علوم اطلاع‌رسانی، دوره ۲۰، شماره ۳و۴ (بهار و تابستان ۱۳۸۴) ۱-۱۶

فناوری‌های امنیت اطلاعات: با یک دیدگاه طبقه‌بندی

مریم اسدی

کارشناس ارشد کتابداری و اطلاع‌رسانی*

چکیده

مهم‌ترین مزیت و رسالت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دستیابی سریع و آسان به اطلاعات است. کنترل دستیابی و نحوهٔ استفاده از منابعی که به اشتراک گذاشته شده‌اند، از مهم‌ترین اهداف یک نظام امنیتی در شبکه است. با گسترش شبکه‌های رایانه‌ای (خصوصاً اینترنت)، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته شده، وارد مرحلهٔ جدیدی گردیده است. در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، به یک راهبرد خاص پایبند باشد و براساس آن، نظام امنیتی را اجرا نماید. نبود نظام مناسب امنیتی، بعضاً پیامدهای منفی و دور از انتظاری را به دنبال دارد. توفیق در ایمن‌سازی اطلاعات، منوط به حفاظت از اطلاعات و نظام‌های اطلاعاتی در مقابل حملات است؛ بدین منظور از سرویس‌های امنیتی متعددی استفاده می‌گردد. مقالهٔ حاضر با توجه به این رویکرد به طبقه‌بندی فناوری‌های امنیت اطلاعات، براساس دو ویژگی خواهد پرداخت: مرحلهٔ خاصی از زمان که در هنگام تعامل فناوری با اطلاعات، عکس‌العمل لازم در برابر یک مشکل امنیتی، ممکن است کنشی یا واکنشی باشد، و سطوح پیاده‌سازی نظام‌های امنیتی در یک محیط رایانه‌ای.

کلیدواژه‌ها: امنیت اطلاعات/ اطلاعات/ فناوری/ رده‌بندی/ شبکه کامپیوتری

مقدمه

اطلاعات در سازمان‌ها، مؤسسات پیشرفته و جوامع علمی، شاهرگ حیاتی محسوب می‌گردد. دستیابی به اطلاعات و عرضهٔ مناسب و سریع آن، همواره مورد توجه سازمان‌هایی است که اطلاعات در آن‌ها دارای نقش محوری و سرنوشت‌ساز است. سازمان‌ها و مؤسسات باید یک زیرساخت مناسب اطلاعاتی برای خود ایجاد کنند و در جهت سازماندهی اطلاعات در سازمان خود حرکت نمایند. اگر می‌خواهیم ارائه‌دهندهٔ اطلاعات در عصر اطلاعات، و نه صرفاً مصرف‌کنندهٔ اطلاعات باشیم، باید در مراحل بعد، امکان استفاده از اطلاعات ذیربط را برای متقاضیان محلی و جهانی در سریع‌ترین زمان ممکن فراهم نماییم.

* پست الکترونیکی: masadi1355@yahoo.com

سرعت در تولید و عرضهٔ اطلاعات ارزشمند، یکی از رموز موفقیت در سازمان‌ها، مؤسسات و جوامع علمی در عصر اطلاعات است. پس از سازماندهی اطلاعات باید با بهره‌گیری از شبکه‌های رایانه‌ای، زمینهٔ استفادهٔ قانونمند و هدفمند از اطلاعات را برای دیگران فراهم کرد. به موازات حرکت به سمت یک سازمان پیشرفته و مبتنی بر فناوری اطلاعات، باید تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده شود.

مهم‌ترین مزیت و رسالت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دستیابی سریع و آسان به اطلاعات است. کنترل دستیابی و نحوهٔ استفاده از منابعی که به اشتراک گذاشته شده‌اند، از مهم‌ترین اهداف یک نظام امنیتی در شبکه است. با گسترش شبکه‌های رایانه‌ای خصوصاً اینترنت، نگرش به امنیت اطلاعات و دیگر منابع به اشتراک گذاشته شده، وارد مرحلهٔ جدیدی گردیده است. در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، به یک راهبرد خاص پایبند باشد و براساس آن، نظام امنیتی را پیاده‌سازی و اجرا نماید.

نبود نظام مناسب امنیتی، ممکن است پیامدهای منفی و دور از انتظاری را به دنبال داشته باشد. توفیق در ایمن‌سازی اطلاعات منوط به حفاظت از اطلاعات و نظام های اطلاعاتی در مقابل حملات است؛ بدین منظور از سرویس های امنیتی متعددی استفاده می‌شود. سرویس‌های انتخابی باید پتانسیل لازم در خصوص ایجاد یک نظام حفاظتی مناسب، تشخیص بموقع حملات، و واکنش سریع را داشته باشند. بنابراین می توان محور راهبردی انتخاب شده را بر سه مؤلفهٔ حفاظت، تشخیص، و واکنش استوار نمود. حفاظت مطمئن، تشخیص بموقع و واکنش مناسب، از جمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت کرد (مدیریت شبکه شرکت سخا روش، ۱۳۸۲).

خوشبختانه پژوهش‌های زیادی در زمینهٔ امنیت رایانه و شبکه‌ها در رابطه با فناوری‌های امنیتی پیشگیرانه (کنشی) و نیز مواجهه با مشکلات امنیتی (واکنشی) صورت گرفته است. مقالهٔ حاضر در صدد بیان تعدادی از فناوری‌های موجود در رابطه با امنیت اطلاعات با یک دیدگاه طبقه‌بندی است.

