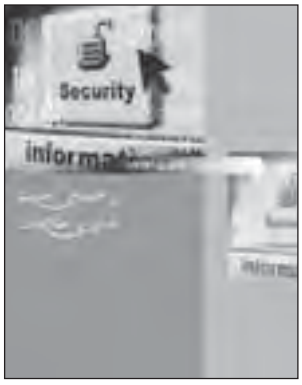
راهنمای امنیت فنّاوری اطلاعات



سادوی اسکای، جورج؛ و دیگران. راهنمای امنیت فناوری اطلاعات[1]، ترجمهٔ مهدی میردامادی و دیگران. تهران: دبیرخانهٔ شورای اطلاع‌رسانی،۱۳۸٤، ۵۰۹ ص، شابک: x - ۲٦ - ۸۸٤٦ - ۹٦٤

• **دکتر حمزه‌علی نورمحمدی[2]**
عضو هیأت علمی دانشگاه شاهد

مقدمه

مفهوم امنیت در دنیا مفهومی حیاتی و شناخته شده برای همه بشر بوده و است. در دوران ابتدایی امنیت در برابر حملات و همچنین امنیت برای تأمین غذا بسیار حائز اهمیت بوده است. به‌تدریج این امنیت گسترش یافته و امنیت در برابر حوادث، بیماری‌ها و داشتن امنیت فیزیکی بدون مواجهه با خطر از جمله نیازهای مهم بشری شده است. با پیشرفت‌های مختلف بشری در زمینه‌های گوناگون، محدودهٔ امنیت افزایش یافته و حریم وسیعی از جمله امنیت عمومی، اجتماعی، مالی، سیاسی، ملی و اقتصادی را دربرگرفت. در دهه‌های اخیر تحولات چشمگیری را شاهد بودیم که بسیاری از مناسبات و معادلات را به‌طور اساسی دست‌خوش تغییر کرده است. این تحولات که با کاربرد رایانه به‌عنوان ابزار خودکارسازی آغاز گردید، با فناوری اطلاعات و ارتباطات امکان‌پذیر شده و درواقع با ایجاد فضای همکاری و مشارکت، عملاً زندگی فردی و اجتماعی بشر را دگرگون ساخته است.

همان‌طور که مورخان پس از پیدایش خط و کتابت، آن را به دورهٔ ماقبل و ما بعد تاریخ تقسیم کردند، ورود به فناوری اطلاعات و ارتباطات نیز دورهٔ جدیدی را در تمدن بشری رقم زد. به‌صورتی‌که به عصر اطلاعات و ارتباطات شهرت یافت. این تحولات بزرگ الزامات و تبعات فراوانی را به‌دنبال داشته که مهم‌ترین آنها داشتن سخت‌افزارها و نرم‌افزارهای مناسب و ایمن در این زمینه است. مهم‌تر از همه داشتن اشتراک و ارتباط بین آنها برای اشتراک منابع است. امنیت اطلاعات در محیط‌های مجازی همواره به‌مثابهٔ یکی از زیرساخت‌ها و الزامات اساسی در توسعهٔ فراگیر مورد تأکید بوده است. اطمینان از ایمن بودن سرمایه‌های اطلاعاتی و تجهیزات زیرساختی درواقع کلید قفل فرصت‌های بی‌شماری در زمینه‌های گوناگون می‌باشد. علاوه بر این در دنیای امروز اعتبارات مالی هرچه بیشتر به‌صورت الکترونیکی جابه‌جا می‌شوند و اطلاعات مختلف با حساسیت‌های متفاوت از طریق شبکه انتقال می‌یابند. امروزه رایانه‌ها با سرعت بسیار زیاد با هم گره می‌خورند. این امر سوء استفادهٔ ماجراجویان و سودجویان جنایتکار را نیز موجب شده است. اکثر قریب به اتفاق سازمان‌ها در معرض انواع تهدیدات خرابکاران قرار دارند. در کنار این مسائل جرائم سازمان‌یافته در دنیای مجازی بر پیچیدگی امور برای تأمین امنیت زیرساخت‌ها افزوده است. با این اوصاف تدوین و اجرای تدابیر امنیتی در قبال این تهدیدات ضرورتی اجتناب‌ناپذیر برای سازمان‌ها محسوب می‌شود. تدابیر مناسب می‌تواند احتمال وقوع این تهدیدات را به حداقل برساند و حتی در صورت وقوع، میزان خسارت وارده ناچیز و قابل جبران خواهد بود.

