استفاده از منابعی که به اشتراک گذاشته شده‌اند، از مهم‌ترین اهداف یک نظام امنیتی در شبکه است. با گسترش شبکه‌های رایانه‌ای به‌ویژه اینترنت، نگرش به امنیت اطلاعات و دیگر منابع به اشتراک گذاشته‌شده، وارد مرحله جدیدی شده 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 کند.

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 نظام‌های اطلاعاتی در برابر حمله‌ها است؛ بدین منظور از سرویس‌های امنیتی پرشماری استفاده می‌شود. سرویس‌های انتخابی باید پتانسیل لازم در خصوص ایجاد یک نظام حفاظتی مناسب، تشخیص به‌هنگام حمله‌ها و واکنش باسرعت را داشته باشند. بنابراین می‌توان محور راهبردی برگزیده را بر سه مؤلفه استوار کرد:

۱. حفاظت
۲. تشخیص
۳. واکنش

حفاظت مطمئن، تشخیص به‌هنگام و واکنش مناسب، ازجمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت کرد. خوشبختانه پژوهش‌های زیادی در زمینهٔ امنیت رایانه و شبکه‌ها در مورد فناوری‌های امنیتی پیشگیرانه (کُنشی) و نیز رویارویی با دشواری‌های امنیتی (واکنشی) انجام گرفته است. نوشته حاضر درصدد بیان، شماری از فناوری‌های موجود دربارهٔ امنیت اطلاعات با یک دیدگاه طبقه‌بندی است.

۹ـ۶ طبقه‌بندی فناوری‌های امنیت اطلاعات از نگاه مؤسسهٔ INFOSE

طبقه‌بندی ارائه‌شده در نوشته حاضر از فناوری‌های امنیت اطلاعات، در وهلهٔ اول براساس دو ویژگی پایه‌گذاری شده است.

۹ـ۶ـ۱ براساس مرحلهٔ ویژه‌ای از زمان

بدین معنا که در زمان تعامل فناوری با اطلاعات، واکنش لازم در برابر یک دشواری امنیتی می‌تواند کنشی (Proactive) یا واکنشی (Reactive) باشد.

غرض از «کنشگرایانه»، انجام فرایندهای پیشگیرانه پیش از وقوع یک دشواری ویژهٔ امنیتی است. در چنین مواردی به موضوع‌هایی اشاره می‌شود که ما را در پیشگیری از وقوع یک دشواری کمک خواهد کرد (چه کار باید انجام دهیم تا...؟).

غرض از «واکنشی» انجام دادن واکنش لازم پس از وقوع یک دشواری ویژهٔ امنیتی است. در چنین مواردی به موضوع‌هایی اشاره می‌شود که ما را در مقابله با یک دشواری پس از وقوع آن، کمک خواهند کرد (اکنون که... چه کار باید انجام بدهیم؟).

۹ـ۶ـ۲ براساس سطوح پیاده‌سازی نظام‌های امنیتی در یک محیط رایانه‌ای

فناوری امنیت اطلاعات را، خواه از نوع کنشی باشد یا واکنشی، می‌توان در سه سطح ـسطح شبکه (Network Level)، سطح میزبان (Host Level) و سطح برنامه کاربردی (Application Level)ـ پیاده‌سازی کرد (همان). بدین منظور می‌توان نظام امنیتی را در سطح شبکه و خدمات ارائه‌شدهٔ آن، در سطح برنامهٔ کاربردی ویژه، یا در محیطی که شرایط لازم برای اجرای یک برنامه را فراهم می‌کند (سطح میزبان) پیاده کرد.

فناوری‌های امنیت اطلاعات کنشگرایانه

رمزنگاری (Cryptography)

به بیان ساده، رمزنگاری به معنای «نوشتن پنهان» و علم حفاظت، اعتمادپذیری و تأمین تمامیت داده‌ها است. این علم شامل اعمال رمزگذاری، رمزگشایی و تحلیل رمز است. در اصطلاح‌های رمزنگاری، پیام را متن آشکار (plaintext or cleartext) می‌نامند. کدگذاری مضامین را به شیوه‌ای که آنها را از دید بیگانگان پنهان کند، (encryption) یا سِرگذاری (encipher) می‌نامند. پیام رمزگذاری‌شده را متن رمزی (ciphertext) و فرایند بازیابی متن آشکار از متن رمزی را رمزگشایی(decryption) یا سِرّگشایی (decipher) می‌نامند.

الگوریتم‌هایی که امروزه در رمزگذاری و رمزگشایی داده‌ها به کار می‌روند از دو روش بنیادی استفاده می‌کنند: 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 به‌سادگی از کلید رمزگذاری استخراج می‌شود. مانند:

DES (Data Encryption Standard), CCEP (The Commercial Comsec Endoremment Program), IDEA (International Data Encryption Algoritm)

در حالی که الگوریتم‌های بی‌تقارن 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 (مانند RSA).

تجزیه‌وتحلیل رمز (cryptanalysis)، هنر شکستن رمزها و به عبارت دیگر، بازیابی متن آشکار بدون داشتن کلید مناسب است؛ افرادی که فرایند رمزنگاری را انجام می‌دهند، رمزنگار (cryptographer) نامیده می‌شوند و افرادی که در تجزیه‌وتحلیل رمز فعالیت دارند رمزکاو (cryptanalyst) هستند.

رمزنگاری با همهٔ جنبه‌های پیام‌رسانی امن، تعیین اعتبار، امضاهای رقومی، پول الکترونیک و نرم‌افزارهای کاربردی دیگر ارتباط دارد. رمزشناسی (cryptology) شاخه‌ای از ریاضیات است که پایه‌های ریاضی مورد استفاده در شیوه‌های رمزنگاری را مطالعه می‌کند.