تعاریف:

فناوری‌های امنیت اطلاعات

«امنیت اطلاعات»[1] به حفاظت از اطلاعات (Maiwald & Sieglein، ۲۰۰۲) و به حداقل‌رساندن خطر افشای اطلاعات در بخش های غیرمجاز اشاره دارد (King, Dalton, & Osmanoglu، ۲۰۰۱). امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری (هاشمیان، ۱۳۷۹) و علم مطالعهٔ روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است (عبداللهی، ۱۳۷۵). با توجه به تعاریف ارائه شده، امنیت به مجموعه‌ای از تدابیر، روش‌ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام‌های رایانه‌ای و ارتباطی اطلاق می‌شود. «فناوری» به کاربرد علم، خصوصاً برای اهداف صنعتی و تجاری (Lexico Publishing Group، ۲۰۰۲) یا به دانش و روش‌های مورد استفاده برای تولید یک محصول گفته می‌شود.

بنابراین «فناوری امنیت اطلاعات» به بهره‌گیری مناسب از تمام فناوری‌های امنیتی پیشرفته برای حفاظت از تمام اطلاعات احتمالی روی اینترنت اشاره دارد (INFOSEC، ۲۰۰۲).

طبقه‌بندی[2]

طبقه‌بندی، دسته‌بندی اشیا است در یک فهرست سازمان یافته یا در قالب روابط سلسله‌مراتبی که روابط طبیعی بین اشیا را نشان می‌دهد (Conway & Sliger، ۲۰۰۲). طبقه‌بندی به عنوان یک فرایند، عبارت است از ایجاد نظامی منطقی از رتبه‌ها که در آن، هر رتبه از تعدادی اشیا تشکیل شده، به گونه‌ای که در صورت نیاز می‌توان به آسانی به اجزای آن دسترسی پیدا کرد.

طبقه‌بندی ارائه‌شده در مقالهٔ حاضر از فناوری‌های امنیت اطلاعات، در وهلهٔ اول براساس دو ویژگی پایه‌گذاری شده:

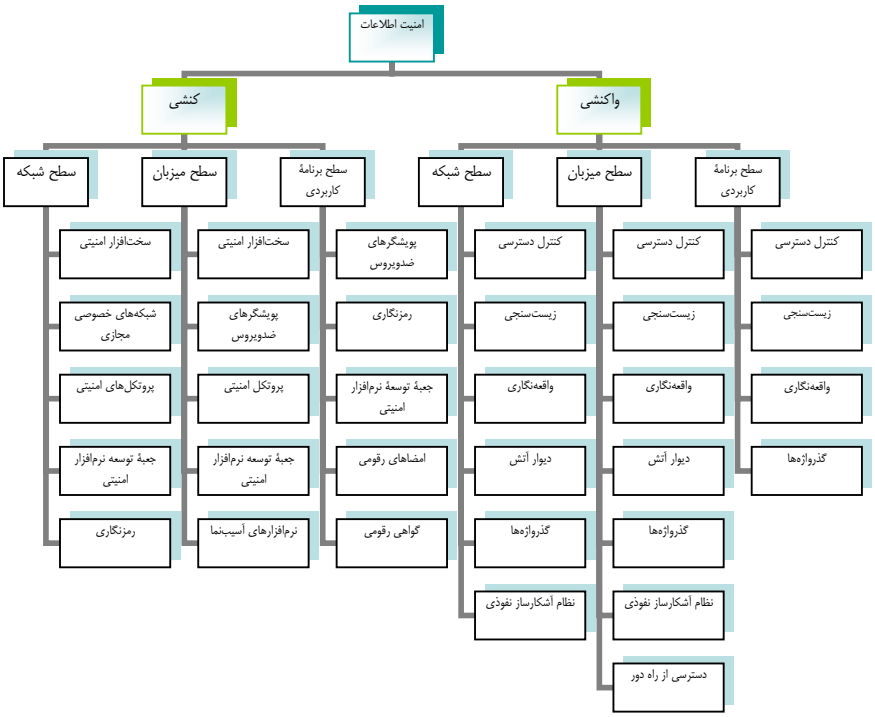
۱. براساس مرحلهٔ خاصی از زمان: بدین معنا که در زمان تعامل فناوری با اطلاعات، عکس‌العمل لازم در برابر یک مشکل امنیتی می‌تواند کنشگرایانه (کنشی)[3] یا واکنشی[4] باشد (Venter & Eloff، ۲۰۰۳).

غرض از «کنشگرایانه»، انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی است. در چنین مواردی به موضوعاتی اشاره می گردد که ما را در پیشگیری از وقوع یک مشکل کمک خواهد کرد (چه کار باید انجام دهیم تا ...؟).

غرض از «واکنشی» انجام عکس‌العمل لازم پس از وقوع یک مشکل خاص امنیتی است. در چنین مواردی به موضوعاتی اشاره می‌گردد که ما را در مقابله با یک مشکل پس از وقوع آن، کمک خواهند کرد (اکنون که ... چه کار باید انجام بدهیم؟).

۲. براساس سطوح پیاده‌سازی نظام‌های امنیتی در یک محیط رایانه‌ای: فناوری امنیت اطلاعات را، خواه از نوع کنشی باشد یا واکنشی، می‌توان در سه سطح – سطح شبکه[5]، سطح میزبان[6]، سطح برنامهٔ کاربردی[7]- پیاده‌سازی کرد (Venter & Eloff، ۲۰۰۳). بدین منظور می‌توان نظام امنیتی را در سطح شبکه و خدمات ارائه شدهٔ آن، در سطح برنامهٔ کاربردی خاص، یا در محیطی که شرایط لازم برای اجرای یک برنامه را فراهم می نماید (سطح میزبان) پیاده کرد.