دربارهٔ کتاب

کتاب حاضر علاوه بر اینکه مجموعه‌ای از تعاریف و راهکارهای امنیت عمومی را ارائه کرده، جنبه‌های فنی مدیریتی آنها را نیز مد نظر قرار داده است. تلاش شده تا حد امکان مطالب به‌گونه‌ای بیان شوند که فهم و درک آنها به دانش اختصاصی در این حوزه نیاز نداشته باشد و مورد استفادهٔ جامعهٔ گسترده‌ای از کاربران فناوری اطلاعات قرار گیرد. این کتاب با نگاه

کلان به موضوع امنیت، کوشیده مفاهیم مطرح در هریک از حوزه‌های آن را شرح دهد، و جایی که لازم بوده از بررسی جنبه‌های فنی نیز غفلت نشده است. همچنین نویسندگان هیچ‌گاه وارد آن دسته از مسائل فنی نشده‌اند که کلان‌نگری خود را از دست بدهند. این کتاب شامل شش بخش، یک پیشگفتار، دیباچه و پیش‌درآمد می‌باشد.

معرفی بخش‌های مختلف کتاب

بخش اول. امنیت فناوری اطلاعات در عصر دیجیتال

در این بخش دربارهٔ ظهور فناوری دیجیتال توضیحاتی بیان می‌شود. فناوری دیجیتال که یکی از مهم‌ترین پیشرفت‌های فناوری در نیم قرن اخیر به‌شمار می‌آید، و به‌مثابهٔ عامل حیاتی در زندگی بشر امروز درآمده است. در این فصل فوائد و آثار استفاده از اینترنت تشریح و چهار اصل مهم در این زمینه مورد توجه قرار گرفته است. این چهار اصل عبارت‌اند از:

ـ اینترنت مرزهای جغرافیایی را درنوردیده و روند جهانی سازی را تسهیل نموده است؛

ـ اینترنت تأثیر شگرفی در فرآیند حذف واسطه‌های تجاری داشته است؛

نرخ بهره‌وری به‌خصوص در فناوری اطلاعات به‌سرعت افزایش خواهد یافت؛

ـ ایمن‌سازی و ایمن نگهداشتن محل ذخیرهٔ اطلاعات و خطوط ارتباطی را در این محیط جدید الزامی کرده است.

نویسنده سپس ضمن طرح بحث انقلاب دیجیتالی، فناوری دیجیتال را از حیطهٔ رایانه‌ها فراتر می‌داند. به‌اعتقاد وی پیشرفت‌های فناوری در صنعت میکرو الکترونیک امکان ساخت ابزارهای پیچیدهٔ الکترونیکی در مقیاس‌های بسیار کوچک را فراهم آورده است. به‌طوری که اکنون می‌توان تجهیزات ارتباطی و محاسباتی بسیار پیچیده را در جیب جای داد. مفهوم امنیت مبحث بعدی است. در این مبحث بیان می‌شود که هنگامی در فضای سایبر ایمن هستید که دسترسی به منابع اطلاعاتی شما تحت کنترل خودتان باشد. یعنی هیچ‌کس بدون کسب اجازهٔ شما نتواند به این منابع اطلاعاتی دسترسی داشته باشد. مؤلف آنگاه به مشکلات امنیتی سیستم عامل ویندوز پرداخته و به پیدایش و رشد اینترنت و موضوعات مطرح‌شده در حوزهٔ امنیت اشاره می‌کند و انگیزه‌های خرابکاران امنیتی را در زندگی واقعی بسیار بالا می‌داند. وی از دلایل عمدهٔ این خرابکاری را انتقام‌گیری، آسیب‌رساندن و به‌دست‌آوردن پول برمی‌شمرد. اهمیت امنیت برای سازمان‌های کوچک و متوسط در کشورهای در حال توسعه و مفهوم نوینی از قابلیت اطمینان، بحث بعدی این بخش است. در جمع‌بندی فناوری‌های دیجیتالی را ابزارهای جدید مهیجی می‌داند که هریک می‌توانند نقش بسزایی در آموزش، بهداشت، رفاه، تجارت و سایر بخش‌های جامعه مدنی داشته باشند. به‌اعتقاد مؤلف تمام افراد و کشورها از فناوری اطلاعات بهره می‌جویند، اما این فناوری برای کشورهای در حال توسعه جاذبهٔ خاصی دارد و در تسریع در جا افتادن آنها در جامعهٔ اقتصاد جهانی موثر است.

اطمینان از ایمن بودن سرمایه‌های اطلاعاتی و تجهیزات زیرساختی درواقع کلید قفل فرصت‌های بی‌شماری در زمینه‌های گوناگون می‌باشد