رمزنگاری، یک فناوری امنیت اطلاعات از نوع کنشگرایانه است، زیرا اطلاعات را پیش از آنکه یک تهدید بالقوه بتواند اعمال خرابکارانه انجام دهد، از راه رمزگذاری داده‌ها ایمن می‌کنند. به علاوه، رمزنگاری در سطوح متنوع، به گونه‌ای که در طبقه‌بندی بیان شد، در سطوح برنامه‌های کاربردی و در سطوح شبکهٔ قابل پیاده‌سازی است.

امضاهای دیجیتال یا رقومی (Digital Signatures)

امضاهای رقومی، معادل «امضای دست‌نوشت» و مبتنی بر همان هدف هستند: نشانه منحصربه‌فرد یک شخص، با یک بدنه متنی. 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 به گونهٔ معمول به یک پیام پست الکترونیک یا یک گواهی‌نامه پیوست می‌شود تا هویت واقعی تولیدکننده پیام را تأیید کند.

امضای رقومی یک فناوری امنیت اطلاعات از نوع کنشگرایانه است، زیرا پیش از وقوع هر تهدیدی، می‌توان با استفاده از آن فرستندهٔ اصلی پیام و صاحب امضا را شناسایی کرد. افزون بر این، فناوری در سطح یک برنامه کاربردی قابل پیاده‌سازی است. در این سطح، امضای رقومی در یک برنامه کاربردی ویژه و پیش از آنکه به یک گیرنده ویژه فرستاده شود، ایجاد می‌شود.

گواهی‌های رقومی (Digital certificates)

گواهی‌های رقومی به حل مسئلهٔ «اطمینان» در اینترنت کمک می‌کنند. گواهی‌های رقومی متعلق به «شخص ثالث مورد اعتماد» (Trusted Third Parties) هستند و همچنین به «مراجع صدور گواهی» اشاره دارند. مراجع صدور گواهی (Certificate Authorities)، مؤسسه‌های تجاری هستند که هویت افراد یا سازمان‌ها را در وب تأیید و تأییدیه‌هایی مبنی بر درستی این هویت‌ها صادر می‌کنند.

برای به‌دست آوردن یک گواهی، ممکن است از فرد خواسته شود که یک کارت شناسایی (مانند گواهینامهٔ رانندگی) را نشان دهد. بنابراین گواهی‌های رقومی، یک شبکه امن در میان کاربران وب و مکانی برای تأیید صحت و جامعیت یک فایل یا برنامه الکترونیک ایجاد می‌کنند. این گواهی‌ها دارای نام فرد، شماره سریال، تاریخ انقضا، یک نسخه از گواهی نگاهدارنده کلید عمومی (که برای رمزگذاری پیام‌ها و امضاهای رقومی به کار می‌رود) هستند.

گواهی‌های رقومی، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا از این فناوری برای پخش کلید عمومی از یک گروه ارتباطی به گروه ارتباطی دیگر استفاده می‌شود. همچنین این روش، پیش از آنکه هر ارتباطی میان گروه‌ها اتفاق بیفتد، اطمینان ایجاد می‌کند. این فناوری در سطح برنامه کاربردی قابل پیاده‌سازی است؛ برای نمونه پیش از آغاز هر ارتباط مرورگر وب، تأیید می‌کند که آن گروه ویژه قابل اطمینان است.

شبکه‌های مجازی خصوصی (virtual private networks)

فناوری شبکه‌های مجازی خصوصی، گذر و مرور شبکه را رمزگذاری می‌کند. بنابراین این فناوری برای تضمین درستی و امنیت داده‌ها، به رمزنگاری وابسته است. این شبکه بسیار امن، برای انتقال داده‌های حساس (ازجمله اطلاعات تجاری الکترونیک) از اینترنت به عنوان رسانه انتقال بهره می‌گیرد. شبکه‌های مجازی خصوصی، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا داده‌ها پیش از آنکه در شبکهٔ عمومی منتشر شوند، با رمزگذاری محافظت می‌شوند و این سبب می‌شود که تنها افراد مجاز توانا به خواندن اطلاعات باشند.

افزون بر این، این فناوری در سطح شبکه قابل پیاده‌سازی است و از فناوری رمزگذاری میان دو میزبان شبکه مجازی خصوصی، در مرحله ورود به شبکه و پیش از آنکه داده‌ها به شبکهٔ عمومی فرستاده شود، استفاده می‌شود.

نرم‌افزارهای اسکنر آسیب‌پذیری (vulnerability scanners)

نرم‌افزارهای آسیب‌نما برنامه‌هایی برای بررسی نقاط ضعف یک شبکه یا سامانه یا سایت هستند. بنابراین نرم‌افزارهای آسیب‌نما یک نمونه ویژه از نظام آشکارساز نفوذی از فناوری امنیت اطلاعات هستند.

همچنین این نرم‌افزارها به یک پویش فاصله‌مدار اشاره دارند؛ بدین معنا که میزبان‌های روی شبکه را در فاصله‌های ویژه و نه به گونهٔ پیوسته، پویش می‌کنند. به مجرد اینکه یک نرم‌افزار آسیب‌نما بررسی یک میزبان را پایان داد، داده‌ها در درون یک گزارش، نمونه‌برداری می‌شوند، که به یک عکس فوری (snapshot) شباهت دارد (مانند: cybercop scanner، cisco secure scanner و Net Recon).

