِ کلی موسوم به *حفاظت داده‌ها*[۱۲۰] تعمیم دادند.

راهبردهای سازمان همکاری و توسعهٔ اقتصادی

سازمان همکاری و توسعه اقتصادی (OECD)[۱۲۱] در سال ۱۹۸۰ یک رشته راهبردهای حریم خصوصی را بکار گرفت و آنها را ارائه کرد. بخشی از این راهبردها برای هماهنگ‌سازی ضوابط درحال افزایش حریم خصوصی در کشورهای صنعتی طراحی شده بودند. این راهبردها بطور خاص طراحی شده بودند تا به مشکلات روزافزون جریان فرامرزی داده‌ها – حرکت اطلاعات شخصی از کشوری که داده‌های شخصی در آن به شدت تحت حفاظت قرار دارند به کشوری دیگر که داده‌های شخصی در آن از حفاظت کمتری برخوردارند – بپردازند. راهبردهای OECD در مورد حفاظت از حریم خصوصی و جریان فرامرزی داده‌ها از هشت اصل تشکیل شده است:

اصل محدودیت جمع‌آوری[۱۲۲]

برای جمع‌آوری داده‌های شخصی باید محدودیت وجود داشته باشد. هر دادهٔ شخصی باید با استفاده از ابزارهای قانونی و منصفانه، در شرایط درست، و با دانش و رضایت فردی که اطلاعات به او مربوط می‌شود بدست بیاید.

اصل کیفیت داده‌ها[۱۲۳]

داده‌های شخصیِ جمع‌آوری‌شده باید مرتبط با هدفی که برای استفاده از آن اطلاعات اعلام شده و یا حوزه-های مرتبط با آن هدف باشند. این داده‌ها باید دقیق، کامل، و به‌روز نگهداری شوند.

اصل تعریف هدف[۱۲۴]

هدف از جمع‌آوری اطلاعات شخصی باید در همان لحظهٔ جمع‌آوری داده‌ها و نه دیرتر از آن مشخص باشد. استفاده‌های بعدی از اطلاعات جمع‌آوری‌شده باید به همان اهداف محدود شود؛ و اگر هدفهای بعدی با اهداف اولیه سازگاری ندارند باید این تغییر اهداف را

119 *Antijunk-Fax Telephone Consumer Privacy Act*
120 *Data Protection*

121 *Organization for Economic Cooperation & Development*
122 *Collection Limitation Principle*
123 *Data Quality Principle*
124 *Purpose Specification Principle*

صراحتاً اعـلام کـرد و نیـز اعـلام رضـایت فـرد بـرای استفاده از اطلاعات وی در اهداف جدید ضروری است.

اصل محدودیت استفاده[۱۲۵]

داده‌های شخصی نباید افشا شـوند، در دسـترس عمـوم قرار گیرند، یا برای اهدافی غیر از آنچه که اعلام شـده – همانطور که در اصول قبل گفتـه شـد – بکـار رونـد، مگر:

- با رضایت فردیِ مالک اطلاعات؛ یا
- با یک مجوز قانونی.

اصل حفاظهای امنیتی[۱۲۶]

داده‌های شخصی باید با حفاظهای امنیتـی مناسـب در مقابل خطراتی از قبیل ناقص شدن، دسترسی، تخریب، تغییر، افشا، و استفادهٔ غیرمجاز مراقبت شوند.

اصل باز بودن[۱۲۷]

باید یک سیاست کلی دربارهٔ شـفاف بـودن راهکارهـا و سیاستها با نگاه خاص به داده‌های شخصی وجود داشته باشد. باید ابزارهایی وجود داشته باشـند کـه بـه آسـانی بتوانند طبیعت داده‌های شخصی، هدف اصلی استفاده و همچنین مدت متعارف نگهداری از آنها را معین کنند.

اصل مشارکت فردی[۱۲۸]

هر کسی باید این حق را داشته باشد که:

- بفهمـد اطلاعـاتی از وی در دسـت گردآورنـدهٔ اطلاعات وجود دارد یا خیر؛
- با گردآورندهٔ اطلاعات مربوط بـه خـود: در یـک زمان معقول، با هزینه‌ای ارزان، با روشی معقول، و در حالتی که اطلاعات برایش شـفاف باشـد در ارتباط باشد؛
- اگر یکی از درخواسـتهای بـالا رد شـد بـرای آن دلیل بخواهد و بتواند آنرا به چالش بکشد؛ و
- بتواند دربارهٔ اطلاعات مربوط به خود بحث کند و اگر در بحث موفق شـد قـادر باشـد اطلاعـات را حذف، اصلاح و یا تکمیل نماید.

اصل پاسخگویی[۱۲۹]

هر گردآورندهٔ اطلاعات باید در قبـال عمـل بـه اصـول ذکرشدهٔ بالا پاسخگو باشد.

در راهکارهای OECD اجبار قانون به چشم نمی‌خـورد، امـا در عوض هنگام بررسی قوانین هریک از کشورهای عـضو، از این هشت اصل بعنوان راهبرد استفاده می‌شود.

برای مشاهدهٔ یک فهرست کنترل سـاده در مـورد معیارهـای حفاظت از اطلاعات – که درصورت جمع‌آوری اطلاعـات در مورد مشتریان از روی پایگاه وب باید از آنها اسـتفاده کـرد – می‌توانید به فصل یازدهم از همین بخش کتاب مراجعه کنید.

125 Use Limitation Principle
126 Security Safeguards Principle
127 Openness Principle
128 Individual Participation Principle

129 Accountalility Principle

فصل نهم
جرائم رایانه‌ای

کلیات

امیدواریم هیچوقت مجبور نشوید بر اساس اطلاعات موجود در این فصل عمل کنید. ممکن است این کتاب را با کوشش فراوان مطالعه کرده باشید و همهٔ گامهای مهم در جهت حفظ امنیت سیستم خود را برداشته باشید، اما با تمام این احوال همچنان ممکن است سیستم شما مورد سوء استفاده قرار بگیرد. شاید فردی که قبلاً کارمند شما بوده با استفاده از یک حساب قدیمی به سیستم نفوذ و بعضی از سوابق را حذف کند. علیرغم تمام تلاشهای شما برای جلوگیری از عملیات نفوذ، شاید فردی از یک کشور خارجی بتواند به سیستم شما وارد شود. در این شرایط شما چه مدرکی برای ارائه به دادگاه در اختیار خواهید داشت؟ علاوه بر این می‌توان پرسید هنگامی که از سیستم استفادهٔ عادی می‌کنید، چه خطراتی از جانب قانون و سیستم حقوقی شما را تهدید می‌کنند؟ اگر هدف یک شکایت قانونی قرار بگیرید چه می‌کنید؟ این فصل تلاش دارد این مسائل را روشن کند. به آنچه که در این فصل بیان شده صرفاً باید بعنوان توصیه‌های کلی توجه کرد و نه مسائل قانونی و حقوقی؛ چراکه برای جزئیات بیشتر و مسائل ریزتر باید از وکلای خوب و مشاوران حقوقی مجرب بخواهید بر حسب قوانین کشور محل اقامتتان شما را راهنمایی کنند.

گزینه‌های حقوقی موجود در پی وقوع یک نفوذ

اگر رایانه‌های شما در اثر نفوذ دچار آسیب شوند ممکن است در سیستم حقوقی و قانونی کشور محل اقامتتان گزینه‌های متعددی وجود داشته باشد که بتوانید از آنها استفاده کنید. این فصل نمی‌تواند شما را در استفادهٔ دقیق از جنبه‌های مختلف قانون یاری کند، چراکه در قوانین و سیستمهای حقوقی کشورهای مختلف تفاوتهای زیادی وجود دارد. لذا در این فصل به چیزی فراتر از قوانین ایالات متحده نخواهیم پرداخت.[۱۳۰] با اینحال دسترسی جهانی به اینترنت، وجود قوانینی که از داخل ایالات متحده نشأت نگرفته‌اند را ضروری کرده است.

قبل از هرگونه تصمیم به آغاز مراحل قانونی با یک وکیل زبده مشورت کنید. چون در استفاده از رویکردهای قانونی خطرات و مشکلاتی وجود دارد، باید قبل از شروع پیگرد قانونی نسبت به انجام آن مطمئن باشید.

در برخی موارد ممکن است چاره‌ای نداشته باشید و ملزم به انجام پیگرد قانونی باشید. مثلاً:

- اگر بخواهید برای شرکت بیمه ادعانامه‌ای تنظیم کنید تا خسارتی که در اثر یک نفوذ به شما وارد شده را جبران کند، ممکن است از جانب شرکت بیمه ملزم به انجام پیگرد قانونی علیه نفوذگران شوید.
- اگر اطلاعات خاص و طبقه‌بندی شده‌ای را پردازش می‌کنید ممکن است قوانین دولتی شما را ملزم به انجام تحقیقات و ارائه گزارش در مورد فعالیتهای مشکوک کنند.
- اگر از یک فعالیت غیرقانونی آگاه شوید و آنرا گزارش نکنید از نظر قانون بعنوان "معاونت در جرم" مسئولیت خواهید داشت، بخصوص اگر رایانهٔ شما هم در آن فعالیتهای غیرقانونی مورد استفاده قرار گرفته باشد.
- اگر از رایانهٔ شما برای انجام کارهای غیرمجاز و نادرست استفاده شود و شما در قبال آن کاری نکنید ممکن است به خاطر خرابیهای ایجاد شده علیه شما شکایت کیفری صورت بگیرد.
- اگر مدیر اجرایی یک شرکت دولتی باشید و تصمیم بگیرید که فعالیتهای غیرقانونی را تحت پیگرد و تجسس قرار ندهید، سهامداران شرکت شما می‌توانند علیه شما اقامهٔ دعوی کنند.

---

۱۳۰ *یک مباحثهٔ گسترده‌تر در مورد مباحث حقوقی و قانونی در ایالات متحده را می‌توان در کتاب "جرائم رایانه‌ای" مشاهده کرد:*
A Crimefighter's Handbook (O'Reilly)
ما توصیه می‌کنیم چنانچه در مورد مطالبی که در این فصل به آنها اشاره می‌کنیم به توضیحات بیشتری نیاز دارید به این کتاب مراجعه کنید. کتاب فوق دیگر به چاپ نمی‌رسد، ولی کپی‌ها و نسخه‌های قدیمی آن موجود هستند.

- اگر مدیر اجرایی یک شرکت خصوصی باشید، حتی اگر شرکت فاقد سهامدار هم باشد ممکن است شرکتهای همکار، حامیان و یا مشتریان – بسته به قوانین جرائم رایانه‌ای هر کشور – از شما شکایت نمایند.

اگر در یک شرکت کار می‌کنید و می‌دانید که سیستم شما به شدت در معرض مخاطره قراردارد قاعدتاً باید بعنوان بخشی از برنامه‌ریزی امنیتی (قبل از وقوع رخداد امنیتی) با مشاور حقوقی سازمان خود گفتگو کنید. سازمانها بسته به دخالت یا عدم دخالت نیروهای انتظامی سیاستهای متفاوتی را اتخاذ می‌کنند. با تمرین فعالیتهای زمان بحران، احتمال دنبال‌شدن واقعی سیاستها هنگامی که به آنها نیاز است را افزایش دهید.

بعنوان چند مقدمه برای شروع بحث، این قسمت مروری بر چند مسئله – که به احتمال قوی شما نیز روزی با آن مواجه می‌شوید – خواهد داشت:

تنظیم شکوائیه جزایی

در ایالات متحده هر زمان که احساس کنید کسی خلاف قانون عمل‌کرده می‌توانید علیه او اقدام قانونی نمایید و این روند با تنظیم شکوائیه قضایی در مراجع رسمی شروع می‌شود. سپس از دادیار اجازه گرفته می‌شود که بر اساس ادعای انجام‌شده تحقیق بعمل آید و اگر جرمی تشخیص داده شد بر اساس آن یک دادخواست تنظیم شود.

در برخی و شاید اکثر موارد، تحقیقات جنایی نتیجه‌ای برای شما در پی ندارد. چنانچه اعمال غیرقانونی انجام شده تکرار نشود و نفوذگر ردپایی از خود باقی نگذاشته باشد، یا اگر سیستم شما از یک کشور خارجی مورد حمله قرار گرفته باشد، بسیار بعید است که بتوانید نفوذگران را شناسایی و دستگیر کنید. نفوذگران حرفه‌ای بندرت از خود رد پایی باقی می‌گذارند.[۱۳۱]

تنظیم و ارائه شکوائیه لزوماً به تعقیب قضایی منجر نمی‌شود. دادیار مربوطه (در سطوح مختلف کشوری، ایالتی یا محلی) در مورد قانون نقض شده، شدت جرم، لزوم همکاری بازرسان آموزش‌دیده و نوع محکومیت تصمیم می‌گیرد. به خاطر داشته باشید که دستگاه قضایی مملو از پرونده‌های گوناگون است. بنابراین احتمال انجام تحقیقات در پرونده‌های جدید درصورتی وجود خواهد داشت که مربوط به جرائم خاص و یا تهدیدات جدی باشند. مثلاً احتمال انجام تحقیقات در پرونده‌ای که در آن ۲۰۰،۰۰۰ دلار داده از بین رفته، از یک مورد که در آن یکنفر مکرراً از طریق مودم، رایانهٔ شخصی شما را پویش می‌کند بسیار بیشتر است.

اطلاعات راجع به تحقیقات ممکن است به شما داده بشود یا نشود. حتی ممکن است در جریان تحقیقات اطلاعات نادرست به شما ارائه گردد – مثلاً درحالیکه بازرسان شدیداً مشغول کار هستند به شما گفته شود هیچگونه تحقیقاتی در کار نیست.

این امکان وجود دارد که انجام تحقیقات، شما را در موقعیتی ناپایدار قرار دهد. اگر افراد ناشناس به نفوذ خود به سیستم شما ادامه دهند، ممکن است مراجع قانونی از شما بخواهند که سیستم خود را باز بگذارید تا بازرسان اتصالات سیستم را ردیابی کنند و برای دستگیری متهم به جمع‌آوری مدارک بپردازند. متأسفانه بازگذاشتن درهای سیستم بعد از مشخص‌شدن اینکه سیستم شما مورد سوء استفاده قرار دارد، درصورتیکه نفوذگران از سیستم شما جهت انجام خرابکاری روی سیستمهای دیگر استفاده کنند می‌تواند با یک دادنامهٔ ثالث شما را در مظان اتهام قرار دهد، چراکه همکاری با نهادهای قانونی مانع از وارد شدن اتهام به شما نیست. پس بهتر است قبل از پذیرش چنین مخاطراتی جوانب امر را کاملاً بررسی کنید.

تماس با مراجع مربوطه

در زمینهٔ جرائم رایانه‌ای بسته به اینکه چه نوع سیستم قانونی و جزائی در کشور شما وجود دارد ممکن است لازم باشد که اقدامات خاصی را جهت برقراری تماس با مسئولین محلی یا کشوری انجام دهید. ذیلاً بعضی توصیه‌های کلی آورده شده اما طبیعتاً اگر آنها را طبق روشهای مناسب کشور خودتان بکار ببرید تأثیر بیشتری خواهند داشت.

- اگر امکان آن وجود داشته باشد بهتر است اول به مراجع محلی یا استانی مراجعه کنید. اگر مراجع استانی تشخیص دهند که مسئله توسط عوامل کشوری بهتر

---

۱۳۱ *البته تعداد بسیار کمی از نفوذگران واقعاً به اندازه‌ای باهوش هستند که خودشان فکر می‌کنند.*

می‌تواند مورد تحقیق قرار گیرد به شما پیشنهاد می‌کنند که به آنها مراجعه نمایید. هرچند متأسفانه برخی از دوایر محلیِ اجرای قوانین علاقه‌ای به استفاده از نیروی کمکیِ مأموران کشوری ندارند. این امر ممکن است سبب شود رخداد امنیتی مربوط به شما بدرستی تحت تحقیقات قرار نگیرد.

- مراجع محلی ممکن است به پیگیری شکایت شما علاقهٔ بیشتری داشته باشند؛ چون به احتمال زیاد مشکلی که برای شما پیش آمده در کنار هزاران مورد مشابه دیگر (به آن اندازه که در سطح کشوری وجود دارد) قرار ندارد. بنابراین احتمال بیشتری وجود خواهد داشت که مسئولان محلی به مشکل شما اهمیت دهند؛ حتی اگر آن مشکل خیلی کوچک باشد.
- هرچند برخی از مسئولان محلی ممکن است در زمینهٔ رایانه و جرائم رایانه‌ای مهارت زیادی داشته باشند، اما حتی در ایالات متحده هم عموماً مسئولان محلی از مسئولان ایالتی و کشوری تجربهٔ کمتری دارند و ممکن است انجام تحقیقات پیشرفته برایشان سخت باشد. در عوض بسیاری از سازمانهای کشوری از کارشناسانی بهره‌مندند که می‌توان آنها را به سرعت وارد جریان حل مشکلات کرد.
- در ایالات متحده مقامات ایالتی نسبت به مقامات کشوری علاقهٔ بیشتری به تعقیب و کشف جرائم جوانان و نوجوانان نشان می‌دهند. اگر می‌دانید که از جانب یک نوجوان که در ایالت خودتان اقامت دارد مورد حمله قرار گرفته‌اید بهتر است به مقامات محلی رجوع نمایید. گاهی اوقات هم بهتر است که راههای پیگرد قانونی را کنار بگذارید و مستقیماً با والدین یا معلمین آن مهاجم جوان صحبت کنید (یا از یک حقوقدان یا پلیس بخواهید اینکار را برای شما انجام دهد).

مخاطرات پیگرد متهمان

در استمداد از مراجع قانونی مشکلات بالقوهٔ زیادی وجود دارد که محدود به مسائلی چون تجربهٔ کارِ آنها با رایانه و شبکه و یا تعقیب جرائم رایانه‌ای نمی‌شود. گاهی اوقات ممکن است مراجعی که اطلاعات و تجربهٔ کافی در زمینهٔ رایانه ندارند بمنظور درک نکات پرونده، شما را دعوت به همکاری نمایند. در حالات دیگر ممکن است از اطلاعات شما صرفنظر کنند تا فقدان اطلاعات خود را بپوشانند و از زیر سؤال رفتن اعتبار دوایر اجرای قوانین جلوگیری نمایند. لازم به ذکر است که در بسیاری از موارد این احتمال وجود دارد که خود قربانی هم در فعالیتهای جنایی نقش داشته باشد. یک بازرس باتجربه در دنیای واقعی، به نظرات قربانی اطمینان کامل و بی شک و شبهه نمی‌نماید؛ و این مسئله برای جرائم دنیای سایبر هم صدق می‌کند.

اگر از شما و کارمندانتان خواسته شد که در فرآیند تحقیق برای کمک به شناخت موضوع مشارکت نمائید، اطمینان یابید که این عمل به دستور دادگاه انجام شده است؛ چراکه در غیراینصورت ممکن است بنظر بیاید که مشتاق قربانی‌شدن بوده‌اید. بهتر است که یک شخص بیطرف را برای همکاری با نمایندگان نیروهای انتظامی و دوایر اجرای قانون معرفی کنید.

منش و رفتار مجریان قانون گهگاه مشکلات جدی بوجود می‌آورد. ممکن است برخی تجهیزات شما به بهانهٔ بازجویی یا کنترل برای مدتهای غیرقابل توجیهی توقیف شوند – حتی اگر خود، قربانی یک جرم رایانه‌ای باشید. اگر شما قربانی بوده‌اید و رخداد امنیتی را خودتان گزارش کرده‌اید، معمولاً مقامات شما را از تلاشهایشان مطلع می‌کنند تا نارضایتی شما را به حداقل برسانند. با اینحال اگر نفوذگران از کارمندان خودتان باشند و یا پای مسائل حساسی چون اطلاعات رسمی و نظامی در میان باشد، ممکن است شما نظارتی روی روش و مدتی که سیستمها و رسانه‌های ذخیره‌سازیتان تحت بررسی قرار می‌گیرند نداشته باشید. این مشکل زمانی حادتر می‌شود که بازرسان پرونده نیازمند همکاری متخصصانی خارج از دفاتر محلی خود نیز باشند. اطمینان حاصل کنید که زمان ایجاد وقفه در کار بدلیل شرایط اجباری انجام تحقیقات را محاسبه می‌نمایید؛ چراکه این زمان و خسارتهای ناشی از آن می‌تواند بعنوان قسمتی از آسیبهای واردهٔ هنگام پیگرد قرار گیرد و متعاقباً در هر دادخواست مدنی (دادخواستهایی که می‌تواند علیه مهاجم و گاهی اوقات نیز علیه خود دوایر اجرای قوانین تنظیم شود) بکار رود.

در جریان تحقیقات نسخه‌های پشتیبان از منابع بسیار با ارزش به شمار می‌روند. علاوه بر این، درصورت لزوم

می‌توانید هنگامیکه سیستمهای اصلی شما تحت بازرسی و آزمایش است، از سیستمهای پشتیبان استفاده نمایید.

وقتی با دوایر اجرای قانون برای انجام تحقیقات همکاری می‌کنید، ممکن است در اثر سنگینی و ناکارآمدی آن تحقیقات، دید جامعهٔ رایانه‌ای نسبت به شما منفی شود. بیشتر کاربران رایانه دیدگاهی منفی نسبت به مجریان قانون دارند و اگر شما هم در آن جایگاه قرار بگیرید، این احساسات متوجه شما نیز می‌شود. چنین قضاوتهایی می‌تواند جایگاه شما را در انظار پایینتر از آنچه که مستحق آن هستید قرار دهد و از همکاری شما نه تنها با آن تحقیقات بلکه با سایر فعالیتهای تخصصی نیز جلوگیری کند. علاوه بر این پس از پایان‌یافتن بازرسی ممکن است آماج حملات الکترونیکی یا سایر سوء استفاده‌ها قرار بگیرید.

این رفتارها مایهٔ تأسفند، چراکه به هر حال بسیاری از بازرسان، دقیق و حرفه‌ای هستند و ممکن است برای جلوگیری از یک فعالیت مشکوک یا تهاجم دائمی، واقعاً به بازرسیهای موشکافانه نیاز داشته باشند. امروز می‌توانیم بگوییم که این مشکل در سالهای اخیر کمتر شده و نگرانیها در مورد آن نسبت به دههٔ گذشته کاهش یافته است. به مرور زمان و با آگاهتر شدن مردم نسبت به خسارتهای نفوذگران – حتی آنها که سوء نیتی نداشته‌اند– انتظار این است که این احساسات منفی نسبت به مراجع قانونی از این هم کمرنگتر شود.

توصیهٔ اکید ما به شما این است که هنگام تصمیم‌گیری در مورد درمیان گذاشتن هرگونه مشکل امنیتیِ سیستم خود با مراجع قانونی خوب فکر کنید و جوانب امر را مورد بررسی قرار دهید. در بیشتر مواقع بهتر است بسنجید که در چه صورت مراجعه به مراجع قضایی لازم است: درصورتیکه واقعاً چیزی را از دست داده و متحمل ضرر شده‌اید و یا درصورتیکه شخصاً قادر به کنترل وضعیت پیش‌آمده نیستید. بعضی اوقات هیاهوی ناشی از یک اتفاق خطرناکتر از سایر خسارتهایی است که در پی وقوع آن اتفاق به بار می‌آید.

بعد از اینکه تصمیم به استمداد از مراجع قانونی گرفتید از به‌پا کردن هیاهو در این زمینه بپرهیزید. در بعضی موارد دخالت مراجع قانونی می‌تواند عامل دلسردی نفوذگران باشد، اما در بعضی موارد نیز می‌تواند شما را در کانون توجه آنها و درنتیجه حملات بیشتر قرار دهد. آگاه باشید که ممکن است مشکل فعلی شما جزئی از یک مشکل گسترده‌تر باشد که درحال توسعه و گسترش است و لذا درصورتیکه بدرستی آنرا مدیریت نکنید باعث وارد آمدن آسیبهای فراوانی به شما و دیگران شود.

ما علاقه‌مندیم که خوشبینانه به این موضوع نگاه کنیم. مراجع قانونی بطور کلی از نیاز به ارتقای سطح خود در بررسی جرائم رایانه‌ای اطلاع دارند و معمولاً در تلاشند که مراکز آموزشی راه‌اندازی کنند، تشکیلات و تسهیلات تحلیل قانونی تهیه نمایند، و ابزارهای دیگری برای انجام تحقیقات ثمربخش را بکار گیرند. معمولاً در دادسراها (خصوصاً در مناطق پیشرفتهٔ کشور) بعضی بازرسان و دادیارها تجربهٔ زیادی کسب می‌کنند و لذا باید در تلاش باشند که اطلاعات خود را به سایر همکارانشان نیز انتقال دهند. نتیجهٔ این فرآیند در سالهای اخیر یک ارتقای اساسی در سطح موفقیت فعالیت نیروهای انتظامی و انجام شدن تعداد زیادی تحقیقات و دادرسیهای موفق در حوزهٔ جرائم سایبر بوده است. بهتر است به فواید بیشمار گزارش‌کردن جرائم رایانه‌ای – نه تنها برای خودتان، بلکه برای تمام جامعه – توجه داشته باشید: دادرسیهای موفق می‌توانند باعث جلوگیری از سوء استفاده‌های بعدی از سیستمهای شما و نیز دیگران شوند.

مسئولیت گزارش جرم

در پایان به یاد داشته باشید که یک جرم تنها درصورتی مورد پیگرد قضایی قرار می‌گیرد که شما آنرا گزارش کرده باشید. در غیراینصورت اینکار انجام نمی‌شود و این نه به سود شماست و نه هیچکس دیگر؛ و دست نفوذگر را نیز برای وارد آوردن آسیبهای بیشتر و به افراد دیگر باز می‌گذارد. به یاد داشته باشید که ممکن است آنچه شما با آن برخورد کرده‌اید جزئی از یک مجموعهٔ عظیم جرائم رایانه‌ای و اعمال خرابکارانه باشد. بدون انجام بررسیهای لازم نمی‌توان ادعا کرد که آنچه بر سر شما آمده یک رخداد مجزا و بی‌ارتباط با سایر اجزای سیستم بوده و یا جزئی از یک تهاجم بزرگتر.

مشکلِ دیگرِ عدم گزارش جرائم سنگین رایانه‌ای این است که برخی به غلط تصور خواهند کرد که این جرائم بندرت رخ می‌دهند و درنتیجه احتمال وقوع این مشکلات در سیستمهای خود را ناچیز خواهند پنداشت، روی بودجه‌بندی و آموزش مأموران جدید اجرایی تأکید زیادی بعمل نخواهد آمد؛

برای بهبود قوانین فعلی تلاش ناچیزی خواهد شد؛ و جامعه نیز به موضوعاتی از این قبیل توجه کمتری نشان خواهد داد؛ و خلاصه اینکه نتیجه این خواهد بود که محیط رایانه‌ای برای همهٔ بازیگران آن خطرناکتر از آنچه ممکن است بنظر بیاید خواهد شد.

احتیاط بیشتر...