بخش دوم. امنیت فناوری اطلاعات و کاربران منفرد

این بخش شامل هشت فصل و سه ضمیمه است. در فصل اول که در حکم مقدمه است، ضمن تأکید بر تأمین امنیت کاربران رایانه، چگونگی حفاظت از رایانه شخصی تشریح شده است. فصل دوم، «درک مفاهیم امنیتی»، به تبیین ضرورت برقراری امنیت و حفاظت از شبکه و رایانه اختصاص دارد. در این فصل به پیامدهای نفوذ امنیتی، اقدامات اولیه برای مقابله با آن، و نیز چند تعریف فنی از مباحث امنیتی پرداخته می‌شود. موضوع فصل سوم امنیت رایانه و داده‌هاست. نویسنده در این فصل به بررسی راه‌هایی می‌پردازد که از طریق آنها می‌توان رایانه را از لحاظ فیزیکی ایمن و از سرقت داده‌ها و برنامه‌های رایانه‌ای جلوگیری کرد. مباحث عمدهٔ این فصل عبارت‌اند از: امنیت فیزیکی، نسخه‌های پشتیبان، و تصدیق فوریّت و استفاده از نام کاربری و رمز عبور. فصل چهارم به امنیت سیستم عامل و نرم‌افزارهای کاربردی اختصاص دارد. در این فصل فنونی بررسی می‌گردد که از آنها برای کاهش آسیب‌پذیری سیستم عامل و نرم‌افزارهای کاربردی در برابر نفوذهای امنیتی استفاده می‌شود.

موضوع فصل پنجم بررسی نرم‌افزارهای مخرب است. در این فصل مفهوم و انواع مختلف نرم‌افزارهای مخرب نظیر ویروس‌ها، کرم‌های اینترنتی و تراواها، و روش‌ها و مکانیزم‌هایی که از سوی آنها اعمال می‌شوند، تشریح می‌گردد. فصل ششم دربارهٔ امنیت خدمات شبکه است. پست الکترونیکی و وب از کاربردهای اصلی اینترنت هستند. در این فصل عملکرد این خدمات به‌طور جزئی توضیح داده شده و استفادهٔ نامناسب از آنها که باعث ایجاد ناامنی می‌گردد، بررسی می‌شود. مواردی مثل ارتباط بی‌سیم، اشتراک فایل‌ها و قابلیت ارسال پیام فوری از دیگر موضوعات حساس مرتبط با امنیت شبکه‌اند که در این فصل به آنها پرداخته می‌شود. فصل هفتم به ابزارهای ارتقای امنیت اختصاص دارد. در این فصل بسته‌های نرم‌افزاری امنیتی و روش‌های افزایش امنیت شبکه‌ها و رایانه‌ها مورد بررسی قرار می‌گیرد. منظور از بسته‌های نرم‌افزاری امنیتی همان

ویروس‌یاب‌ها، دیواره‌های آتش، و ابزارهای دسترسی از راه دور است. فصل هشتم ضمن پرداختن به نکات ویژهٔ بسترهای مختلف، به رایانه‌های شخصی مبتنی بر ویندوز، مکینتاش، لینوکس و یونیکس اشاره دارد و نقاط و قوت و ضعف این سیستم‌های عامل را برمی‌شمارد. ضمیمهٔ اول بخش دوم به آشنایی با کدگذاری و رمزگذاری و فرآیند آن می‌پردازد. ضمیمهٔ دوم به فرآیند پروتکل تی. سی. پی/ آی. پی[۳] و آدرس‌دهی در اینترنت و ضمیمهٔ سوم به تعریف واژه‌ها و اصطلاحات فنی اختصاص دارد.

بخش سوم. امنیت فناوری اطلاعات و سازمان‌ها

این بخش شامل ۱۳ فصل است. موضوع فصل اول امنیت فناوری اطلاعات در سازمان‌ها و خطرهای تهدیدآمیز چندگانه است. در فصل دوم دربارهٔ روش‌های کاهش آثار خطرات امنیت الکترونیکی بحث شده است. نویسنده در این فصل به شناسایی، تعریف، و بحث دربارهٔ مجموعهٔ سیاست‌ها و روال‌های مهم می‌پردازد. جهت اتخاذ سیاست‌های امنیتی مناسب و اجرای صحیح آنها خطر از دست دادن ناگهانی اطلاعات را کاهش می‌دهد، ورود غیرمجاز به سیستم را بسیار مشکلتر می‌کند و ابزار امنیتی برای شناسایی حملات و اصلاح رخنه‌های امنیتی را فراهم می‌سازد. برای حفظ داده‌های محرمانه و کمک به یکپارچگی برنامه‌ها و داده‌های ذخیره‌شده و انتقال این داده‌ها از طریق شبکه، باید تلفیقی از سیاستگذاری و پیاده‌سازی آن انجام شود. این بخش اجزای مختلف سیاستهای امنیتی مؤثر برای سازمان‌های مختلف مانند شرکت‌های تجاری، دولت‌ها، دانشگاه‌ها و سازمان‌های غیرانتفاعی را پوشش می‌دهد. همچنین یک زیرساخت کلی به منظور تقویت محیط امن الکترونیکی برای بخش خدمات مالی می‌پردازد. این بخش برای سیاستگذارانی که با عرضه‌کنندگان خدمات مالی به‌ویژه ادارات اجرایی، مدیران ارشد اطلاعات، و مدیران ارشد امنیت کار می‌کنند، تهیه شده است. نکات فنی این بخش برای کسانی که سیستم‌های امنیت الکترونیکی را راهبری می‌کنند و بازرسان بانک‌ها که کارآیی امنیت الکترونیکی را ارزیابی می‌کنند، در نظر گرفته شده است. در فصل سوم ضمن بررسی برآورد مخاطره و تحلیل زیان و آسیب‌های امنیتی از دیدگاه تجاری، منشأ، عملکردو احتمال برخورد به هر نوع مشکل و شدت اثرات خطرات امنیتی بر فعالیت‌های روزمره را مورد مطالعه قرار می‌دهد. مؤلف در این فصل بر آن بوده تا نکات