شکل ۱ فناوری‌های امنیت اطلاعات را براساس دو ویژگی یادشده ترسیم می‌نماید. توصیف مختصری از هریک از فناوری ها در بخش‌های بعد ارائه خواهد شد.



شکل ۱. فناوری‌های امنیت اطلاعات با دیدگاه طبقه‌بندی (اقتباس از Eloff & Venter، ۲۰۰۳)

الف. فناوری‌های امنیت اطلاعات کنشگرایانه

۱. رمزنگاری[8]

به بیان ساده، رمزنگاری به معنای «نوشتن پنهان»، و علم حفاظت، اعتمادپذیری و تأمین تمامیت داده‌ها است (McClure, Scambray, & Kurtz، ۲۰۰۲). این علم شامل اعمال رمزگذاری، رمزگشایی و تحلیل رمز است. در اصطلاحات رمزنگاری، پیام را «متن آشکار»[۹] می‌نامند. کدگذاری مضامین را به شیوه‌ای که آن‌ها را از دید بیگانگان پنهان سازد، «رمزگذاری»[۱۰] یا «سرّگذاری»[۱۱] می‌نامند*. پیام رمزگذاری شده را «متن رمزی»[۱۲]، و فرایند بازیابی متن آشکار از متن رمزی را رمزگشایی[۱۳] یا «سرّگشایی»[۱۴] می نامند.

الگوریتم‌هایی که امروزه در رمزگذاری و رمزگشایی داده‌ها به کار می‌روند از دو روش بنیادی استفاده می کنند: الگوریتم‌های متقارن، و الگوریتم‌های نامتقارن یا کلید عمومی. تفاوت آن‌ها در این است که الگوریتم‌های متقارن از کلید یکسانی برای رمزگذاری و رمزگشایی استفاده می‌کنند، یا این که کلید رمزگشایی به سادگی از کلید رمزگذاری استخراج می‌شود (مثل: DES(Data Encryption Standard)، CCEP(The Commercial Comsec Endoremment Program)، IDEA(International Data Encryption Algoritm)، FEAL). در حالی که الگوریتم‌های نامتقارن از کلیدهای متفاوتی برای رمزگذاری و رمزگشایی استفاده می‌کنند و امکان استخراج کلید رمزگشایی از کلید رمزگذاری وجود ندارد. همچنین کلید رمزگذاری را کلید عمومی، و کلید رمزگشایی را کلید خصوصی یا کلید محرمانه می‌نامند (مثل: RSA، LUC).

تجزیه و تحلیل رمز[۱۵]، هنر شکستن رمزها و به عبارت دیگر، بازیابی متن آشکار بدون داشتن کلید مناسب است؛ افرادی که عملیات رمزنگاری را انجام می‌دهند، رمزنگار[۱۶] نامیده می‌شوند و افرادی که در تجزیه و تحلیل رمز فعالیت دارند رمزکاو[۱۷] هستند.

رمزنگاری با تمام جوانب پیام‌رسانی امن، تعیین اعتبار، امضاهای رقومی، پول الکترونیکی و نرم افزارهای کاربردی دیگر ارتباط دارد. رمزشناسی[۱۸] شاخه‌ای از ریاضیات است که پایه‌های ریاضی مورد استفاده در شیوه‌های رمزنگاری را مطالعه می‌کند ("آشنایی با ..."، ۱۳۸۳).

رمزنگاری یک فناوری امنیت اطلاعات از نوع کنشگرایانه است، زیرا اطلاعات را قبل از آن که یک تهدید بالقوه بتواند اعمال خرابکارانه انجام دهد، از طریق رمزگذاری داده‌ها ایمن می‌سازند. به علاوه، رمزنگاری در سطوح متنوع، به طوری که در طبقه‌بندی شکل ۱ بیان شد، در سطوح برنامه‌های کاربردی و در سطوح شبکه قابل پیاده‌سازی است.

۲. امضاهای رقومی[۱۹]

امضاهای رقومی، معادل «امضای دست‌نوشت» و مبتنی بر همان هدف هستند: نشانهٔ منحصر به فرد یک شخص، با یک بدنهٔ متنی (Comer، ۱۹۹۹، ص. ۱۹۱). به این ترتیب، امضای رقومی مانند امضای دست‌نوشت، نباید قابل جعل باشد. این فناوری که با استفاده از الگوریتم رمزنگاری ایجاد می‌شود، تصدیق رمزگذاری‌شده‌ای است که معمولاً به یک پیام پست الکترونیکی یا یک گواهی‌نامه ضمیمه می‌شود تا هویت واقعی تولیدکنندهٔ پیام را تأیید کند.

امضای رقومی یک فناوری امنیت اطلاعات از نوع کنشگرایانه است، زیرا قبل از وقوع هر تهدیدی، می‌توان با استفاده از آن فرستندهٔ اصلی پیام و صاحب امضا را شناسایی کرد. به علاوه این فناوری در سطح یک برنامهٔ کاربردی قابل پیاده‌سازی است. در این سطح، امضای رقومی در یک برنامه کاربردی خاص و قبل از آن که به یک گیرندهٔ خاص فرستاده شود، ایجاد می‌گردد.