در این بخش خلاصه‌ای از پیشنهادات دیگر برای جلوگیری از سوء استفادهٔ احتمالی از رایانه‌ها ارائه شده است:

- در متن برنامه‌ها و داده‌های رایانه، اطلاعات مربوط به حق نسخه‌برداری و مالکیت انحصاری خود را در ابتدایی‌ترین بخش هریک از فایلها قرار دهید. اگر صراحتاً به حق نسخه‌برداری اشاره کرده‌اید، حتماً امکان پرکردن یک فرم مخصوص در همین رابطه را برای هر مشتری پیش‌بینی کنید. انجام اینکار می‌تواند به بازرسی دقیق‌تر و ترمیم خسارتها کمک کند.
- اطمینان حاصل کنید که کاربران دربارهٔ بایدها و نبایدهای فعالیتها و مسئولیتها خود آگاهی کامل دارند.
- تمام کاربران را از هر چیزی که در شبکهٔ شما تحت نظارت قرار دارد مطلع کنید (درصورتیکه با انجام اینکار سیاستهای شما نقض نمی‌شود). این نظارت می‌تواند شامل نامه‌های الکترونیکی، فشرده‌شدن کلیدها، و دسترسی به فایلها شود. چنانچه در مورد این نظارت هشدار داده نشود، ممکن است نظارت بر کارهای یک مهاجم هم بعنوان نقض قوانین حریم خصوصی تلقی شود.
- نسخه‌های پشتیبان را خوب تهیه کنید و از آنها در جای امنی نگهداری کنید. اگر برای کشف حقیقت لازم است این نسخه‌ها را با یکدیگر مورد مقایسه قرار دهید باید قادر باشید افرادی که به نسخه‌ها دسترسی داشته‌اند را مشخص نمایید. نگهداری از پشتیبانها در محیطهای عمومی باعث می‌شود بعدها نتوان از آنها بعنوان مدرک استفاده کرد.
- درصورت مشاهدهٔ هرگونه مورد مشکوک یا اتفاقی که نیاز به دخالت مراجع قضایی دارد، یادداشت‌برداری را شروع کنید. مشاهدات و فعالیتهای خود و زمان هریک از آنها را یادداشت نمایید. از فایلهای ثبت و ردگیری‌ها نسخهٔ چاپی تهیه و آنها را ضمیمهٔ یادداشتهایتان کنید. هنگام انجام بازرسیها و تحقیقات، وجود یک سابقهٔ کتبی از اتفاقاتی که رخ داده می‌تواند بسیار ارزشمند باشد. زمان و موضوع کلیهٔ تماسها با مراجع قانونی را نیز به ثبت برسانید.
- سعی کنید سطوح اختیارات کلیهٔ کارمندان و کاربران را بصورت کتبی تعریف کنید و هرآنچه که فرد به آن دسترسی قانونی دارد (و نیز هرچه که به آن دسترسی ندارد) را در این تعاریف بیاورید. برای ابلاغ این تعاریف به افراد ساز و کاری بیاندیشید که هر کس بتواند بخوبی آنرا بفهمد و به کار ببندد، و محدودیتهای حاصل از آنرا نیز درک کند.
- به کارمندان خود صراحتاً گوشزد کنید که ملزم هستند در پایان کارشان و یا هر زمان که از آنها خواسته شد کلیهٔ منابعی که در اختیارشان بوده (مثل متن برنامه‌ها و کتابچه‌های راهنما) را بازگردانند.
- اگر اتفاقی رخ داده که بنظر شما انجام تحقیقات پلیسی را لازم می‌کند، اجازه ندهید کارکنان به تحقیقات خودسرانه بپردازند. تلاشهای خودسرانه ممکن است باعث شوند بعضی مدارک در بازرسیهای رسمی سندیت خود را از دست بدهند. همچنین ممکن است بازرسان با مشاهدهٔ دخالت شما در تحقیقات، نسبت به شما دید منفی پیدا کنند.
- کارمندان خود را به امضای توافقنامه‌ای در زمینهٔ مسئولیتهایشان در قبال اطلاعات حساس، کاربرد رایانه، استفاده از پست الکترونیکی و دیگر مسائل رایانه‌ای که ممکن است بعدها مطرح شوند ملزم نمایید. اطمینان حاصل کنید که سیاستها صریح و عادلانه هستند و همهٔ کارمندان از آن آگاهی دارند و موافقتنامه مربوطه را امضا کرده‌اند. تصریح کنید که کلیهٔ دسترسیها و حقوق دسترسی هنگام پایان‌یافتن دورهٔ کاری پایان می‌یابد و هرگونه دسترسی غیرمجاز در خلال یا پس از پایان دورهٔ کاری تحت پیگرد قانونی قرار خواهد گرفت.

مخاطرات جنایی در حوزهٔ تجارت

اگر شما یک ISP هستید یا پایگاه وب و یا به هر صورتی در محل کار خود شبکه‌های رایانه‌ای دارید، درصورتیکه از دستگاههای شما استفاده نادرست شود ممکن است خودتان تحت تعقیب قانونی قرار بگیرید.

اگر مقامات قضایی به این نتیجه برسند که رایانه‌های شما توسط یک کارمند برای نفوذ به رایانه‌های دیگر، انتقال و ذخیرهٔ اطلاعات طبقه‌بندی شده (اعم اسرار تجاری، تصاویر مستهجن کودکان، و ...) یا همکاری در جرائم رایانه‌ای مورد استفاده قرار گرفته، ممکن است رایانه‌های شما با یک حکم توقیف، برای انجام بررسیها مصادره شوند. اگر در خلال تحقیق بتوانید ثابت کنید که دسترسی آن کارمند به سیستم شما محدود بوده، ممکن است دایرهٔ این توقیف‌ها کاهش پیدا کند، اما باز هم به احتمال زیاد بخشی از ماشینهای شما طی انجام تحقیقات رسمی در توقیف باقی خواهند ماند.

بسته به راهکارهای پذیرفته‌شده در سیستم قانونی هر کشور، اگر پلیس محلی یا مقامات کشوری معتقد باشند مدارکی مبنی بر تخطی از قانون وجود دارد از یک قاضی تقاضای مجوز برای انجام تحقیق می‌کنند و قاضی نیز حکم تحقیق صادر می‌نماید. در سالهای اخیر تعدادی از بازرسان و مسئولان کشوری ایالات متحده، در برخی ایالتها جایگاهی را برای انجام تحقیقات گسترده و سنگین بوجود آورده‌اند. یک دلیل این امر، عدم تجربهٔ کافی دوایر اجرای قوانین برای برخورد با جرائم رایانه‌ای است که بنظر می‌رسد با انجام اینکار و نیز کارهای مشابه، به مرور زمان بهتر شود.

احتیاط بیشتر...

- خود را به سیستمهای نظارت بر شبکه و نظارت بر صفحه‌کلید مجهز کنید. این نرم‌افزارها می‌توانند بر تمام اطلاعات فرستاده‌شده یا دریافت‌شده نظارت کنند و آنها را ضبط نمایند. اگر احساس کردید که مورد نفوذ قرار گرفته‌اید سریعاً عملیات نظارت و ضبط را آغاز کنید و منتظر حکم دادگاه نباشید؛ چراکه نیروهای انتظامی معمولاً بدون کسب اجازه از دادگاه نمی‌توانند به شما مجوزی بدهند که بتوانید بعنوان مجری قانون عمل نمایید و دریافت حکم قاضی مبنی بر اجازهٔ دادگاه نیز ممکن است مدتها به طول بیانجامد.
- با کمک وکیل و شرکت بیمهٔ خود برای کارها، تحقیقات مرتبط، و هر فعالیت مربوط که باید هنگام وقوع یک نفوذ انجام دهید برنامه‌های اقتضائی تدوین کنید.
- آندسته از مجریان قانون که شایستگی دارند روی مشکلات بالقوه تحقیق کنند را مورد شناسایی قرار دهید؛ خود را به ایشان معرفی کنید، و نگرانیهایتان را پیش از وقوع حادثه با آنها در میان بگذارید. چنانچه در آینده به مشکلی برخورد کردید که لازم بود در آن از کمک دوایر اجرایی قانون و نیروهای انتظامی بهره بگیرید، یک آشنایی بسیار اولیه با این افراد می‌تواند بسیار کارساز باشد.
- پیوستن به جوامع و سازمانهایی که بصورت مداوم در مورد امنیت به افراد آگاهی و آموزش می‌دهند تا تخصص آنها در این زمینه افزایش یابد را فراموش نکنید.

فصل دهم
مدیریت مخاطرات سیار: خدمات مالی الکترونیکی در محیط بی‌سیم[۱۳۲]

کلیات

در این فصل به بررسی مخاطراتی می‌پردازیم که در نتیجهٔ استفاده از فناوریهای بی‌سیم در خدمات مالی بوجود می‌آیند و از طریق سرقت هویت، تسخیر فعالیتهای سیستم، و سایر اقدامات مشابه، امنیت الکترونیکی را تهدید می‌کنند. این فصل روشن می‌کند که اگرچه "حجم" معاملاتی که در محیط انجام می‌شوند بر گستردگی حوزهٔ اقدامات ضروریِ امنیتی تأثیرگذار است، اما صِرف استفاده از فناوری بی‌سیم نیز می‌تواند به آشکار شدن نقاط ضعف امنیتی بیانجامد. در این فصل چند نکتهٔ مهم مورد اشاره قرار می‌گیرند که راهبران سیستم (بخصوص در بانکها) می‌توانند جهت کاهش مخاطرات تا بیشترین حد ممکن و معمولاً بدون افزایش زیاد هزینهٔ تمام‌شده، آنها را انجام دهند. اقدامات پیشنهادی این فصل برای کاهش مخاطرات، به نوعی الگوهای سرآمدی موجود در ارائه خدمات مالی مبتنی بر فناوری بی‌سیم را نیز در بر می‌گیرد.

فناوری بی‌سیم در صنایع و بخشهای جدید

رشد سریع استفاده از فناوری بی‌سیم در بسیاری از بازارهای درحال رشد خدمات مالی، توجه دقیق به مسائل امنیت الکترونیکی در حوزهٔ این فناوری را ضروری کرده است. این موضوع در هیچیک از بازارهای درحال رشد به اندازهٔ حوزهٔ فناوری بی‌سیم – که باعث رواج فناوری تلفن همراه در این بازارها شده – از اهمیت برخوردار نیست. هرچه کشورها در استفاده از این فناوری برای ارائه خدمات مالی بیشتر تلاش کنند، توجه به خطرات بالقوهٔ امنیتی در فناوری بی‌سیم و اینکه شرکای تجاری در بازار و راهبران سیستم در بانکها و سایر مؤسسات خدماتی چقدر بهتر می‌توانند امنیت را تضمین کنند حیاتی‌تر می‌شود. بنابراین هدف این فصل توضیح این مطلب است که چرا و چگونه امنیت الکترونیکی به یک دغدغه تبدیل می‌شود و چگونه می‌توان بدون پرداخت هزینهٔ اضافی به ارائه‌کنندگان خدمات مالی این مخاطرات را کاهش داد. با توجه به این نکتهٔ بسیار مهم که تغییرات بسیار سریع فناوری امکان ارائه راهکارهای ثابت و تغییرناپذیر را از راهبران سیستمهای خدمات مالی سلب کرده، بسیاری از اقداماتی که در این کتاب توصیه شده‌اند مربوط به امنیت چندلایه در کاربردهای بی‌سیم خدمات مالی می‌باشند، و نمایانگر آنچه امروز بعنوان الگوهای سرآمدی امنیت الکترونیکی شناخته می‌شوند هستند.

این فصل به قسمتهای زیر تقسیم شده: قسمت "الف" خواننده را با گسترهٔ وسیع کاربردهای فناوری بی‌سیم و خدمات مالی الکترونیکی در سراسر دنیا آشنا می‌کند؛ قسمت "ب" به معرفی مخاطرات ذاتی فناوری بی‌سیم می‌پردازد؛ قسمت "ج" نقاط ضعف *شبکه‌های محلی بی‌سیم* (WLANs)[۱۳۳] و روالهای کاهش مخاطرات که برای تأمین امنیت آنها لازم هستند را شرح می‌دهد؛ قسمت "د" به تکامل *شبکه‌های سراسری مخابرات سیار* (شبکه‌های GSM)[۱۳۴] و آسیبهای موجود در آنها می‌پردازد؛ قسمت "ه" جزئیات روشهای صحیح مواجهه با مخاطرات شبکه‌های GSM را توضیح می‌دهد؛ قسمت "و" به ارائه الگوهای سرآمدی مدیریت مخاطره در ارائه خدمات پرداخت می‌پردازد؛ و قسمت "ز" نیز یک جمع‌بندی نهایی و دورنمایی از آینده (نسل سوم؛ 3G) ارائه می‌کند.

هدف این فصل ارائه مجموعه‌ای از راهکارهای مدیریت مخاطرات و تأمین امنیت برای بانکها و سیستمهای پرداخت است. این فصل تلاش می‌کند بستری برای ارزیابی

۱۳۲ مراجعه کنید به مقالهٔ بانک جهانی به قلم Tom Kellerman تحت عنوان:
"Mobile Risk Management: e-Finance for the Wireless Environment (2002)": http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/SearchGeneral?openform&E-Security/E-Finance&Publications

133 Wireless Local Area Networks
134 Global System for Moblile Communication Networks

مخاطرات امنیتی ارائه کند که در محیط بی‌سیم قابل کاربرد باشد.

الف. کلیات خدمات مالی الکترونیکی[۱۳۵]

خدمات مالی الکترونیکی چه بصورت اینترنتی و چه با مکانیزمهای راه دور، رشد سریعی داشته‌اند. کشورها و مصرف‌کنندگان با روند فزاینده‌ای به هم متصل می‌شوند. این فناوریها نه تنها کشورهای عضو در شبکه را گسترش می‌دهند، بلکه راههای جدیدی برای ارائه خدمات مالی بوجود می‌آورند. از اواسط دهۀ ۹۰ سرمایه‌گذاریهای صنعت بانکداری برای افزایش رضایتمندی مشتریان روی بانکداری اینترنتی تمرکز کرده‌اند. خدمات مالی الکترونیکی منجر به کاهش هزینه‌های خدمات مالی شده است. شبکۀ اینترنت علاوه بر صرفه‌جویی در هزینه‌های ثابت توسعه و نگهداری شعب، بسیاری از مراحل اضافه را نیز حذف کرده و هزینه‌ها را کاهش داده است. انجام یک تراکنش عادی از طریق یک شعبه یا تماس تلفنی هزینه‌ای معادل یک دلار آمریکا دارد، درحالیکه انجام همان تراکنش بصورت اینترنتی هزینه‌ای معادل ۰،۰۲ دلار خواهد داشت. هزینه‌های نازل خدمات مالی اینترنتی باعث رواج استفاده از آن شده است. خدمات مبتنی بر اینترنت در بازارهای درحال رشد گاهی اوقات به اندازۀ خدمات صنعتی رایج هستند. برای مثال بانکداری اینترنتی در برزیل همچون ایالات متحده گسترش یافته است. به علت عدم وجود زیرساخت مناسب خطوط در غالب کشورهای درحال توسعه، بیشتر مؤسسات مالی خدمات خود را در بسترهای بی‌سیم پیاده‌سازی کرده‌اند تا دسترسی به آنها را گسترش داده باشند. همزمان با این واقعیتها، چهار گرایش مرتبط با فناوری جدید در صنعت ایجاد شده است: برونسپاری، معماری باز، استراتژیهای یکپارچه، و روشهای جدید پرداخت الکترونیکی.[۱۳۶]

خدمات مالی الکترونیکی از چهار قسمت اصلی تشکیل شده: *انتقال سرمایه‌های الکترونیکی* (EFT)[۱۳۷]، *تبادل دادۀ الکترونیکی* (EDI)[۱۳۸]، *انتقال سود الکترونیکی* (EBT)[۱۳۹] و *تأیید تجارت الکترونیکی* (ETC)[۱۴۰]. EFT در واقع قدیمی‌ترین صورت تبادل پول الکترونیکی است که از اوایل دهۀ ۱۹۶۰ مرسوم شد. در مقیاس جهانی مقدار بسیار زیادی EFT در داخل و میان بانکها وجود دارد که خزانۀ ایالات متحده میزان آنرا حدود ۲ تریلیون دلار در روز یا ۷۰۰ تریلیون دلار در سال تخمین زده است. بخش عمده‌ای از EFT بانکیِ شبکۀ SWIFT بوسیلۀ خطوط بین‌المللی ماهواره صورت می‌گیرد. درحال حاضر حدوداً نیمی از ۲۰۰ کشور دنیا اینترنت و شبکه‌های داخلی بزرگ خود را از طریق خطوط ماهواره‌ای تأمین می‌کنند. اگرچه غالب این کشورها از لحاظ اقتصادی توسعه یافته هستند، اما این مسئله باعث ترافیک زیاد و حجم وسیع عملیات اقتصادی می‌شود؛ و این مسئله از نقطه‌نظر آسیب‌پذیریهای امنیتی یک دغدغۀ بزرگ به حساب می‌آید.[۱۴۱] تا سال ۲۰۰۵ سهم بانکداری اینترنتی در کشورهای صنعتی از ۸،۵٪ به ۵۰٪ و در بازارهای درحال رشد از ۱٪ به ۱۰٪ خواهد رسید. درصورت برقراری بهتر اتصالات در بازارهای درحال رشد ممکن است تراکنشهای بانکداری اینترنتی در سال ۲۰۰۵ تا ۲۰٪ افزایش یابند؛ که رقمی بیش از شش تریلیون دلار معاملۀ اینترنتی *تجارت-به-تجارت* (B2B)[۱۴۲] خواهد بود.[۱۴۳]

در پی رشد خدمات مالی الکترونیکی یک نگرش دیگر نیز درحال شکل‌گیری است: گسترش روزافزون کاربرد ارتباطات بی‌سیم در کشورهای توسعه‌یافته و درحال توسعه. این رسانۀ نسبتاً جدید بسرعت درحال تبدیل شدن به رسانۀ اصلی تجارت الکترونیک و خدمات مالی الکترونیکی است. تحول کسب و کارها از سیستمهای کاغذی به بسترهای مبتنی بر اینترنت بسیار عمیق بوده است. همینطور که بستر انواع خدمات از خطوط زمینی به فناوریهای بی‌سیم با امکان

---

۱۳۵ *برای مشاهدۀ یک تحلیل دقیقتر در زمینۀ امنیت الکترونیکی به منبع زیر نوشتۀ T. Glaessener ،T. Kellerman، و V. McNevin (سال ۲۰۰۲) مراجعه کنید:*
"E-Security Risk Mitigation for Financial Transactions"

136 *Gilbride, Edward. Emerging Bank Technology and the Implications for E-crime Presentation, September 3, 2001*

137 *Electronic Funds Transfers*
138 *Electronic Data Interchange*
139 *Electronic Benefits Transfers*
140 *Electronic Trade Confirmation*
141 *Dr. Joseph N. Pelton, "Satellite Communications 2001: The Transition to Mass-Consumer Markets, Technologies, and Systems".*
142 *Business To Business*
143 *Jupiter Communications, 2001*

دسترسی بیشتر تبدیل می‌شود، اثرات منفی این پدیده نیز گسترش می‌یابد.

دستگاههای سیار امروزه بعنوان لبهٔ درحال پیشرفت فناوریهای جهان محسوب می‌شوند. در سال ۱۹۹۰ تنها یازده میلیون مشترک تلفن همراه در تمام دنیا وجود داشت.[۱۴۴] تا سال ۱۹۹۹ و با گسترش فناوریهای بی‌سیم این رقم به چیزی فراتر از پانصد میلیون رسید و درحال حاضر نیز تقریباً دو برابر آن مقدار شده است. بررسی آمار مشابه در کشورهای درحال توسعه، جهشی که در اثر استفاده از دستگاههای سیار بوجود آمده را بخوبی نشان می‌دهد.[۱۴۵] کشور کامبوج درحالیکه پس از حدود ۲۰ سال جنگ شهری شبکهٔ خطی ثابت خود را از دست داده بود، با استفاده از فناوری بی‌سیم توانست بار دیگر اتصالات خود را برقرار کند. در خلال یکسال بعد از آغاز استفاده از فناوری بی‌سیم، تعداد مشترکان تلفنهای سیار از مشتریان تلفنهای ثابت پیشی گرفت. کامبوج درحالیکه یکی از کمترین درآمدهای سرانهٔ دنیا را دارد، در زمینهٔ گسترش عمومی تلفن از ۳۱ کشور – از جمله بعضی کشورها که درآمد بسیار بیشتری از آن دارند – پیشی گرفته است. کشورهای دنیا بجای صرف مقادیر فراوان منابع و زمان برای ایجاد زیرساختهای خطی ثابت جهت تسهیل ارتباطات، این ساختارهای سیمی را با برجهای ارزان تلفن همراه که تولید آنها نیز ساده‌تر است جایگزین نموده‌اند. البته این تحولات مخاطرات امنیتی چندی نیز به همراه داشته که بعضی از آنها بسیار جدی هستند.

توسعهٔ مداوم اقتصادی و راههای جدید ارائه خدمات مالی مثل پروتکلهای بی‌سیم، برای بانکها این امکان را بوجود آورده‌اند که بتوانند خدمات مالی را از راه دور ارائه کنند؛ اما نکته اینجاست که این موقعیتها محدود به اقتصاد رسمی نیستند. در کنار این پیشرفتها اقتصاد زیرزمینی و مجرمانه جهانی هم توانسته به خوبی خود را با فناوری وفق دهد. ارائه خدمات مالی بوسیلهٔ رسانه‌های بی‌سیم فرصتهایی را برای سرقت هویت، تبادل سرمایه‌های جعلی، و همچنین اخاذی فراهم کرده است.

ب. مخاطرات خدمات مالی الکترونیکی در شبکه‌های بی‌سیم

در کنار فواید زیاد فناوری جدید، مخاطراتی هم بوجود آمده است، چراکه فناوری روشهای جدید کلاهبرداری و سرقت را نیز تسهیل می‌کند. اکنون مسائلی چون جعل هویت، دسترسی از راه دور، و چاپ تصاویر اوراق بهادار با کیفیت عالی در دنیای اینترنتی وجود دارد و ابزارها و بسترهای چندمنظوره انجام آنها را تسهیل می‌کنند. با گسترش *دستگاههای خودپرداز تلفنی*[۱۴۶] که در مناطق درحال توسعه امکان استفاده از پول را بوجود می‌آورد، بزهکاران قادرند که اتصال بی‌سیم میان دستگاههای خودپرداز و بانک مادر را دستکاری نموده و کلیهٔ تبادلات ورودی و خروجی دستگاه خودپرداز تلفنی را تسخیر کنند. هنر نفوذ برخط در ابتدا یک تخصص پیچیده بود، اما عصر اطلاعات، زمینه را برای گسترش پایگاههای وب زیرزمینی مربوط به نفوذگران – که امروزه با ارائه ابزارهای مختلف برای نفوذ به زیرساختهای اقتصادی، از کلاهبرداریهای رایانه‌ای پشتیبانی می‌کنند – فراهم نموده است. بعنوان مثال پایگاههایی مانند www.astalavista.box.sk و یا www.attrition.org برنامه‌ها و ویروسهای مخربی دارند که برای افراد مبتدی امکان نفوذ به سیستمهای بانکی را فراهم می‌آورند. شرکت Internet Data Center (www.idc.com) اخیراً در گزارشی اعلام کرده که بیش از ۵۷٪ کل حملات سال گذشته، متوجه بخشهای مالی بوده است.

مخاطرات سنتی سالهای گذشته متحول شده‌اند. در طول تاریخ تا کنون کلاهبرداریها همواره شامل سوء استفاده از اسناد چاپی یا سوء استفاده از افراد بوده، اما در محیط الکترونیکی فرصتهای جدیدی برای جرائم اقتصادی بوجود آمده است. در سال ۲۰۰۱ بیش از یک چهارم (۲۷٪) پایگاه دادههای بانکی و مالی مورد دستبرد قرار گرفته‌اند.[۱۴۷] باندهای نفوذگران اروپای شرقی صدها بانک را در سرتاسر جهان مورد دستبرد قرار داده‌اند. درحال حاضر در جرائم

144 *Box 1 of "E-Finance in Emerging Markets: Is Leapfrogging Possible?", Claessens S., T. Glaessener, D. Klingebiel, 2001.*

۱۴۵ *قسمت اول کتاب:*
"E-Finance in Emerging Markets: Is Leapfrogging Possible?", 2001.
Claessens. S,T. Glaessner, D. Klingebiel به قلم

146 *Dialup ATM*

147 *Evans Data Corp. Survey*

سازمانیافته، نفوذ بعنوان مدلی برای کسب و کار مطرح است. بخش جرائم رایانه‌ای FBI اعلام کرده که اکثر بانکها به علت ترس از بی‌آبرویی و از دست دادن مشتریان، باج می‌پردازند. اخاذی Egghead در سال گذشته یک نمونهٔ مشهور است، که در آن نفوذگران پایگاه داده‌ای شامل ده هزار شمارهٔ کارت اعتباری را مورد حمله قرار دادند و برای اینکه آنها را در یک اتاق گفتگوی اینترنتی منتشر نکنند مبلغ گزافی را از شرکت مزبور باج‌خواهی کردند. بعد از آن نیز در شب کریسمس از موجودی هر کارت مبلغ کوچکی کم کردند. بنابراین مشکل فراتر از مسائل مالی و حیثیتی است. یک پیش‌بینی حاکی از این امر است که حوادث سرقت هویت در ایالات متحده بیش از سه برابر خواهد شد و از ۷۰۰,۰۰۰ دلار[۱۴۸] در سال گذشته به ۱،۷ میلیون دلار در سال ۲۰۰۵ خواهد رسید؛ و هزینهٔ بنگاههای اقتصادی هم با افزایش ۳۰٪ از مرز ۸ میلیون دلار در سال ۲۰۰۵ خواهد گذشت.[۱۴۹]

جرائم سایبر رشد چشم‌گیری داشته است. حمله به سرویس‌دهنده‌ها در سال ۲۰۰۱ نسبت به سال ۲۰۰۰ دو برابر شده و حدود ۹۰٪ شرکتهایی که مورد بررسی قرار گرفتند علیرغم برخورداری از انواع ویروس‌یابها، به ویروسها و کرمهای اینترنتی آلوده شده بودند.[۱۵۰] تحقیق سال ۲۰۰۱ CSI/FBI در مورد جرائم رایانه‌ای و امنیتی نشان داد که بدلیل نفوذها بیش از ۳۷۷ میلیون دلار خسارت به بار آمده است.[۱۵۱]

دلیل اصلی عدم برخورد مناسب با این دسته حوادث در دنیا ترس از انتشار اخبار آنها است.[۱۵۲] شرکتهای مالی بدلیل نگرانی از لکه‌دار شدن وجههٔ عمومی خود، از گزارش آسیبها و ضررهای وارده بیمناک هستند؛ و درنتیجه آسیب‌پذیر ماندن را ترجیح می‌دهند. اگر مشخص شود که یک بنگاه اقتصادی هدف کلاهبرداری رایانه‌ای قرار گرفته، مشتریان ممکن است اعتماد خود را از دست بدهند و از آن پس مایل نباشند اطلاعاتشان در پایگاههای آن بنگاه ذخیره شود. ضروری است که ارائه‌دهندگان خدمات اقتصادی، سیستمهای خود را به نحوی کنترل کنند که ضامن امنیت آنها باشد. رسانهٔ بی‌سیم – که در تمام جهان درحال توسعه است – رسانهٔ امنی نیست. شتاب چشمگیر کشورها جهت سازگاری با بستر فناوری بی‌سیم سرگردانی بزرگی ایجاد کرده است.

ج. شبکه‌های بی‌سیم محلی

شبکه‌های بی‌سیم درحال حاضر به سه شکل در دسترس می‌باشند: شبکه‌های بی‌سیم محلی که از پروتکل 802.11b استفاده می‌کنند؛ شبکه‌های CDMA/TDMA/GSM (تلفن همراه و PCS) مورد استفاده در تلفنهای بی‌سیم و PDAها؛ و سیستمهای مایکروویو پرقدرت که در شرکتهای تلفن جهت تبادل اطلاعات در مسافتهای طولانی کاربرد دارند. با اینکه هر سه مورد فوق در سراسر دنیا معمول هستند، اما همگی یک نقطه‌ضعف اساسی امنیتی دارند و آن استفاده از فرکانس رادیویی (RF) برای انتقال اطلاعات است؛ چراکه این مسئله می‌تواند به افشای داده‌های انتقالی بیانجامد.

شبکه‌های بی‌سیم بصورت انفجاری گسترش پیدا کردند. هزینهٔ ناچیز، سادگیِ نصب و برقراریِ مداوم اتصالات باعث گسترش سریع آنها – بخصوص در مؤسسات خدمات مالی – شده است. در واقع گمان می‌رفت که شبکه‌های بی‌سیم همان کاربرد شبکه‌های سنتی را داشته باشند اما بدون استفاده از کابل. گسترش این شبکه‌ها بدلیل سهولت کار کاربران است و درحال حاضر در ایالات متحده تحت

---

۱۴۸ *این آمار تنها نمایانگر جهتگیری سالانه در ایالات متحده است.*

۱۴۹ *این نتایج در گزارشی از مؤسسهٔ Celent Communications در سال ۲۰۰۱ منتشر شد و در آن از داده‌های FTC استفاده شده است.*

150 *http://www.infosecuritymag.com/articles/october01/images/survey.pdf*

۱۵۱ *نمایندهٔ ویژهٔ آنزمان در سرویس مخفی جرائم مالی، James Savage، گفته: "این آمار حکایت از اشکالات جدی در زیرساختهای حیاتی است، چراکه معنی آن این است که جامعهٔ تجاری تمایل دارد بپذیرد که از این نظر آسیب دیده". او معتقد است که این آمار تنها بیانگر یک قسمت جزئی از واقعیت آسیبهای وارده به جامعهٔ تجاری ایالات متحده می‌باشد. (۳ اکتبر ۲۰۰۳)*

۱۵۲ *نمایندهٔ مخصوص CERT، Cornelius Tate، به این تمایل به گریز از گزارش‌کردن رخدادها اینگونه اشاره می‌کند: "فکر می‌کنم ضررهای مالی بیش از مقداری است که گزارش می‌شود. بر اساس تجربهٔ من شرکتهایی وجود دارند که مایل نیستند ضررهای ناشی از مورد نفوذ قرار گرفتن خود را گزارش کنند. بنظر من سال به سال می‌توان افزایش زیادی در زیان شرکتها از آسیبهای اینچنینی مشاهده کرد، چراکه شرکتها بیشتر به این نتیجه رسیده‌اند که هر کس ممکن است هدف یک حمله قرار بگیرد، و قربانی شدن در حملات بتدریج مورد قبول واقع شده و دیگر انتشار اخبار مربوط به آن به اندازهٔ گذشته باعث از دست رفتن اطمینان عمومی نمی‌شود."*

استاندارد IEEE 802.11 و در اروپا تحت استاندار GSM ارائه می‌شوند. هنگام طراحی شبکه‌های بی‌سیم، نگرانیهای مهم امنیتی وجود دارد که باید به آنها توجه شود.