کتاب حاضر علاوه بر اینکه مجموعه‌ای از تعاریف و راهکارهای امنیت عمومی را ارائه کرده، جنبه‌های فنی مدیریتی آنها را نیز مد نظر قرار داده است

اساسی یک سیاست امنیتی صحیح را تشریح کرده و اصول تحلیل زیان را هنگام رخداد امنیتی واقعی نیز مورد بررسی قرار دهد. فصل چهارم به برنامه‌ریزی برای نیازهای امنیتی اختصاص دارد. مؤلف در این فصل به سیاست‌ها و روش‌های پیش‌گیری و دفاع مؤثر در مقابل تهدیداتی که در فصل قبل دربارهٔ آنها بحث شد، پرداخته و جزئیات فرآیند برنامه‌ریزی را تشریح می‌کند.

فصل پنجم دربارهٔ پیش‌گیری و سیاست سازمانی می‌باشد. در این فصل سطوح مختلف سیاست امنیتی که در آن هر کارمند سازمان در امنیت رایانه‌ها، شبکه‌ها و اطلاعات نقش دارد، تشریح می‌شود. فهرست‌های کنترل مدیریتی را که در این بخش به آنها اشاره شد، نیز می‌توان در فصل‌های پایانی این بخش یافت. نویسنده در فصل ششم که به مسئلهٔ امنیت کارکنان اختصاص دارد، به‌اختصار آن دسته از مسائل امنیتی را بررسی می‌کند که از داخل سازمان نشئت می‌گیرند. به‌اعتقاد وی مسائل امنیتی کارکنان از استخدام و اخراج گرفته تا آموزش و آگاهی آنان نقش حیاتی در عملکرد پیش‌گیرانه و دفاعی سازمان دارد. بحث فصل هفتم برون‌سپاری امنیت است. در این فصل برخی از مزایا و معایب برون‌سپاری امنیت ذکر شده و سؤالاتی که پیش از نهایی کردن مذاکرات با شرکای جدید بخش امنیت باید به آنها پاسخ داد، نیز عنوان شده است. فصل هشتم به قانون‌نویسی، تدوین آیین‌نامه‌های دولتی، و سیاست‌های حریم خصوصی اختصاص دارد. در این فصل نمونه‌هایی از نحوهٔ تدوین سیاست‌های عمومی تجاری برای مؤسسات غیرانتفاعی و دولتی در دنیای متصل به شبکه، همانند قانون‌نویسی برای حفاظت از شهروندان، مشتریان و کودکان از سرقت هویت، کلاهبرداری و مطالب غیراخلاقی ارائه می‌شود. در این فصل تأکید بیشتر بر مسئولیت سازمانی در فضای عمومی است. فصل نهم دربارهٔ جرائم رایانه‌ای است. نویسنده در فصل دهم دربارهٔ مدیریت خطرات سیار و خدمات مالی الکترونیکی در محیط بی‌سیم بحث کرده و به بررسی خطرات می پردازد که در نتیجهٔ استفاده از فناوری‌های بی‌سیم در خدمات مالی به‌وجود می‌آیند و از طریق سرقت هویت، تسخیر فعالیت‌های سیستم،

و سایر اقدامات مشابه، امنیت الکترونیکی را تهدید می‌کنند. در این فصل به چند نکتهٔ مهم اشاره می‌شود که راهبران سیستم‌ها می‌توانند برای کاهش خطرات بدون افزایش زیاد هزینه، آنها را به‌کارگیرند. فصل یازدهم به «الگوی سرآمدی: ایجاد فرهنگ امنیت» اختصاص دارد. مؤلف در این فصل با طرح پیشنهادهایی دربارهٔ به‌کارگیری امنیت چندلایه، یک سیاست امنیتی دوازده‌لایه‌ای ارائه می‌دهد. در ادامهٔ این فصل منتخبی از روش‌های کنترل امنیتی آمده که با یادآوری وظایف روزانهٔ کارمندان و اعضای تیم مدیریت برای ایمنی سازمان به جلوگیری از خدشه‌دارشدن امنیت کمک می‌کند. در فصل دوازدهم دربارهٔ قواعد ایمنی تجارت الکترونیکی برای همهٔ کاربران و شرکت‌ها بحث شده و چهار گام برای ایمنی رایانه‌ها پیشنهاد می‌شود. فصل سیزدهم به گفت‌وگوهای بین‌المللی دربارهٔ موضوع امنیت اختصاص دارد. مؤلف در این فصل سمینارهای جهانی سال ۲۰۰۲ دربارهٔ «امنیت الکترونیکی: کاهش مخاطره در حوزهٔ خدمات مالی» و سمینار سال ۲۰۰۳ دربارهٔ «ایمنی و سلامت الکترونیکی» را معرفی و بررسی کرده است.