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

پویشگرهای پاد (ضد) ویروس(Anti- virus)

در دهه‌های گذشته ویروس‌های رایانه‌ای سبب تخریب بزرگی در اینترنت شده‌اند. ویروس رایانه‌ای یک قطعه مخرب نرم‌افزاری است که توانایی تکثیر خودش را در سراسر اینترنت، با یک بار فعال شدن، دارد. ضد ویروس، برنامه‌های نرم‌افزاری هستند که برای بررسی و حذف ویروس‌های رایانه‌ای، از حافظه یا دیسک‌ها طراحی شده‌اند. این برنامه‌ها از راه جستجوی کدهای ویروس رایانه‌ای، آنها را تشخیص می‌دهند. اگرچه برنامه‌های حفاظت از ویروس نمی‌توانند همهٔ ویروس‌ها را نابود کنند، اما کارهایی که این برنامه‌ها انجام می‌دهند عبارت‌اند از:

۱. ممانعت از فعالیت ویروس؛
۲. حذف ویروس؛
۳. تعمیر آسیبی که ویروس عامل آن بوده است؛
۴. گرفتن ویروس در زمان کنترل و پس از فعال شدن آن.

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

پروتکل‌های امنیتی (security protocols)

پروتکل‌های امنیتی گوناگونی مانند «پروتکل امنیت اینترنت» (Ipsec)[1] و کربروس (161erberos) که در فناوری‌های امنیت اطلاعات طبقه‌بندی می‌شوند، وجود دارند. پروتکل‌ها، فناوری‌هایی هستند که از یک روش استاندارد برای انتقال منظم داده‌ها میان 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 ویژهٔ امنیتی، پیش از آن که اطلاعات توسط خرابکاران به دست آید، استفاده می‌کنند. این فناوری در سطوح گوناگون ـسطح برنامهٔ کاربردی و سطح شبکهـ قابل پیاده‌سازی است. برای نمونه پروتکل «کربروس»، پروتکل و سامانه‌ای است که از آن در تعیین اعتبار سامانه‌های اشتراکی استفاده می‌شود. «کربروس» برای تعیین اعتبار میان فرایندهای هوشمند (مانند از خدمت‌گیرنده به خدمت‌دهنده، یا ایستگاه کاری یک کاربر به دیگر میزبان‌ها) مورد استفاده قرار می‌گیرد و این تعیین اعتبار در سطح برنامه کاربردی و شبکه، قابل پیاده‌سازی است.

سخت افزارهای امنیتی(Security hardware)

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، سامانه‌های هشداردهنده امنیتی در زمان دسترسی غیرمجاز یا ذخیرهٔ فایل‌ها پس از استفاده یا گرفتن فایل پشتیبان هستند.

این فناوری یک فناوری امنیت اطلاعات از نوع کنشگرایانه است، زیرا داده‌ها را پیش از آنکه تهدید بالقوه‌ای بتواند تحقق یابد، حفاظت می‌کنند. برای نمونه از رمزگذاری داده‌ها به منظور جلوگیری از فرایندهای خرابکارانه و جرح و تعدیل ابزار سخت‌افزاری استفاده می‌شود. این فناوری در سطح شبکه قابل پیاده‌سازی است. برای نمونه یک کلید سخت‌افزاری می‌تواند در درون درگاه میزبان برای تعیین اعتبار کاربر، پیش از آنکه کاربر بتواند به میزبان متصل شود به کار رود، یا معیارهای رمزگذاری

1. Internal Protocol Security

سخت‌افزار روی شبکه، یک راه حل مقاوم به دستکاری را فراهم آورد و در نتیجه ایمنی فیزیکی را تأمین کند.

کیت‌های توسعهٔ نرم‌افزار امنیتی(security software development kits (SDKs))

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

فناوری‌های امنیت اطلاعات واکنشی

دیوار آتش (firewalls)

دیوار آتش در اینترنت یک ابزار نرم‌افزاری، به‌ویژه روی یک رایانه پیکربندی‌شده است که به عنوان مانع، فیلتر یا گلوگاه میان یک سازمان درونی یا شبکهٔ امین و شبکهٔ غیرامین یا اینترنت، نصب می‌شود. هدف از دیوار آتش جلوگیری از ارتباطات غیرمجاز در درون یا بیرون شبکه درونی سازمان یا میزبان است. دیوار آتش به عنوان نخستین خط دفاعی در تلاش برای راندن عامل مزاحم، مورد توجه قرار می‌گیرد. اگرچه فناوری رمزگذاری به حل بسیاری از دشواری‌های 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 کند. این فناوری برای پرهیز از دشواری‌های ایجاد شده در اینترنت یا گسترش آنها به رایانه‌های سازمان طراحی می‌شود. دیوار آتش میان نظام‌های سازمان و اینترنت قرار می‌گیرد.

دیوار آتش یک فناوری امنیت اطلاعات از نوع واکنشی است و مهم‌ترین ابزار امنیتی مورد استفاده برای کنترل ارتباطات شبکه‌ای میان دو سازمان است که به یکدیگر

اعتماد ندارند. با قرار دادن یک دیوار آتش روی هر ارتباط خارجی شبکه، سازمان می‌تواند یک دایره امنیتی تعریف کند که از ورود افراد خارجی به رایانه‌های سازمان جلوگیری می‌کند. افزون بر آن، دیوار آتش می‌تواند مانع نفوذ افراد خارجی به منابع موجود در رایانه‌های سازمان و گسترش نامطلوب روی شبکه سازمان شود. این فناوری در سطوح میزبان و در سطح شبکه قابل پیاده‌سازی است.