هفت دسته مخاطرات امنیتی اولیه در مورد شبکه‌های بی‌سیم قابل ذکر است:[۱۵۳]

۱. **حملات درج**[۱۵۴]: نفوذگر سعی می‌کند از طریق یک *نقطه دسترسی سیار*[۱۵۵] ناامن، به شبکهٔ شما "داده" وارد کند.

۲. **سرقت جلسه**[۱۵۶]: که به "man in the middle" نیز معروف است، بر اساس این ایده بوجود آمده که در سیستم تلفنهای بی‌سیم، تلفن هویت خود را برای ایستگاه ثابت تصدیق می‌کند، اما ایستگاه اینکار را برای تلفن انجام نمی‌دهد؛ پس می‌توان یک جلسهٔ بی‌سیم میان تلفن و ایستگاه ثابت را بدون اینکه تلفن بتواند به موضوع پی ببرد سرقت کرد و برای اینکار کافی است یک ایستگاه ثابت شبیه‌سازی شود.

۳. **پارازیت دادن:** این حمله از انواع حملات تخریب سرویس است که در آن نفوذگر با داده‌پراکنی و *پخش عمومی*[۱۵۷] در فرکانسِ کاریِ شبکهٔ شما سعی می‌کند در طیف فرکانس رادیویی شبکهٔ بی‌سیم ایجاد *سرریز*[۱۵۸] کند.

۴. **حملات رمزنگاری**[۱۵۹]: شبکهٔ بی‌سیم مبتنی بر IEEE 802.11 از الگوریتم *WEP*[۱۶۰] برای رمزگذاری استفاده می‌کند. روش رمزگذاری و بردارهای مقدار اولیهٔ این استاندارد بسیار ضعیف هستند و تاکنون بارها شکسته شده‌اند.

۵. **تصاحب ترافیک و انجام دیده‌بانی:** برد تقریبی نقاط دسترسی سیار در استاندارد 802.11b حدود ۳۰۰ فوت است. این به آن معناست که هر فردی با داشتن ابزار مناسب، درصورتیکه در محدوده ارسال بسته‌ها باشد، قادر به دریافت آنها خواهد بود. وسایل تقویت سیگنال و گسترش این محدوده نیز به وفور مهیاست؛ و لذا ناحیه‌ای که تصاحب ترافیک در آن ممکن است، وسیع و ایمن کردن آن مشکل می‌باشد.

۶. **ارتباط نقطهٔ سیار با نقطهٔ سیار دیگر:** اغلب نقاط سیار (مثل رایانه‌های قابل حمل و PDAها) درصورتیکه خدمات اشتراک فایل یا هرگونه خدمات TCP/IP روی آنها فعال باشد، قادر به ارتباط بی‌واسطه و مستقیم با یکدیگر هستند. این مسئله به این معنی است که هر نقطهٔ سیار قادر است یک فایل یا برنامهٔ خطرناک را از طریق شبکهٔ شما منتقل کند.

۷. **تنظیمات نادقیق:** هرگونه ابزار، خدمات، یا برنامهٔ کاربردی که بطور صحیح پیکربندی نشده باشد، کل شبکه را مورد مخاطره قرار می‌دهد. بسیاری از ابزارها و برنامه‌های کاربردی بی‌سیم، بطور پیش‌فرض بگونه‌ای تنظیم شده‌اند که هرگونه درخواست خدمات یا دسترسی را می‌پذیرند. این به آن معنا است که هر سرویس‌گیرندهٔ سیار دلخواه خواهد توانست درخواست جلسهٔ telnet یا ftp نموده و پاسخ آنرا دریافت کند.

۸. **حملات Brute Force**: اغلب نقاط دسترسی بی‌سیم، از یک کلید یا رمز عبور مشترک برای تمام ابزارهای شبکه استفاده می‌کنند. این مسئله شبکه‌های بی‌سیم را در برابر حملات brute force (مثلاً بر اساس یک فرهنگ لغت) ناامن کرده است.

War Driving

جاسوسی صنعتی و جرائم اداری با پیشرفت فناوریهای جدید به بالاترین حد خود رسیده‌اند. War dialing به معنای تماس با تمام شماره تلفنهای سازمان و یافتن شمارهٔ مودم‌های آن، جای خود را به war driving داده است. این مفهوم جدید یعنی جستجو برای یافتن شبکه‌های محلی بی‌سیم مؤسسات اقتصادی، و ضبط ترافیک شبکهٔ آنها با رایانهٔ قابل حمل. بنا به گفته *دیو توماس*[۱۶۱] بازرس ارشد بخش جرائم رایانه‌ای FBI، war driving پدیده‌ای درحال

۱۵۳ *این دسته‌بندی مربوط به یکی از اعضای مرکز تحلیل CERT است.*

154 Insertion Attacks
155 Mobile Access Point
156 Session Hijacking
157 Broadcasting
158 Flooding
159 Encryption
160 Wired Equivalent Privacy
161 Dave Thomas

بخش سوم

گسترش است که امنیت تمام شرکتها و مؤسساتی کـه دارای شبکه محلی بی‌سیم هستند را تهدید می‌کند.

این امکان وجود دارد که راهبر شبکه هنگام تنظیم و اسـتقرار شبکهٔ محلی بی‌سیم ببیند که رایانه‌های قابل حمـل تنهـا در فاصلهٔ محدودی از نقاط دسترسی می‌توانند به شـبکه متـصل شوند و درنتیجه گمان کند که سیگنالهای شبکه در فواصـلی دورتر از آن فاصله قابـل دسترسـی نیـستند، امـا ایـن فـرض نادرست است. در حقیقت سیگنالها در طول هزاران متر – تـا جایی که چیزی آنها را منحرف یا دچـار وقفـه نکنـد – قابـل دریافت هستند. دلیل آن استدلال غلط ایـن اسـت کـه آنـتن کوچک رایانهٔ قابل حمـل نمـی‌توانـد سـیگنالهای ضـعیف را دریافت کند؛ اما با استفاده از یک آنتن خارجی، می‌تـوان بـرد سیگنالها را افزایش داد. بخش بی‌سیم شبکه معمولاً بگونه‌ای است که نفوذگر برای دسترسی به ترافیک آن نیازی ندارد به چیزی دسترسی فیزیکی پیدا کند. به‌همین دلیل این شبکه‌ها نسبت به حملاتی چـون دزدی پیـام، تغییـر پیـام، یـا ارسـال پارازیت میان پیام، دارای ضعف هستند.

مسائل مذکور اهمیت پرداختن به مسئله امنیت در شبکه‌های بی‌سیم را روشن می‌کنند. هریک از ضعفهای فوق را می‌توان با استفادهٔ مناسـب از سیاسـتها و تجربیـات امنیتـی، طراحـی شبکه، برنامـه‌هـای کـاربردی امنیتـی و پیکربنـدی صـحیح کنترلهای امنیتی به حداقل رسانده و یـا از بـین بـرد. آخـرین فصلهای بخش سوم به اطلاعاتی دربـارهٔ نحـوهٔ امـن کـردن شبکه‌های محلی بی‌سیم می‌پردازند.

د. استاندارد تلفن همراه در اروپا: GSM

GSM گسترده‌ترین و درحال رشدترین استاندارد تلفن همراه دیجیتال مورد استفاده در جهان است. درحـال حاضـر چیـزی نزدیک به ۶۰۰ میلیون مشترک GSM در دنیا وجـود دارد – رقمی بیش از دو سوم تعـداد کـل ابزارهـای سـیاری کـه در جهان موجود است.[۱۶۲] این رقم با سرعت چهار کاربر جدید در ثانیه درحال افزایش است. پوشش GSM همهٔ قـاره‌هـا را در بر می‌گیرد، بطوریکه فناوریِ مورد اسـتفادهٔ ۴۰۰ ارائـه‌کننـدهٔ خدمات در بیش از ۱۷۰ کشور دنیا است. امـا ایـن تنهـا آغـاز انقلاب فناوری بی‌سیم است.

محققان صنعتی پیش‌بینی می‌کنند که تا پایان سال ۲۰۰۵ در حدود ۱،۴ میلیارد کاربر GSM وجود خواهد داشت. تلفنهـای GSM در داخل خـود دارای یـک کـارت کوچـک هوشـمند هستند که مشخصات تلفن را در خود ذخیره می‌کند و به نـام *واحد شناسایی مشتری* (SIM)[۱۶۳] شناخته می‌شود. SIM بایـد از مشخصات بصورت محرمانـه و رمزنگـاری‌شـده نگهـداری کند؛ لذا به کارت SIM هم می‌توان بعنوان یک نقطهٔ قوت و هم بعنوان یک نقطهٔ ضعف امنیتـی در فنـاوری GSM نگـاه کرد.

نقاط ضعف GSM

آسیب‌پذیریهای کارت SIM

در سیستمهای GSM آمریکا و اروپا، روش دستیابی به شبکه یکسان است. کارتهـای هوشـمند قابـل جابجـایی در تلفنهـا (کارتهای SIM) برای نگهداری شماره‌هـای تمـاس، اطلاعـات حساب کاربری، و نرم‌افزارهای جانبی مثل مرورگـر وب بکـار می‌روند. داده‌های ذخیره‌شده در کارتها رمزنگاری مـی‌شـوند، اما الگوریتم COMP128 که در اینکار بکار می‌رود پـیش از این شکسته شده و لذا این کارتها در برابر کپی‌برداری (سـاخت یک نسخهٔ مشابه از خـود) ایمـن نیـستند. *War driving* بـرای مشترکین تلفنهـای همـراه کـه از اسـتاندارد GSM اسـتفاده می‌کنند مسئله خطرناکی نیست. مستقل از طیف فرکانسی، با ارسال پارازیت براحتی می‌تـوان سـیگنالهای تلفـن همـراه را دچار وقفه کرد. یک روش بسیار معروف برای بدسـت آوردن *کلید رمزگذاری‌شدهٔ گفتگوی GSM*[۱۶۴] در کمتر از یک ثانیه وجود دارد که در آن از یک رایانهٔ شخصی استفاده می‌شود.

---

۱۶۲ *سیستم GSM آمریکای شمالی درحال حاضـر هنگـام ارتبـاط بـا خدمات رایانه‌های شخصی با سـرعت 1900MHz کـار مـی‌کنـد. خدمات داده‌ای GSM عبارتنـد از SMS (Short Message Servise)، CSD (Analog Cellular Switched Data)، و GPRS (General Packet Radio Service). بیشتر شرکتهای ارائه‌کنندهٔ خدمات تلفن همراه گونـه‌ای از GSM را بکـار مـی‌برنـد کـه یـا در 900MHz و یـا در 1800MHz کار می‌کند. علاوه بر این کـشورهای اروپـایی مـی‌توانند از مدار سوئیچی پرسـرعت داده (High Speed Circuit Switched Data، HSCSD) اسـتفاده کننـد، کـه مـی‌توانـد کانالهـای ارتبـاطی مختلـف را در یـک کانـال بـا قابلیـت کـار 38.4KBPS ادغام کند. GPRS در بیشتر کشورها وجود دارد.*

163 *Subscriber Identification Module*

164 *Encrypted GSM Conversation Key*

امنیت فناوری GSM بستگی به شرایط دارد. از کارت SIM می‌توان نسخهٔ بدل ایجاد نمود. نفوذ به آن نیز امکانپذیر است؛ چراکه الگوریتمهای حساس آن شکسته شده‌اند. این مشکل آخر می‌تواند به ناامن شدن کامل مکالمات تلفنی GSM نیز منجر شود.

در مورد استفادهٔ یک بانک از فناوری GSM مشکلات دیگری هم وجود دارند. برای مثال اگر یک دستگاه خودپرداز راه دور نتواند با یک برج مخابراتی واقعی ارتباط برقرار کند، می‌توان آنرا برای برقراری ارتباط با یک برج جعلی فریب داد. انجام اینکار برای نفوذگر امکان کنترل نقل و انتقالات انجام گرفته در آن دستگاه خودپرداز را پدید خواهد آورد.

آسیب‌پذیری SMS

GSM *خدمات پیامهای کوتاه* (SMS)[۱۶۵] را نیز ارائه می‌دهد. SMS در سیستم GSM کاربردهای گوناگونی دارد، از جمله اعلانهای پست صوتی، به روزرسانی SIM مشتری، ارسال پیامهای کوتاه متنی، و ارتباط با دروازه‌های پست الکترونیکی. با وجود اینکه موارد فوق خدمات پرکاربردی هستند، اما مخاطرات امنیتی جدیدی برای شبکه بوجود می‌آورند. SMS نوعی سرویس ذخیره و ارسال پیام است که ذاتاً ناامن می‌باشد، چراکه در آن تمام پیامها بصورت متن‌ساده و رمزنشده تبادل می‌شوند و ذخیره‌سازی آنها در مرکز SMS پیش از ارسال به مقصد نیز بصورت رمزنشده است. از دیگر مشکلات SMS تأخیر در رسیدن پیام به مقصد می‌باشد. تراکنشهایی که از نظر زمانی اهمیت زیادی دارند نمی‌توانند به این سرویس اطمینان کنند. از طرف دیگر نرم‌افزارهای رایگان زیادی وجود دارند که می‌توان بوسیلهٔ آنها SMS جعلی ساخت، به گوشی‌ها و مراکز SMS سیلی از بمبهای SMS فرستاد، و یا بسته‌های SMS را بگونه‌ای طراحی کرد که منجر به خرابی نرم‌افزارها در بیشتر گوشی‌ها شوند.

فناوری جعبه‌ابزار SIM (STK)[۱۶۶] می‌تواند برای رمزنگاری SMS بکار رود. با اینحال STK یک ساز و کار امنیتی *لایهٔ انتقال*[۱۶۷] است، و نمی‌تواند *محرمانگی پایانه به پایانه*[۱۶۸] را تضمین کند. یک روال دیگر بهبود امنیت SMS می‌تواند بررسی شخصی مشتریان برای یک قطعه پیام قراردادی بمنظور تضمین کل پیام و ارائه‌کنندهٔ خدمات و درنتیجه بررسی شماره‌تلفنهای ثبت‌شدهٔ مشتریان باشد.

آسیب‌پذیری GPRS

GPRS[۱۶۹] نوعی خدمات مبتنی بر IP است که برقراری اتصال دائمی به اینترنت را تضمین می‌کند. مشکل عمدهٔ این مکانیزم این است که هنوز برای تقاضاهای WAP به SMS وابستگی دارد. یک بستهٔ SMS تقلبی می‌تواند به یک تلفن فرستاده شود و یک پایگاه وب جعلی را باز کند، و کاربران را طوری فریب دهد که اطلاعات خود را در یک فرم که گمان می‌کنند از ایمنی برخوردار است اما در حقیقت تقلبی است وارد کنند. بسیاری از تلفنهایی که قابلیت GPRS دارند از قابلیت bluetooth نیز برخوردارند. هر دستگاه با قابلیت bluetooth شامل یک آدرس منحصر به فرد است که به کاربر امکان می‌دهد به نوعی به شخصی که در طرف دیگر ارتباط است نوعی اعتماد پیدا کند. همینکه این شناسه به یک کاربر اختصاص داده شد، با دنبال کردن پیامها و بررسی شناسهٔ آنها می‌توان فعالیتهای کاربر را ضبط نمود. در ابزارهای مبتنی بر bluetooth برای برقراری ارتباط، یک فرآیند مقداردهی اولیه آغاز می‌شود که برای تصدیق هویت از یک PIN استفاده می‌کند. اگرچه برخی ابزارها به شما اجازه وارد کردن شمارهٔ PIN را می‌دهند، اما می‌توان PIN را در حافظهٔ یک دستگاه الکترونیکی یا دیسک سخت نیز ذخیره نمود. درصورتیکه امنیت فیزیکی دستگاه تأمین نباشد ممکن است مشکلات عدیده‌ای به بار بیایند. همچنین رمزهای غالب PINها اعداد چهار رقمی هستند، و شاید در نیمی از موارد این عدد 0000 باشد.

امنیت bluetooth در گرو نگهداری از کلید رمزنگاری بصورت یک راز مشترک میان اعضای شبکه است. اما تصور کنید من و شما با تلفنهای همراه خود که قابلیت bluetooth دارند درحال مکالمه هستیم. برای برقراری امنیت مکالمه، من با استفاده از کلید شما داده‌های مکالمه را رمزنگاری می‌کنم. کمی بعدتر یکی از دوستانتان با شما تماس می‌گیرد و شما مجدداً از کلید خود استفاده می‌کنید. من که کلید شما را می‌دانم با استفاده از یک آدرس جعلی

165 *Short Message Service*
166 *SIM Toolkit Technology*
167 *Transport Layer*
168 *End-to-End Confidentiality*

169 *General Packet Radio Service*

می‌توانم نوع رمزگذاری را تشخیص دهم، و به مکالمهٔ شما گوش کنم. همچنین می‌توانم خودم را به جای شما یا کسی که درحال مکالمه با شما است جا بزنم. بنابراین bluetooth تنها ابزارها را تصدیق هویت می‌کند، نه کاربران را.

ضعفهای WAP

نقطه‌ضعف مشترک تمام ابزارهای بررسی شده – صرفنظر از نوع شبکه – استاندارد *پروتکل کاربرد بی‌سیم* (WAP)[۱۷۰] است که از *زبان علامتگذاری بی‌سیم* (WML)[۱۷۱] و *زبان علامتگذاری وسایل دستی* (HDML)[۱۷۲] تشکیل شده است. توسعه‌دهندگان برای راحت‌تر شدن کار، تا حد ممکن تلاش می‌کنند طراحی سناریوها بگونه‌ای باشد که کاربر هنگام استفاده از خدمات مختلف ملزم به وارد کردن کوتاهترین ورودی ممکن باشد – مثلاً اعدادی که بعنوان شماره کارت اعتباری یا شمارهٔ حساب شخصی وارد رایانه می‌شوند. این به آن معنا است که همچنان قسمت اعظم این داده‌ها درون سرویس‌دهنده ذخیره می‌شوند، و در وسیلهٔ دستی مربوطه تنها یک cookie حاوی رمز عبور قرار دارد؛ که بسیاری اوقات برای کارهایی مثال خرید اینترنتی یا انتقال سرمایه صرفاً به یک PIN نیاز دارد و گاهی حتی از آن هم بی‌نیاز است. بنابراین مسئله امنیت تبادلات میان دستگاهها در شبکهٔ بی‌سیم بر عهدهٔ استاندارد دیگری به نام *امنیت لایهٔ انتقال بی‌سیم* (WTLS)[۱۷۳] می‌باشد.

تا زمانیکه از که از استاندارد *SSL*[۱۷۴] ۱۲۸ بیتی موبایل یا پروتکل IPSec (که بیشتر گوشی‌ها بدلیل کمبود پهنای باند و قدرت پردازش از آن پشتیبانی نمی‌کنند) استفاده نشود، همواره در قسمتی از شبکه یک حلقهٔ ضعیف امنیتی وجود دارد که می‌تواند مورد سوء استفاده قرار بگیرد. حتی در اینصورت نیز ضعفهای امنیتی در داخل وسیله (و نه کانال ارتباطی) همچنان وجود خواهد داشت؛ و لذا امنیت ارتباط به سادگی خدشه‌دار می‌شود. GSM از WAP و WTLS استفاده می‌کند که معادل SSL است اما با یک الگوریتم رمزگذاری ضعیفتر. WTLS با SSL که یک استاندارد صنعتی است سازگار نمی‌باشد. پیامهای بی‌سیم درون یک gateway می‌روند و از آنجا وارد یک شبکه سیمی می‌شوند تا به سمت مقصد نهایی خود هدایت گردند. در آن gateway، پیام WTLS به SSL تبدیل می‌شود. در gateway پیام برای چند ثانیه رمزگشایی می‌گردد و همین امر باعث می‌شود که کل ارتباط نسبت به دزدیِ پیام آسیب‌پذیر گردد.

ه. راه‌حلهای امنیتی برای GSM

نقایص ذاتی GSM براحتی قابل رفع نیستند. تلفنها و PDAهایی که از فناوری GSM استفاده می‌کنند عموماً قادر به استفاده از نرم‌افزارهای محافظ نمی‌باشند. اگرچه GSM مثل همتای آمریکایی خود – استاندارد 802.11 – نسبت به war driving آسیب‌پذیر نیست، اما چند نقطه‌ضعف اساسی دارد. استاندارد 802.11 مربوط به رایانه‌ها است و نه وسایل گوشی‌دار، و لذا امنیت در آن می‌تواند به طرز مؤثری نسبت به GSM بهبود یابد. شبکه‌های خصوصی مجازی (VPNها) فصل مشترک آسیب‌پذیریهای این دو استاندارد هستند، و استفاده از VPN معمولاً بعنوان راه‌حلی برای رفع آسیب‌پذیریهای فعلی 802.11 و GSM بشمار می‌رود. با اینحال در امنیت چندلایه نمی‌توان از یک لایهٔ خاص انتظار معجزه داشت. اطلاعات بیشتر در مورد امنیت شبکه‌های بی‌سیم را می‌توانید در پایان همین بخش کتاب و نیز بخش پنجم (امنیت فناوری اطلاعات و راهبران فنی) بیابید.

و. تجارب امنیت بانکداری

در نتیجهٔ گسترش فراوان استفاده از GSM در خدمات مالی الکترونیکی، استانداردهای کنترلی و امنیتی چندی بوجود آمده‌اند که مؤسسات مالی درصورت استفاده از دسترسی بی‌سیم در خدمات پرداخت باید آنها را مورد توجه قرار دهند.

پرداخت از طریق شخص ثالث

بعنوان یک قاعدهٔ کلی، بانکها باید مستقیماً مشتریان خود را در معاملات مالی بی‌سیم تصدیق هویت کنند. ممکن است بعضی از مشتریان به بانک اختیار دائمی بدهند که بتواند از حساب آنها اعتبار برداشت کند و به حساب برخی اشخاص ثالث واریز نماید. چنین توافقهایی می‌تواند از طریق *موافقتنامه‌های تصدیق اعتبار حسابرسی مستقیم*[۱۷۵] صورت

170 Wireless Application Protocol
171 Wireless Markup Language
172 Handled Device Markup Language
173 Wireless Transport Layer Security
174 Secure Socket Layer
175 Direct Debit Authorization Agreements

بگیرد. با اینحال درصورت عمل به این موافقتنامه‌ها، اشخاص ثالث نباید بتوانند شناسه‌های بانکی مشتریان (IDها و PINها) را بدست آورند یا آنها را ذخیره نمایند.

حسابهای ذخیره

حسابهای ذخیره (SVA)[۱۷۶] توسط مشتریانی استفاده می‌شود که بصورت دوره‌ای به این حسابها پول واریز می‌کنند. SVA می‌تواند روی دستگاههای سیار قرار گیرد. هنگام انجام عملیات پرداخت، هیچ حساب بانکی نباید مورد دسترسی قرار گیرد. برای انتقال اعتبار از یک حساب بانکی به یک حساب SVA حتماً صاحب آن حساب بانکی باید شخصاً به اینکار اقدام کند.

پرداختهای نزدیک بی‌سیم

خدمات *پرداخت نزدیک بی‌سیم*[۱۷۷] معمولاً برای خرده‌فروشیهای خارج از تعداد بکار می‌روند. این تراکنشها تنها باید زمانی کامل شوند که مشتری در نقطهٔ فروش صراحتاً تصدیق هویت شود. اگر چنین تصدیق هویتی صورت نگرفته باشد، این امکان وجود خواهد داشت که حساب بانکی مشتری از طریق SVA مربوطه بطور غیرارادی دچار کسری گردد. بنابراین برای هر نوع درخواست پرداخت وجه، تصدیق هویت صریح مشتری باید اجباری باشد.

پاسخ تعاملی صوتی

خدمات *پاسخ تعاملی صوتی سیار* (Mobile IVR)[۱۷۸] نسبت به استراق‌سمع آسیب‌پذیر هستند. از سیستمهای IVR نباید برای خدمات پربها و یا پرمخاطره استفاده کرد. تمام اتصالات IVR – از جمله شماره تلفن تماس‌گیرنده و ترتیب تراکنشهای انجام‌شده توسط مشتری باید ثبت شود؛ اما این ثبتها به هیچوجه نباید شامل PIN و اطلاعات تصدیق هویت مشتری گردد.

آموزش مشتری

بانکها باید مصرف‌کنندگان خدمات مالی الکترونیکی بی‌سیم را به روشهای زیر آموزش دهند:

- به مشتری باید توصیه شود که برای خدمات مختلف از PINهای متفاوت استفاده کند.
- برای استفادهٔ ایمن از برنامه‌های بانکداری و پرداخت سیار باید دستورالعملهایی در زمینهٔ پیکربندی ابزارهای سیار به مشتری داده شود.
- اطلاعات لازم در مورد مواجهه با مشاجرات، روالهای گزارش‌دهی و زمان مورد انتظار رفع و رجوع شکایات باید به مشتری ارائه گردد.

نگاه به آینده: فناوری نسل سوم

نسل سوم فناوری بی‌سیم به اختصار 3G خوانده می‌شود و به پیشرفتهای ارتباطات بی‌سیم در استانداردهای مختلف اشاره دارد. هدف اولیهٔ این طرح بالابردن سرعت انتقال از ۹،۵ کیلوبیت در ثانیه به ۲ مگابیت در ثانیه است. در زمینهٔ امنیت سیستمها و ارتباطات، هدف اصلی طراحی یک سیستم بدون نقص نیست، بلکه طراحی سیستمی است که اگر نیاز به آن احساس شد بتواند با پیشرفتهای امنیتی سازگاری پیدا کند. بسیاری از حملاتی که وقوع آنها در شبکه‌های نسل دوم و حتی کمی پیشرفته‌تر از آن ممکن بود، در محیطهای نسل سوم بکلی حذف شده‌اند.

استحکام ساختار امنیتی نسل سوم

امنیت نسل سوم بر مبنای امنیت GSM طراحی شده است، اما با تغییرات زیر:

- یکی از تغییرات برای غلبه بر حمله‌ای موسوم به *ایستگاه ثابت جعلی*[۱۷۹] انجام گرفت. در این مکانیزم امنیتی یک شمارهٔ توالی به داده‌های تصدیق هویت اضافه می‌شود که تضمین می‌کند دستگاه سیار خواهد توانست شبکه را مورد شناسایی قرار دهد.
- طول کلید رمز افزایش یافته تا امکان استفاده از الگوریتمهای رمزگذاری قویتر هم فراهم شود.
- مکانیزمهایی برای بهبود امنیت داخل شبکه‌ها و ارتباطات میان آنها لحاظ شده است.

176 *Stored Value Accounts*
177 *Close Proximity Wireless Payments*
178 *Mobile Interactive Voice Response*
179 *False Base Station*

- امنیت به جای ایستگاه ثابت مبتنی بر سوئیچ شده (مثل GSM). بنابراین اتصالات میان ایستگاه ثابت و سوئیچ مورد محافظت قرار دارند.
- *مکانیزمهای یکپارچگی هویت پایانه* (IMEI)[۱۸۰] بجای آنچه که در GSM وجود داشت، از نو طراحی شده‌اند.
- الگوریتم تصدیق هویت تعریف نشده، اما راهنمایی برای انتخاب یک الگوریتم ارائه می‌شود.
- در زمان گشت‌زدن میان شبکه‌ها، مثلاً بین GSM و 3GPP، تنها سطحی از پشتیبانی که بوسیلهٔ کارت هوشمند صورت گرفته اعمال می‌شود. بنابراین کارت هوشمند GSM در شبکه 3GPP در برابر حملهٔ ایستگاه ثابت جعلی همچنان مورد محافظت قرار ندارد.

سیستم نسل سوم نسبت به همتای GSM خود از امنیت بسیار بیشتری برخوردار است. البته همانطور که گفته شد هوشمندی و زیرکی مهاجمین را هیچگاه نباید دست کم گرفت. بنابراین از دید مبتنی بر تئوری، در شبکه‌های نسل سوم نیز امکان وقوع حملات جدی وجود دارد که ذیلاً به آنها اشاره می‌شود.

اعتماد به ایستگاه ثابت جعلی

این حمله، حمله‌ای است که به یک ایستگاه ثابت یا ایستگاه سیار دستکاری‌شده نیاز دارد و از این آسیب‌پذیری استفاده می‌کند که ممکن است کاربر به یک ایستگاه ثابت جعلی متصل شود. یک ایستگاه ثابت جعلی می‌تواند گاهی در نقش تکرارکننده و گاهی نیز در نقش تقویت‌کنندهٔ درخواستهای تبادلی میان شبکه و کاربر عمل کند، و در این میان درخواستها یا پیامهای مورد نظر را تغییر دهد.