بخش چهارم. امنیت فناوری اطلاعات و سیاست‌های دولتی

بخش چهارم به سیاست‌های امنیت سایبر دولت اختصاص دارد. به‌اعتقاد مؤلف دولت‌ها باید ضمن توجه به نقش بخش خصوصی در موضوع امنیت سایبر، استانداردهای نظارتی و قانونگذاری در این زمینه‌ها را نیز مورد اهتمام قرار دهند. این بخش در چهار فصل تنظیم شده است. فصل اول مقدمه‌ای دربارهٔ نقش دولت و اهمیت آن در امنیت فناوری اطلاعات است که مؤلف مفهوم زیرساخت‌های حیاتی را بیان می‌کند. وی سپس ۱۳ گروه زیرساخت حیاتی استراتژی امنیت سایبر دولت ایالات متحده آمریکا را که در سال ۲۰۰۳ به چاپ رسیده و نیز ۱۱ اصل گروه جی ۸ را که برای توسعهٔ استراتژی کاهش خطر زیرساخت اطلاعات حساس مورد نظر قرار می‌گیرد، معرفی می‌کند. فصل دوم دربارهٔ حفاظت از سیستم‌های دولتی است. مؤلف در این فصل ضمن بیان مسائل امنیت رایانه‌ای دولت و سازماندهی آنها، روند تهیهٔ استراتژی ملی امنیت سایبر را ابزار مؤثری برای تصمیم‌گیری دانسته و به پیاده‌سازی استراتژی امنیت سایبر در سیستم‌های دولتی ایالات متحده اشاره می‌کند. فصل سوم به معرفی و بررسی نقش قانون و سیاست‌های دولتی دربارهٔ بخش خصوصی و همچنین قوانین مربوط به ادارهٔ سازمان، حسابداری، ثبت و فروش اوراق بهادار اختصاص دارد.

اغلب کاربران رایانه‌ها در ابتدا بیشتر افراد متخصص بودند، حال آنکه امروزه بیشتر کاربران، افراد غیرحرفه‌ای می‌باشند

بخش پنجم. امنیت فناوری اطلاعات و راهبری فنی

بخش پنجم اطلاعاتی دربارهٔ مسائل امنیتی در سطح فنی ارائه داده است. این بخش با بخش‌های دیگر قدری تفاوت دارد. زیرا فرض بر این است که خواننده سطح معینی از اطلاعات فنی را دریافته است. این بخش برای افرادی طراحی شده است که تجربهٔ کار با سیستم و راهبری آن را دارند. مباحث این بخش تا حد زیادی نظری است، اگرچه نمونه‌هایی از کاربرد چند اصل در سیستم‌های واقعی ارائه شده است. بخش حاضر حاوی ده فصل است. فصل اول خلاصه‌ای از بخش‌های گذشته است. فصل دوم به موضوع امنیت برای راهبران اختصاص دارد. مؤلف در این فصل ضمن ارائهٔ یک تعریف علمی از امنیت برای مدیران اجرایی، دربارهٔ طراحی سیستم‌های ایمن بحث کرده و توضیح می‌دهد که چه کسانی به سیستم‌های رایانه‌ای حمله می‌کنند. وی همچنین برخی از ابزارهای متداول مهاجمان را برشمرده و مطالعهٔ موردی یک نمونه حمله را تشریح می‌کند. فصل سوم به امنیت فیزیکی اختصاص دارد. امنیت فیزیکی اقداماتی است که پیش از فرمان‌ها اجرا می‌شود. از جملهٔ این اقدامات به سیستم اعلام خطر، گذاشتن قفل روی منبع برق رایانه، اتاقک قفل شده و مجهز به دوربین مداربستهٔ رایانه و مقسم‌های برق و منبع برق وقفه ناپذیر[۴] می‌توان اشاره کرد. به‌اعتقاد مؤلف امنیت فیزیکی به‌رغم اینکه مسئلهٔ بسیار مهمی است، غالباً نادیده گرفته می‌شود. در این فصل دربارهٔ بسیاری از تهدیدهای امنیت فیزیکی از جمله خطرات محیطی، خرابکاری و سرقت بحث شده و پیشنهادهایی برای نحوهٔ برخورد با آنها ارائه می‌شود. فصل چهارم به امنیت اطلاعات اختصاص دارد. در این فصل مکانیزم‌هایی که اطلاعات را از انتشار ناخواسته، تحریف یا تخریب حفاظت می‌کنند، مورد توجه قرار گرفته است. این ابعاد امنیت معمولاً حفاظت از اطلاعات شخصی افراد نامیده می‌شود که از دسترسی یا ایجاد تغییر در داده‌ها، برنامه‌ها و یکپارچگی سیستم از سوی کاربران غیرمجاز جلوگیری می‌کند و اطمینان می‌دهد که اطلاعات و نرم‌افزارها دست نخورده و سالم باقی مانده‌اند.