کنترل دسترسی(access control)

کنترل دسترسی به مجموعه سیاست‌ها و اقدام‌های مربوط به اجازه دادن یا ندادن برای دسترسی یک کاربر ویژه به منابع، یا محدود کردن دسترسی به منابع نظام‌های اطلاعاتی برای کاربران، برنامه‌ها، پردازه‌ها یا دیگر سامانه‌های مجاز گفته می‌شود. هدف از این فناوری، حصول اطمینان است از اینکه یک موضوع، حقوق کافی برای انجام فرایندهای ویژه روی سامانه را دارد. این موضوع ممکن است کاربر، یک گروه از کاربران، یک خدمت، یا یک برنامه کاربردی باشد. موضوع‌ها در سطوح گوناگون، امکان دسترسی به اشیای ویژه‌ای 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 راه تأمین کاراکترهای شناسایی و واژهٔ گذر تضمین می‌کند و فناوری امنیت اطلاعات از نوع واکنشی است، زیرا دسترسی به یک نظام را به محض اینکه یک درخواست دسترسی صورت گیرد، مجاز یا غیرمجاز می‌شمارد. این فناوری در سطوح متنوع- در سطح برنامه کاربردی، در سطح میزبان و در سطح شبکه- قابل پیاده‌سازی است.

واژه‌های گذر (passwords)

واژهٔ گذر، یک کلمه، عبارت یا حرف‌های متوالی رمزی است که فرد برای به‌دست آوردن جواز دسترسی به اطلاعات (برای نمونه یک فایل، برنامه کاربردی یا نظام رایانه‌ای) باید وارد کند. این کلمه برای شناسایی و برای اهداف امنیتی در یک نظام رایانه‌ای به کار می‌رود. به هر کاربر مجموعه معینی از الفبا و عدد اختصاص داده می‌شود تا به همه یا بخش‌هایی از نظام رایانه‌ای دسترسی داشته باشد. واژهٔ گذر، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا به منظور گرفتن مجوز و دسترسی به نظام، به محض اینکه یک فرد یا فرایند بخواهد به یک برنامه کاربردی، میزبان یا شبکه متصل شود، به کار می‌رود. این فناوری در سطوح متنوع- در سطح برنامه کاربردی، سطح میزبان، سطح شبکه- پیاده‌سازی می‌شود.

زیست‌سنجی (biometric)

زیست‌سنجی، علم و فناوری سنجش و تحلیل داده‌های زیستی است. در فناوری اطلاعات، زیست‌سنجی به گونهٔ معمول به فناوری‌هایی برای سنجش و تحلیل ویژگی‌های بدن انسان (مانند اثر انگشت، قرنیه و شبکیه چشم، الگوهای صدا، الگوهای چهره و اندازه‌های دست) به‌ویژه به منظور 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 کرد و کاربران می‌توانند هم از کارت هوشمند و هم از اثر انگشت یا چهره خود برای تعیین اعتبار در امور بازرگانی، بانک‌ها یا ارتباط تلفنی استفاده کنند.

زیست‌سنجی فناوری امنیت اطلاعات از نوع واکنشی است، زیرا از آن می‌توان با استفاده از هندسه بخشی از بدن کاربر برای گرفتن مجوز یا برای جلوگیری از دسترسی به نظام، به محض اینکه کاربر بخواهد به یک برنامه کاربردی، میزبان یا شبکه متصل شود، استفاده کرد. افزون بر این، این فناوری در سطوح متنوع، با توجه به طبقه‌بندی بیان‌شده، قابل پیاده‌سازی است.

واقعه‌نگاری(logging)

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

دسترسی از راه دور (remote accessing)

دسترسی از راه دور به دسترسی به یک سامانه یا برنامه، بدون نیاز به حضور فیزیکی در محل توجه دارد. با این حال به گونهٔ معمول دسترسی به خدمات از راه دور، کنترل‌شده نیستند، زیرا ممکن است دسترسی به یک خدمت از راه دور به گونهٔ ناشناس انجام 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. برای نمونه شماری از نظام‌ها ممکن است به غلط برای مجوز گرفتن

اتصال، به صورت ناشناس با یک پیش‌فرض پیکربندی کنند، در حالی که 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، توانا به دستیابی بر طبق امتیازهای دسترسی است. این فناوری در سطح میزبان قابل پیاده‌سازی است.

۹ـ۷ ضرورت توجه به امنیت اطلاعات

استراتژی «دفاع در عمق» یک چارچوب امنیتی مناسب برای حفاظت و نگهداری ایمن زیرساخت فناوری اطلاعات یک سازمان است. در این مدل، زیرساخت فناوری اطلاعات یک سازمان به عنوان مجموعه‌ای از لایه‌های مرتبط به هم در نظر گرفته شده و به منظور حفاظت و ایمن‌سازی هر لایه از سازوکارها و روش‌های حفاظتی ویژه‌ای استفاده می‌شود.

۹ـ۷ـ۱ بررسی لایه سیاست‌ها، رویه‌ها و اطلاع رسانی

در نخستین لایهٔ مدل امنیتی «دفاع در عمق»، سیاست‌ها و رویه‌های امنیتی تعریف و همهٔ کاربران صرف‌نظر از موقعیت شغلی خود باید با آنان آشنا شوند. با توجه به جایگاه برجسته این لایه و تأثیر آن بر عملکرد دیگر لایه‌ها، باید با حوصله و دقت بیشتری این لایه بررسی و پیش از هر چیز سیاست‌های امنیتی در یک سازمان تعریف شود. در زمان تعریف سیاست‌های امنیتی باید به موارد زیر توجه کرد:

- تعریف عنصرهای زیادی مانند: استفاده پذیرفتنی از منابع موجود، دستیابی از راه دور، حفاظت اطلاعات، تهیه نسخه‌های پشتیبان از اطلاعات، امنیت پیرامون شبکه، ایمن‌سازی و ایمن نگهداشتن دستگاه‌ها و رایانه‌های میزبان و...
- یک سیاست امنیتی مناسب باید قادر به برقراری ارتباط مناسب با کاربران بوده و با ارائهٔ یک ساختار اساسی آنان را در زمان بروز یک رویداد و یا دشواری امنیتی کمک کند.
- تدوین رویه‌های مناسب به منظور برخورد با یک دشواری امنیتی. در این رویه‌ها باید محدودهٔ مسئولیت‌ها به دقت مشخص شود.
- تعیین دقیق نوع و مکان ذخیره‌سازی اطلاعات مهمی که برای یک سازمان ارزش زیستی دارند.