معماری امنیتی نمی‌تواند از دستکاری پیامهای تبادلی میان شبکه و کاربر جلوگیری نماید. حفاظت از جامعیت پیامهای حیاتی شبکه می‌تواند به پیشگیری از وقوع برخی حملات تخریب سرویس – که با ایجاد تغییر در محتوای پیام صورت می‌گیرد – نیز کمک کند. در اینجا، حملهٔ تخریب سرویس تنها تا زمانی می‌تواند ادامه یابد که نفوذگر فعال باشد؛ برخلاف حملات بالا که بعد از پایان دخالت نفوذگر هم ادامه پیدا می‌کنند. این حملات قابل قیاس با حملاتی چون ارسال پارازیتهای رادیویی هستند که اگر بخواهیم آنها را در تمام سیستمهای رادیویی خنثی کنیم، با مشکلات زیادی روبرو هستیم.

اجبار به ارتباطات رمز نشده

این نوع حمله نیز به یک ایستگاه ثابت یا ایستگاه سیار دستکاری‌شده نیاز دارد. زمانیکه کاربر مورد نظر به ایستگاه ثابت جعلی اعتماد می‌کند، مهاجم قربانی را با یک تماس تلفنی مخاطب قرار می‌دهد. کاربر نیز روال راه‌اندازی اولیه را – که مهاجم میان شبکهٔ ارائه‌کنندهٔ خدمات و او برقرار کرده – آغاز می‌کند و باعث می‌شود عناصر ارسال سیگنالها طوری تغییر کنند که برای شبکه اینطور بنظر برسد که گویی کاربر مورد نظر نمی‌خواهد در تبادل داده‌ها از رمزگذاری استفاده کند. پس از تصدیق هویت، مهاجم ارتباط خود با کاربر را قطع می‌کند و با حق‌اشتراک آن کاربر، از شبکه برای برقراری تماسهای جعلی استفاده می‌نماید.

حفاظت از جامعیت پیامها می‌تواند به جلوگیری از این نوع حمله منجر شود. بطور خاص، تصدیق هویت داده‌ها و جلوگیری از ارسال غیرمستقیم درخواستهای اتصال، به شبکه امکان می‌دهد که اعتبار درخواستهای مشروع را تشخیص دهد. بعلاوه ارسال دوره‌ایِ پیامهای حفاظت‌شدهٔ جامعیت در طول یک اتصال، به جلوگیری از سرقت اتصالات رمزنشده پس از برقراری اولیهٔ اتصال کمک می‌کند. با اینحال سرقت اتصال میان پیامهای دوره‌ای حفاظتی نیز ممکن است، هرچند معمولاً چندان بکار نفوذگران نمی‌آید. بطور کلی اتصالاتی که رمزگذاری آنها غیرفعال است همیشه در برابر دسته‌ای از حملات آسیب‌پذیر هستند.

مجدداً این نکته را یادآوری می‌کنیم که این قبیل حملات بر اساس اینکه فناوری چگونه مورد استفاده قرار بگیرد همگی جنبهٔ تئوری دارند. در کل، سیستمهای نسل سوم از لحاظ فناوری امنیتی پیشرفت کرده‌اند، اما برای پشتیبانی از امنیت ارتباطات سیار، لازمست ، سایر مراقبتهای امنیتی نیز بصورت مداوم رعایت شوند.

180 *Integrity Mechanisms for the Terminal Identity*

ز. نتیجه‌گیری

باید گفت که هر چه شبکه‌ها بیشتر توزیع‌شده باشند، قابلیت استراق‌سمع و دسترسی غیرمجاز در آنها بیشتر می‌شود. بیشترین آسیب‌پذیری استراق‌سمع معمولاً در نقاطی است که کابلهای فیبر، سیمهای مسی، ماهواره و سیستمهای بی‌سیم زمینی به هم متصل می‌شوند. استانداردهای واسطهای هوایی یکی از مثالهای مخابرات مدرن و سیستمهای فناوری اطلاعات هستند که می‌توانند مورد استراق‌سمع قرار گیرند.

همانطور که *پلتن مرج*[۱۸۱] اشاره کرده، "این گرایش بازار به تداوم ارتقای کیفی استانداردهای یکپارچهٔ واسطها بوده که امکان اتصال بی‌عیب و نقص فناوریهای مختلفی مثل فیبر، سیمهای مسی، بی‌سیم زمینی، ماهواره و دیگر فناوریهای درحال رشد را فراهم کرده، اما چالش آنجا بوجود می‌آید که بخواهیم استانداردی تهیه کنیم که در عین برقراری ارتباط قابل اطمینان و ساده میان این فناوریها، امنیت را نیز فراهم کند."

یک راه‌حل ممکن، بازنگری در مدل هفت‌لایه‌ای مخابرات ISO و بطور خاص ایجاد یک لایهٔ جدید – برای تأمین امنیت لازم بر مبنای یک کد ۲۵۶ یا حتی ۱۰۲۴ بیتی که قابل به‌روزرسانی باشد – است. اینکه راه‌حل نهایی برای دستیابی به این هدف ایجاد یک لایهٔ جدید است یا می‌توان از مهندسی مجدد قسمتی از لایه‌های فعلی نتایج بهتری گرفت همچنان به مطالعه بیشتر نیاز دارد. به هر ترتیب مخاطرات خدمات مالی بی‌سیم همچنان بسیار زیاد است.

تهدیدهایی که از جانب پروتکلهای 802.11 و GSM متوجه محرمانگی و جامعیت ارتباطات شده را می‌توان تا حد زیادی کاهش داد. علاوه بر استفاده از VPNها، حفاظت از gatewayها و سرویس‌دهنده‌ها هم بسیار ضروری است. این نکته برای بانکها بسیار اهمیت دارد که در کنار استفاده از VPN برای برقراری دسترسی مجاز، روشهای مختلف دیگر را نیز برای محافظت از منابع شبکه بکار گیرند. بانکها و شرکای مخابراتی آنها باید به پیاده‌سازی ساز و کارهای امنیت چندلایه بخصوص در سطح gatewayها اقدام کنند. به موازات استفادهٔ روزافزون تجارت و اقتصاد از فناوریهای یکپارچه و آسیب‌پذیر، کاهش مخاطرات فناوری ارتباطات سیار حیاتی‌تر می‌شود. سازگاری روزافزون نهادهای اقتصادی با شبکه‌های محلی بی‌سیم و فناوری GSM باعث تضعیف امنیت سیستمهای دریافت و پرداخت شده، و این درحالی است که این واسطهای نفوذپذیر اساساً برای تبادل سرمایه‌های دیجیتالی طراحی نشده بودند. در همانحال که گرایشهای خدمات مالی الکترونیکی ادامه می‌یابد، "مدیریت مخاطرات سیار" نیز در سالهای پیش‌رو برای صنعت بانکداری اهمیت فزاینده‌ای خواهد یافت.

181 Pelton Merge

فصل یازدهم
الگوهای سرآمدی:
ایجاد فرهنگ امنیت

کلیات

تا اینجای بخش سوم نقش امنیت و کارکردهای آن در سازمانهای مختلف اعم از سازمانهای کوچک و متوسط، مؤسسات غیر انتفاعی، آموزشگاهها، و ادارات دولتی مورد مطالعه قرار گرفت. در بحثهای مربوط به مسئولیت در امنیت سازمانی تأکید شد که یکنفر باید نقش رهبر را بر عهده بگیرد ولی فرض بر این گذاشته نشد که این فرد در یک جایگاه انحصاری سازمان مثل "مدیریت ارشد امنیت" قرار داشته باشد (به استثنای سازمانهای بزرگ). در سازمانهای کوچک و متوسط معمولاً از نظر بودجه و تعداد کارمندان با محدودیت مواجه هستیم و این امر باعث می‌شود بندرت بتوان از یکنفر بعنوان مدیر ارشد امنیت یا کارشناس تمام وقت امنیتی بهره گرفت. با این همه، هر شرکتی که به نحوی با فناوری مرتبط است باید یک فرد یا حداکثر یک گروه کوچک از کارشناسان امنیتی را در اختیار داشته باشد. بهره‌گیری از آیین‌نامه‌های یکپارچه، رعایت استانداردهای مناسب در تهیهٔ گزارشها، برقراری روابط هوشیارانه و در عین حال دوستانه با سایر کارمندان، پیمانکاران خارجی، فروشندگان، و مشتریان، همه و همه عواملی هستند که می‌توانند به این گروه و یا شخص خاص در اجرای فعالیتهای مورد نیاز سازمان کمک نمایند. این فصل پیشنهاداتی مشروح دربارهٔ بکارگیری امنیت چندلایه مطرح می‌کند، و یک سیاست امنیتی دوازده لایه‌ای نیز ارائه می‌دهد. بدنبال آن، منتخبی از فهرستهای کنترل امنیتی آمده که با یادآوری وظایف روزانهٔ کارمندان و اعضای تیم مدیریت در قبال ایمنی سازمان، به جلوگیری از خدشه‌دار شدن امنیت کمک می‌کند.

الگوهای سرآمدی:
دوازده لایهٔ امنیت الکترونیکی[۱۸۲]

مدیریت مخاطرات امنیتی را می‌توان نوعی فرآیند دووجهی دانست. اولین مرحلهٔ آن ارزیابی مخاطره است که شامل سه قسمت عمده می‌باشد: شناسائی و جمع‌آوری دارائیها، تجزیه و تحلیل و تعیین ارزش هریک از دارائیها، و تعیین اینکه هرکدام از دارائیها به ترتیب اولویت چقدر حیاتی هستند. گام دوم امنیت، تدوین یک شیوه برای مدیریت مخاطرات است. قسمتهای عمدهٔ این مرحله عبارتند از تدوین و پیاده‌سازی سیاستها و روالهای کاری، آموزش کاربران (اعم از کارمندان و مشتریان) و بازبینی و نظارت برای تضمین و کنترل کیفیت. یک نظریهٔ معقول بیان می‌کند که: "بپذیر که ممکن است هدف حمله قرار بگیری؛ و برای نجات خود برنامه‌ریزی کن".

سه اصل کلی که در تدوین یک برنامهٔ امنیتی باید مدنظر قرار گیرند بعبارت زیر هستند:

- حملات و آسیبها اجتناب‌ناپذیرند؛
- تأمین امنیت فرآیندی زمانگیر است؛ و
- یک شبکه، حداکثر به اندازهٔ ضعیفترین جزء خود، ایمن است.

برای حفظ جامعیت داده‌ها و کاهش مخاطرات محیطهای با معماری باز، دوازده لایهٔ اصلی امنیت باید درنظر گرفته شوند؛ و طبق تجربه مشخص شده که پیاده‌سازی صحیح هیچیک از این لایه‌ها به سرمایه‌گذاری هنگفتی نیاز ندارد.

۱. **مسئول امنیت اطلاعات** – ایجاد سمت مدیریت امنیت اطلاعات که از توجه به یازده لایهٔ دیگر در سیاستهای سازمان و پیاده‌سازی صحیح آنها طبق الگوهای سرآمدی زیر کسب اطمینان می‌کند.[۱۸۳]

---

۱۸۲ منبع:
Glaessner, Thomas, Kellerman, Tom, McNevin, "Electronic Security: Risk Mitigation in Financial Transactions - Public Policy Issues", June 2002, The World Bank

۱۸۳ برای جزئیات بیشتر به کتاب زیر نوشتهٔ Glaessner، Kellerman و McNevin مراجعه کنید:
"Electronics Security: Risk Mitigation in Financial Transaction"

۲. **مدیریت مخاطرات** – یک مفهوم وسیع بر مبنای الگوی OCTAVE – متعلق به CERT – برای مدیریت دارائیها و مخاطرات مربوط به آنها.

۳. **کنترلهای دسترسی و تصدیق هویت** – بررسی مجاز بودن رایانه یا کاربر پیش از اعطای دسترسی به اطلاعات درخواستی. در طول این فرآیند، کاربر یک نام یا شماره حساب (دادهٔ معرفی) و پس از آن رمز عبور (دادهٔ تصدیق هویت) را وارد سیستم می‌کند. کنترلهای دسترسی اولین خط تدافعی به حساب می‌آیند و می‌توانند بر اساس رمزهای عبور، نشانها، مشخصه‌های زیستی، و یا زیرساخت کلید عمومی باشند.

۴. **دیواره‌های آتش** – ایجاد یک سیستم و یا ترکیبی از چند سیستم که میان دو یا چند شبکه، مرز مشخص کند.

۵. **غربال کردن محتوا بصورت فعال** – در سطح مرورگرهای وب، لازم است هر آنچه که مناسب محیط کار نیست یا با سیاستهای مصوب مغایر است تصفیه شود.

۶. **سیستم مهاجم‌یاب (IDS)** – این یک سیستم مختص شناسایی نفوذها یا تلاشهای نفوذ است، نفوذهایی که ممکن است بصورت دستی و یا با کمک سیستمهای خبرهٔ نرم‌افزاری انجام شوند. این سیستم از *فایلهای ثبت*[۱۸۴] و سایر اطلاعات شبکه استفاده می‌کند. روشهای نظارت بسته به عواملی چون انواع حملاتی که سیستم باید بتواند در مقابل آنها دفاع کند، مبادی نفوذ، انواع دارائیها، و میزان نگرانی در مورد هریک از تهدیدها، بسیار متنوع هستند.

۷. **ویروس‌یابها** – کرمها، تراواها و ویروسها همه ابزارهایی برای انجام حملات هستند. ویروس برنامه‌ای است که می‌تواند با آلوده کردن برنامه‌های سیستم، خود را توزیع کند. تراواها خود را توزیع یا به سایر فایلها متصل نمی‌کنند. ویروس‌یابها برنامه‌های مخرب و آسیب‌رسان را می‌یابند و از کار می‌اندازند.

۸. **رمزگذاری** – الگوریتمهای رمزگذاری برای حفاظت از اطلاعات درحال انتقال و یا در معرض سرقت (از روی رسانهٔ ذخیره‌سازی؛ مثلاً رسانهٔ پشتیبان یا رایانهٔ قابل حمل) بکار می‌روند.

۹. **آزمون آسیب‌پذیری** – منظور از این آزمون، بدست آوردن اطلاعاتی دربارهٔ آسیب‌پذیریهای موجود در رایانه یا شبکه و بکارگیری این اطلاعات جهت عبور از موانع معمول تصدیق هویت و نهایتاً دسترسی به منابع مختلف آن رایانه یا شبکه است.

۱۰. **راهبری صحیح سیستمها** – این مورد باید با تهیهٔ فهرستی از خطاهای رایج راهبری که عموماً در مؤسسات یا شرکتهای مالی رخ می‌دهد و نیز فهرستی از الگوهای سرآمدی تکمیل گردد.

۱۱. **نرم‌افزار مدیریت سیاست** – لازم است که یک برنامهٔ نرم‌افزاری به کنترلِ اجرای صحیح سیاستها و روالهایی که برای استفادهٔ کارمندان از رایانه‌ها تدوین شده‌اند بپردازد.

۱۲. **طرح واکنش به رخداد (IRP)**[۱۸۵] **و تداوم کسب و کار (BCP)**[۱۸۶] – این سند اصلی‌ترین سندی است که سازمان در آن می‌گوید چگونه یک رخداد امنیتی را شناسایی می‌کند، به آن واکنش نشان می‌دهد، و آسیبهای آنرا ترمیم می‌نماید. داشتن یک IRP و آزمایش دوره‌ای آن یکی از اصلی‌ترین حربه‌های برقراری امنیت است.

فهرست کنترل پشتیبانی اجرایی[۱۸۷]

همانطور که در فصلهای قبل دیدیم آگاهی از نکات امنیتی برای ایجاد محیطی که کارمندان در آن به نحو احسن قادر به همکاری جهت حفاظت از سازمان خود باشند یک نکتهٔ کلیدی است. کارمندان از نحوهٔ برخورد مدیران با قواعد امنیتی و میزان سرمایه‌گذاری آنها در حوزهٔ آموزش و ارتباطات امنیت و سایر زمینه‌های مربوطه، تأثیر می‌پذیرند.

184 *Log Files*

185 *Incident Response Plan*
186 *Business Continuity Plan*
۱۸۷ منبع: ITS فصل سوم، *پشتیبانی اجرایی*، ص ۵۰

این فهرست کنترل برای مسئولین اجرایی شرکت که اجـرای سیاستهای امنیتی را رهبری می‌کنند تنظیم شده است.

- آیا خلاصه‌های مدیریتی بطور منظم تهیه مـی‌شـوند؟ هر چند وقت یکبار؟
- آیا از سطوح بالای مدیریت تا کارکنان خط تولید یـک مسیر ارتباطی مشخص وجود دارد؟
- آیا همه مـی‌داننـد کـه آن مـسیر ارتبـاطی چیـست و کجاست؟
- آیا مسئولیت امنیت صراحتاً بر عهدهٔ یکـی از مـدیران، مثلاً قائم مقام مدیر عامل سازمان، یا مدیر امنیـت، یـا یکی دیگر از مدیران سازمان گذاشته شده است؟
- آیا مدیریت با ارائه و اعمـال برنامـهٔ امنیتـی سـازمان، تعهد خود را به آن نشان داده است؟
- آیا روی برنامه‌های امنیتی سرمایه‌گذاری مناسب انجام شده و بودجهٔ مربوطـه واقعـاً بـه آن تخـصیص یافتـه است؟
- آیا همهٔ راهبران سیستمهای مختلف اهمیت گزارش و حل سریع مشکلات امنیتی را درک می‌کنند؟
- آیا ارتقای سطح آگاهیهای امنیتـی بعنـوان بخـشی از برنامه‌های سازمان برای کارمندان جدید همـهٔ سـطوح – از کارکنـان خـط تولیـد گرفتـه تـا سـطوح بـالای مدیریتی – پذیرفته شده است؟
- آیا برای اطمینان از آگاهی کارمندان تمام رده‌ها نسبت به سیاستهای حفاظـت از اطلاعـات شـرکت گامهـای لازم برداشته شده است؟
- آیـا هنگـام تـدوین سیاسـتها و روالهـای امنیتـی بـه واقعیتهای مربوط به فرهنگ شـرکت (روابـط مـدیران و کارمندان) توجه شده است؟
- آیا کارمندان می‌دانند که هنگام برخـورد بـا مـشکلات امنیتی (یا در جایی که نسبت به وظایف خود آگاه نیستند) باید از چه کسی کمک بخواهند؟
- آیا بازبینی و ممیزی امنیتی بطور منظم انجام می‌شود؟ هر شش ماه یکبار؟ هر سال یکبار؟

مسئولیتهای کارکنان

بمنظور ترویج فرهنگ امنیتی، مدیران باید:

- توضیح دهند که عناصر یک برنامهٔ امنیتی خـوب چـه چیزهایی هستند.
- تأکید کنند که امنیت در تمام سـطوح سـازمان بـسیار مهم است.
- افراد را نسبت به پرسیدن سـؤال در زمینـهٔ فناوریهـا و روالهای امنیتی ترغیب نمایند.
- از کلیهٔ کارکنان بخواهند در این رابطه بـسیار هوشـیار باشند و هرگونه فعالیت غیرمعمول (در محـیط اداره یـا در سطح شبکه) را گزارش دهند.
- مشخص کنند که چه کارهایی جهت حفاظت از حریم خصوصی و ایمنی کارکنان صورت می‌گیـرد، و بـرای همه روشن نمایند که وفـاداری بـه سـازمان در درجـهٔ اول قـرار دارد و نفوذهـای امنیتـی عمـدی قابـل چشم‌پوشی نمی‌باشند.

فهرست زیر با هدف کمک به مدیران طراحی شده تا بتواننـد کارکنان را برای همکاری در تأمین امنیـت سـازمان آمـوزش دهند:

فهرست کنترل آموزشهای امنیتی[۱۸۸]

- آیا همهٔ مدیران رده‌های مختلف به یک برنامهٔ امنیـت سازمانی متعهد هستند؟
- آیا با سرمایه‌گذاری جهت آموزشـهای امنیتـی، از ایـن تعهد حمایت کرده‌اند؟
- آیا آن برنامـهٔ آموزشـی شـامل جزئیـات پیکربنـدی و پشتیبانی امنیت نیز می‌باشد؟
- آیا برای آموزش امنیتی سیاستهای تعیین‌شده‌ای وجود دارد؟
- آیا این سیاستها کامل و به‌روز هستند و آیا کارکنـان از آنها اطلاع دارند؟

۱۸۸ منبع: ITS فصل پنجم، آموزش امنیت، ص ۸۱

بخش سوم

- آیا همهٔ کارمندان (از جمله مدیران اجرایی) دربارهٔ مسئولیتهای امنیتی خود در قبال شرکت آموزش دیده‌اند؟
- آیا چارچوبی برای توسعه و تداوم آگاهی امنیتی وجود دارد؟

چارچوب کنترل و مدیریت مخاطرات

در فصلهای دوم، سوم، و چهارم، تهدیدهای رایج امنیتی را بررسی کردیم (ارزیابی مخاطره) و روشهای تحلیل خسارتها را شرح دادیم، و در فصلهای بعدی نیز به ارائه راهبردهایی برای تدوین سیاستها و روالهای امنیتی – که به تقویت سازمان در مقابل حملات و خسارات اتفاقی منجر می‌شوند – پرداختیم. چنانکه در آن مباحث دیدیم، طرح واکنش شامل فهرستی از نتایج ارزشیابی عملی امنیت در مورد دارائیها است و طیفی از اقدامات تدافعی اولیه را پیشنهاد می‌کند.

فهرستهای کنترل زیر جزئیات بیشتری را در رابطه با ارزیابی مخاطرات و پیشگیری از زیان ارائه می‌دهند.

فهرست کنترل بازنگری مخاطرات[۱۸۹]

- آیا اخیراً ارزیابی مخاطرات صورت گرفته است؟ این ارزیابی هر چند وقت یکبار به‌روز می‌شود؟
- آیا سیستمها بر حسب حساسیت مخاطرات (غیرحساس، حساس، و بسیار حساس) تقسیم‌بندی شده‌اند؟
- آیا اهداف مدیریتی بر اساس اصول امنیتی هستند؟
- آیا برای آزمودن نتایج ارزیابی مخاطرات، بازبینیهای منظم انجام می‌گیرد؟
- آیا هنگامیکه مخاطرات باید مورد ارزیابی قرار گیرند و کاهش داده شوند، از ممیزهای خارج از سازمان استفاده می‌شود؟
- آیا تمام کارمندان (حتی مدیران و راهبران سیستم) بر اساس اهداف امنیتی مورد ارزشیابی قرار گرفته و منصوب شده‌اند؟

فهرست کنترل پیشگیری از زیان[۱۹۰]

- آیا به آنچه که در تلاش برای حفظ آن هستید واقفید؟
- آیا مدیریت نیز در ارزیابی مخاطرات دخیل بوده است؟
- آیا سیاستها به نثر روان نوشته شده‌اند و براحتی قابل درک هستند؟
- آیا همهٔ افراد به یک نسخه از سیاستها دسترسی دارند؟
- آیا کسی شخصاً در زمینهٔ سیاستها و روالها مسئولیت صریح دارد؟
- آیا کسی که مسئولیت سیاستها بر عهدهٔ اوست در کنفرانسهای امنیتی شرکت می‌کند و دانش امنیتی خود را به‌روز نگه می‌دارد؟
- آیا بصورت دوره‌ای به بازبینی می‌پردازید تا مطمئن شوید مکانیزمهای امنیتی همچنان پابرجا هستند؟
- آیا مطمئن هستید تمام اشخاصی که سیستمهای شما را نصب می‌کنند طبق سیاستهای و روالها امنیتی شرکت شما آموزش دیده‌اند؟
- آیا پیش از بکارگیری سیستمهای نرم‌افزاری و سخت‌افزاری، از رفع و رجوع تمام مشکلات امنیتیِ شناخته‌شده اطمینان حاصل می‌کنید؟
- آیا گزارشهای بازبینی را مورد بررسی قرار می‌دهید؟ هر چند وقت یکبار؟

امنیت فیزیکی: شبکه‌های داخلی و خارجی

مبحث امنیت فیزیکی در سطوح مختلفی از جزئیات در بخشهای دوم (امنیت فناوری اطلاعات و کاربران انفرادی)، سوم (همین بخش) و پنجم (امنیت فناوری اطلاعات و راهبران و فنی) پوشش داده شده است. از دیدگاه فنی، بعضی زمینه‌ها باید از منظر امنیتی تحت پوشش قرار گیرند؛ مثل شبکه‌های داخلی، شبکه‌های خارجی، و کنترل دسترسی به شبکه‌ها. فهرستهای کنترل زیر جهت کمک به حفظ منابع فیزیکی یک محیط شبکه‌ای طراحی شده‌اند.

۱۸۹ همان منبع، فصل ششم، امنیت برنامه‌ریزی نشده، ص ۹۵

۱۹۰ همان منبع، فصل دوم، امنیت مبتکرانه، ص ۳۲

فهرست امنیتی شبکهٔ داخلی[۱۹۱]

- آیا برای پیکربندی سیستمها، سیاستها و روالهای معین وجود دارد؟
- آیا این سیاستها و روالها شامل مجوزهای دسترسی به فایلها، رمزهای عبور، و وصلهها میشوند؟
- آیا خدمات غیرضروری را غیرفعال کردهاید؟
- آیا سیاستی برای امنیت فیزیکی وجود دارد؟
- آیا همهٔ کاربران رمز عبور دارند؟
- آیا حسابهای پیشفرض که در سیستم موجود هستند تغییر داده شدهاند؟
- آیا استفاده از حسابهای کاربری پیشفرض "Guest" طبق سیاست امنیتی ممنوع شده است؟
- آیا حسابهایی که مورد استفاده قرار نمیگیرند بصورت منظم غیرفعال میشوند؟
- آیا بعنوان بخشی از فرآیند نصب سیستمها، وصلههای امنیتی جدید اعمال میشوند؟
- آیا در سیستمهایی که پشتیبانی از آنها با شماست برای شکستن رمزهای عبوری که به سادگی قابل حدس هستند تلاش میکنید؟ هر چند وقت یکبار؟
- آیا مراقب تغییرات غیرمجاز در فایلها هستید؟ هر چند وقت یکبار؟
- آیا هنگام نسخهبرداری از فایلها جوانب احتیاط را رعایت میکنید؟

فهرست کنترل شبکههای خارجی و دیوارههای آتش[۱۹۲]

- آیا نقشها و مسئولیتهای امنیتی به روشنی تعریف شدهاند؟
- آیا فردی بصورت منظم تنظیمات دیوارهٔ آتش را بازبینی میکند؟ هر چند وقت یکبار؟
- آیا کسی مسئولیت انجام *آزمون نفوذ*[۱۹۳] روی دیوارهٔ آتش را بر عهده دارد؟
- آیا مشخص است که مسئولیت بهروزرسانی دیوارهٔ آتش (درصورت لزوم) بر عهدهٔ کیست؟
- آیا برای امور راهبری، بهروزرسانی، و نگهداری دیوارهٔ آتش سرمایهگذاری مناسب انجام شده است؟
- آیا مدیران به نقش خود در فرآیند امنیت و نقش افرادی که به آنها گزارش میدهند واقفند؟
- آیا نقشها و مسئولیتهای فوریتی بوضوح و بصورت رسمی تعریف شدهاند؟
- آیا کارکنان بخش پشتیبانی از روالهای پیشگیرانهٔ معینی پیروی میکنند؟
- آیا نرمافزارهای مهاجمیاب روی سیستمها و شبکه نصب شدهاند؟
- آیا نرمافزار ممیزی روی تمام سیستمهای بسیار حساس نصب شده است؟
- آیا نرمافزار ضدویروس در تمام نقاط ورود شبکه نصب شده است؟
- آیا برای بهبود فرآیندها، تجربیات نفوذ بهاشتراک گذاشته میشوند؟

فهرست کنترل دسترسی به شبکه

- آیا مدیریت در فرآیند تأیید اتصال به شبکههای خارجی دخیل است؟
- آیا کسی اتصالات به خارج سازمان را دنبال میکند؟
- آیا مدیران از تعداد کارمندان و پیمانکارانی که متصل به خارج سازمان هستند مطلعند؟
- آیا خدمات غیرضروری شبکه غیرفعال شدهاند؟
- آیا پیش از تأیید اتصالات خارجی، نیاز واقعی به آنها مورد بررسی قرار میگیرد؟

۱۹۱ *همان منبع، فصل هشتم، امنیت شبکهٔ داخلی، ص ۱۲۱*
۱۹۲ *همان منبع، فصل هفتم، پشتیبانی از امنیت، ص ۱۰۹*

193 Penetration Testing

- آیا شرکت برای کنترل اتصالات خارجی بصورت منظم آنها را بازبینی می‌کند؟
- آیا برای غیرفعال کردن اتصال افراد یا پیمانکاران مستعفی، روال خاصی وجود دارد؟
- آیا برای نصب دیوارهٔ آتش، سیاستها و روالهای مخصوص موجود است؟
- آیا برای برقراری اتصالات مشتریان به شبکه‌های خارجی سیاست و روال خاصی وجود دارد؟
- آیا همهٔ سیاستها و روالهای مربوط به اتصالات بصورت اجباری اعمال می‌شوند؟

بازبینی امنیت

در عین اینکه یک سازمان مقادیر هنگفتی زمان و پول را جهت تدوین سیاستها و روالهای امنیتی، آموزش کارمندان و توجه به مدیران و کارشناسان امنیتی صرف می‌کند، اثربخشی این تلاشها نیز لحظه به لحظه باید مورد ارزیابی قرار گیرد. بازبینی امنیتی، آندسته از نقاط ضعف برنامهٔ جامع امنیتی را که با رشد و تغییر در طول عمر سازمان بوجود آمده و یا به هر ترتیب نمی‌توانسته مورد توجه قرار گیرد را آشکار می‌کند. بازبینی‌ها می‌توانند یک مزیت دیگر نیز به همراه داشته باشند و آن اینکه اگر متخلفان بدانند که شما در جستجوی آنان هستید ممکن است فعالیت خود را محدود کنند.