فصل پنجم به موضوع شناسایی و تصدیق هویت اختصاص دارد. شناسایی ارتباط‌دادن یک هویت با یک موضوع است. تصدیق هویت، اعتبار یک هویت را ثابت می‌کند و تصدیق اختیار، ارتباط‌دادن حقوق یا امتیازات با یک هویت می‌باشد. شناسایی و تصدیق هویت ممکن است به‌تنهایی از طریق یک ایستگاه کاری که فرد از آن استفاده می‌کند، انجام شود یا ممکن است یک سیستم مبتنی بر شبکهٔ تصدیق هویت را بر عهده داشته باشد که در آن هویت‌های کاربران در یک سرویس‌دهندهٔ مرکزی ذخیره و از سوی گروه‌های سرویس‌گیرنده به اشتراک گذاشته شده

است. فصل ششم به امنیت سرویس‌دهنده اختصاص دارد. سرویس‌دهنده به‌طورکلی رایانه‌ای است که میزبانی برنامه‌های مختلف سرویس‌دهنده را برعهده دارد و این سرویس‌دهنده‌ها روی آن اجرا می‌شوند. در این فصل برخی از مشکلات امنیتی رایج در کاربرد رایانه‌ها به‌عنوان سرویس‌دهندهٔ خدمات اطلاعاتی مورد بحث قرار گرفته و نحوهٔ استقرار و پیکربندی سرویس‌دهنده‌ها برای به حداقل‌رساندن این مشکلات تشریح می‌شود. در ادامهٔ این فصل ابتدا امنیت میزبان و سپس نکات امنیتی برنامه‌های کاربردی یعنی سرویس‌دهنده‌های پستی، فایل، وب، پایگاه داده و نام بررسی می‌شود. موضوع فصل هفتم امنیت شبکه است. مؤلف در این فصل رایانه‌ها را به‌مثابهٔ ایستگاه‌های کاری مستقلی در نظر گرفته و اشاره می‌کند که بیشتر رایانه‌ها از طریق مودم، شبکه‌ها یا ارتباطات بی‌سیم به رایانه‌های دیگر متصل می‌شوند. وی سپس مسائل امنیتی را برای راهبرانی که رایانه‌ها را برای اتصال به شبکه‌ها پیکربندی می‌کنند، مورد بحث قرار می‌دهد. در این فصل ابتدا نحوهٔ اتصال رایانه به شبکه با استفاده از مودم‌ها، مسیریاب‌ها و ابزار بی‌سیم و با توجه ویژه به مسائل امنیتی هریک از آنها بررسی شده و سپس دربارهٔ اصول امنیت شبکه در شبکه‌های اینترنت یا اینترانت بحث می‌شود. فصل هشتم دربارهٔ انواع حملات و روش‌های مقابله با آنهاست. برای حمله به ایستگاه‌های کاری و سرویس‌دهنده‌ها از فنون بسیاری استفاده شده است. این فنون به‌طورکلی به سه دستهٔ مجزا تقسیم شده که عبارت‌اند از:

ـ تخریب سرویس‌دهنده و بهره‌برداری از راه دور. در بسیاری از رایانه‌ها آسیب‌پذیری‌هایی وجود دارد که باعث می‌شود مهاجمان بتوانند سیستم را از کار بیندازند. در بسیاری از موارد این نوع حمله می‌تواند روی شبکه، حتی بدون ورود به سیستم انجام پذیرد. در موارد دیگر مهاجمان برای نفوذ و تسخیر سیستم‌های آسیب‌پذیر نیاز دارند که به شبکه دسترسی دسترسی داشته باشند.

ـ تهدیدات برنامه‌ای. راه دیگر تسخیر یک سیستم از سوی مهاجم، فرستادن یک برنامهٔ مخرب به کاربران سیستم و انتظار برای اجرای این برنامه از سوی آنهاست. برخی از این برنامه‌ها سرویس‌های پنهانی نصب می‌کنند که کنترل رایانه را از راه دور برای مهاجم مهیا می‌کنند و برخی دیگر تکثیر شده و به رایانه‌ها منتقل می‌شوند.

ـ مهندسی اجتماعی. در یک حمله مهندسی اجتماعی مهاجم از خصوصیات طبیعی و اجتماعی کاربران و راهبران سیستم‌ها استفاده می‌کند تا آنها را به افشای اسرار یا انجام کارهای مخل امنیت وادار کند.