- مشخص کردن اقدام‌هایی که باید پس از بروز یک دشواری امنیتی انجام شود.
- سیاست‌های امنیتی به عنوان اصول فرایندی رویه‌های امنیتی مطرح هستند. بنابراین، باید به اندازهٔ کافی عمومی باشند تا بتوان آنان را با استفاده از فناوری‌ها و پلت فرم‌های موجود پیاده‌سازی کرد.
- سیاست‌های امنیتی باید اطلاعات لازم برای کارشناسان حرفه‌ای فناوری اطلاعات در خصوص شیوهٔ پیاده‌سازی کنترل‌های امنیتی به منظور پشتیبانی از سیاست‌های امنیتی را ارائه کنند.
- محدودهٔ سیاست‌های امنیتی برای یک سازمان، به اندازه و پیچیدگی‌های آن بستگی دارد.
- رویه‌های امنیتی شیوهٔ انجام فرایندی ویژه بر روی دستگاه‌هائی بخصوص مانند شیوهٔ پیکربندی یک سرویس‌دهندهٔ وب جدید را مشخص می‌کنند.
- اطلاع‌رسانی یک عنصر امنیتی است که بیشتر به فراموشی سپرده می‌شود. بیشتر کاربران فعالیت‌های روزمره خود را با نادیده گرفتن مسائل امنیتی انجام می‌دهند. بدون وجود آموزش‌های لازم، بیشتر کارکنان در ابتدا می‌کوشند کار خود را به گونه‌ای که آسان‌تر است، انجام دهند و در مرحلهٔ بعد به امنیت انجام کار فکر کنند. تدوین سیاست‌ها و رویه‌های امنیتی بدون اینکه کاربران نسبت به آنان آگاهی داشته باشند، نتیجه‌های مثبت و مشهودی را در زمینهٔ ایجاد یک سامانهٔ ایمن به دنبال نخواهد داشت.

۹ـ۷ـ۲ تهدیدهای لایهٔ سیاست‌ها، رویه‌ها و اطلاع‌رسانی

- بسیاری از کاربران قوانین امنیتی را به عنوان یک ضرورت در نظر نگرفته و از آنان تبعیت نمی‌کنند. این گونه کاربران متأسفانه نسبت به مسائل امنیتی شناخت مناسبی نداشته و از تبعات زیان‌بار آن آگاهی ندارند. بدیهی است زمانی که کاربران از اهمیت امنیت اطلاعات شناخت مناسبی نداشته باشند، نمی‌توانند از رمزهای گذر خود، حفاظت کرده و یا از اطلاعات سازمان خود محافظت کنند (مانند پیکربندی سخت‌افزارها و یا نرم‌افزارها با رعایت مسئله‌های امنیتی).

تعداد زیادی از حمله‌ها مبتنی بر «مهندسی اجتماعی» است. این نوع حمله‌ها از مزایای ضعف امنیت و رعایت نکردن نکات ایمنی در زندگی روزمره ما استفاده

می‌کنند. یک مهاجم می‌تواند زمان زیادی را در محل کار و یا زمان‌های فراغت خود صرف کند تا بتواند اعتماد یک کاربر را جلب کند. زمانی که یک مهاجم پرسش‌هایی را مطرح و پاسخ آنان را دریافت می‌کند، با قرار دادن اطلاعات بالا در کنار یکدیگر و تجزیه آنان می‌تواند به اطلاعات اررشمندی دست یابد که از آنان به منظور برنامه‌ریزی حمله‌ها استفاده کند.

دو نمونه از حمله‌های مبتنی بر مهندسی اجتماعی

یک مهاجم با مسئول فنی یک مرکز ارائه‌دهندهٔ خدمات اینترنت (ISP) تماس می‌گیرد و در مدت زمان مکالمه تلفنی با وی به این نکته اشاره می‌کند که دارای یک خودرو است که قصد دارد آن را با بهای مناسبی بفروشد. مسئول فنی ISP برای خرید خودرو اظهار تمایل می‌کند. مهاجم به وی پیشنهاد می‌کند که یک mail را که دارای تصویر خودرو است برای وی ارسال خواهد کرد. مهاجم، در برابر ارسال تصویر خودرو (به عنوان یک فایل پیوست) یک برنامه مخرب از نوع backdoor را به همراه email برای مسئول فنی ISP ارسال می‌کند. زمانی که مسئول فنی ISP نامه را دریافت و فایل پیوست را فعال می‌کند، برنامه مخرب ارسالی اجرا و یک حفرهٔ امنیتی را در بطن شبکه ISP ایجاد می‌کند.