معمول‌ترین اشتباهاتی که با روالهای ممیزی امنیت قابل شناسایی هستند عبارتند از:

- نصب نبودن وصله‌های امنیتی؛
- مجوز دسترسی بیش از حد به فایلها؛
- ساده و قابل حدس بودن رمز عبور؛
- فعال بودن خدمات شبکه‌ای غیرضروری؛ و
- روشن نبودن یا اعمال نشدن قوانین دیوارهٔ آتش.

فهرست کنترل زیر جهت تعیین یک مبنا برای بازبینی‌های امنیتی – چه توسط کارمندان شرکت و چه توسط کارشناسان منابع خارجی – ارائه شده است.

فهرست کنترل روالهای بازبینی[۱۹۴]

- آیا یک سیاست رسمی برای بازبینی دارید؟
- آیا برای آزمون امنیت، روالهای کتبی بازبینی تهیه کرده‌اید؟
- آیا بازبینی‌ها طبق یک برنامهٔ منظم زمانی به انجام می‌رسند؟
- آیا نرم‌افزار بازبینی روی همهٔ انواع سیستم‌عاملهای شما (Unix/Linux, Mac, Windows) نصب شده‌اند؟
- آیا برای خرید ابزارهای مورد نیاز بازبینی، بودجهٔ مناسب اختصاص داده می‌شود؟
- آیا مدیران با فراهم کردن امکان آموزش صحیح ممیزان، از فرآیند بازبینی امنیت پشتیبانی مناسب بعمل می‌آورند؟

استفاده از منابع خارجی

نهایتاً به این امر واقفیم که پیچیدگی امنیت فناوری اطلاعات ممکن است بعضی سازمانها را برای تأمین نیازهای امنیتی به استفاده از کارشناسان خارجی وادار کند. در فصلی که به این مفهوم اختصاص داده شده بود در مورد نکات قابل توجه در انتخاب شرکت همکار، چگونگی مدیریت فعالیتهای آن، و اینکه چه هنگام باید فعالیتهای آنرا به دقت زیر نظر گرفت بحث عمیقی صورت گرفت.

فهرست امنیت زیر می‌تواند بعنوان یک منبع دیگر برای شرکتهایی که مایلند از یک پیمانکار خارجی جهت انجام فعالیتهای امنیتی خود استفاده کنند مورد استفاده قرار گیرد:

فهرست کنترل استفاده از منابع خارجی در امنیت[۱۹۵] (ملاحظات فنی)

- آیا اتصالات میان ارائه‌کنندگان و مشتریان (اتصالات شبکه‌های خارجی) بصورت منظم بازبینی می‌شود؟ هر چند وقت یکبار؟

---

۱۹۴ منبع: ITS فصل نهم، واگذاری امور به منابع خارجی، ص ۱۳۳

۱۹۵ منبع: ITS فصل نهم، واگذاری امور به منابع خارجی، ص ۱۳۳

- آیا برای اتصال ارائه‌کنندگان و مشتریان به شبکهٔ شما از طریق شبکه‌های خارجی، یک معماری رسمی وجود دارد؟
- آیا یک سیاست رسمی برای تعیین اینکه اتصال از شبکهٔ خارجی در چه زمانی، تحت چه شرایطی، و به چه صورتی مجاز خواهد بود وجود دارد؟
- آیا آغاز شدن یک اتصال از شبکه خارجی، نیاز به تأیید مدیریت دارد؟
- آیا پیش از اتصال یک شبکهٔ خارجی، انجام نوعی بازبینی رسمی الزامی است؟

فصل دوازدهم
قواعد ایمنی تجارت الکترونیکی برای همهٔ کاربران و شرکتها

چهار گام آسان برای رایانهٔ امن‌تر

راه‌اندازی یک رایانه بصورت امن مستلزم تلاش بسیار زیادی است. چنانچه شما برای ارزیابی مخاطرات و تحلیل سود و زیان وقت کافی ندارید توصیه می‌کنیم دست‌کم چهار مرحلهٔ سادهٔ زیر را دنبال کنید:

۱. **مشخص کنید که امنیت برای ادارهٔ شما واجد چه درجه‌ای از اهمیت است.** اگر فکر می‌کنید که امنیت از اهمیت بالایی برخوردار است و درصورت وقوع رخداد امنیتی دچار خسارتهای زیادی خواهید شد، پرداختن به امنیت باید از اولویت کافی برخوردار باشد. اگر برای جلوگیری از بروز مشکلات امنیتی، از یک برنامه‌نویس پرکار که هیچ آموزش رسمی در زمینهٔ امنیت ندیده استفادهٔ پاره‌وقت کنید، بدون شک به استقبال مشکلات امنیتی رفته‌اید.

۲. **کاربران خود را آموزش و در تدوین روالها دخالت دهید.** آیا کاربران ادارهٔ شما از مخاطرات ناشی از ضعف امنیتی (و اینکه چه عملکردهایی از نظر امنیتی ضعیف هستند) آگاهی دارند؟ کاربران درصورت مشاهدهٔ یک مورد غیرعادی یا مشکوک باید بدانند که چه کنند و با چه کسی تماس بگیرند. تهیهٔ یک برنامهٔ آموزشی مناسب برای کاربران می‌تواند آنها را به قسمتی از سیستم تدافعی شما تبدیل کند. ناآگاه نگهداشتن کاربران نسبت به محدودیتها و عملکرد سیستم باعث افزایش امنیت نمی‌گردد؛ چراکه همواره منابع اطلاعاتی دیگری وجود دارد که در دسترس مهاجمان مصمم باشد.

۳. **برای تهیه و ذخیرهٔ نسخه‌های پشتیبان یک طرح مشروح تدوین کنید.** باید خارج از محل ادارهٔ خود نیز نسخه‌های پشتیبانی داشته باشید تا درصورت بروز فجایع جدی هم بتوانید سیستم خود را مجدداً بازسازی کنید.

۴. **شکاک و کنجکاو باشید.** چنانچه اتفاقی افتاد که به نظر غیرمعمول می‌نمود، به وجود مهاجم شک کنید و در آن مورد به بررسی بپردازید. معمولاً در خواهید یافت که مشکل از یک اشتباه و یا یک اشکال در روش استفاده از آن منبع بوده است. اما برخی مواقع هم ممکن است مشکل جدی‌تری پیدا شود. به همین دلیل هرگاه مسئله‌ای رخ می‌دهد که قادر به حلاجی دقیق آن نیستید باید نسبت به امنیتی بودن مشکل مظنون شوید و آنرا مورد بررسی دقیق قرار دهید.

بیست و پنج قاعدهٔ خاص دیگر برای استفاده ایمن‌تر از رایانه

قاعدهٔ ۱. پیش از وقوع سرقت رایانه‌ای در مورد آن بیاندیشید.

قاعدهٔ ۲. بطور منظم نسخهٔ‌پشتیبان تهیه کنید و مطمئن شوید که درصورت تهدید فیزیکی رایانه، به آنها آسیبی وارد نمی‌شود و قابل استفاده خواهند بود.

قاعدهٔ ۳. رمزهای عبور را بگونه‌ای انتخاب کنید که بسادگی بتوانید آنها را به یاد بیاورید اما حدس زدن آن برای افراد دیگر مشکل باشد.

قاعدهٔ ۴. سیستم‌عامل و نرم‌افزارهای کلیدی خود را همواره به‌روز نگهدارید.

قاعدهٔ ۵. برنامهٔ پست الکترونیکی خود را بگونه‌ای پیکربندی کنید که *ضمیمه‌ها*[۱۹۶] را بصورت خودکار باز نکند.

قاعدهٔ ۶. قبل از باز کردن هر نوع ضمیمهٔ نامهٔ الکترونیکی، به نام آن دقت کنید تا مطمئن شوید که یک برنامهٔ اجرایی نیست.

196 *Attachment*

قاعدهٔ ۷. به هیچوجه ضمیمه‌ای را که از یک غریبه دریافت کرده‌اید باز نکنید، مگر اینکه مطمئن باشید فایل مربوطه نمی‌تواند حاوی قطعه‌برنامهٔ مخرب باشد.

قاعدهٔ ۸. از گشودن ضمیمه‌ای که از طرف یک فرد آشنا و مطمئن فرستاده شده هم پرهیز کنید، مگر آنکه مطمئن باشید که آگاهانه ارسال شده است.

قاعدهٔ ۹. برنامهٔ پست الکترونیکی خود را طوری تنظیم کنید که *قطعه‌برنامه‌های تفننی HTML*[۱۹۷] را پردازش نکند و برای دیگران هم ارسال ننماید.

قاعدهٔ ۱۰. از ISP خود بپرسید که آیا نامه‌های الکترونیکی را پیش از تحویل به شما از نظر ویروس و یا تهدیدهای مشابه بررسی می‌کند یا نه.

قاعدهٔ ۱۱. به پایگاه‌های وب امکان download و اجرای برنامه‌هایی که ممکن است مشکلساز باشند را ندهید، مگر اینکه مطمئن باشید پایگاه مربوطه قابل اعتماد است.

قاعدهٔ ۱۲. نمایش آدرس پایگاه وبی که مرور می‌کنید و آدرسی که درحال اتصال به آن هستید را فعال کنید. همچنین هنگام مرور پایگاههای ناآشنا بسیار مراقب باشید، خصوصاً اگر به آنها اجازهٔ اجرای برنامه روی رایانهٔ خود را می‌دهید.

قاعدهٔ ۱۳. بررسی کنید که cookieها تحت چه شرایطی در رایانهٔ شما ذخیره می‌شوند. اگر قادر به کنترل آنها نیستید (مثل زمانیکه از رایانه‌ای در اماکن عمومی استفاده می‌کنید)، مراقب باشید که اطلاعات خصوصی خود را وارد سیستم نکنید.

قاعدهٔ ۱۴. چنانچه هرگونه اطلاعات خصوصی و محرمانه‌ای روی صفحهٔ وب به نمایش در آمد، پس از اتمام کار، *حافظهٔ نهان*[۱۹۸] را پاک کنید. اگر قادر به اینکار نیستید (مثل زمانیکه از رایانه‌ای در اماکن عمومی استفاده می‌کنید) شاید بهتر باشد از انجام کار خصوصی خود روی آن رایانه‌ها بپرهیزید.

قاعدهٔ ۱۵. اگر از *اشتراک فایل*[۱۹۹] استفاده نمی‌کنید، آنرا غیرفعال کنید. اگر از اشتراک فایل استفاده می‌کنید، نامهای کاربری و رمزهای عبور مستحکم برگزینید و مجوزهای دسترسی را تا حداقل ممکن که همچنان امکان انجام کار مورد نظر را به شما می‌دهد محدود نمایید.

قاعدهٔ ۱۶. اگر با کاربران دیگری فایل به اشتراک گذاشته‌اید، اطمینان حاصل کنید که آنها نیز نکات امنیتی را جدی می‌گیرند.

قاعدهٔ ۱۷. پیامهای فوری می‌توانند بسیار کارآمد و مفید باشند، ولی آنها را با مراقبت و آگاهی مورد استفاده قرار دهید.

قاعدهٔ ۱۸. برای انجام کارهایی که به دسترسی راهبری نیازی ندارند – مثل مرور پایگاههای وب – حتی در رایانه‌های تک‌کاربره نیز به هیچوجه از حساب کاربری راهبر استفاده نکنید.

قاعدهٔ ۱۹. تمام خدمات اینترنتی که مورد نیاز نیستند یا کاربرد زیادی ندارند را غیرفعال کنید.

قاعدهٔ ۲۰. هر رایانه‌ای که نسبت به ویروس آسیب‌پذیر است را به نرم‌افزار ضدویروس مجهز کنید و برای دریافت نشانهای جدید ویروس نیز بصورت روزانه آنرا به‌روز نمایید. همچنین باید بصورت دوره‌ای تمام فایلهای دستگاه را از نظر وجود ویروس، بررسی کنید.

قاعدهٔ ۲۱. حتی در مورد رایانه‌هایی که بطور خاص تحت تهاجم ویروسها قرار ندارند - مثل سیستمهای مبتنی بر یونیکس – نیز باید اطمینان حاصل شود نامه‌هایی که از آنها به رایانه‌های دیگر فرستاده می‌شوند آلوده به ویروس نمی‌باشند و برای گیرنده خطری در بر ندارند.

قاعدهٔ ۲۲. تمام رایانه‌ها باید با یکی از انواع دیواره‌های آتش مورد محافظت قرار داشته باشند، چه بصورت نرم‌افزاری روی همان رایانه و چه بصورت یک

197 HTML Fancy Scripts
198 Cache
199 File Sharing

دیوارهٔ آتش جداگانه برای محافظت از تمام رایانه‌های موجود در یک شبکه.

قاعدهٔ ۲۳. اگر برای کنترل یک رایانه از ابزار دسترسی از راه دور استفاده می‌کنید، مطمئن شوید که از امنیت مستحکمی برخوردار است (در حالت حداقلی، شناسهٔ کاربری و رمز عبورِ مناسب) تا مبادا مهاجمان نیز از ابزارهای مشابه برای دسترسی به سیستم استفاده کنند.

قاعدهٔ ۲۴. ثبت گزارشات برای عملکردها و کاربردهای سیستم باید بصورت منطقی فعال باشد. این گزارشات را طبق یک روال مشخص مورد بررسی قرار دهید.

قاعدهٔ ۲۵. هر از چندگاه تدابیر امنیتی خود را با روشها و آزمونهای مختلف مورد بازبینی قرار دهید تا بتوانید اشکالات احتمالی را پیش از وقوع سانحه رفع کنید.

فهرست شرکتهای استفاده‌کننده از تراکنشهای کارتهای اعتباری

الف) اگر رایانهٔ شما متصل به شبکه نیست

- رایانه‌های شرکت باید در محلی نگهداری شوند که از نظر فیزیکی ایمن باشد.
- برای باز کردن قفل رایانه باید از رمز عبور مستحکمی استفاده شده باشد و حداقلِ افراد ممکن باید آنرا بدانند.
- دسترسی فیزیکی فرد را قادر می‌کند که بتواند رمزهای عبور را به سرقت ببرد؛ بنابراین امنیت فیزیکی بسیار مهم است. اگر به رایانه دسترسی فیزیکی داشته باشید می‌توانید آنرا با یک دیسک فلاپی یا دیسک فشرده راه‌اندازی مجدد کنید و بدینوسیله تمام سدهای امنیتی سیستم‌عامل و برنامه‌های کاربردی (بجز رمزنگاری) را دور بزنید.
- جهت محدود کردن دسترسی به داده‌ها باید در سطح فایلها از مکانیزمهای امنیتی استفاده شود. تنها اشخاصی که قرار است با داده‌ها کار کنند باید به آنها دسترسی داشته باشند (این مسئله برای ماشینهای Windows به این معنی است که باید از سیستم فایل NTFS استفاده نمایید)
- وصله‌های امنیتی به‌روز را روی سیستم‌عاملها، پایگاههای داده، و تمام نرم‌افزارهای کاربردی اعمال کنید. دقت داشته باشید که امن کردن نگارشهای جدید سیستم‌عاملها آسانتر از نگارشهای قدیمی‌تر است.
- در سیستمهای خود از نرم‌افزارهای ضدویروس و مهاجم‌یاب استفاده کنید.
- برای رمزگذاریِ فایلهای داده‌ایِ کارتهای اعتباری باید از الگوریتمهای پیشرفتهٔ رمزنگاری استفاده شود.
- باید مراقب بود که *فایلهای موقتی*[۲۰۰] شامل اطلاعات رمزنشده نباشند. درصورتیکه نیازی به آنها نباشد نه‌تنها باید از روی سیستم پاک شوند، بلکه باید آنها را طوری حذف کرد که دیگر قابل بازیابی هم نباشند.
- تمام دسترسیها به فایلهای حساس باید در فایلهای گزارش ثبت شوند، و این گزارشات باید در فواصل زمانی معین تحت بررسی قرار گیرند تا مشکلات یا خطاهای بالقوه آشکار گردند. این گزارشها باید در دو فایل ثبتها نوشته شوند و از نسخهٔ دوم باید در جایی غیر از رایانه‌ای که برنامهٔ کاربردی روی آن اجرا می‌شود نگهداری کرد.
- همواره گروههای پست الکترونیکیِ هشدارهای امنیتی را بررسی کنید تا اگر نقطه‌ضعفی گزارش شده بود که احیاناً مربوط به سیستم شما می‌شد، سریعاً از آن مطلع شوید.
- درصورت وقوع حمله، تمام احتیاطهای ممکن برای کاهش مخاطره را مد نظر قرار دهید.

200 *Temporary Files*

- اطمینان حاصل کنید که تمامی کارمندان – مخصوصاً مدیران ارشد – باور دارند که امنیت برای سازمان بسیار اهمیت دارد.
- اگر اطلاعاتی مثل داده‌های کارت اعتباری و دیگر داده‌های مالی را از روی دیسک سخت حذف می‌کنید، مطمئن شوید که آن داده دیگر به هیچوجه قابل بازیابی نخواهد بود. این فرآیند فراتر از پاک کردن سادهٔ فایلها است. چنانچه نمی‌دانید که داده‌ها را چطور بصورت کامل از بین ببرید، برای انجام اینکار از افراد متخصص کمک بگیرید.
- در فواصل منظم زمانی نسخهٔ پشتیبان تهیه کنید و از ایمنی نسخه‌هایی که حاوی اطلاعات کارت اعتباری هستند کسب اطمینان کنید.
- با انتشار یک "سیاست حریم خصوصی" به کاربران اعلام کنید چه داده‌هایی را ذخیره و از آن برای چه منظوری استفاده می‌نمایید، و چگونه آنرا مورد محافظت قرار می‌دهید (می‌توانید چگونگی حفاظت را بصورت غیرمستقیم و مبهم توضیح دهید).
- اگر برای برداشت از کارتهای اعتباری، اعتبار آنها را بصورت برخط ارزیابی می‌کنید اطمینان حاصل کنید که خط ارتباطیِ مورد استفاده از امنیت لازم برخوردار است. اگر از یک مودم استفاده می‌نمایید، مطمئن شوین که امکان برقراری تماس از بیرون وجود ندارد.
- اگر سوابقی شامل داده‌های کارت اعتباری را به چاپ می‌رسانید، از لحاظ فیزیکی نیز باید امنیت آنها را تأمین کنید و بلافاصله پس از اینکه دیگر مورد نیاز نبودند آنها را با دستگاه کاغذخردکن از بین ببرید.
- از منابع معتبر، چند کتاب به‌روز در زمینهٔ امنیت تجارت الکترونیکی بخرید، آنها را مورد مطالعه قرار دهید، و توصیه‌هایشان را دنبال کنید. انتشارات *اوریلی و شرکا*[۲۰۱]، *جان وایلی و پسران*[۲۰۲]، و مک *گروهیل*[۲۰۳] کتابهای خوبی در باب امنیت فناوری اطلاعات منتشر کرده‌اند. قیمت این کتابها بسته به محل زندگی شما ممکن است متفاوت باشد، اما به هر حال خرید و استفادهٔ مؤثر از آنها سرمایه‌گذاری بسیار مفیدی به حساب می‌آید.

ب) اگر لازم است که رایانه از شبکهٔ داخلی قابل دسترس باشد:

- تمام نکاتی که در مورد قبلی گفته شد، بعلاوهٔ نکات زیر:
- یک دیوارهٔ آتش نصب کنید تا مطمئن شوید تنها کاربران و تراکنشهای مجاز می‌توانند به رایانه دسترسی داشته باشند و از دسترسی عمومی به آن جلوگیری خواهد شد.
- وصله‌های امنیتی به‌روز را روی تمام تجهیزات شبکه (مسیریابها، دیواره‌های آتش، سوئیچها، و ...) نصب کنید.
- برای کلیهٔ پیامهای مربوط به کارت اعتباری که روی خط منتقل می‌شوند از رمزگذاری استفاده کنید.
- همهٔ خدمات شبکه‌ای غیرضروری (مثل سرویس‌دهندهٔ Web، *فراخوانی تابع از راه دور*[۲۰۴]، و *پروتکل انتقال فایل*[۲۰۵]) را غیرفعال کنید.

ج) اگر اطلاعات کارت اعتباری از طریق شبکهٔ جهانی وب قابل دسترسی است:

- تمام نکاتی که در مورد قبلی گفته شد، بعلاوهٔ نکات زیر:
- اطلاعات مربوط به کارت اعتباری را در رایانه‌هایی که از طریق اینترنت قابل دسترسی هستند قرار ندهید. داده‌ها را روی دستگاهی دیگر و پشت دیوارهٔ آتش قرار دهید و برای

201 O'Reilly & Associates

202 John Wiley and Sons
203 Osborne / McGraw-Hill
204 Remote Procedure Call (RPC)
205 File Transfer Protocol (FTP)

دسترسی به آن از فراخوانی تابع از راه دور یا سایر روشهای ارتباطی به همراه یک سیستم غربال‌ساز خوب در سطح دیوارهٔ آتش استفاده کنید.

- تمام تراکنشهای روی شبکه را با استفاده از قویترین الگوریتمهای موجود (درصورت امکان با کلید ۱۲۸ بیتی) رمزگذاری نمایید.
- اطمینان حاصل کنید که اطلاعات کارت اعتباری که موقتاً در سرویس‌دهندهٔ وب ذخیره شده است، بلافاصله پس از اتمام تراکنش پاک می‌شود.

د) اگر اطلاعات کارت اعتباری حتماً باید روی رایانهٔ قابل دسترسی از اینترنت قرار بگیرد:

- تمامی موارد بالا را اعمال کنید، اما با هوشیاری بیشتری نسبت به مخاطرات امنیتی. آن رایانه، تراکنشهای آن، و گزارشهای فعالیتها باید به دقت تحت نظارت دائمی باشند.

فهرست کنترل
حفاظت از داده‌های مشتری در پایگاه وب

در اینجا یک روش ساده اما قابل اجرا ذکر شده که آنرا به پایگاههای وبی که به حریم خصوصی افراد اهمیت می‌دهند پیشنهاد می‌کنیم. در صفحهٔ اول پایگاه وب خود در مورد سیاستهایتان در قبال حریم خصوصی به افراد توضیح دهید، و اگر نقطهٔ ابهامی در مورد سیاستهایتان وجود دارد اجازه دهید شرکتتان توسط ممیزهایی از خارج شرکت مورد بازبینی قرار گیرد.

- جهت استفاده از پایگاه وب، اشخاص را ملزم به ثبت‌نام و ورود اطلاعات اضافی نکنید.
- اگر کاربران علاقه‌مند به دریافت بولتن هستند، اجازه دهید که برای ثبت نام تنها از آدرس پست الکترونیکی خود استفاده کنند.
- بدون اجازهٔ صریح کاربر، آدرس پست الکترونیکی و اطلاعات شخصی کاربران را در اختیار سازمانهای دیگر نگذارید.
- هرگاه نامه‌ای برای افراد ارسال می‌کنید، به آنها توضیح دهید که آدرس پستی آنها را چگونه بدست آورده‌اید و آنها چگونه می‌توانند آدرس خود را از فهرست دریافت‌کنندگان نامه‌های شما حذف کنند.
- فایلهای ثبت خود را در دسترس عموم قرار ندهید و درصورت امکان آنها را رمزگذاری کنید.
- زمانیکه دیگر نیازی به فایلهای ثبت ندارید، آنها را پاک کنید.
- اگر لازم است فایلهای ثبت برای مدت زیادی از طریق اینترنت قابل دسترسی باشند، اطلاعاتی که باعث شناسایی اشخاص می‌شود را از روی آن حذف کنید.
- ناقضان سیاست حریم خصوصی را تأدیب یا اخراج نمایید.

فهرست کنترل ISPها

این فهرست نسبت به آنچه که بسیاری از ISPها استفاده می‌کنند مفصل‌تر است، اما بسیار اهمیت دارد که همهٔ گزینه‌ها مورد بررسی قرار گیرند و تصمیم عاقلانه‌ای دربارهٔ پیاده‌سازی آنها اتخاذ گردد.

- از آنجا که گاهی اطلاعات کارت اعتباری یا سایر اطلاعات مالی مشتری را ذخیره می‌کنید، تمام قوانین ذخیره‌سازی داده‌های اعتباری باید اعمال شوند.
- تأمین امنیت یک فرآیند بی‌ضابطه یا کلیشه‌ای نیست. موضوعات مختلف را درک کنید و برای هریک طرحی کلی بریزید.
- یک سیاست امنیتی تدوین کنید شامل: میزان تعهد شما به محرمانه ماندن اطلاعات حریم خصوصی مشتریان (در مقابل دسترسی کارمندان خود یا سازمانهای دیگر)؛ و روندهای گزارش‌دهی هنگام وقوع یک حملهٔ

- امنیتی (گزارش به عوامل داخلی سازمان، به ISPها، و نیز مقامات مسئول)
- مسئولیتهای قانونی خود را شناسایی کنید (آیا تنها مسئولیت حفظ اطلاعات با شماست، فایلهای ثبت را تا چه مدت باید نگهداری کنید، و ...).
- سیاستهایی تدوین کنید در خصوص چگونگی واکنش به هشدارهای امنیتی، نگرانیهای مشتریان، ISPهای همتا، ارائه‌دهندگان عمدهٔ پهنای باند، و سایر کاربران اینترنت.
- آگاه باشید که ممکن است مشتریان خدمات شما به سیستمهای بیرونی حمله کنند. می‌توانید برای پاسخگویی به گزارشات سایر ISPها مبنی بر دست داشتن مشتریان شما در حملات، یک سیاست تدوین نمایید.
- درصورتیکه در سطح ISP از نرم‌افزارهای ویروس‌یاب استفاده می‌کنید، ممکن است تصمیم بگیرید برای فرستندهٔ نامه‌های آلوده هشدارهایی مبنی بر "عدم انتقال نامه بدلیل آلودگی به ویروس" ارسال کنید.
- یک *سیاست کاربرد مجاز* (AUP)[۲۰۶] تدوین کنید که شامل وظایف متقابل ISP و مشتریان باشد. این سیاست باید در تمام قراردادهای مشتری مورد اشاره قرار گیرد.
- شبکه را بگونه‌ای طراحی کنید که تا حد امکان کاربردی و عملی باشد. سیستمهایی که شبکهٔ شما را کنترل و اداره می‌کنند (از جمله سیستم میزبان حسابهای کاربری) باید بوسیلهٔ دیوارهٔ آتش از اینترنت مجزا شده باشند.
- اطمینان پیدا کنید که برای تمام رایانه‌های بخش مدیریت، بخش خدمات (مثل سرویس‌دهنده‌های پست الکترونیکی، وب، تصدیق هویت، Proxy و DNS) و تمام تجهیزات مسیریابی و کنترلی شبکه از رمزهای عبور مستحکم و قوانین دسترسی محدودشده استفاده می‌کنید.
- اطمینان یابید که همهٔ خدمات غیرضروری (مثل finger، icq، ftp، کامپایلرها و ...) روی دستگاههای قابل اتصال به اینترنت، غیرفعال شده‌اند.
- مطمئن شوید که همهٔ دستگاهها – خصوصاً آنهایی که قابل اتصال به اینترنت هستند – با اعمال وصله‌های امنیتی به‌روز نگهداشته می‌شوند.
- یک سیستم کنترل مداوم شبکه ایجاد کنید تا بتوانید مشکلاتی از قبیل حملات تخریب سرویس و فعالیتهای عمدهٔ ویروسها و هرزنامه‌ها را تشخیص دهید. این نیازمند آن است که قادر باشید الگوهای طبیعی ترافیک شبکهٔ خود را درک کنید.
- برای رایانه‌ها قابلیت کنترل ایجاد کنید تا بهتر بتوانید مهاجمان را تشخیص دهید (ماشینهای میزبان فایلهای ثبت و اطلاعات حسابهای کاربری را فراموش نکنید).
- ویروس‌یاب‌ها را در هر جایی که ورود یا خروج پست الکترونیکی صورت می‌گیرد نصب کنید.
- با تهیه ضدویروسهای رایگان یا ارزان‌قیمت، مشتریان خود را ترغیب کنید که دستگاه خود را ایمن سازند.
- مراقب باشید که سرویس‌دهندهٔ پست الکترونیکی به یک توزیع‌کنندهٔ هرزنامه تبدیل نشود.
- مکانیزمهای کنترل هرزنامه را نصب کنید.
- کلیهٔ دسترسیها به سرویس‌دهنده‌ها و برقراری و قطع اتصال به شبکه را ثبت کنید تا توانایی خود برای جمع‌آوری مدارک قانونی علیه نفوذگران را افزایش داده باشید.
- از روالهای تهیهٔ پشتیبان از اطلاعات خود و کاربران مجموعه‌ای سختگیرانه و همپوشان ایجاد کنید.
- وصله‌های امنیتی را download و از طریق دیسکهای فشرده و یا شبکهٔ توزیع محلی، توزیع کنید. با اینکار علاوه بر اینکه به‌روز بودن و تأمین امنیت را برای مشتریان تسهیل کرده‌اید، پهنای باند مصرفی خود را نیز کاهش داده‌اید.