۳. گواهی‌های رقومی[۲۰]

گواهی‌های رقومی به حل مسئلهٔ «اطمینان» در اینترنت کمک می‌کنند. گواهی‌های رقومی متعلق به «سومین دستهٔ اطمینان»[۲۱] هستند و همچنین به «متصدی‌های گواهی» اشاره دارند (Tiwana، ۱۹۹۹). متصدی‌های گواهی، مؤسسات تجاری هستند که هویت افراد یا سازمان‌ها را در وب تأیید، و تأییدیه‌هایی مبنی بر درستی این هویت‌ها صادر می‌کنند. برای به دست‌آوردن یک گواهی، ممکن است از فرد خواسته شود که یک کارت شناسایی (مانند کارت رانندگی) را نشان دهد. بنابراین گواهی‌های رقومی، یک شبکه امن در میان کاربران وب، و مکانی برای تأیید صحت و جامعیت یک فایل یا برنامهٔ الکترونیکی ایجاد می‌کنند. این گواهی‌ها حاوی نام فرد، شمارهٔ سریال، تاریخ انقضا، یک نسخه از گواهی نگاهدارندهٔ کلید عمومی (که برای رمزگذاری پیام‌ها و امضاهای رقومی به کار می‌رود) می‌باشند** (Encyclopedia and learning center، ۲۰۰۴).

گواهی‌های رقومی، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا از این فناوری برای توزیع کلید عمومی از یک گروه ارتباطی به گروه ارتباطی دیگر استفاده می‌شود. همچنین این روش، قبل از آن که هر ارتباطی بین گروه‌ها اتفاق بیفتد، اطمینان ایجاد می‌کند. این فناوری در سطح برنامهٔ کاربردی قابل پیاده‌سازی است؛ مثلاً قبل از آغاز هر ارتباط مرورگر وب، تأیید می‌کند که آن گروه خاص قابل اطمینان می‌باشد.

۴. شبکه‌های مجازی خصوصی[۲۲]

فناوری شبکه‌های مجازی خصوصی، عبور و مرور شبکه را رمزگذاری می‌کند. بنابراین این فناوری برای تضمین صحت و امنیت داده‌ها، به رمزنگاری وابسته است. این شبکهٔ بسیار امن،

برای انتقال داده‌های حساس (از جمله اطلاعات تجاری الکترونیکی) از اینترنت به عنوان رسانهٔ انتقال بهره می‌گیرد. شبکه‌های مجازی خصوصی، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا داده‌ها قبل از آن که در شبکهٔ عمومی منتشر شوند، با رمزگذاری محافظت می‌شوند و این باعث می‌گردد که تنها افراد مجاز قادر به خواندن اطلاعات باشند. به علاوه این فناوری در سطح شبکه قابل پیاده‌سازی است، و از فناوری رمزگذاری بین دو میزبان شبکهٔ مجازی خصوصی، در مرحلهٔ ورود به شبکه و قبل از آن که داده‌ها به شبکهٔ عمومی فرستاده شود، استفاده می‌گردد.

۵. نرم‌افزارهای آسیب‌نما[۲۳]

نرم‌افزارهای آسیب‌نما برنامه‌هایی برای بررسی نقاط ضعف یک شبکه یا سیستم یا سایت هستند. بنابراین نرم‌افزارهای آسیب‌نما یک نمونهٔ خاص از نظام آشکارساز نفوذی از فناوری امنیت اطلاعات هستند (Bace، ۲۰۰۰، ص ۴-۳). همچنین این نرم‌افزارها به یک پویش فاصله‌مدار اشاره دارند؛ بدین معنا که میزبان‌های روی شبکه را در فواصل خاص و نه بطور پیوسته، پویش می‌کنند. به مجرد این که یک نرم‌افزار آسیب‌نما بررسی یک میزبان را خاتمه داد، داده‌ها در درون یک گزارش، نمونه‌برداری می‌شوند، که به یک «عکس فوری»[۲۴] شباهت دارد (مثل: cybercop scanner، cisco secure scanner، Net Recon).

نرم‌افزارهای آسیب‌نما، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا از آن‌ها برای کشف عامل‌های نفوذی قبل از آن که بتوانند با عملیات‌های خرابکارانه یا بدخواهانه از اطلاعات سوء استفاده کنند، استفاده می‌شود. نرم‌افزارهای آسیب‌نما در سطح میزبان قابل پیاده‌سازی هستند.

۶. پویشگرهای ضد ویروس[۲۵]

در دهه‌های گذشته ویروس‌های رایانه‌ای باعث تخریب عظیمی در اینترنت شده‌اند. ویروس رایانه‌ای یک قطعهٔ مخرب نرم‌افزاری است که توانایی تکثیر خودش را در سراسر اینترنت، با یک بار فعال‌شدن، دارد (McClure et al، ۲۰۰۲). پویشگرهای ضد ویروس، برنامه‌های نرم‌افزاری هستند که برای بررسی و حذف ویروس‌های رایانه‌ای، از حافظه یا دیسک‌ها طراحی شده‌اند. این برنامه‌ها از طریق جستجوی کدهای ویروس رایانه‌ای، آن‌ها را تشخیص می‌دهند. اگرچه برنامه‌های حفاظت از ویروس نمی‌توانند تمام ویروس‌ها را نابود کنند، اما اعمالی که این برنامه‌ها انجام می‌دهند عبارت‌اند از: ۱) ممانعت از فعالیت ویروس، ۲) حذف ویروس، ۳) تعمیر

آسیبی که ویروس عامل آن بوده است، و ۴) گرفتن ویروس در زمان کنترل و بعد از فعال‌شدن آن (Caelli, Longley, & Shain، ۱۹۹۴).