یک مهاجم می‌تواند نام‌های مهم کارکنان یک سازمان را از راه تماس با آن واحد به دست آورد. در ادامه وی طی تماس با محل کار و یا منزل و شنیدن پیام دستگاه پیام‌گیر آنان از این موضوع آگاه می‌شود که کدام مدیر در خارج از شهر است. در ادامه، مهاجم با مراجعه به آن سازمان وانمود می‌کند که کلید خود را جا گذاشته است تا بتواند وارد ساختمان شود. پس از ورود مهاجم (که ممکن است از کارکنان همان سازمان باشد) به ساختمان اصلی سازمان مورد نظر، وی وارد دفتر کار کارکنانی می‌شود که در خارج از شهر هستند و بدون نگرانی رایانه وی را بررسی و با به‌کارگیری انواع نرم‌افزارهای موجود تلاش می‌کند که به اطلاعات موجود بر روی رایانه دست پیدا کند.

۹ـ۷ـ۳ حفاظت لایهٔ سیاست‌ها، رویه‌ها و اطلاع رسانی

- برای مقابله با انواع تهدیدها، باید سیاست‌ها و رویه‌های امنیتی به صورت روشن تدوین، پیاده‌سازی و توسط همهٔ کارکنان به کار گرفته شوند. هر فرایند و یا فرایندی که در خصوص سیاست‌های امنیتی تعریف می‌شود، باید دارای دستور کارهای مستند و روشنی باشد.

- کارکنان سازمان باید دربارهٔ سیاست‌ها و رویه‌های امنیتی آموزش ببینند. آموزش امنیت یک امر ضروری است تا این اطمینان به دست آید که کاربران در مورد کارهائی که باید در راستای تأمین سیاست‌ها و رویه‌های امنیتی انجام دهند، توجیه و آنان را رعایت می‌کنند. شیوهٔ آموزش باید به گونه‌ای باشد که تصویری واقعی از جایگاه و اهمیت امنیت اطلاعات را برای کاربران تشریح تا آنان نیاز به امنیت را همواره و در همهٔ سطوح احساس و به آن پایبند باشند.
- یک سیاست امنیتی ترکیبی از خواسته‌ها و فرهنگ یک سازمان است که متأثر از اندازه و اهداف یک سازمان است. برخی سیاست‌ها ممکن است به همهٔ سایت‌ها اِعمال شود و برخی دیگر ممکن است در محیط‌هائی ویژه به‌کار آید. یک سیاست امنیتی باید سطح کنترل را با سطح بهره‌وری بالانس کند. در صورتی که یک سیاست امنیتی محدودیت‌های زیادی را برای کاربران در پی داشته باشد، کاربران روش‌های نادیده گرفتن آن را بررسی و برای آن راه‌حل‌های ویژهٔ خود را پیدا خواهند کرد.
- اطلاع‌رسانی در خصوص مسئله‌های امنیتی باید ترویج و در دستور کار قرار گیرد. برای نمونه می‌توان از پوسترهای امنیتی و کارت‌های checklist برای اطلاع‌رسانی استفاده کرد. پوسترها و کارت‌های checklist دارای کارایی به مراتب بهتری نسبت به مستندات حجیم سیاست‌های امنیتی هستند که ممکن است برای استفادهٔ عموم بر روی شبکه اینترانت سازمان منتشر شده باشد. پوسترها و کارت‌های checklist را باید در مکانی نصب کرد که در معرض دید بیشتری باشند.

به منظور بررسی وضعیت برخی سیاست‌های امنیتی مانند رمزهای گذر و پیکربندی امنیتی، می‌توان از ابزارهائی مانند Microsoft Baseline Security استفاده کرد.

۹ـ۸ بررسی انواع ویروس‌ها و آسیب‌پذیری‌ها و تهدیدهای امنیتی که رایانه را مورد حمله قرار می‌دهند

ویروس‌ها

ویروس‌های رایانه‌ای، متداول‌ترین نوع تهدیدهای امنیتی در سالیان اخیر بوده که تاکنون دشواری‌های گسترده‌ای را ایجاد و همواره از خبرسازترین موضوع‌ها در زمینهٔ رایانه و شبکه‌های رایانه‌ای، بوده‌اند. ویروس‌ها، برنامه‌هائی رایانه‌ای هستند که برنامه‌نویسان

گمراه و در عین حال ماهر می‌نویسند و به گونه‌ای طراحی می‌شوند که توانا به تکثیر خود و آلودگی رایانه‌ها بر اثر وقوع یک رویداد ویژه، باشند. برای نمونه ویروس‌هایی که از آنان با نام «ماکرو ویروس» یاد می‌شود، خود را به فایل‌هایی شامل دستور کارهای ماکرو ملحق کرده و در ادامه، هم‌زمان با فعال شدن ماکرو، شرایط لازم به منظور اجرای آنان نیز فراهم می‌شود. برخی از ویروس‌ها بی‌آزار بوده و تنها سبب بروز اختلالات موقت در روند انجام فرایند در رایانه می‌شوند (مانند نمایش یک پیام مضحک بر روی صفحه نمایشگر هم‌زمان با فشردن یک کلید ویژه). برخی دیگر از ویروس‌ها دارای عملکردی مخرب‌تر بوده و می‌توانند مسئله‌ها و دشواری‌های بیشتری مانند حذف فایل‌ها و یا کاهش سرعت سامانه را به دنبال داشته باشند. یک رایانه تنها زمانی آلوده به یک ویروس می‌شود که شرایط و امکان ورود ویروس از یک منبع خارجی (بیشتر از راه فایل پیوست یک نامه الکترونیک و یا دریافت و نصب یک فایل و یا برنامهٔ آلوده از اینترنت)، برای آن فراهم شود. زمانی که یک رایانه در شبکه‌ای آلوده شد، دیگر رایانه‌های موجود در شبکه و یا دیگر رایانه‌های موجود در اینترنت، دارای استعدادی مناسب به منظور مشارکت و همکاری با ویروس، خواهند بود.