206 *Acceptable Use Policy*

شانزده گام برای ایمن‌سازی WLAN

امنیت شبکهٔ بی‌سیم بسیار شبیه امنیت فیزیکی درب ورودی یک ساختمان است: هر کسی با انگیزه، بودجه، منابع، و زمان کافی قادر است آنرا خدشه‌دار کند. با شبکهٔ بی‌سیم باید مثل یک شبکهٔ همگانی و قابل دسترس برای عموم رفتار کرد. راهبر سیستم به هیچوجه نباید تصور کند که داده‌های انتقالی شبکهٔ بی‌سیم، خصوصی و امن است. توصیه‌های ایمنی زیر که برگرفته از پیشنهادات و توصیه‌های پیشگامان این صنعت است، نکات ساده‌ای برای ایجاد یک زیرساخت جهت ایمن‌سازی شبکهٔ بی‌سیم ارائه می‌دهد:

۱. یک راهکار در سطح سازمان برای ابزارهای بی‌سیم تهیه کنید. سیاستها و خطمشی‌های امنیت سازمان و استفاده از شبکه را طوری تنظیم کنید که با یکدیگر سازگار باشند.

۲. بررسی کنید که چند نفر از کارمندان در منزل از WLAN سازمان استفاده می‌نمایند. این کاربران راه دور باید تحت نظارت باشند تا بتوان نقاط تماس غیرمجاز به شبکه را مسدود کرد.

۳. برای مدیریت حسابهای کاربری، یک فرآیند تهیه کنید تا بتوان بصورت امن آنها را مدیریت کرد.

۴. خدمات غیرضروری را روی تمام سرویس‌دهنده‌ها و سرویس‌گیرنده‌ها غیرفعال کنید. اصولاً کلیهٔ خدمات ناشناخته یا بی‌استفاده باید غیرفعال باشند.

۵. تنظیمات پیش‌فرض محصولات خود را تغییر دهید. بسیاری از راهبران مرتکب این اشتباه می‌شوند که اطلاعات SSID یا آدرس IP نقاط دسترسی را از مقدار اولیهٔ آنها تغییر نمی‌دهند. SSID را طوری تغییر ندهید که نام، بخشها، و محصولات شرکت را مشخص کند. در غیراینصورت از آنجا که SSID بوسیلهٔ نقطهٔ دسترسی اعلان عمومی می‌شود، به محض اینکه نفوذگر کلید WEP را بشکند، براحتی متوجه می‌شود که به شبکهٔ چه کسی دسترسی پیدا کرده است.

۶. رمز عبور پیش‌فرض نقطهٔ دسترسی یا مسیریاب بی‌سیم را تغییر دهید. نفوذگران معمولاً رمزهای عبور پیش‌فرض تولیدکنندگان را می‌دانند و ابتدا آنها را مورد آزمایش قرار می‌دهند.

۷. پوشش شبکهٔ بی‌سیم را حداکثر به اندازهٔ وسعت ساختمان خود تنظیم کنید و نه بیشتر. همینطور که ادارهٔ خود را برای یافتن محلی مناسب جهت استقرار نقطهٔ تماس بررسی می‌کنید، درنظر داشته باشید که محل آنرا در جایی متمایل به مرکز ساختمان برگزینید؛ چراکه اگر آنرا نزدیک پنجره‌ها قرار دهید ممکن است سیگنالهای قویتری به خارج از ساختمان تشعشع یابند و درنتیجه دیگران شبکهٔ شما را آسانتر پیدا کنند.

۸. برای بخشهای بی‌سیم، آنتنهای جهتدار تهیه کنید. بیشتر دستگاههای بی‌سیم از آنتنهای چندجهتی استفاده می‌کنند. چنین آنتنهایی به مهاجم امکان ضبط کلیهٔ ارتباطات را می‌دهند. این درحالی است که آنتنهای جهتدار اگر در فرکانسی حدود ۲،۴ گیگاهرتز یا بالاتر کار کنند، گسترهٔ انتشار سیگنال بسیار کمتر خواهد بود.

۹. WEP را فعال کنید. برای اینکار کلید پیش‌فرض WEP را تغییر دهید و بعد از آن بصورت هفتگی اینکار را تکرار نمایید.[۲۰۷]

۱۰. میان دیوارهٔ آتش و شبکهٔ بی‌سیم، از تونل VPN استفاده کنید. اگرچه این امر مستلزم راه‌اندازی سرویس‌دهنده VPN می‌باشد، اما در طرف دیگر، نرم‌افزار سرویس‌گیرندهٔ VPN در بیشتر سیستم‌عاملها مثل Windows 98 SE، Windows 2000، و Windows XP تعبیه شده است.

۱۱. روی شبکهٔ بی‌سیم، یک سیستم مهاجم‌یاب مبتنی بر شبکه (NIDS)[۲۰۸] تعبیه کنید.[۲۰۹]

۱۲. در سطح سازمان، نرم‌افزارهای ضدویروس را روی تمام سرویس‌گیرنده‌های بی‌سیم نصب کنید.

---

۲۰۷ منبع: NIPC
http://www.nipc.gov/publications/nipcpub/best pract.html

208 Network Based Intrusion Detection System

۲۰۹ منبع: Chris Bateman، تحلیلگر CERT

۱۳. از مکانیزم *تصدیق هویت دوعاملی*[۲۱۰] استفاده کنید، چراکه درصد زیادی از مخاطرات را کاهش می‌دهد. دو روش برای استفاده از تصدیق هویت دوعاملی وجود دارد. روش اول استفاده از "کارتهای هوشمند مبتنی بر نشانه" است که اطلاعات زیستی افراد را در خود ذخیره می‌کنند.[۲۱۱] روش دوم استفاده از سرویس‌دهنده‌های *RADIUS*[۲۱۲] است که رایانه را برای شبکه تصدیق هویت می‌کنند و ارتباط شما با نقطهٔ تماس را نیز برقرار می‌سازند. کاربر صرفاً بمنظور تصدیق هویت برای سایر سرویس‌دهنده‌ها به سرویس‌دهندهٔ RADIUS متصل می‌شود. در حقیقت در این روش سرویس‌دهنده‌های RADIUS مثل نگهبان یک سالن، عبور و مرور را کنترل می‌کنند.[۲۱۳]

۱۴. از یک دیوارهٔ آتش بی‌سیم بعنوان gateway استفاده کنید.[۲۱۴] این دستگاه مثل یک دیوارهٔ آتش استاندارد از نوع *دومنزلی*[۲۱۵] عمل می‌کند بطوریکه شبکهٔ بی‌سیم در یک طرف و شبکهٔ مورد اعتماد داخلی در طرف دیگر آن قرار دارد. دیوارهٔ آتش از نرم‌افزارهای امنیتی مثل IPSec و سایر مکانیزمهای VPN استفاده می‌کند و تنها پس از تصدیق هویت می‌توان از طریق آنها به شبکهٔ داخلی دسترسی پیدا کرد. برای محدود کردن مقصد ترافیک خارج‌شده از شبکهٔ بی‌سیم می‌توان از قوانین دیوارهٔ آتش استفاده کرد. اطمینان حاصل کنید که دیوارهٔ آتش میان تمام نقاط دسترسی بی‌سیم و شبکهٔ داخلی یا اینترنت وجود دارد.

۱۵. سرویس DHCP را غیرفعال کنید و برای کارتهای شبکهٔ بی‌سیم خود از آدرس IP ثابت استفاده کنید. همچنین محدودهٔ پیش‌فرض آدرس IP شبکهٔ بی‌سیم را از آنچه تولیدکننده تعیین کرده تغییر دهید.

۱۶. تنها نقاط دسترسی قابل ارتقا خریداری کنید. همیشه پیشرفتهایی در امنیت اینگونه ابزارها ایجاد می‌شود، و لذا باید مطمئن باشید که همواره خواهید توانست نقاط دسترسی خود را به‌روز نگهدارید.

اطلاعات دیگری در خصوص VPN

برای محافظت از اطلاعات سیستمهایی که از هریک از فناوریهای مذکور استفاده کنند، باید VPN راه‌اندازی کنید، بطوریکه همهٔ gatewayها قابل اطمینان شبکهٔ داخلی این VPN باشند و هر کاربر هنگام دسترسی به شبکه‌های مورد اطمینان، از این مکانیزم استفاده کند. اساساً VPN یک اتصال خصوصی میان دو دستگاه است که اطلاعات محرمانه را در یک شبکهٔ عمومی و به‌اشتراک گذاشته‌شده مثل اینترنت بصورت امن انتقال می‌دهد. فناوری VPN به سازمان امکان می‌دهد که خدمات شبکهٔ خود را برای کاربران راه دور، واحدها، و شرکتهای همکار بصورت ایمن و از طریق اینترنت در دسترس قرار دهد. به عبارت دیگر VPN اینترنت را به یک شبکهٔ شبیه‌سازی‌شدهٔ خصوصی *WAN*[۲۱۶] تبدیل می‌کند. VPN همچنین به کاربران راه دور این امکان را می‌دهد که بتوانند به سرویس‌دهنده‌های شرکت خود دسترسی داشته باشند.

برای استفاده از اینترنت بعنوان یک شبکهٔ ارتباطی وسیع خصوصی، سازمانها باید بر دو مانع اصلی فائق آیند. اول اینکه شبکه‌ها غالباً با استفاده از پروتکلهای مختلفی ارتباط برقرار می‌کنند، اما VPN راهی برای عبور پروتکلهایی غیر از IP از یک شبکه به شبکهٔ دیگر فراهم می‌سازد. دوم اینکه بسته‌های اطلاعات در اینترنت بصورت متن‌ساده انتقال

---

210 *Two Factor Authentication*

۲۱۱ *Bateman توصیه می‌کند از روشی که او آنرا e-thenticator می‌نامد استفاده کنیم، که در آن یک دستگاه مخصوص، اثر انگشت شست را در یک کارت هوشمند ذخیره می‌کند.*

212 *Remote Authentication Dial-In User Service*

۲۱۳ *RADIUS یا همان "سرویس تلفنی تصدیق هویت راه دور کاربر"، یک سرویس تصدیق هویت است که اطلاعات کاربر را بررسی می‌کند و پس از اینکه اطلاعات را مورد تأیید قرار داد به کاربر اجازهٔ دسترسی به خدمات شبکه را می‌دهد. قسمتی از آنچه RADIUS می‌تواند آنرا فراهم کند، ارتباط رمزگذاری‌شده میان سرویس‌گیرنده-های راه دور و سرویس‌دهندهٔ RADIUS است. شبکه‌های خصوصی مجازی (VPNها) نیز بصورت مشابه کار می‌کنند، اما بجای برقراری ارتباط میان میزبان راه دور و شبکه، میان دو شبکه ارتباط برقرار می‌سازند. پس از اینکه رایانهٔ راه دور تصدیق هویت شد و بوسیلهٔ سرویس‌دهندهٔ RADIUS به شبکهٔ داخلی متصل گشت، بگونه‌ای عمل می‌کند که گویی از نظر فیزیکی در کنار شبکه و متصل به آن است. به عبارت دیگر، رمزگذاری سرویس‌دهندهٔ RADIUS تنها میان آن سرویس‌دهنده و سرویس‌گیرندهٔ آن وجود دارد، و نه در تمام شبکه.*

۲۱۴ *Rick Fleming، قائم مقام رئیس دایرهٔ امنیت شرکت Digital Defense*

215 *Dual Homed*

216 *Wide Area Network*

می‌یابند، و درنتیجه هـرکس کـه بتوانـد ترافیـک اینترنـت را ببیند، خواهد توانـست اطلاعـات موجـود در بـسته‌هـا را نیـز بخواند. این یک مشکل بـزرگ اسـت، بخـصوص اگـر مـثلاً بانکهـا بخواهنـد از اینترنـت بـرای تبـادل داده‌هـای مهـم و محرمانهٔ تجاری استفاده کنند. VPN با استفاده از مکـانیزمی به نام *تونل*[۲۱۷] بر این مشکلات غلبه می‌کند. در این مکـانیزم داده‌ها بجای ارسال‌شدن بصورت عادی، برای امنیـت بیـشتر ابتدا رمزگذاری می‌شوند، درون یک بستهٔ IP قرار می‌گیرنـد، و سپس از طریق اینترنت ارسال می‌گردند.

بـسیاری از محـصولات مثـل محـصولات Nokia، Cisco، Nortel، Checkpoint، و Microsoft دارای فنـــــاوری VPN ایمن و مناسب هستند[۲۱۸] که می‌تواند در نقاط مختلف شبکه قرار گیرد. اگرچه VPN از محتـوای داده‌هـای تبـادلی روی شبکه حفاظت می‌کند، امـا بـسته بـه اینکـه چگونـه در شـبکه قـرار گرفتـه باشـد ممکـن اسـت نتوانـد از دسترسـی غیرمجاز از بیرون شبکه جلوگیری نمایـد. بـه عبـارت دیگـر هرچند کاربر غیرمجاز بخاطر وجود VPN نمی‌تواند محتـوای داده‌ها را ببیند، اما ممکن است همچنان بتواند به منابع شبکه دسترسی پیدا کند و پهنای باند را بگونـه‌ای تغییـر دهـد کـه ظرفیت شبکه سرریز شود و علیه کاربران مجاز حملهٔ تخریب سرویس انجـام گیـرد. کنتـرل دسترسـی، تـصدیق هویـت و رمزگـذاری از عناصـر حیـاتی یـک اتـصال امـن هـستند. از *پروتکل نقطه به نقطه* (PPP)[۲۱۹] برای مدت مدیـدی بعنـوان پروتکل جهانی *لایهٔ اتصال*[۲۲۰] جهت ایجاد تونل میان ابزارهـا در اینترنت استفاده می‌شد؛ اما در سالهای اخیر *پروتکل تونـل نقطه به نقطه* (PPTP)[۲۲۱] و *پروتکل تونل لایـهٔ دو* (L2TP)[۲۲۲] برای اینکار ترجیح داده شده‌اند.[۲۲۳]

---

217 *Tunneling*

۲۱۸ *درحال حاضر IETF درحال اصلاح استانداردهای VPN است تا IPSec را ایمن‌تر و نیز با ارتباطات ماهواره‌ای سازگار کند.*

219 *Point-to-Point Protocol*

220 *Link Layer*

221 *Point-to-Point Tunneling*

222 *Layer 2 Tunneling Protocol*

۲۲۳ *مقالهٔ Karen Bannas با عنوان "Safe Passage" در مجلهٔ PC Magazine، هفت شرکت ارائه‌دهندهٔ VPN را برای محصولات مناسب جهت کاربرد در شرکتهای متوسط با بودجه‌ای حدود ده هزار دلار که به VPN برای ارتباط میان دفتر مرکزی و شعبه‌ها نیاز دارند مورد بررسی قرار می‌دهد:*
http://www.pcmag.com/print_article/0,3048,a%3D12352,00.asp

فصل سیزدهم
گفتگوهای بین‌المللی پیرامون موضوع امنیت

کلیات

مثالهایی که از رخنه‌های امنیتی، راه‌حلها و سیاستهای مبتکرانهٔ مقابله با آنها در پی می‌آیند، برگرفته از دو سمینار هستند که توسط بانک جهانی برگزار شده‌اند – سمینار اول با عنوان "امنیت الکترونیکی: کاهش مخاطره در حوزهٔ خدمات مالی" در ۲۵ سپتامبر ۲۰۰۲، و "ایمنی و جامعیت الکترونیکی" در ۱۰ سپتامبر ۲۰۰۳. فیلمهای ویدئویی هر دو جلسه از طریق اینترنت در دسترس قرار دارد.[۲۲۴] این فصل شامل نکات مهم این سمینارها و توضیحات نمایندگان کشورهای شرکت‌کننده است.

سمینار جهانی سال ۲۰۰۲: کاهش مخاطره در حوزهٔ خدمات مالی[۲۲۵]

جلسه با مقدمه‌ای بر *مخاطرهٔ الکترونیکی*[۲۲۶] آغاز شد و مقالات به تبدیل شدن "شبکه‌های بسته" به "شبکه‌های باز" در خلال ده سال اخیر اشاره داشتند. در شبکه‌های باز، وابستگی به قابلیتهایی مثل SSL که اخیراً الگوریتم آن شکسته شده بود باعث بروز مشکلاتی می‌شد، چراکه این امر می‌توانست آسیب‌پذیریها را تا مدتها ماندگار کند. برای بانکها، نه‌تنها تهدیداتی چندوجهی مثل Code Red وجود دارد، بلکه خطر حلقه‌های جرائم سازمانیافتهٔ نفوذ نیز محتمل است. بسیاری از این حلقه‌های عملیات مجرمانه از کازینوهای اینترنتی بعنوان ابزار پولشویی استفاده می‌کنند. طبق تخمین شرکت Internet Data، حدود ۵۷٪ نفوذها علیه صنایع سرمایه‌گذاری انجام گرفته است. علاوه بر این، به موازات پیچیده‌تر شدن روشهای نفوذ، سطح مهارت نفوذگران کاهش می‌یابد؛ چون تکه‌برنامه‌های خرابکارانه برای download و کاربرد، در دسترس همگان قرار دارد. حتی کسانیکه دانش چندان عمیقی ندارند نیز با این امکانات می‌توانند اقدام به نفوذهای بزرگ کنند.

کلاهبرداریهای الکترونیکی بخصوص در نفوذهایی که از اروپای شرقی علیه ایالات متحده انجام می‌گیرد غالباً یا سرقت هویت و یا اخاذی بوده‌اند. روشهای دیگر نیز عبارتند از *salami slicing*[۲۲۷]، انتقال سرمایه، و دستکاری در سهام. در آسیا، نفوذها متوجه اهداف مشخص بخش اقتصادی و همچنین اهداف حیاتی بخشهای فناوری بوده است.

بحث مقدماتی مخاطرات الکترونیکی به موضوع آسیب‌پذیریهای فناوری بی‌سیم بخصوص استاندارد GSM هم پرداخت. به دو نکتهٔ کلیدی مربوط به مخاطرات فناوری بی‌سیم اشاره شد که عبارت بودند از آسیب‌پذیریهای gateway و حملات "man in the middle". مورد دوم به این دلیل اتفاق می‌افتد که برجهای تلفن همراه نمی‌توانند هویت خود را برای تلفنهای همراه تصدیق کنند.

نکاتی در مورد قوانین و ضوابط

درحالیکه قوانین تجارت الکترونیکی در پنج سال قبل چندان مرسوم نبودند، امروز چهل کشور دارای این قوانین هستند و این رقم نیز درحال افزایش است. قوانین مربوط به معاملات الکترونیکی و حقوق و مسئولیتهای مصرف‌کننده از اهمیت خاصی برخوردارند و بسرعت درحال گسترش می‌باشند. موضوعات کلیدی این بحث عبارتند از:

۲۲۴ *فایل ویدئویی خلاصهٔ مذاکرات نشستهای سالهای ۲۰۰۲ و ۲۰۰۳ از پایگاه وب بانک جهانی بترتیب با آدرسهای زیر قابل دسترسی هستند:*
http://www.worldbank.org/wbi/B-Span/sub_e-security.htm
http://www1.worldbank.org/finance

۲۲۵ *این جلسه با حضور اعضای گروه یکپارچه‌سازی بانک جهانی برگزار شد. اعضای حاضر در جلسه عبارت بودند از:* Thomas Glaessner، Tom Kellerman، و Valerie McNevin، *بعلاوهٔ شرکت‌کنندگان در این سمینار جهانی از از کشورهای برزیل، شیلی، مکزیک، اوکراین، اسلواکی، سنگاپور، کرهٔ جنوبی، فیلیپین، هنگ‌کنگ، سریلانکا، و جمهوری خلق چین*

۲۲۷ *برداشت مقادیر بسیار کم از تعداد زیادی حساب بانکی مختلف بصورت متناوب*

- اعتبار امضاها و معاملات الکترونیکی؛
- حفاظت از اطلاعات شخصی، و اعلام راهبردهای اجرایی استفادهٔ ایمن از اطلاعات؛
- سیستمهای امن پرداخت میان بانکها بخصوص بانکهای الکترونیکی؛
- پولشویی و سطح همکاری بین المللی که برای جلوگیری از آن مورد نیاز است؛ و
- توسعه قوانین جرائم سایبر، که مقولهٔ استفاده از رایانه در فعالیتهای مجرمانه را نیز در بر بگیرد.

اجرای صحیح این موارد نیازمند پذیرش ضوابط توسط عموم، دست کشیدن از تکروی و یکه‌تازی، و بالا بودن دانش قانونگذاران است. درحالیکه از قبل میان صنایع متفاوت در سطوح مختلف همکاری وجود داشته، امنیت پرداختهای الکترونیکی از مواردی است که کاملاً به تداخل بخشهای مخابرات و بانکداری انجامیده است. صنعت بانکی شاخصهای امنیت و صحت را تحت عنوان "دسترسی بدون تبعیض به سیستمهای اقتصادی سالم و امن" تعریف کرد، و از طرف دیگر آرمان صنعت مخابرات "دسترسی همگانی بر اساس علاقه و رفاه عمومی" بود. اینگونه تعاریف متفاوت از "خدمات امن"، سازمانها را برای ایمن‌کردن شبکه‌ها و درنظر گرفتن نیازهای اقتصادی بصورت همزمان، دچار مشکل می‌کند.

نظارت و پیشگیری

با وجود مشکلات فراوان پرداختن به نیازمندیهای دوگانهٔ امنیت و صحت، امنیت الکترونیکی یک نیاز حیاتی برای بیشتر سازمانها است و باید برای کاهش مخاطرات عملی، قانونی و حیثیتی در محیط فناوری اطلاعات، تلاش و هماهنگی زیادی صورت پذیرد. طرحهایی که برای افزایش امنیت سیستمها داده می‌شوند باید موارد زیر را در بر بگیرند:

- آموزش، آگاهی و یادگیری مهارت. تحقیق بانک جهانی نشان می‌دهد که حدود ۵۰٪ نفوذهای امنیتی ناشی از تهدیدهای داخلی هستند. اگر اجرای نادرست یا ناتوانی از پیاده‌سازی ملاحظات امنیتیِ رایانه را نیز به این آمار بیافزاییم، این درصد باز هم افزایش خواهد یافت.
- ممیزی و آزمون فرآیندها. برای تسریع رفع و رجوع کارها باید همکاری وسیعی میان همهٔ طرفهای درگیر انجام گیرد. بعنوان مثال بانکهای اتحادیهٔ اروپا دارای سرویس‌دهندهایی در Antigua هستند. اگر این سرویس‌دهنده‌ها از کار بیافتند، بانک هم قادر به ارائه خدمات نخواهد بود، و اگر همکاریهای فرابخشی با مشکل مواجه شود، اقدامات فوریتی در این زمینه به تعویق می‌افتد.
- همکاری دولت و بخش خصوصی. ممکن است مخاطراتی که برای سازمان جنبهٔ حیثیتی دارند منجر به خودداری از گزارش کردن حوادث شوند. درنتیجه برگزاری میزگردهایی برای بحث پیرامون ضوابط قانونی و تهدیدهای موجود ضروری است. بعنوان مثالهایی از همکاری و شراکت عملیاتی بخش خصوصی و دولت می‌توان از مؤسسهٔ InfraGard NIPC نام برد، که محصول یک همکاری میان بخش خصوصیِ صنعت و دولت ایالات متحده بود و توسط FBI نمایندگی می‌شد. شکل دیگر این نوع همکاری با نام *FIRST*[۲۲۸] میان تعدادی از تیمهای امنیت رایانهٔ بخش دولتی، اقتصادی و دانشگاهی تشکیل شده است. اهداف FIRST ایجاد هماهنگی و همکاری برای پیشگیری از مخاطرات، واکنش سریع به حوادث امنیتی و ترویج اشتراک اطلاعات میان کاربران در سطوح وسیع عنوان شده است. از دیگر مثالها در این زمینه می‌توان به *پیمان امنیت اینترنت*[۲۲۹] و مرکز فوریتهای امنیت رایانه‌ای (CERT) اشاره کرد، که محصول یک همکاری مشترک میان مرکز بین‌المللیِ CERT در دانشگاه Carnegie Mellon و تعدادی از شرکتهای بین‌المللی غیردولتی است.
- امنیت چندلایه. مهمترین راهکار امنیت فناوری اطلاعات، شیوهٔ چندلایه است که در آن ایمنی تنها توسط فناوری تأمین نمی‌شود، بلکه افراد و فرآیندها نیز در آن نقش عمده‌ای دارند. اعتماد بیش از حد به فناوریهای ارزشمندی چون رمزگذاری لزوماً سازمان را

228 *Forum of Incident Response and Security Teams*
229 *Internet Security Alliance (www.isalliance.org)*

در مقابل همهٔ تهدیدهای ممکن حفاظت نمی‌کند. دوازده لایهٔ امنیتی برای کنترل یکپارچگی اطلاعات و کاهش مخاطرات محیطهای باز معماری باز تعریف شده و در بسیاری از موارد، پیاده‌سازی واقعی هر لایه، نیاز به سرمایه‌گذاری هنگفتی ندارد. این دوازده لایه در فصل یازدهم از همین بخش کتاب توضیح داده شده‌اند.

نقش کشورها

هنگ‌کنگ

نمایندگان ادارهٔ ممیزی مالی هنگ‌کنگ با مروری بر سه مورد کلاهبرداری بحث خود را آغاز کردند:

۱. نفوذگری با استفاده از یک تراوا به سرقت تعدادی رمز عبور و شناسه اقدام کرد و توانست بیش از ۳۵,۰۰۰ دلار آمریکا را بصورت غیرمجاز جابجا کند.

۲. یک مورد کلاهبرداری بدلیل ضعف آگاهی مشتری در مورد امنیت رمز عبور در سیستم پرداخت الکترونیکی در استرالیا روی داد. بدلیل اعمال نشدن محدودیتهای لازم، نفوذگران توانستند وارد سیستم شده و حدود سه میلیون دلار سرقت کنند.

۳. در یک کلاهبرداری اینترنتی نفوذگران توانستند حدود ۵ میلیون سهم (با ارزشی برابر ۲۱،۷ میلیون دلار آمریکا) را فروخته و در قیمت سهام نوسان شدیدی ایجاد کنند.

درسهایی که می‌توان از این رویدادها گرفت عبارتند از:

۱. تغییرات حسابهای اشخاص ثالث را ثبت کنید. این امر به معنی کنترل کلیهٔ دسترسیها و انتقالهای غیرمجاز نیز می‌باشد.

۲. معاملات بانکی الکترونیکی را کنترل کنید، و در مورد معاملات و حسابهای مشکوک با صاحبان حسابها هماهنگی مجدد بعمل آورید (از طریق SMS، یا از طریق پست الکترونیکی).

۳. برای تصدیق اعتبار مشتری از عوامل چندگانه استفاده کنید (بر اساس ابزاری که تنها مشتری آنرا دارد؛ مثل کارت هوشمند). توجه کنید که برای این منظور از هر رمز عبور تنها برای یکبار می‌توان استفاده کرد.

۴. آگاهی مشتری (ضعیفترین حلقهٔ زنجیر امنیتی) را افزایش دهید تا بتوانند از روشها و کانالهای مختلف برای انتقال اطلاعات بصورت امن استفاده کنند. ارتباطات نیز باید امن باشند، که اینکار شامل نصب *دیواره‌های آتش شخصی*[۲۳۰] و به‌روزرسانی سیستمهای مهاجم‌یاب نیز می‌شود.

۵. رویدادها باید مدیریت شده و بسرعت گزارش شوند تا نسبت به واکنش موفقیت‌آمیز تیم امنیت اطمینان حاصل شود.

در هنگ‌کنگ، دولت با بانکها و پلیس برای کنترل رویدادها و خطرات همکاری می‌کند و با اعمال مدیریت اثربخش، پاسخگویی را تضمین، رویدادها را گزارش، خسارتها را کنترل، و اعتماد عمومی را جلب می‌نماید. همچنین به این نکته اشاره می‌کند که با توجه به طیف وسیع مشکلات امنیتی ISPها، تنوع استانداردهای موجود باعث می‌شود نحوهٔ کنترل، ایمن‌سازی، و آگاه‌کردن عموم در مورد ملاحظات امنیتی دشوار گردد.