پویشگر ضدویروس، یک فناوری امنیت اطلاعات از نوع کنشگرایانه است. این پویشگرها در سطوح متنوع، و به طوری که در طبقه‌بندی بیان شده در سطح برنامه‌های کاربردی و در سطح میزبان، قابل پیاده‌سازی هستند.

۷. پروتکل‌های امنیتی[۲۶]

پروتکل‌های امنیتی مختلفی مانند «پروتکل امنیت اینترنت»[۲۷] و «کربروس»[۲۸] که در فناوری‌های امنیت اطلاعات طبقه‌بندی می‌شوند، وجود دارند. پروتکل‌ها فناوری‌هایی هستند که از یک روش استاندارد برای انتقال منظم داده‌ها بین رایانه‌ها استفاده می‌کنند، یا مجموعه‌ای از مقررات یا قراردادها هستند که تبادل اطلاعات را میان نظام‌های رایانه‌ای، کنترل و هدایت می‌کنند.

پروتکل‌های امنیتی، یک فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا برای حفاظت از اطلاعات حساس از یک پروتکل خاص امنیتی، قبل از آن که اطلاعات به وسیلهٔ خرابکاران به دست آید، استفاده می‌کنند. این فناوری در سطوح مختلف _ سطح برنامهٔ کاربردی و سطح شبکه- قابل پیاده‌سازی است. مثلاً پروتکل «کربروس»، پروتکل و سیستمی است که از آن در تعیین اعتبار سیستم‌های اشتراکی استفاده می‌شود. «کربروس» برای تعیین اعتبار میان فرآیندهای هوشمند (نظیر از خدمت‌گیرنده به خدمت‌دهنده، یا ایستگاه کاری یک کاربر به دیگر میزبان‌ها) مورد استفاده قرار می‌گیرد و این تعیین اعتبار در سطح برنامهٔ کاربردی و شبکه، قابل پیاده‌سازی است.

۸. سخت افزارهای امنیتی[۲۹]

سخت افزار امنیتی به ابزارهای فیزیکی که کاربرد امنیتی دارند، اشاره می‌کند؛ مانند معیارهای رمزگذاری سخت‌افزاری یا مسیریاب‌های سخت‌افزاری.

ابزارهای امنیت فیزیکی شامل امنیت سرورها، امنیت کابل‌ها، سیستم‌های هشداردهندهٔ امنیتی در زمان دسترسی غیرمجاز یا ذخیرهٔ فایل‌ها بعد از استفاده یا گرفتن فایل پشتیبان هستند.

این فناوری یک فناوری امنیت اطلاعات از نوع کنشگرایانه است، زیرا داده‌ها را قبل از آن که تهدید بالقوه‌ای بتواند تحقق یابد، حفاظت می‌کنند. مثلاً از رمزگذاری داده‌ها به‌منظور جلوگیری از اعمال خرابکارانه و جرح و تعدیل ابزار سخت‌افزاری استفاده می‌شود. این فناوری در

سطح شبکه قابل پیاده‌سازی است. مثلاً یک کلید سخت‌افزاری می‌تواند در درون درگاه میزبان برای تعیین اعتبار کاربر، قبل از آن که کاربر بتواند به میزبان متصل شود به کار رود، یا معیارهای رمزگذاری سخت‌افزار روی شبکه، یک راه حل مقاوم به دستکاری را فراهم آورد و در نتیجه ایمنی فیزیکی را تأمین نماید.

۹. جعبه‌های توسعهٔ نرم‌افزار امنیتی[۳۰]

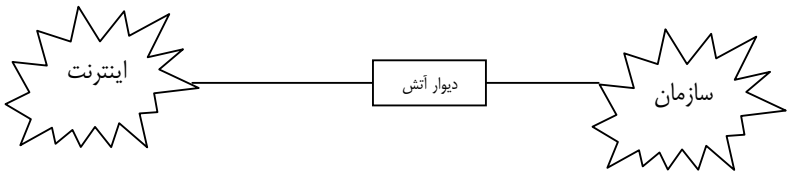
جعبه‌های توسعهٔ نرم‌افزار امنیتی، ابزارهای برنامه‌نویسی هستند که در ایجاد برنامه‌های امنیتی مورد استفاده قرار می‌گیرند. «Java security manager» و «Microsoft.net SDKs» نمونهٔ نرم‌افزارهایی هستند که در ساختن برنامه‌های کاربردی امنیتی (مانند برنامه‌های تعیین اعتبار مبتنی بر وب) به کار می‌روند. این جعبه‌ها شامل سازندهٔ صفحهٔ تصویری، یک ویراستار، یک مترجم، یک پیونددهنده، و امکانات دیگر هستند. جعبه‌های توسعه نرم‌افزار امنیتی، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا از آن‌ها در توسعهٔ نرم افزارهای متنوع برنامه‌های کاربردی امنیتی (که داده‌ها را قبل از آن که تهدید بالقوه تحقق یابد، حفاظت می‌کنند) استفاده می‌شوند. به‌علاوه این فناوری در سطوح متنوع- سطح برنامه‌های کاربردی، سطح میزبان، سطح شبکه- قابل پیاده‌سازی است.