برنامه‌های اسب تروا (دشمنانی در لباس دوست)

برنامه‌های اسب تروا و یا Trojans، به منزلهٔ ابزارهایی برای پخش کدهای مخرب هستند. تروجان‌ها، می‌توانند بی‌آزار بوده و یا حتی نرم‌افزاری سودمندی مانند بازی‌های رایانه‌ای باشند که با تغییر قیافه و با لباسی مبدل و ظاهری سودمند خود را عرضه می‌کنند. تروجان‌ها، توانا به انجام فرایند متفاوتی مانند حذف فایل‌ها، ارسال یک نسخه از خود به سیاهه (لیست) نشانی‌های پست الکترونیک، هستند. این نوع از برنامه‌ها تنها می‌توانند از راه تکثیر برنامه‌های اسب تروا به یک رایانه، دریافت فایل از راه اینترنت و یا باز کردن یک فایل پیوست همراه یک نامه الکترونیک، اقدام به آلودگی یک سامانه کنند.

ویرانگران، بدافزار (Malware)

در وب سایت‌های پرشماری از نرم‌افزارهائی مانند اکتیوایکس‌ها و یا اپلت‌های جاوا استفاده می‌شود. این نوع برنامه‌ها به منظور ساخت انیمیشن و دیگر افکت‌های ویژه استفاده می‌شود و گیرایی و میزان تعامل با کاربر را افزایش می‌دهند. با توجه به دریافت و نصب آسان این نوع از برنامه‌ها، برنامه‌های بالا به ابزاری مطئمن و آسان به منظور

آسیب‌رسانی به دیگر سامانه‌ها بدل شده‌اند. این نوع برنامه‌ها که به «ویرانگران» شهرت یافته‌اند، به شکل یک برنامهٔ نرم‌افزاری و یا اپلت ارائه و در دسترس استفاده‌کنندگان قرار می‌گیرند. برنامه‌های بالا، توانا به ایجاد دشواری‌های پرشماری برای کاربران هستند (از بروز اشکال در یک فایل تا ایجاد اشکال در بخش اصلی یک سامانهٔ رایانه‌ای).

حمله‌ها

تاکنون حمله‌های پرشماری متوجه شبکه‌های رایانهٔ بوده که می‌توان همهٔ آنان را به سه گروه عمده تقسیم کرد:

- **حمله‌های شناسائی:** در این نوع حمله‌ها، مهاجمان اقدام به گردآوری و شناسائی اطلاعات با هدف تخریب و آسیب رساندن به آنان می‌کنند. مهاجمان در این رابطه از نرم‌افزارهای ویژه‌ای مانند Sniffer و یا Scanner به منظور شناسائی نقاط ضعف و آسیب‌پذیر رایانه‌ها، سرویس‌دهندگان وب و برنامه‌ها، استفاده می‌کنند. در این رابطه برخی تولیدکنندگان، نرم‌افزارهایی را با هدف‌های خیرخواهانه طراحی و پیاده‌سازی کرده‌اند که متأسفانه از آنان در جهت اهداف مخرب نیز استفاده می‌شود. برای نمونه به منظور تشخیص و شناسائی رمزهای گذر، نرم‌افزارهای پرشماری تاکنون طراحی و پیاده‌سازی شده است. نرم‌افزارهای بالا با هدف کمک به مدیران شبکه، افراد و کاربرانی که رمز گذر خود را فراموش کرده و یا آگاهی از رمز گذر افرادی که سازمان خود را بدون اعلام رمز گذر به مدیر شبکه، ترک کرده‌اند، استفاده می‌گردند. به هر حال وجود این نوع نرم‌افزارها واقعیتی انکارناپذیر بوده که می‌تواند به منزلهٔ یک سلاح مخرب در اختیار مهاجمان قرار گیرد.
- **حمله‌های دستیابی:** در این نوع حمله‌ها، هدف اصلی مهاجمان، نفوذ در شبکه و دستیابی به نشانی‌های پست الکترونیک، اطلاعات ذخیره‌شده در بانک‌های اطلاعاتی و دیگر اطلاعات حساس، است.
- **حمله‌های از کار انداختن سرویس‌ها:** در این نوع حمله‌ها، مهاجمان سعی در ایجاد مزاحمت به منظور دستیابی به همه و یا بخشی از امکانات موجود در شبکه برای کاربران مجاز می‌کنند. حمله‌های بالا به اشکال متفاوت و با بهره‌گیری از فناوری‌های پرشماری صورت می‌پذیرد. ارسال حجم بالایی از داده‌های غیرواقعی برای یک ماشین متصل به اینترنت و ایجاد ترافیک کاذب در شبکه، نمونه‌هایی از این نوع حمله‌ها هستند.

رهگیری داده (استراق سمع)

بر روی هر شبکه رایانهٔ روزانه اطلاعات متفاوتی جابه‌جا می‌شود و همین امر می‌تواند موضوعی مورد علاقه برای مهاجمان باشد. در این نوع حمله‌ها، مهاجمان اقدام به استراق سمع و یا حتی تغییر بسته‌های اطلاعاتی در شبکه می‌کنند. مهاجمان به منظور رسیدن به اهداف مخرب خود از روش‌های پرشماری به منظور شنود اطلاعات، استفاده می‌کنند.