سنگاپور

بحث کشور سنگاپور حول چهار محور اصلی بود: آمارها و نکاتی در مورد کشور کره، وضعیت اقتصاد الکترونیکی، زیرساخت ملی کلید عمومی، و واکنشهای دولت در حوادث اخیر. بحث با ارائه شواهدی از رشد سریع فناوری در خلال سالهای ۱۹۹۸ تا ۲۰۰۱، از مورد اول شروع شد:

- در سال ۱۹۹۸ درآمدهای تجارت الکترونیکی حدود ۴۰ میلیون دلار بود و در سال ۲۰۰۱ به ۹۱ میلیون دلار رسید.
- در سال ۱۹۹۸ تعداد ۱۴,۰۰۰ خانوار به شبکه‌های با سرعت بالا متصل بودند و این تعداد در سال ۲۰۰۱ به ۷،۸ میلیون معادل ۶۴٪ جمعیت رسید.

230 *Personal Firewalls*

- در سال ۱۹۹۸ تنها ۳ میلیون کاربر اینترنت وجود داشت، که این رقم در سال ۲۰۰۱ به ۲۴ میلیون نفر (نیمی از جمعیت کره) رسید.
- درحال حاضر دستگاههای سیار توسط بیش از ۵۰٪ جمعیت استفاده می‌شوند.

عمومیت بانکداری الکترونیکی در سنگاپور کاملاً اثبات شده است. بانکهای الکترونیکی در این کشور بسیار فراگیر و محبوب هستند. علیرغم جمعیت اندک ۴ میلیونی، تقریباً ۲۵٪ جمعیت از خدمات بانکداری الکترونیکی بهره می‌گیرند. علاوه بر اینها صنعت نیز بسرعت درحال گسترش است. تجارت اینترنتی در سال ۱۹۹۷ شروع شد و اکنون حدود ۵۰٪ کل معاملات را به خود اختصاص داده است. اما در نقطهٔ مقابل، صنعت بیمهٔ این حوزه به این سرعت درحال رشد نیست، اگرچه طبیعت آن اینطور ایجاب می‌کند. خدمات بیمه معمولاً نیاز به بومی‌سازی دارند و کمتر می‌توان برای همه‌جا یک استاندارد ثابت و کارآی بیمه تعیین کرد.

با نگاه به جنبهٔ جنایی این تحولات، آمارها نشاندهندهٔ وقوع تقریباً ۱۰۰ رخداد امنیتی در خلال سالهای ۱۹۹۶ و ۱۹۹۷ هستند. در سال ۲۰۰۰ این آمار به عدد ۵,۰۰۰ رسید و درحال حاضر نیز بصورت تصاعدی درحال افزایش است. اگرچه بانکداری الکترونیکی عمومیت دارد، اما دو رخداد امنیتی اخیر (که ذیلاً به آنها اشاره شده) بار دیگر اهمیت سیاستها و روالهای امنیتی در محیطهای خدمات مالی الکترونیکی را روشن می‌کنند:

۱. در یک رخداد، رایانه‌های مشتریان بزرگترین بانک سنگاپوری آلوده به انواعی از تراواها شد. این تراواها بطور ناخواسته اطلاعات محرمانهٔ کاربران را دریافت و برای آدرسهای از پیش تعیین‌شده ارسال می‌کردند و بدینوسیله سارقین می‌توانستند مقادیر عظیمی پول به سرقت ببرند. این تراوای خاص آنقدر پیشرفته بود که از ضدویروسها و مهاجم‌یابها به سلامت عبور می‌کرد. از این موضوع می‌توان نتیجه گرفت که این ابزارها (ضدویروس و مهاجم‌یاب) نباید تنها مکانیزمهای دفاعی برای یک محیط اقتصادی باشند.

۲. حادثهٔ دیگر در دومین بانک بزرگ سنگاپور روی داد، اما توجه بین‌المللی را به اندازهٔ کافی به خود جلب نکرد. در این مورد، سیستمهای بانکی به این دلیل آسیب دیدند که وصله‌های امنیتی روی آنها اعمال نشده بود. جزئیات این حمله بدلیل مسائل امنیتی فاش نشد. با اینحال این حادثه نیز بار دیگر لزوم همکاری میان سازمانهای مختلف قانونی را به نمایش گذاشت.

دولت سنگاپور بطور فعال به موضوع زیرساخت کلید عمومی (PKI) پرداخته است. "قانون امضای دیجیتال" سنگاپور (مصوب سال ۱۹۹۹) مسئولیت PKI این کشور را به وزارتخانهٔ ارتباطات و اطلاعات سپرده است و برنامهٔ PKI ملی این کشور، *مراکز صدور گواهی*[۲۳۱] معتبر را معین می‌کند.

اما از گواهی نوعی شناخت دوجانبه وجود دارد و *سازمان امنیت اطلاعات کره* (KISA)[۲۳۲] بیشتر با موضوعات تکنیکی مثل نظارت بر صدور گواهی، تصدیق این مراکز، و انجام تحقیقات و توسعه دربارهٔ PKI سیمی و بی‌سیم سر و کار دارد. درحال حاضر در این کشور شش مرکز معتبر صدور گواهی فعالیت می‌کنند. چون گواهی‌ها توسط تمام مراکز صدور گواهی قابل شناسایی هستند، مشتری می‌تواند در معاملات مختلف یک امضای واحد داشته باشد. بدین ترتیب کاربران امضای الکترونیکی تحت حمایت قانون قرار دارند. با اینحال چالشهایی هم وجود دارد. برای مثال، از مراکز معتبر صدور گواهی در صنعت بانکی استفادهٔ گسترده‌ای می‌شود. اما این در مورد سازمانهای واسطه‌ای (دلالها) صادق نیست: از ۳۶ مؤسسهٔ اینچنینی تنها چهار مؤسسه از مراکز معتبر صدور گواهی استفاده می‌کنند. دو دلیل می‌توان برای این امر بر شمرد:

۱. تجارت اینترنتی در سال ۱۹۹۷ – دو سال پیش از تصویب قانون امضای دیجیتال – شروع شد. لذا این کاربران قبل از بوجود آمدن مراکز صدور گواهی، مشکلی برای انجام کار نداشتند.

۲. استفاده از مراکز صدور گواهی می‌تواند باعث تأخیر در انجام معاملات ایمن شود، اما مشتریان نمی‌خواهند در تجارت دچار تأخیر یا گرفتار دردسرهای دیگر شوند.

با اینحال یک حادثهٔ امنیتی در کره بحث امنیت الکترونیکی در فعالیتهای تجاری اینترنتی را دگرگون ساخت. در ماه

231 *Certification Authorities*
232 *Korean Information Security Agency*

آگوست سال گذشته چند شرکت واسطه‌ای حسابهای غیرفعال و مسکوتی را یافتند که تنها بعنوان بخشی از کارهای خود حدود ۲۰ میلیون دلار آمریکا سهام از سرمایه‌گذاران خریده بودند. در واکنش به این مسئله، ملاحظات امنیتی افزایش یافت و استفاده از مراکز معتبر صدور گواهی اجبار گسترده‌تری پیدا کرد. در اول دسامبر سال ۲۰۰۲، گواهی‌های خصوصی "فاقد اعتبار" اعلام شدند و از آن پس تنها گواهی‌هایی که از *مراکز تأییدشدهٔ صدور گواهی* (LCAs)[۲۳۳] صادر شده بودند معتبر به حساب می‌آمدند و تا ماه می سال ۲۰۰۳ نیز همهٔ گواهی‌ها باید مورد تأیید مجدد قرار می‌گرفتند. ضروری شد که همهٔ شرکتهای واسطه‌ای از نوامبر ۲۰۰۲ و مؤسسات کوچکتر از ژانویه ۲۰۰۳ به بعد، در تجارت اینترنتی از گواهی‌های مراکز تأییدشدهٔ صدور گواهی استفاده کنند.

سنگاپور بنا داشت در بهار سال ۲۰۰۳ خط‌مشی‌های مدیریت مخاطرات فناوری خود را منتشر کند. فعالیتهای این کشور بر اساس تجربیات مفید صنعت، با کمک نهادهای بین‌المللی، و بر مبنای چکیدهٔ جلسات مختلف میان بانکهای فعال صنعتی و مقامات دولتی هدایت می‌شود. یکی از پرسشهای اصلی سنگاپور که دارای تنها یک نهاد برای تدوین استاندارد می‌باشد این بود که چگونه دولتی به بزرگیِ ایالات متحده و با داشتن مراجع متعدد استانداردسازی، می‌تواند ضوابط خود را بصورت یکپارچه اعمال کند.

فیلیپین

بحث فیلیپین روی نتایج سه نگرش ممکن در زمینهٔ رشد فزایندهٔ تهدیدهای جرائم سایبر متمرکز بود. این سه نگرش عبارت بودند از گسترش ویروسها (مثل ویروس I Love You)، سرقت مداوم کارتهای اعتباری، و نیز حادثهٔ یازدهم سپتامبر. نمایندگان کشور فیلیپین از حادثهٔ یازدهم سپتامبر برای تشریح محاسبات دولت خود برای حفاظت از مؤسسات ملی اقتصادی استفاده کردند.

در فیلیپین، گسترش ویروس "I Love You" بسرعت نهادهای قانونی را به واکنش وادار کرد. این حادثه از آن جهت که ضعفهای دولت و بخش خصوصی را فاش می‌ساخت از اهمیت ویژه‌ای برخوردار بود. این مسئله همچنین ظرفیت قدرت قانونیِ فهم و واکنش مؤثر به حوادث مربوط به فناوری را به منصهٔ ظهور رساند و در نتیجهٔ یک برنامهٔ آموزش امنیت برای کارکنان دولت به اجرا گذاشته شد و دولت برای ورود در این عرصه قوانین تجارت الکترونیکی و *استراتژی سایبر*[۲۳۴] را از دایرهٔ تصویب گذراند.

درحال حاضر کلاهبرداری کارت اعتباری در حوزهٔ خدمات مالی الکترونیکی فیلیپین (مثل هر کشور دیگری) به یک معضلِ اساسی تبدیل شده است. این کشور دارای ۲ تا ۳ میلیون دارندهٔ کارت اعتباری است و حدود ۱۷ بانک، خدمات اعتباری این کارتها را ارائه می‌کنند و در سال چندین میلیون تبادل تجاری الکترونیکی انجام می‌شود. تخمین زده شده که حدود ۴۰۰ میلیون پزو (معادل ۸ میلیون دلار آمریکا) سوء استفادهٔ مالی را می‌توان به کلاهبرداریهای صورت‌گرفته از کارتهای اعتباری نسبت داد. دستگاههای خودپرداز نیز بطور گسترده‌ای مورد استفاده هستند و در سراسر کشور چیزی حدود ۱۰ میلیون مشتری دارند.

سومین موضوع بحث این بود که یازدهم سپتامبر بانکها را مجبور ساخت که برای ارتقای امنیت الکترونیکی به تلاش جهت افزایش همکاری با کشورهای دیگر بپردازند.

همانند سایر نقاط جهان، اقتصاد الکترونیکی فیلیپین هم هنوز در مراحل اولیهٔ توسعه قرار دارد. فیلیپین در این راستا به قسمتهایی از هشت رکن پیشنهادی امنیت الکترونیکی برای کاهش مخاطرات نیز پرداخته است: پیوند چارچوب قانونی با روشهای اعمال ضوابط، برقراری همکاری میان دولت و شرکتهای خصوصی، و نیز بهبود تواناییهای نیروهای انتظامی در حوزهٔ جرائم فضای سایبر. با اینهمه فیلیپین هنوز نیازمند کارشناسان خبرهٔ قانونی، بخصوص برای دادگاههای تخصصی است. از دیگر نیازهای این کشور می‌توان به پایگاههای داده و آموزش کلیهٔ افراد درگیر در حوزهٔ خدمات مالی شامل مشتریان، فروشندگان، و شرکتهای ارائه‌کنندهٔ خدمات اشاره کرد.

فیلیپینی‌ها دو سؤال عمده مطرح کردند: ۱) ایالات متحده چگونه میان گزارش رویدادها و حفظ مسائل محرمانه، توازن برقرار کرده است؟ و ۲) جایگاه پلیس بین‌الملل در قوانین جرائم جزایی چیست؟

233 Licensed Certificate Authorities

234 Cyber-Strategy

سریلانکا

نمایندگان سریلانکا صحبت خود را با ارائه پیش‌زمینه‌ای از اقتصاد الکترونیکی و بحث دربارهٔ محدودیتهای گسترش آگاهی امنیتی کاربران اینترنت آغاز کردند. آنها عقیده داشتند که مسائل مربوط به گسترش ارتباطات به زودی حل خواهند شد و مشکل عدم آگاهی نیز بیشتر در سطح مدیریت وجود دارد و به همین دلیل جلب حمایت در زمینه‌هایی مثل گسترش ارتباطات بسیار دشوار است. نقطه‌ضعف دیگری که می‌توان آنرا در میان مشتریان یافت، عدم آگاهی از نحوهٔ انجام یک معاملهٔ اینترنتی ایمن است. درنتیجه اعتماد میان مشتریان کاهش یافته و کمتر مایل به شرکت در معاملات اینترنتی می‌شوند. ایجاد و ارائه خط‌مشی‌ها و مبانی کاری به ارائه‌دهندگان خدمات می‌تواند به ایجاد اعتماد در مشتریان هم کمک کند.

پرسش سریلانکا متوجه فراهم‌کنندگان خدمات اینترنتی بود. آنها می‌خواستند بدانند که آیا راهبردهای رسمی و مبانی کاری برای ISPها در زمینهٔ امنیت الکترونیکی وجود خواهد داشت یا خیر. آنها همچنین خواستار دریافت اطلاعاتی دربارهٔ سازمان امنیت کره شدند – اینکه آیا خصوصی یا دولتی است، و اینکه چه نقشهایی را تحت پوشش قرار می‌دهد.

بلغارستان

خدمات نوین بانکی بلغارستان در سال ۱۹۸۹ با فرهنگی مشابه ایالات متحده و اروپا راه‌اندازی شد. این خدمات شامل سیستمهای پرداخت و بسته‌های نرم‌افزاری خاص صنعت بانکداری بود (برای مثال می‌توان به BANKNET اشاره کرد). بلغارستان راهکارهای امنیتی را با سؤالات اساسی در زمینهٔ اینکه "چه چیزی باید حفاظت شود" آغاز کرد، و سپس عناصر حیاتی اینکار – مثل شبکه‌های فیزیکی، سیستمهای اطلاعات داخلی، و برنامه‌های کاربردی حفاظت از داده‌ها (علی‌الخصوص داده‌های تبادلی میان بانکها و مشتریان) – را معرفی نمود.

از بعد سازمانی، بلغارستان یک کمیتهٔ داخلی داشت که مسئول تحلیل و ارائه راهکارها بود. تدوین خط‌مشی‌های امنیت الکترونیکی نیازمند نظارت بر شبکه‌های ارتباطی و کاربرد آنها است که شامل نرم‌افزارها و سخت‌افزارهای به‌روز و فهرست فعالیتهای خاص و پیچیده است. بلغارها ایمنی سیستمهای پرداخت را بسیار حیاتی می‌دانند. تغییرات نظارتی و پیشگیرانهٔ این کشور شامل آموزش – یکی از اجزای مهم طرح امنیتی بلغارستان – نیز می‌شود. آنها همچنین اشاره کردند که باید روی مبانی قانونی و اجرایی این مسئله (مشتمل بر قراردادهای فنی میان مشترکان شبکه‌های مختلف) همچنان کار کنند.

در بلغارستان یک چارچوب قانونی برای امضای الکترونیکی وجود دارد که شامل قانون سند الکترونیکی، تنظیم فعالیتهای قانونی مراکز صدور گواهی، و نیازمندیهای پیشرفتهٔ امضای الکترونیکی می‌شود. درحال حاضر بانکها مایل به ایجاد PKI هستند. بانکها می‌خواهند در کاربردهای خاصِ این سیستم، نقش مرکز صدور گواهی را بر عهده بگیرند. بنابراین نیاز به انعطاف‌پذیری درونی و نیز استفاده از فناوریهای سازگار بین بانکی وجود دارد. بلغارستان در زمینهٔ سیاستهای امنیتی نیز یک ملاحظهٔ خاص دارد و آن اینکه علاوه بر تعریف نیازهای تجاری باید قابلیت اطمینان را نیز تعریف کند. پیاده‌سازی و استفادهٔ عمومی از مفهوم امضای الکترونیکی در بسیاری از فعالیتها دشوار است. عوامل کلیدی در سیستمهای پرداخت بلغارستان عبارتند از فروشنده، قابلیت اطمینان، و قیمت. خدمات بانکی در یک منطقهٔ حفاظت‌شده هستند که این حفاظت شامل وجود gateway خاص برای هر برنامهٔ کاربردی و نیز وجود دیوارهٔ آتش است. با استفاده از بستهٔ نرم‌افزاری BANKNET قابلیت دسترسی به بانکها از طریق اینترنت وجود دارد. بسیاری از حملات علیه پایگاههای وب و سرویس‌دهنده‌های پست الکترونیکی به این دلیل انجام می‌شود که امکان دسترسی به آنها از طریق اینترنت میسر است. اما در پشت یک دیوارهٔ آتش، سطح مناسبی از امنیت برای خدمات بانکی و برنامه‌های کاربردی بین بانکی تأمین می‌شود.

در بلغارستان یا هر جای دیگر، بانکهای مرکزی برای سیستمهای پرداخت الکترونیکی چارچوبهای قانونی تصویب می‌کنند. این چارچوبها معمولاً شامل روشهای جدید پرداخت و قوانین حاکم بر سیستمهای ملی پرداخت هستند. از این طریق، مبانی قانونی جدیدی برای سیستمهای ملی پرداخت از جمله سیستمهای پرداخت مرکزی و نیز سیستمهای کارتی بوجود می‌آید. بلغارستان به این نتیجه رسید که پول رایج بدلیل شرایط سخت ترازهای بانکی مشکلساز شده است. آنها

در خصوص نقش نظارت در امنیت الکترونیکی سیستمهای پرداخت پرسش دارند و می‌خواهند بدانند که آیا باید بر سیستمها نظارت سختگیرانه‌تری اعمال کرد یا نه. بعنوان مثال برزیل و آفریقای جنوبی روشهای سخت‌گیرانه‌ای برای نظارت بر سیستمهای پرداخت دارند و معتقد هستند که یک سیستم کارآ و رقابتی طراحی کرده‌اند. در بعضی شرایط، قوانین می‌توانند به یک عامل انحصار برای سیستمهای خرده‌فروشی تبدیل شوند و از فعالیت آنها جلوگیری کنند ، و لذا مستندات ضوابط باید شامل ارزیابیهای دقیقی از نحوهٔ تأثیر فناوریها بر سیستمهای خرده‌فروشی نیز بشوند.

نتیجه‌گیری

همهٔ کشورهای شرکت‌کننده بر ضرورت آموزشهای فرابخشی و گسترده در زمینه امنیت الکترونیکی تأکید داشتند، و نهایتاً گروه یکپارچه‌سازی بانک جهانی مسئولیت ارائه گزارشات الگوهای سرآمدی و برگزاری سمینارها در موضوع کاهش مخاطرات الکترونیکی را بر عهده گرفت.

سمینار جهانی سال ۲۰۰۳: ایمنی و سلامت الکترونیکی[۲۳۵]

این نشست با عنایت به رشد روزافزون مخاطرات، اهمیت توجه به موضوعات امنیت الکترونیکی را در قالب جهانی یادآوری می‌کرد. درصورت بی‌نظمی در روالهای گزارش‌دهی، همهٔ رخدادهای امنیتی می‌توانند خطرسازتر شوند. بیشتر اطلاعات مربوط به امنیت الکترونیکی نادقیق هستند. علاوه بر این، کرمها، ویروسها، و سایر انواع تهدیدات الکترونیکی برای زیرساختهای حیاتی دنیا عوارض جدی بوجود آورده‌اند.

مشکلات امنیت الکترونیکی معمولاً عبارتند از کمبود تیمهای امنیتی تعلیم‌دیده، فقدان فرآیندهای کارآی دولتی برای کنترل صحت، و فناوریهای درحال رشد مثل ارتباطات سیار. ستونهای فناوری اطلاعات بسرعت درحال رشد هستند و به این دلیل که تهدیدهای سایبر و آسیب‌پذیریها هم به همان سرعت درحال گسترش می‌باشند، میلیاردها دلار سرمایه در معرض خطر قرار دارد. هدف گفتگوهای بین‌المللی پرداختن به این نیست که چرا نفوذهای امنیتی رخ می‌دهند، بلکه آن است که برای حل مشکلات چه کاری می‌توان انجام داد.

کاهش مخاطرات امنیت الکترونیکی: ترکیبی از زیربناهای نرم و سخت

یک تعریف ممکن برای امنیت الکترونیکی عبارت است از "هر ابزار، فن، و فرآیندی که داراییهای اطلاعاتیِ یک سیستم را در مقابل تهدیداتی که متوجه محرمانگی، جامعیت یا در دسترس بودن آنها است، محافظت کند". امنیت الکترونیکی از دو زیرساخت تشکیل شده است: زیربنای نرم شامل سیاستها، روالها، فرآیندها و پروتکلها؛ و زیربنای سخت شامل سخت‌افزارها و نرم‌افزارها. افزایش وابستگی به فناوری باعث افزایش احتمال وقوع تهدیدها و احیاناً گسترده‌تر شدن تأثیرات و خسارتهای آنها می‌شود. از طرف دیگر همانطور که پیش از این دیدیم به علت فعالیتهای سازماندهی‌شده و گاه تروریستی، بر سرعت و شدت حملات افزوده می‌شود. همهٔ این موارد دست به دست هم می‌دهند تا کاهش مخاطرات را به یکی از مهمترین قسمتهای یک طرح امنیتی ایده‌آل و اثربخش تبدیل کنند.

گسترش برنامه‌های امنیت الکترونیکی به چند دلیل با چالشهای عظیمی روبرو است:

اول، معمولاً انتظار آن است که فعالیتهای امنیتی بجای کنشی بودن، واکنشی باشند. باید این دیدگاه را تغییر داد تا بتوان بصورت فعالانه و مداوم با تهدیدهای فعلی و آینده به مبارزه پرداخت.

دوم، همکاری در زمینه‌های بین‌المللی از اهمیت ویژه‌ای برخوردار است، بخصوص برای سازمانهای قانونی و ناظران؛ اما می‌دانیم که حتی در یک کشور واحد هم همکاری میان سازمانهای داخلی می‌تواند امری پیچیده باشد.

---

۲۳۵ *این جلسه با حضور اعضای گروه یکپارچه‌سازی بانک جهانی برگزار شد. اعضای حاضر در جلسه عبارت بودند از: Thomas Glaessner، Tom Kellerman، و Valerie McNevin، بعلاوهٔ شرکت‌کنندگان در این سمینار جهانی از کشورهای برزیل، شیلی، کلمبیا، مکزیک، عربستان سعودی، اوکراین، استرالیا، چین (پکن)، چین (هنگ‌کنگ)، مالزی، فیلیپین، سنگاپور، و سریلانکا. برای دستیابی به اسناد اصلی این نشستها می‌توانید به آدرس زیر مراجعه کنید:*
http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/SearchGeneral?openform&E-Security/E-Finance&Presentations

سوم، عدم گزارش رویدادها یک مانع جدی برای درک محدودهٔ تهدیدهای موجود است؛ چراکه هنوز بی‌میلی قابل توجهی نسبت به گزارش عمومی نفوذهای امنیتی وجود دارد.

چهارم، علاوه بر بی‌علاقگی مؤسسات به گزارش‌کردن رخدادها، بازهٔ زمانی واکنش به رخدادها نیز در بسیاری از موارد زیاد است.

سرانجام آنکه کارکنان همچنان نقش محوری بازی می‌کنند و تنها یک کاربر بی‌تجربه می‌تواند امنیت تمام شبکه را زیر سؤال ببرد؛ و لذا ضروری است که آگاهی تمام افراد نسبت به تهدیدات افزایش یابد. درصورتیکه تهدیدات الکترونیکی به درستی مدیریت نشوند، ناگزیر اعتماد عمومی نسبت به فناوری خدشه‌دار خواهد شد. با درنظر داشتن این موارد، برای دستیابی به سطوح بالاتری از امنیت الکترونیکی باید گامهای متعدد دیگری نیز برداشت:

اول، قانونگذاران، مؤسسات مالی و سایر دست‌اندرکاران بازار باید در جهت شناسایی و گسترش الگوهای سرآمدی امنیت الکترونیکی اقدام کنند.

دوم، همکاری باید به امری عادی و همیشگی تبدیل شود؛ بخصوص با عنایت خاص به رفع تهدیدات کلیدی که متوجه سازمانها و عموم مشتریان است.

سوم، ارائه خدمات آموزشی به کارکنان و ممیزان قسمت امنیت باید از اولویت بالایی در فعالیتهای تجاری و دولت برخوردار باشد. تعریف و گسترهٔ عملی مخاطرات باید شامل انواع مخاطرات سایبر بعلاوهٔ اَشکال سنتیِ تهدیدات اطلاعاتی و فیزیکی نیز باشد.

نظارت بر امنیت اطلاعات و مخاطرات فناوری

در حالی که بخش فناوری اطلاعات فراتر از مرز تواناییها و استعدادهای محلی رشد می‌کند، رجوع به منابع خارجی برای تأمین امنیت به یک کار رایج تبدیل شده و خصوصاً استفاده از منابع بین‌المللی برای این منظور، هم تهدیدها و هم فرصتهایی را برای سازمانها در سراسر دنیا بوجود آورده است. فعالیتهایی که در سالهای اخیر جهت کاهش تهدیدهای الکترونیکی انجام می‌شود را می‌توان یک توفیق اجباری برای بانکها دانست که آنها را ملزم می‌کند یک برنامهٔ واکنشی برای حفاظت از داده‌های مشتری در برابر تهدیدها تدوین کنند و در این مسیر تمام راهنماییهای لازم را نیز برای آنها فراهم می‌آورد. در چنین برنامه‌ای باید فرآیندهای آگاهی‌یافتن مشتریان از رخدادهای افشای غیرمجاز اطلاعات نیز مد نظر قرار گرفته باشد.

علیرغم سیاستها و روالهای پیچیدهٔ ابتکاری ، هنوز هم امنیت به امری ساده تبدیل نشده است و بنابراین همچنان مراقبت و آموزش مداوم ضروری است. بعضی حوزه‌های جدید مباحث امنیتی که درحال حاضر توجه بیشتری می‌طلبند عبارتند از: ارزیابی آسیب‌پذیری، آزمون نفوذ، سیستمهای مهاجم‌یاب، و قوانین جرائم فضای سایبر.

فناوریهای سیار: دستاوردها و مخاطرات جدید

در سال ۲۰۰۲، GSM حدود ۷۸۷ میلیون کاربر در سراسر دنیا داشت. فناوری بی‌سیم با سرعتی معادل سه برابر سرعت خطوط زمینی درحال رشد است. این فناوری نیز مانند سایر فناوریهای ارتباطی نسبت به تکه‌برنامه‌های مخرب مثل تراواها، ویروسها و حملات تخریب سرویس آسیب‌پذیر می‌باشد. فناوری بی‌سیم در محیط خصمانهٔ اینترنت، پاشنهٔ آشیل امنیت به حساب می‌آید. معمولاً اتصال بی‌سیم ضعیفترین حلقهٔ زنجیر امنیتی محسوب می‌شود. آسیب‌پذیریهای GSM عبارتند از آسیب‌پذیری کارت SIM، بمباران SMS، آسیب‌پذیریهای WAP، و نیز حمله‌ای که با نام "man in the middle" شناخته می‌شود.[۲۳۶]

اگرچه ایمن‌سازی کامل فناوری GSM ممکن نیست، اما کاربر با چند گام ساده می‌تواند از خود حفاظت بسیار بیشتری بعمل آورد:

- فعال کردن رمز عبورِ راه‌اندازی؛
- نصب نرم‌افزار ضدویروس؛
- نصب یک دیوارهٔ آتش شخصی با قابلیت رمزگذاری؛

---

۲۳۶ *در این نوع حمله یک تلفن همراه دستکاری‌شده خود را بعنوان یک ایستگاه ثابت جعلی برای سایر تلفنهای همراه معرفی می‌کند و بدین ترتیب مهاجم می‌تواند اطلاعات را بدزدد. اطلاعات در gatewayها کاملاً خالص و بدون هرگونه رمزگذاری هستند، و این باعث می‌شود کاربران و اطلاعات آنها با آسیب‌پذیریهای بزرگی روبرو باشند.*

- اطمینان از نگهداری ایمن از وسایل، و حفاظت از نرم‌افزارهای کاربردی با رمزهای عبور؛
- نصب نرم‌افزار VPN. در مورد کارتهای هوشمند نیز اشخاص ثالث نباید شماره‌های PIN را مدیریت کنند.