ب. فناوری‌های امنیت اطلاعات واکنشی

۱. دیوار آتش[۳۱]

دیوار آتش در اینترنت یک ابزار نرم‌افزاری، خصوصاً روی یک رایانهٔ پیکربندی‌شده می‌باشد که به عنوان مانع، فیلتر یا گلوگاه بین یک سازمان داخلی یا شبکهٔ امین و شبکهٔ غیرامین یا اینترنت، نصب می‌شود (Tiwana، ۱۹۹۹). هدف از دیوار آتش جلوگیری از ارتباطات غیرمجاز در درون یا بیرون شبکهٔ داخلی سازمان یا میزبان است (Oppliger، ۱۹۹۸، ص. ۵۸). دیوار آتش به عنوان اولین خط دفاعی در تلاش برای راندن عامل مزاحم، مورد توجه قرار می‌گیرد. اگرچه فناوری رمزگذاری به حل بسیاری از مشکلات ایمنی کمک می‌کند، به یک فناوری ثانوی نیز نیاز داریم. فناوری معروف به دیوار آتش اینترنت کمک می‌کند تا رایانه‌ها و شبکه‌های یک سازمان را از ترافیک نامطلوب اینترنت محافظت کنید. این فناوری برای پرهیز از مشکلات ایجاد شده در اینترنت یا گسترش آن‌ها به رایانه‌های سازمان طراحی می‌گردد. دیوار آتش بین نظام‌های سازمان و اینترنت قرار می‌گیرد. شکل ۲ این مفهوم را نشان می‌دهد (امنیت شبکه...، ۱۳۸۳).

دیوار آتش یک فناوری امنیت اطلاعات از نوع واکنشی است و مهم‌ترین ابزار امنیتی مورد استفاده برای کنترل ارتباطات شبکه‌ای بین دو سازمان که به یکدیگر اعتماد ندارند، می‌باشد. با قراردادن یک دیوار آتش روی هر ارتباط خارجی شبکه، سازمان می‌تواند یک دایرهٔ امنیتی تعریف نماید که از ورود افراد خارجی به رایانه‌های سازمان جلوگیری می‌کند. علاوه بر آن، دیوار آتش می‌تواند مانع نفوذ افراد خارجی به منابع موجود در رایانه‌های سازمان و گسترش نامطلوب روی شبکهٔ سازمان شود. این فناوری در سطوح میزبان و در سطح شبکه قابل پیاده‌سازی است.



شکل ۲. تصویری از یک دیوار آتش برای حفاظت سازمان در مقابل نفوذ غیرمجاز به شبکه

۲. کنترل دسترسی[۳۲]

کنترل دسترسی به مجموعهٔ سیاست‌ها و اقدامات مربوط به دادن اجازه یا ندادن اجازه برای دسترسی یک کاربر خاص به منابع، یا محدودکردن دسترسی به منابع نظام‌های اطلاعاتی برای کاربران، برنامه‌ها، پردازه‌ها یا دیگر سیستم‌های مجاز اطلاق می‌شود. هدف از این فناوری، حصول اطمینان است از این که یک موضوع، حقوق کافی برای انجام عملیات‌های خاص روی سیستم را دارد (King et al.، ۲۰۰۱). این موضوع ممکن است کاربر، یک گروه از کاربران، یک خدمت، یا یک برنامهٔ کاربردی باشد. موضوعات در سطوح مختلف، امکان دسترسی به اشیای خاصی از یک سامانه را دارند. این شیء ممکن است یک فایل، راهنما، چاپگر یا یک فرایند باشد. کنترل دسترسی ابزاری است که امنیت شبکه را از طریق تأمین کاراکترهای شناسایی و کلمهٔ عبور تضمین می‌کند و فناوری امنیت اطلاعات از نوع واکنشی است، زیرا دسترسی به یک نظام را به محض این که یک درخواست دسترسی صورت گیرد، مجاز می‌شمارد یا غیرمجاز. این فناوری در سطوح متنوع- در سطح برنامهٔ کاربردی، در سطح میزبان و در سطح شبکه- قابل پیاده‌سازی است.

۳.کلمات عبور[۳۳]

کلمهٔ عبور، یک کلمه، عبارت یا حروف متوالی رمزی است که فرد برای به‌دست آوردن جواز دسترسی به اطلاعات (مثلاً یک فایل، برنامهٔ کاربردی یا نظام رایانه‌ای) باید وارد نماید

(Lexico Publishing Group، ۲۰۰۲). این کلمه برای شناسایی و برای اهداف امنیتی در یک نظام رایانه‌ای به کار می‌رود. به هر کاربر مجموعهٔ معینی از الفبا و عدد اختصاص داده می‌شود تا به تمام یا قسمت‌هایی از نظام رایانه‌ای دسترسی داشته باشد. کلمهٔ عبور، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا به‌منظور گرفتن مجوز و دسترسی به نظام، به محض این که یک فرد یا فرایند بخواهد به یک برنامهٔ کاربردی، میزبان یا شبکه متصل شود، به کار می‌رود. این فناوری در سطوح متنوع- در سطح برنامهٔ کاربردی، سطح میزبان، سطح شبکه- پیاده‌سازی می‌شود.

۴. زیست‌سنجی[۳۴]

زیست‌سنجی، علم و فناوری سنجش و تحلیل‌داده‌های زیستی است. در فناوری اطلاعات، زیست‌سنجی معمولاً به فناوری‌هایی برای سنجش و تحلیل ویژگی‌های بدن انسان (مانند اثر انگشت، قرنیه و شبکیهٔ چشم، الگوهای صدا، الگوهای چهره، و اندازه‌های دست) خصوصاً به‌منظور تعیین اعتبار اشاره دارد. یکی از ویژگی‌های ذاتی علم زیست‌سنجی این است که کاربر باید با یک الگوی مرجع مقایسه شود. اثر انگشت، چهره یا داده‌های زیست‌سنجی دیگر را می‌توان جایگزین کارت هوشمند نمود و کاربران می‌توانند هم از کارت هوشمند و هم از اثر انگشت یا چهرهٔ خود برای تعیین اعتبار در امور بازرگانی، بانک‌ها یا ارتباط تلفنی استفاده نمایند (Encyclopedia and learning center، ۲۰۰۴).