مؤلف در فصل نهم که به کشف و مدیریت نفوذ اختصاص دارد، به بحث دربارهٔ تدابیری چون بازبینی، ثبت وقایع و انجام اقدامات قانونی برای کشف دست‌کاری‌ها و تشخیص تغییرات می پردازد و می‌کوشد که مرحله به مرحله راه به دست گرفتن مجدد کنترل رایانه را نشان دهد. فصل پایانی به نکات ویژهٔ بسترهای مختلف پرداخته و به توصیه‌های فنی خاص برای سیستم‌های عامل یونیکس[5]، لینوکس[6]، مایکروسافت ویندوز[7]، و مک [8] ۷ـ۹ می‌پردازد.

بخش ششم. پیوست‌ها

بخش ششم شامل پنج پیوست است. پیوست اول واژه‌نامهٔ اصطلاحات می‌باشد. در این پیوست اصطلاحات ارائه شده در متن کتاب توضیح داده شده است. پیوست دوم کتابنامه است. پیوست سوم به منابع الکترونیکی اختصاص دارد. در این پیوست به مشکلات فراوان تهیه یک فهرست جامع از منابع الکترونیکی در یک سند چاپی اشاره شده است. در پیوست چهارم که به سازمان‌های امنیتی اختصاص دارد، اطلاعات برخی از سازمان‌های مفید جمع‌آوری شده و دریافت کمک و جمع‌آوری اطلاعات بیشتر از آنها مفید قلمداد می‌شود. مؤلف در پیوست پنجم به منابع چاپی پرداخته و منابع فهرست شده در این فهرست را مناسب دانسته و آن را به‌مثابهٔ نقطهٔ شروعی برای به‌دست‌آوردن اطلاعات بیشتر مفید می‌داند. وی همچنین کوشیده که فهرست ارائه‌شده را به مراجع در دسترس و ارزشمندتر محدود کند تا یافتن آنها برای خوانندگان دشوار نباشد.

در پایان کتاب نیز هفت صفحه به لغات و اصطلاحات رایج امنیتی اختصاص یافته و معادل فارسی واژگان لاتین ذکر شده است.

نقد و نظر

از آنجاکه پیشرفت فناوری اطلاعات و ارتباطات و نوآوری‌ها موجب استفادهٔ چشمگیر از انواع خدمات مربوط به این فناوری‌ها شده و همچنین تحقیقات صورت‌گرفته در این زمینه موجب افت سریع قیمت این محصولات شده و استفاده از آنها نیز تعمیم یافته است، در کنار این خدمات همیشه فرصت‌طلبان و سودجویانی وجود دارند که با انگیزهٔ سودطلبی یا مردم‌آزاری به فکر ضربه زدن و تخریب هستند. مشکلات مربوط به امنیت سیستم‌های اطلاعاتی و فرآیندهای آن از جمله ذخیره، بازیابی و ارسال اطلاعات از زمان شکل‌گیری آن وجود داشته و سیستم‌های بانکداری و مسائل مالی نیز به آن اضافه شده است. در سیستم‌های تجاری همیشه

همیشه امنیت مطلق دست نیافتنی بوده، ولی ایجاد سطحی از امنیت که به اندازهٔ کافی، متناسب با نیازها و سرمایه‌گذاری انجام شده باشد، تقریباً در تمام شرایط محیطی امکان‌پذیر است

استفاده از این روش برای ارتکاب جرم و نفوذ به شبکه‌های رایانه‌ای و سیستم‌های مالی انگیزه قوی وجود دارد. با توجه به اینکه همواره احتمال اینگونه فعالیت‌های تبهکارانه وجود دارد و از سوی دیگر بین صدها میلیون رایانه ارتباط وجود دارد که برای پردازش هرگونه اطلاعات قابل تصوری آماده‌اند، مشکلات این عرصه نیز بیشتر شده است. می‌توان گفت که اغلب کاربران رایانه‌ها ابتدا بیشتر افراد متخصص بودند، حال آنکه امروزه بیشتر کاربران، افراد غیرحرفه‌ای می‌باشند. این مسئله و عدم اطلاعات کافی آنان موجب شده که نفوذگران و تبهکاران رایانه‌ای به سیستم‌های مختلف صرف نظر از محل جغرافیایی نفوذ کرده و از فرصت بدست‌آمده سوء استفاده کنند. از این رو نیاز مبرم به اطلاعات کامل در این زمینه و مقابله با آن برای کاربران احساس می‌شود. کتاب حاضر توانسته به برخی از آنها پاسخ دهد. امنیت اطلاعات در محیط‌های مجازی همواره به‌عنوان یکی از زیرساخت‌ها و ملزومات اساسی در توسعهٔ خودکارسازی مورد توجه بوده است. همیشه امنیت مطلق دست نیافتنی بوده، ولی ایجاد سطحی از امنیت که به اندازهٔ کافی، متناسب با نیازها و سرمایه‌گذاری انجام شده باشد، تقریباً در تمام شرایط محیطی امکان‌پذیر است. همچنین اطمینان از ایمن‌بودن سرمایه‌های اطلاعاتی و تجهیزات زیرساختی هر کشور گذشته از ابعاد گستردهٔ امنیت ملی، در واقع کلید قفل فرصت‌های بسیاری از ابعاد تجاری و غیرتجاری است.