سخنرانیهای نمایندگان کشورها

در طول برگزاری این نشست جهانی از نمایندگان کلیهٔ کشورها خواسته شد که به سه سؤال زیر پاسخ دهند:

۱. در زمینهٔ رخدادهای امنیت الکترونیکی چه نگرشهایی می‌بینید؟ بزرگترین چالشها یا آسیب‌پذیریها کدامند؟ (سرقت هویت، تخریب سرویس، پولشویی اینترنتی، یا سایر اَشکال کلاهبرداری الکترونیکی)

۲. درحال حاضر مؤسسات اقتصادی در کشور شما از چه فرآیندهایی جهت کاهش مخاطرات امنیت الکترونیکی پیروی می‌کنند و چه تغییراتی را در فرآیند نظارت خود درنظر دارند؟

۳. مؤسسات چندجانبه و چندملیتی چطور می‌توانند با همکاری سایر سازمانهای نظارتی به شما کمک کنند؟

برزیل

نمایندهٔ برزیل خاطرنشان کرد که رقابت، شرکتها را به ساخت فناوریهای پیشرفته هدایت می‌کند، اما این فناوریها مستعد آسیب‌پذیری هستند. میان هزینه‌های خدمات از یک سو و کلاهبرداریها از سوی دیگر، یک توازن وجود دارد. کارآیی فنون برگزاری آزمون برای دوره‌های آموزشی در برزیل درحال افزایش است.

در پاسخ به این سؤال که مؤسسات چندملیتی چگونه می‌توانند به کشورها کمک کنند، برزیلی‌ها مایل بودند که در زمینه‌های زیر به آنها کمک شود: برگزاری آزمون برای دوره‌های آموزشی، تدوین راهکارها و استانداردهای امنیت، و نیز ایجاد مدلهای امنیت با حداقل قوانین بانکی.

پرسش

برزیلی‌ها پرسیدند که با توجه به طبیعت پویا و پیشرفت سریع فناوری که قانونگذاری را مشکل ساخته، چگونه می‌توان زیرساخت قانونی برخورد با جرائم را ایجاد کرد.

پاسخ

یک نمایندهٔ کشور سنگاپور، در پاسخ به این پرسش پیشنهاد جریمه‌های شدید اداری و به‌روزکردن مقررات در فواصل زمانی منظم را داد؛ چراکه معتقد بود قوانینی مثل "قانون سوء استفاده از رایانه"، فایدهٔ خود را در تشخیص جرائم رایانه‌ای و کاهش جاذبهٔ آن برای نفوذگران غیرحرفه‌ای نشان داده‌اند.

یک نمایندهٔ FBI نیز بیان کرد که این یک پدیدهٔ اجتماعی بین‌المللی و غیروابسته به مرزها است. در بعضی موارد فرد خطاکار شدت جرمی که درحال ارتکاب آن است را تشخیص نمی‌دهد. در حقیقت بعضی افراد جرائم رایانه‌ای را بعنوان جرم واقعی به رسمیت نمی‌شناسند. بعلاوه بانکها هم برای جذب مشتری بیشتر اینطور وانمود می‌کنند که افسانهٔ امنیت را جاودانی کرده‌اند. بنابراین لازم است که شناخت بیشتری در مورد مخاطرات خدمات مالی و تجارت الکترونیکی به عموم مردم داده شود، چراکه در این حوزه مسدود کردن اطلاعات تنها مشکلات را حادتر می‌کند. بخصوص، مشکلات شگرفی در رابطه با طبیعت فرابخشی جرائم الکترونیکی، از جمله نفوذهای سایبر و دستکاری پایگاههای بانکی وجود دارد. بنابراین همکاری بین‌المللی در این زمینه لازم است.

مکزیک

در پاسخ به نگرشهای ممکن در رخدادهای امنیت الکترونیکی، مکزیک اشاره کرد که امکان دسترسی به‌شماره‌های PIN از طریق وب رو به افزایش است و این مسئله جدیت مخاطرات را بیشتر می‌کند. در هر صورت آنها تلاشهای زیادی برای کاهش مخاطرات الکترونیکی می‌کنند، مؤسسات مالی ظرفیتهای کنترلی قوی دارند و شرکتهای امنیتی و نظارتی بسیاری هستند که در زمینهٔ فناوری اطلاعات تخصص داشته باشند. بعلاوه مکزیک توصیه‌های BASEL را برای کنترل مخاطرات فناوری لحاظ کرده است.

در پاسخ به سؤال سوم، مکزیکی‌ها برای به اشتراک گذاشتن تجربیات، ارزیابی‌ها و نیازها پیشنهاد کردند اطلاعات جهانی میان سازمانهای مختلف مبادله شود.

پرسش
مکزیک درخصوصِ عمق خطمشی‌های سنگاپور سؤال کرد.

پاسخ
تجربیات کلی امنیت در سنگاپور بصورت اینترنتی در دسترس است.[۲۳۷] این خطمشی‌ها شامل ۲۶ فعالیت در حوزه‌های سیستم‌عامل، وصله‌ها، نقشها و مسئولیتها، نرم‌افزارهای ضدویروس، دیوارهٔ آتش، و غیره هستند.

کلمبیا

نمایندهٔ کلمبیا بیان داشت که مشکلات ایمنی آنها مانند سایر کشورها است و آنها نیز خود را آسیب‌پذیر می‌بینند. درحال حاضر این کشور استانداردی برای واکنش به رخدادها ندارد و مرکز فوریتهای امنیت رایانه‌ای نیز در آن راه‌اندازی نشده است. سرویس‌گیرنده‌های کلمبیایی مستعد هستندکه قربانی حملات قرار بگیرند، سرقت هویت درحال افزایش است، کارتهای بانکی جعل می‌شوند، قانونی برای تضمین محرمانگی وجود ندارد، کاهش مخاطرات تنها بر عهدهٔ ممیزها است، PKI و کارتهای هوشمند بکار می‌روند اما امنیت الکترونیکی بانکها در حد مقدماتی است، کارمندان معمولاً به دستورات ایمنی بی‌توجهی می‌کنند و امنیت در فرهنگ بانکی کلمبیا در جایگاه صحیح خود قرار ندارد، و علاوه بر همهٔ اینها در این کشور به‌روز ماندن نیز یک مشکل اساسی می‌باشد.

بدیهی است که در این زمینه مؤسسات چندجانبه نقشی اساسی دارند. بعنوان مثال UNCITRAL برای جرائم رایانه‌ای در حوزه‌هایی چون آزار و اذیت، تخریب سرویس، و همچنین معاملات، یک قانون مرجع دارد. خصوصیت قوانین مرجع این است که برخلاف قوانین عادی باید مبتنی بر قوانین مدنی باشند.

پرسش
نمایندهٔ کلمبیا پرسید که جامعیت امنیت در مؤسسات مالی، بخصوص با ملاحظات سود و زیان، چطور زیر سؤال می‌رود. مسائلی چون مسئولیت و مدیریت مخاطرات، نگرانیهای اساسی هستند؛ خصوصاً وقتی مشتریان درنظر گرفته شوند.

پاسخ
بدلیل ملاحظات قضایی، حتی در تشخیص محل وقوع جرم نیز همکاری میان سازمانهای مختلف ضروری است. برای آغاز باید یک زبان مشترک توصیف مشکلات، راهکارهای کاهش آنها و استانداردهای فرابخشی تدوین شوند. مثلاً تعریف "کلاهبرداری" در اتحادیهٔ اروپا با مشکلاتی همراه بود. یک نمونه از سازمانهای فرابخشی فعال در این زمینه، *کمیتهٔ فعالیتهای مالی* (FATF)[۲۳۸] است که با پولشویی و تروریسم مبارزه می‌کند.

اوکراین

پس از استقلال اوکراین، در سیستم بانکی این کشور تغییراتی رخ داد و باعث شد در آن از فناوریهای الکترونیکی استفاده شود. فناوریهای امنیتی مثل امضای الکترونیکی و رمزنگاری توسط بانک ملی اداره می‌شوند.[۲۳۹] از زمان استقلال این کشور، قوانین امضا و معاملات الکترونیکی به اجرا در آمده‌اند. علیرغم برخی تلاشها برای نفوذ به سیستم بانکی، تاکنون خسارت خاصی گزارش نشده است.

در حوزهٔ قوانین، اوکراین در سال ۲۰۰۱ معاهدهٔ جرائم سایبر را امضا کرد و از آن پس به تعقیب سوء استفاده‌های رایانه‌ای پرداخت. علاوه بر این پارلمان آن کشور یک قانون در زمینهٔ حفاظت از اطلاعات شخصی به تصویب رسانده است. در متن قوانین جنایی به جرائم سایبر نیز توجه شده، اما با اینحال این قوانین تأثیر کمی بر جای می‌گذارند، چراکه برای اعمال آنها ابتدا باید عامل "عمد" و "قصد" در ارتکاب جرم به اثبات برسد. با توجه به این موارد، تعقیب ناکافی جرائم به یک روال روزمره بدل شده، چون ارائه مدارک محکمه‌پسند برای اثبات تعمدی بودن چنین جرائمی واقعاً دشوار است. کارکنان بخش امنیت نیروهای انتظامی باید در زمینهٔ جمع‌آوری مدارک اثبات جرم آموزش کافی ببینند.

پرسش
سئوال اصلی اوکراین در مورد برآوردن مسئولیت و تعهد با

237 *http://wbln0018.worldbank.org/ html/Financial SectorWeb.nsf/(attachmentweb)/Singpore_TRMguidelines28Feb03/$FILE/Singpore_TRMguidelines28Feb0*

238 *Financial Action Task Force*

۲۳۹ *در این کشور تمام بانکها جزئی از سیستم بانک ملی محسوب می‌شوند.*

استفاده از مکانیزمهای نظارت داخلی و گزارش بود. بعنوان نمونه، گزارش رویدادها توسط مأموران بانکی برای ایمنی بانک ضروری است. برای کمک به ظرفیتهای واکنش به رخدادها، یک مرکز فوریتهای امنیت رایانه‌ای در اوکراین بوجود آمده است.

پاسخ

در مورد مدارک محکمه‌پسند، به این نکته اشاره شد که داده‌های الکترونیکی در معرض نابودی سریع هستند و در حوزهٔ جرائم رایانه‌ای نیز هیچ استانداردی برای مدارک قانونی وجود ندارد. با اینکه دنیا نیازمند راهبردهایی برای پیگردهای قانونی بصورت دیجیتال است، اما درحال حاضر روش استانداردی که مورد تأیید دادگاهها باشد وجود ندارد.

استرالیا

استرالیا جهت طبقه‌بندی اطلاعات، BASEL2 را انتخاب و پیاده‌سازی کرده است. با اینحال آنها دریافته‌اند که استفادهٔ روزافزون از سیستمهای مهاجم‌یاب با اینهمه تشخیصهای مثبت ناصحیح (false positive) و سیستمهای تنظیم‌نشده چندان آسان نیست. فناوریهای جدید بر مبنای فناوریهای پیشین ساخته می‌شوند، و این به پیچیدگی و وابستگی سیستمها به یکدیگر دامن می‌زند. در همینحال ممکن است نحوهٔ کار سیستمها نیز به خوبی مستندسازی نشده باشد. یادگیری در مورد چگونگیِ وابستگی سیستمها به یکدیگر بسیار حیاتی است، اما معمولاً مستندات در دسترس، بسیار محدود هستند. نمایندهٔ استرالیا به این مسئله اشاره کرد که در این کشور مطالب آموزشی رایگان در زمینه‌های عمومی و تخصصی برای download کردن فراهم است.

استرالیا سه نکته اساسی را مطرح کرد.
اول، تا اکتبر ۲۰۰۳ در تمامی کشورهای عضو APEC در زمینهٔ جرائم سایبر قوانینی وجود خواهد داشت؛ که مواردی چون کلاهبرداری الکترونیکی و اعمال قوانین الکترونیکی بصورت فرابخشی و بین‌المللی را در بر می‌گیرند.

دوم، آموزش و همکاری در زمینهٔ اجرای قانون در همهٔ سطوح لازم است و استانداردهای فناوری اطلاعات بصورت خلاصه در این دوره‌ها قرار خواهند داشت. برنامهٔ امنیت سایبر APEC به فناوری بی‌سیم نیز خواهد پرداخت و بطور خلاصه به مخاطرات فناوریهایی چون Wi-Fi هم می‌پردازد.

سوم، تا آخر اکتبر ۲۰۰۳ در تمام کشورهای عضو APEC مراکز فوریتهای امنیت رایانه‌ای تشکیل خواهد شد.

چین، پکن

نمایندهٔ چین بیان داشت که آگاهی عمومی درخصوص جایگاه امنیت الکترونیکی باید افزایش یابد و برای نیل به این مقصود ارزیابیهای خارجی بیشتری مورد نیاز است. یکی از عمدهٔ مشکلاتی که چین در زمینهٔ امنیت الکترونیکی با آن مواجه می‌باشد فقدان آگاهی و توانایی مدیریتی برای ارزیابی مخاطرات (بخصوص با توجه به ماهیت پیچیدهٔ فناوریها) است. این مشکل در کشور چین بدلیل همکاری ضعیف میان مراکز قانونگذاری و مراکز نظارتی تشدید هم شده است.

علیرغم اوضاع نامساعد امنیتی، بانکهای اینترنتی در چین بسرعت درحال رشد هستند. تعداد این بانکها در خلال سالهای ۱۹۹۹ تا ۲۰۰۳ از یک به بیست و هفت رسیده و نیز حجم فعالیتهای بانکی بیش از ۱۰۰ برابر رشد داشته است. به این نکته اشاره شد که در زمان شیوع بیماری سارس، بانکداری اینترنتی رونق زیادی پیدا کرد. نهایتاً کشور چین پیشنهادهای زیر را ارائه داد:

۱. تشویق اشتراک اطلاعات در سطوح ملی و بین‌المللی
۲. ایجاد استانداردهای بین المللی امنیت الکترونیکی
۳. افزایش شفافیت در بانکداری الکترونیکی

چین، هنگ‌کنگ

در هنگ‌کنگ، نامه‌های الکترونیکی جعلی، ویروسها، و کرمها بسیار رایج هستند. در کنار این مسائل نحوهٔ رفتار مهاجمین هم دچار تغییر شده است. در این کشور بجای هدف قرار گرفتن مستقیم بانکها، ضعیفترین حلقه – یعنی مشتری – مورد حمله قرار گرفته است و لذا آموزش مشتریان بسیار حیاتی است.

اتفاقی که اخیراً در یک پایگاه وب متعلق به یک بانک جعلی روی داد، مشکلات امنیتی را آشکارتر کرد. این بانک در پایگاه وب، یک آدرس پستی ناقص قرار داده بود و از گواهی

دیجیتال هم استفاده نمی‌کرد، و همچنین ادعا داشت که دفاتری در نیویورک و نقاط دیگر دارد؛ اما در بازرسیها معلوم شد که هم آن پایگاه وب (که در چین میزبانی می‌شد) و هم بانک مورد ادعا جعلی هستند. این واقعه بار دیگر نیاز حیاتی به همکاریهای فرابخشی را آشکار کرد، بخصوص به این دلیل که تبهکاران جرائم سایبر، خود بصورت فرابخشی عمل می‌کنند.

کشور هنگ‌کنگ درحال تهیهٔ مقدماتی برای ایجاد بسترهای نظارت بر مشتریان و آموزش به آنها است، مثل انتشار راهنماهایی برای افزایش آگاهی عمومی در ابعاد حیاتی امنیت الکترونیکی و اعلان هشدارهایی برای مقابله با جرائم رایانه‌ای. برای ارتقای امر نظارت در امنیت الکترونیکی، این کشور با *ثبت‌کنندگان دامنه*[۲۴۰] رابطهٔ نزدیکی دارد و برای کنترل نامهای دامنهٔ محلی (hk.) از فرآیندی خودکار استفاده می‌کند: اگر واژهٔ "بانک" یا هر شکل دیگر آن در نام دامنه بکار رفته باشد، موضوع بلافاصله برای بررسی به مراجع ذیصلاح ارجاع داده می‌شود. نیروهای پلیس، مرکز فوریتهای امنیت رایانه‌ای، و نیز دولت هنگ‌کنگ هم برای ایجاد قابلیت واکنش سریع به رخدادها، با نهادهای مختلفی در سطوح بین‌المللی همکاری دارند. *سیستم نظارت بر خودارزیابی* (CSA)[۲۴۱] در چیزی حدود ۷۰ تا ۸۰ بانک وجود دارد و بدلیل مشکلات خاص ارزیابی سالانه، این ارزیابی نیز بصورت خودکار انجام می‌شود.

جمهوری کره

با اینکه کره نتوانست در این بحث جهانی شرکت کند، اما به سؤالات مطرح شده توسط بانک جهانی پاسخ داد. آنها اشاره کردند که اگرچه کره دارای شبکه‌های اطلاعاتی پیشرفته‌ای است، اما سطح امنیت آنها هنوز جا برای ارتقا دارد. در کره ۶۵٪ معاملات بورس بصورت اینترنتی انجام می‌شود و حدود ۲۵ میلیون نفر از اینترنت استفاده می‌کنند. رخدادهای اخیر مثل آسیبهای کرم Slammer در ژانویهٔ ۲۰۰۳ تأثیرات شدیدی در کره داشت و طبیعت شکنندهٔ شبکه‌ها را آشکار کرد.

کره آماری ارائه کرد که نمایانگر سطح پایین آگاهی افراد در خصوص ایمنی سیستم بود. به گفتهٔ وزارت اطلاعات و ارتباطات، تنها ۱۲،۹٪ شرکتهای تجارت الکترونیکی، ۱۶،۷٪ مؤسسات آموزشی، و ۹،۲٪ سازمانهای دیگر دارای بخشی برای امنیت اطلاعات هستند. کره اشاره کرد که امنیت الکترونیکی از دید بسیاری از شرکتها بعنوان یک هزینهٔ مبهم است که تنها با تخصیص منابع و زمان کافی به انجام می‌رسد. بعنوان مثال تنها حدود ۱۲،۹٪ شرکتهای تجارت الکترونیکی و ۶،۱٪ تمام شرکتها در این کشور برای حفاظت از خود از سیستمهای مهاجم‌یاب استفاده می‌کنند.

سریلانکا

نمایندهٔ سریلانکا بیان داشت که در آن کشور تهدیدهایی مثل کرمها و آسیب‌پذیریهای بی‌سیم وجود دارد اما مقامات سریلانکا تا کنون هیچ گزارشی درخصوص حملات به سیستمهای بانکی دریافت نکرده‌اند. این کشور حدود ۲۰ سال است که از دستگاههای خودپرداز استفاده می‌کند. هرچند بانکداری الکترونیکی در سریلانکا در ابتدای راه است اما به سرعت درحال رواج می‌باشد. تبادل سهام و پول بصورت اینترنتی قابل انجام است، اما اینگونه امکانات نیز هنوز در مراحل اولیهٔ توسعهٔ خود هستند. درحال حاضر در سریلانکا مهمترین رخداد امنیتی، سرقت شناسه‌های کاربری و رمزهای عبور است. برای مؤسسات خدمات مالی، سطح آگاهی از مخاطرات یک مسئله کلیدی است و همچنین مخاطرات باید به دقت ارزیابی شوند.

امنیت سایبر در بخش مالی سنگاپور

تونی چو[۲۴۲] مدیر نظارت بر مخاطرات فناوری در *ادارهٔ امور پولی سنگاپور* (MAS)[۲۴۳] مروری اجمالی بر مقدمات امنیت سایبر داشت. وی بحث خود را با بیان این مطلب آغاز کرد که مسئولیت بخش او این است که "به مؤسسات آگاهی دهد، آنها را تحت نظارت قرار دهد، و یا نسبت به آنها سختگیری نماید". سنگاپور می‌کوشد تا به یک کانون بین‌المللی خدمات مالی تبدیل شود و به همین دلیل موضوع امنیت فناوری اطلاعات برای آن از اهمیت خاصی برخوردار است.

240 Domain Registrar
241 Supervisory Control Self-Assessment

242 Tony Chew
243 Monetary Authority of Singapore

بزرگترین بانکهای سنگاپور در سالهای ۲۰۰۱ و ۲۰۰۲ توسط نفوذگران مورد حمله قرار گرفتند؛ که این امر نشاندهندهٔ نیاز فوری این کشور به راهبردهای کاهش مخاطرات امنیتی است. در سال ۲۰۰۱ بزرگترین بانک سنگاپور (UOB) وجود یک نفوذگر را در سیستم اینترنتی بانکداری خود کشف کرد. با اینکه بیشتر اطلاعات مربوط به این رخداد محرمانه باقی ماند، اما معلوم شدکه نفوذگرهایی از اروپای شرقی به سیستم بانکی حمله کرده بودند. دادههای بانک مورد بررسی قرار گرفت و سیستم بانکی جهت بهروزآوری حساب مشتریان دستکاری شد. نهتنها چند ماه طول کشید تا متخصصین اصل مشکل را بیابند، بلکه تلاش زیاد و هزینهٔ گزافی صرف شد تا کشف شود که چه کسانی و یا چه چیزهایی عوامل این مشکل بودهاند.

در سال ۲۰۰۲، حملهٔ دیگری به دومین بانک بزرگ سنگاپور (DBS) صورت گرفت. در این رویداد نفوذگران بدلیل قابلیتهای اشتراکی شبکه و پیکربندی نامناسب سیستمها توانستند سیستمهای مشتریان را هدف قرار دهند. نفوذگران اسپهای تراوا و ثبتکنندههای صفحهکلید را در حسابهای ۲۱ مشتری بانک تعبیه کردند که به آنها اجازه میداد تا شمارهٔ شناسایی فردی (PIN) و شمارهٔ شناسایی کاربری را بدست آورند. این حادثه سبب شد ۶۲,۰۰۰ دلار به حسابهای مشتریان ضرر وارد شود، اما نکتهٔ قابل توجه آن است که تأثیر منفی این رخداد در افکار عمومی بسیار بیش از این بود؛ چراکه روزنامههای کشور به مدت یکماه در این خصوص مطلب نوشتند. امثال این رخدادها میتوانند به بحران بیاعتمادی مردم به سیستمهای بانکداری اینترنتی منجر شوند.

یک نقطهضعف اساسی که در تمام این رخدادها تأثیر داشت استفاده از تصدیق هویت تکعاملی بود. هماکنون نیز بیشتر دستگاههای خودپرداز از روشهای بسیار اولیهٔ تصدیق هویت استفاده میکنند، و تنها یک یا دو حادثهٔ دهشتناک میتواند بانکها را به تجدید نظر در این روند وادار کند. همچنین نوعی اعتماد و اطمینان بیش از حد به فناوری SSL وجود دارد؛ اما امنیتی که SSL بوجود میآورد بسیار محدود است، چراکه تنها در خلال انتقال اطلاعات از آنها حفاظت میکند، و نه در مبدأ یا مقصد. پایگاههای داده و دیگر رسانههای ذخیرهسازی باید همیشه بصورت رمزگذاریشده باشند تا امنیت آنها تضمین شود. برای PINها نیز باید از رمزنگاری قوی استفاده شود؛ اما این به تنهایی کافی نیست، چون PINها کوچک هستند و نفوذگران براحتی میتوانند آنها را دریافت کنند.

ادارهٔ امور پولی سنگاپور برای مؤسسات خدمات مالی "راهبردهای مدیریت مخاطرات فناوری" شامل ۲۶ توصیه در زمینهٔ ایجاد امنیت لایهای تدوین کرد. سه دستهٔ اصلی این راهبردها عبارتند از:

۱. ایجاد یک فرآیند مستحکم برای مدیریت مخاطره
۲. تقویت قابلیت دسترسی، امنیت، و قابلیت بازیابی
۳. استفاده از رمزنگاری قوی برای حفاظت از دادهها

علاوه بر تدوین سیاستهایی در مورد فناوری، ادارهٔ امور پولی سنگاپور بانکها را ملزم به انجام حداقل سالی یکبار آزمون نفوذ و ارزیابی محیط کار نمود. این اداره دارای یک تیم ارزیابی مخاطرات فناوری و یک سیستم برای درجهبندی بانکها در سیستم اقتصادی سنگاپور است؛ که بر مبنای شش معیار که توسط ادارهٔ امور پولی سنگاپور تعیین شده انجام میگیرد. این معیارها، مؤسسات را از لحاظ میزان ایمنی به پنج دسته تقسیم میکنند که شمارهٔ ۱ نشانگر امنترین و شمارهٔ ۵ نشانگر ناامنترین آنها است. بانکها ملزم هستند که در این ارزیابی حداقل به درجهٔ ۲ دست یابند، و علاوه بر آن باید برای سیستم خود طرح بازیابی و ترمیم سریع نیز داشته باشند. برای ایجاد انگیزهٔ پیشرفت در امنیت بانکها و القای حس استانداردسازی، نتایج این درجهبندی بصورت عمومی منتشر میشود. علاوه بر این بانکها ملزم به گزارش هرگونه رخداد امنیتی نیز میباشند.

با افزایش استفاده از دستگاههای سیار پرداخت، آسیبپذیریهای فناوری بیسیم نیز باید مورد توجه قرار گیرند. درحال حاضر تجربیات امنیتی در بانکداری بیسیم سنگاپور همچنان تحت بررسی هستند.

جمعبندی سؤالات و پیشنهادات

توصیهها و پرسشهای پایانی شامل نقاط کلیدی این سمینار جهانی بود.

اول، اطلاعرسانی و آگاهی در آموزش عمومیِ نیازهای حال حاضر امنیتی نقشی حیاتی ایفا میکند. قوانین دولتی مثل

"الزام گزارش فعالیتهای مشکوک" تنها درصورتی مفید هستند که به مرحلهٔ اجرا در آیند.

دوم، شفافیت و انتشار اطلاعات رخدادها برای ارتقای سطح ایمنی سیستمهای آینده اهمیت زیادی دارد. به این نکته اشاره شد که گاهی پوشش خبری وقایع می‌تواند مضر باشد، چراکه مشتریان در هرصورت از مطبوعات تأثیر می‌پذیرند. درعوض شرکتها باید وضعیت را بسرعت اصلاح کنند. پرداختن به مشکل با ایجاد یک طرح عملیاتی، راه بهتری برای مقابله با یک نفوذ امنیتی است. سؤال عمده‌ای که در اینجا بوجود می‌آید این است که در چه حدی و در چه زمانی باید این اطلاعات را منتشر کرد. در بخشهای دیگر این کتاب در این زمینه راهکارهایی ارائه شده است.

سوم، بیشتر کشورهای شرکت‌کننده به لزوم همکاریهای فرابخشی تأکید داشتند. یکی از بخشهایی که همکاری در آن مثمر ثمر خواهد بود برنامه‌های اعطای گواهینامه هستند. در این قسمت سازمانها باید با جامعهٔ نرم‌افزاری همکاری نمایند تا نیازهای امنیتی هر بخش مشخص شود. EBG، یکی از شبکه‌های ارتباطی و اطلاع‌رسانی و نیز InfraGard که یک شبکهٔ خصوصی- عمومی متعلق به FBI است دو نمونه از این قبیل مؤسسات هستند. InfraGard تمامی زیرساختهای حیاتی را در بر می‌گیرد و حدود ۱۰،۰۰۰ عضو دارد. هدف این سازمان ایجاد اعتماد و تشویق اشتراک اطلاعات میان اعضا است. این سازمان می‌تواند بعنوان مثالی از نحوهٔ ایجاد ارتباط در حوزهٔ امنیت فناوری اطلاعات درنظر گرفته شود.

چهارم، برای بوجود آمدن نوعی تعهد در امنیت الکترونیکی، نقشها و مسئولیتها باید تعیین شوند؛ و لذا تدوین یک استاندارد مراقبت و انجام وظایف امانتداری برای سازمانهای اقتصاد الکترونیکی یکی از مسائل بسیار مهم است. عناوین مباحث این موضوع عبارتند از سپرده‌ها و تراکنشها، اعتماد عمومی، و اطمینان سیستمهای خدمات مالی.

سرانجام استفاده از منابع خارج از سازمان یکی از نگرانیهای مهم شرکت‌کنندگان بود. نمونه‌ای از مشکلات موجود در این زمینه در سال ۲۰۰۱ رخ داد؛ هنگامیکه یک شرکت خدمات میزبانی وب در ایالات متحده مورد نفوذ قرار گرفت و درنتیجه امنیت بیش از ۳۰۰ بانک خدشه‌دار شد. جزئیات بیشتر در زمینهٔ استفاده از منابع خارج از سازمان را می‌توان در بخشهای دیگر این کتاب و سایر منابعی که در قسمت ضمائم به آنها اشاره شده پیدا کرد.

در خاتمه خاطرنشان می‌کنیم که برای قانونگذاران و بازرسان، ارزیابی مجدد چتر تقنینی (خصوصاً در زمینهٔ انتقال پول توسط اشخاص ثالث، مثل شرکتهای میزبانی وب) امری بسیار حیاتی است.