زیست‌سنجی فناوری امنیت اطلاعات از نوع واکنشی است، زیرا از آن می‌توان با استفاده از هندسهٔ بخشی از بدن کاربر برای گرفتن مجوز یا برای جلوگیری از دسترسی به نظام، به محض این که کاربر بخواهد به یک برنامهٔ کاربردی، میزبان یا شبکه متصل شود، استفاده نمود. به‌علاوه این فناوری در سطوح متنوع، با توجه به طبقه‌بندی بیان‌شده، قابل پیاده‌سازی است.

۵. نظام‌های آشکارساز نفوذی[۳۵]

نظام‌های آشکارساز نفوذی، یک نظام تدافعی است که فعالیت‌های خصمانه را در یک شبکه تشخیص می‌دهد. بنابراین نکتهٔ کلیدی در نظام‌های آشکارساز نفوذی، تشخیص و احتمالاً ممانعت از فعالیت‌هایی است که ممکن است امنیت شبکه را به خطر بیندازند. یکی از ویژگی‌های مهم این نظام‌ها، توانایی آن‌ها در تأمین نمایی از فعالیت‌های غیرعادی، و اعلام هشدار به مدیران نظام‌ها و مسدود نمودن ارتباط مشکوک است. نظام‌های آشکارساز نفوذی فرایندی برای شناسایی و تقابل با فعالیت‌های مشکوک است که منابع رایانه‌ای و شبکه‌ها را هدف قرار داده‌اند. علاوه بر این، ابزارها و تجهیزات این نظام می‌توانند بین تهاجم‌های داخلی از داخل سازمان (کارمندان یا مشتریان) و تهاجم‌های خارجی (حملاتی که توسط هکرها انجام می‌شود) تمایز قایل شوند (مثل

Snort IDS، ISS Real Secure، Cisco IDS) (سیستم‌های شناسایی...،۱۳۸۳). این فناوری، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا از آن برای کنترل میزبان‌های روی شبکه، آشکارسازی، ثبت گزارش، و متوقف ساختن هر نوع حمله و استفادهٔ غیرقانونی استفاده می‌شود. این فناوری در سطوح میزبان و شبکه، قابل پیاده‌سازی است.

۶. واقعه‌نگاری[۳۶]

واقعه‌نگاری به ثبت اعمال یا تراکنش‌های انجام‌شده توسط کاربر یا یک برنامه، تولید سابقه، و ثبت نظام‌مند رویدادهای مشخص به ترتیب وقوع آن‌ها برای فراهم‌کردن امکان تعقیب و پیگیری داده‌ها در تحلیل‌های آتی اطلاق می‌شود. واقعه‌نگاری، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا به علت‌جویی حوادث امنیتی بعد از وقوع می‌پردازد. این فناوری در سطوح برنامهٔ کاربردی، میزبان و شبکه قابل پیاده‌سازی است.

۷. دسترسی از راه دور[۳۷]

«دسترسی از راه دور» به دسترسی به یک سیستم یا برنامه، بدون نیاز به حضور فیزیکی در محل توجه دارد. با این حال معمولاً دسترسی به خدمات از راه دور، کنترل‌شده نیستند، زیرا ممکن است دسترسی به یک خدمت از راه دور به طور ناشناس صورت بگیرد که در این مورد دسترسی به خدمت، خطر جعل هویت را به همراه دارد. در این زمینه با توجه به شرایط و امکانات، باید ایمن‌ترین پروتکل‌ها و فناوری‌ها را به خدمت گرفت. مثلاً تعدادی از نظام‌ها ممکن است به غلط برای مجوزگرفتن اتصال، به صورت ناشناس با یک پیش‌فرض پیکربندی کنند، در حالیکه اتصال ناشناس بر طبق خط‌مشی امنیتی سازمان نباید اجازه یابد که وارد نظام شود. دسترسی از راه دور، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا یک فرد یا فرایند برای اتصال از راه دور، قادر به دستیابی بر طبق امتیازات دسترسی می‌باشد. این فناوری در سطح میزبان قابل پیاده‌سازی می‌باشد.

نتیجه‌گیری

اگر چه اغلب سازمان‌ها تمایل به داشتن شبکه‌های ایمن دارند، ارائهٔ تعریفی واحد از امنیت که همهٔ نیازهای شبکه را تأمین نماید ممکن نیست. در عوض هر سازمان باید ارزش اطلاعات خود را ارزیابی کند و سپس یک خط‌مشی امنیتی برای مواردی که باید مورد حفاظت قرار گیرند مشخص نماید. مثلاً روش‌های تعیین اعتبار زیست‌سنجی از نظر قدرت و در دسترس بودن، در حال بهبود هستند، اما در حال حاضر با نوعی تردید با آن‌ها برخورد می‌شود و این تردید ناشی از هزینه‌های نسبتاً بالا و مشکلات مرتبط با دغدغه‌های حفظ حریم خصوصی

می‌باشد. البته نظراتی وجود دارند که به موجب آن‌ها می‌توان از ترکیب فناوری‌های متنوع امنیتی، برای تشکیل فناوری‌های امنیتی قوی در زمینهٔ امنیت اطلاعات استفاده نمود. مثلاً در آیندهٔ نزدیک با ترکیب دیوار آتش، نظام‌های آشکارساز نفوذی و فناوری‌های پویشگرهای ضد ویروس، به تشکیل یک فناوری نیرومند در زمینهٔ امنیت اطلاعات خواهیم رسید.