در بخش مقدمه به‌خوبی اهمیت امنیت اطلاعات مورد توجه قرار گرفته است. اگرچه این مقدمه به صور مختلف و با عناوین پیشگفتار، یادداشت مترجمان، دیباچه، پیش‌درآمد و خلاصهٔ اجرایی مطرح شده که می‌توانست در پیشگفتار و مقدمه همهٔ این مطالب بیان شود. البته در اینجا بنا نداریم که مفاهیم آنها را یکسان بگیریم، زیرا هرکدام از آنها مفهوم خاصی دارند و می‌توانند جداگانه نیز مطرح شوند. مؤلفان در بخش‌های مختلف کوشیده‌اند تا با نگاهی کلان به موضوع امنیت، مفاهیم مطرح در هریک از حوزه‌ها را شرح دهند. در پایان کتاب نیز فهرستی از لغات و اصطلاحات رایج امنیتی که در کتاب به‌کار رفته و نیز معادل فارسی آنها آمده است که از ویژگی‌های کتاب می باشد.

نقص فنی و امنیتی شبکه در همه کشورها اتفاق می‌افتد و ممکن است حتی سبب شود که دولت‌ها نیز تحت فشار قرار گیرند. معمولاً بسیاری از این نقص‌ها گزارش نمی‌شوند، زیرا اطلاع مردم از آنها می‌تواند نتایج نامطلوبی را به بار آورد. به همین دلیل کشورهای در حال توسعه باید به این موضوع توجه خاصی داشته باشند و تأمین امنیت را اولویت اصلی خود قرار دهند. چراکه خطر فعالیت‌های تبهکارانه بیشتر متوجه مکان‌هایی است که کنترل کافی بر آنها وجود ندارد. تجارت الکترونیک در کشورهایی که امنیت فناوری اطلاعات در آنها کمتر تامین شده، اهداف جذاب‌تری برای حمله هستند. این مطالب در پیش‌درآمد کتاب به‌خوبی بیان شده است، ولی جا داشت تا در یکی از بخش‌ها به‌خصوص دربارهٔ کشورهای درحال‌توسعه که با تب و تاب بیشتری برای خودکارسازی و همچنین تجارت از این فناوری‌ها استفاده می‌کنند، بیشتر به آن پرداخته می‌شد و مسائل و مشکلات بیشتر بررسی می‌شد. اگرچه در کتاب نیز بحث‌های فراوانی دربارهٔ ماهیت موضوع امنیت مطرح شده است و خود مؤلفان نیز مدعی‌اند که این کتاب بهترین و جدیدترین راهکارها را در زمینهٔ فناوری اطلاعات ارائه می‌دهد، اما در اصل برای خوانندگان کشورهای در حال توسعه نوشته شده است.

بدون اطلاع از موارد و مشکلات در زمینهٔ امنیت اطلاعات و نبود افراد حرفه‌ای در این بخش راه نفوذ و شکاف برای ورود تبهکاران حرفه‌ای بازتر می‌باشد.

نکات بارز

از جمله نکات بارز کتاب مستقل بودن هر بخش است که می‌تواند جداگانه مطالعه شود. مطالب و مباحث برای راهبران فنی مناسب می‌باشد. از نکات بارز دیگر کتاب می‌توان به منابع پایانی کتاب اشاره کرد. ترجمهٔ کتاب نیز نسبتاً خوب و روان است.

نکات ضعف

در بخش اول اطلاعات مفیدی دربارهٔ برخی از مسائل موجود در دنیای رایانه و نرم‌افزارهای سیستمی به‌خصوص ویندوز و مشکلات آن ارائه شده است، ولی ارتباط چندانی با عنوان ندارد و بهتر بود، به امنیت فناوری اطلاعات در عصر دیجیتال بیشتر پرداخته می‌شد.

عناوینی که در فصول مختلف بخش‌ها آمده، زیاد است. مؤلفان می‌توانستند با جمع‌بندی آنها از تعداد عناوین کم کنند و بدین ترتیب مطالب به صورت جمع‌بندی شده ارائه شود. عدم ارائه مطالب به صورت منسجم موجب می‌شود خواننده سردرکم بماند و آن چیزی را که با عنوان و سر فصل‌ها برای خود دنبال می‌کند به آن نمی‌رسد.

پی‌نوشت‌ها:

1. IT Security Handbook
2. nurmohammadi.h@googlemail.com
3. TCP/IP
4. Uninterruptable Power Supply
5. Unix
6. Linux
7. MS Windows
8. Mac 7 - 9