برای یک سازمان، شناختن فناوری‌های امنیت اطلاعات قابل دسترس، مهم است، تا از آن برای تدوین خط‌مشی‌های امنیتی با توجه به نوع و حساسیت اطلاعات سازمان خود، استفاده نمایند. به علاوه، ارائهٔ این طبقه‌بندی از فناوری‌ها، زمینه‌ساز پژوهش جدیدی خواهد بود.

منابع

Bace, R. G. (2000). *Intrusion detection*. Indianapolis, IN: Macmillan Technical Publishing.

Caelli, W., Longley, D., & Shain, M. (1994). *Information security handbook*. England: MacMillan.

Comer, D. E. (1999). *Computer networks and Intranets: with Internet Applications*. New York: Prentice-Hall.

Conway, S., & Sliger, C. (2002). building taxonomies. In *Unlocking knowledge assets* (pp. 105-124). Washington: Microsoft press.

Information Security & Prevention of Computer Related Crime (INFOSEC). (2002). *What is information security?* Retrieved June 24, 2004, from http://www.infosec.gov.hk/english/general/infosec/what-infosec.htm

King, C. M., Dalton, C. E., & Osmanoglu, T. E. (2001). *Security Architecture: Design, Deployment and Operations*. London: McGraw-Hill.

Lexico Publishing Group, LLC. (2002). *Dictionary.com*. Retrieved June 24, 2004, from http://www.dictionary.com

Maiwald, E., & Sieglein, W. (2002). *Security planning & disaster recovery*. Osborne: McGraw-Hill.

McClure, S., Scambray, J., & Kurtz, G. (2002). *Hacking exposed. (3rd ed.)*. London: McGraw-Hill.

Oppliger, R. (1998). *Internet & Intranet security*. Boston: Artech House.

Tiwana, A (1999). *Web Security*. Boston: Digital press.

Venter, H. S., & Eloff, J. H. P. (2003). A taxonomy for information security technologies [Electronic version in Elsevier Database]. *Computers & Security*, 22(4), 299-307.

Encyclopedia and learning center. (2004). *TechTarget Network: What is.com*. Retrieved June 24, 2004, from http://whatis.techarget.com/definitionscategory/.

آشنایی با رمزنگاری cryptography. (۱۳۸۳). *بزرگراه رایانه*. ۷(۶۶)، ۴۲-۳۹.

مدیریت شبکه شرکت سخا روش. ۱۳۸۲. *استراتژی حفاظت از اطلاعات در شبکه‌های کامپیوتری (بخش اول و دوم)*. دسترسی در ۱۷ خرداد ۱۳۸۳، از سایت http://www.srco.ir

امنیت شبکه: شبکه‌های ایمن و خط مشی های امنیتی. (۱۳۸۳). *بزرگراه رایانه*. ۷(۶۶)، ۱۲۵-۱۲۴.

سیستم‌های شناسایی تجاوز یا IDS. (۱۳۸۳). *بزرگراه رایانه*. ۷(۶۶)، ۳۵-۳۱.

عبداللهی ازگمی، محمد. (۱۳۷۵). *طراحی و پیاده‌سازی سرویس‌های امن برای شبکه‌های کامپیوتری*. پایان‌نامه کارشناسی‌ارشد. دانشگاه صنعتی شریف.

هاشمیان، وحید. (۱۳۷۹). روش های رمزنگاری اطلاعات. *رایانه شریف*. ۵(۸)،۲۱-۱۸.

پی‌نوشت

[1]. Information security
[2]. INFOSEC
[3]. Proactive
[4]. Reactive
[5]. Network Level
[6]. Host Level
[7]. Application Level
[8]. Cryptography
[9]. plaintext or cleartext
[10]. encryption
[11]. encipher

[*] براساس زبانشناسی تفاوت بین Encrypt و Encipher در قالب عملکردی است که انجام می‌دهند، که در اولی عمل مدفون‌سازی اطلاعات و در دومی فراگردش اطلاعاتی به ترتیبی خاص صورت می‌گیرد. اما در حوزهٔ حفاظت اطلاعات به هر دو، رمز می گویند. مثلاً در مورد ماشین‌های Enigma عمل رمزگذاری به صورت خودکار، و عمل رمزگشایی توسط کلید رمز صورت می‌گرفت.

[12]. ciphertext
[13]. decryption
[14]. decipher
[15]. cryptanalysis
[16]. cryptographer
[17]. cryptanalyst
[18]. cryptology
[19]. digital signatures
[20]. Digital certificates
[21]. trusted third parties

[**] برای مثال می‌توان به تعدادی از مؤسسات تجاری و فروشندگانی که ارائه‌دهندگان خدمات و صدور گواهی‌های رقومی هستند اشاره نمود:

www.verisign.com
www.inc-it-now.com
www.searchthis.ws
www.open.com.au/catool
www.arx.com
www.geocerts.com
www.verisign.com
www.inc-it-now.com
www.searchthis.ws
www.open.com.au/catool

www.arx.com
www.geocerts.com
[22]. virtual private networks
[23]. vulnerability scanners
[24]. snapshot
[25]. Anti- virus scanner
[26]. security protocols
[27]. Internet Protocol Security (IPsec)
[28]. kerberos
[29]. security hardware
[30]. security software development kits (SDKs)
[31]. firewalls
[32]. access control
[33]. passwords
[34]. biometrics
[35]. intrusion detection systems (IDS)
[36]. logging
[37]. remote accessing