کلاهبرداری (ابتدا جلب اعتماد و سپس تهاجم)

کلاهبرداران از روش‌های پرشماری به منظور اعمال شیادی خود استفاده می‌کنند. با گسترش اینترنت این نوع افراد فضای مناسبی برای اعمال مخرب خود یافته‌اند (چراکه می‌توان به هزاران نفر در زمانی کوتاه و از راه اینترنت دستیابی داشت). در برخی موردها شیادان با ارسال نامه‌های الکترونیک وسوسه‌انگیز از خوانندگان می‌خواهند که اطلاعاتی ویژه را برای آنان ارسال کرده و یا از یک سایت به عنوان طعمه در این رابطه استفاده می‌کنند. به منظور پیشگیری از این گونه اعمال، می‌بایست کاربران دقت لازم در خصوص درج نام، رمز گذر و دیگر اطلاعات شخصی در سایت‌هایی که نسبت به هویت آنان شک و دو دلی وجود دارد را داشته باشند. با توجه به سهولت جعل نشانی‌های پست الکترونیک؛ باید به این نکته توجه شود که پیش از ارسال اطلاعات شخصی برای هر فرد، هویت وی شناسایی شود. هرگز بر روی لینک‌ها و یا ضمائمی که از راه یک نامه الکترونیک برای شما ارسال شده است، کلیک نکرده و همواره باید به شرکت‌ها و مؤسسه‌هایی که به گونه‌ای شفاف نشانی فیزیکی و شماره تلفن‌های خود را یاد نمی‌کنند، شک و تردید داشت.

نامه‌های الکترونیک ناخواسته

از واژهٔ Spam در ارتباط با نامه‌های الکترونیک ناخواسته و یا پیام‌های تبلیغاتی ناخواسته، استفاده می‌شود. این نوع از نامه‌های الکترونیک، همگی بی‌ضرر بوده و تنها ممکن است مزاحمت و یا دردسر ما را بیشتر کنند. دامنه این نوع مزاحمت‌ها می‌تواند از به هدر رفتن زمان کاربر تا هرز رفتن فضای ذخیره‌سازی بر روی رایانه‌های کاربران را شامل می‌شود.

تهدیدها

زمانی که شما به عنوان مسئول و کارشناس امنیت اطلاعات یک شرکت یا سازمان به شمار می‌آیید، در واقع شما مسئول حفاظت از دارایی‌های اطلاعاتی یک سازمان در برابر کسانی یا چیزهایی هستید که می‌خواهند از آن دارایی‌ها سوءاستفاده کنند. ممکن است برخی از این افراد هم اکنون در سازمان و در کنار خود شما باشند، اما بیشتر این افراد در خارج از سازمان قرار دارند و همیشه قصد نفوذ به شبکه و سازمان را دارند. این جمله طلایی را همیشه به خطر بسپارید: **هیچ چیز برای یک مسئول یا کارشناس امنیت اطلاعات خطرناک‌تر و هولناک‌تر از کاربران خود آن شبکه نیست.**

متأسفانه این عمل چندان هم آسان نیست، در حال حاضر نقاط ضعف و آسیب‌پذیری‌های سامانه‌های تجاری در حال رشد است و این نقاط روز به روز بیشتر و بیشتر می‌شود، حال کافی است شما تنها یک روز از این اطلاعات بی‌خبر باشید و همین کافی است تا به شبکه و سازمان شما نفوذ شود. برای نمونه اگر از ویندوز نسخه اصلی یا اورجینال استفاده کرده باشید و به اینترنت متصل بشوید می‌بینید که همواره در حال به‌روزرسانی خود است به‌گونه‌ای که همه روزه بسته‌های امنیتی خود را بروز می‌کند و بر روی سامانهٔ شما نصب می‌کند، این یعنی اینکه همه روزه حمله‌های گسترده‌ای در سطح جهان به سامانه‌ها انجام می‌شود که سبب ایجاد نقاط ضعف در سامانه‌ها می‌شود و برای جلوگیری از نفوذ از راه این نقاط، بسته‌های امنیتی برای آنها ساخته و عرضه می‌شود.

دشمنان شما می‌توانند به‌آسانی با استفاده از موتورهای جستجو، نقاط ضعف و آسیب‌پذیر هر فرآورده یا سیستم‌عامل را بیابند، آنان برای اینکه بتوانند به شبکه شما وارد شوند و از نقاط ضعف شما بهره‌برداری کنند، می‌توانند کتاب‌های آموزش هک بخرند، به عضویت گروه‌های خبری امنیتی و هک در اینترنت در بیایند و یا به وب سایت‌هایی دسترسی پیدا کنند که در آنها اطلاعات روشن و با جزئیاتی در خصوص شبکه شما وجود دارد.

در بسیاری از موردها شما نرم‌افزاری را خریداری می‌کنید که خود آن نرم‌افزار به صورت ذاتی دارای نقاط ضعف امنیتی است و این نقاط ضعف امنیتی به خودی خود سبب به زیر پرسش رفتن امنیت سازمان شما خواهد شد، برای نمونه نرم‌افزار مجموعه

آفیس را خریداری می‌کنید و در آن نقاط ضعف امنیتی وجود دارد که هکرها می‌توانند از راه آن به سیستم‌عامل حمله و به آن دسترسی یابند.

متأسفانه در کشور عزیز ما ایران به دلیل عدم وجود قانون کپی رایت نرم‌افزارهایی که توسط برنامه‌نویس‌ها نوشته می‌شود زیر نظر هیچ سازمان مرکزی ویژه‌ای قرار ندارند، تا مشکلات احتمالی آنها را بررسی و به آنها رسیدگی کند. البته بخشی در مرکز پژوهش‌های صنایع انفورماتیک ایران برای آزمایش برخی نرم افزارهای ویژه ایجاد شده است اما به هیچ عنوان پاسخ‌گوی این سطح حجیم از نرم افزارهای تولیدی در درون کشور را ندارد، بنابراین اعتماد کردن به این گونه نرم افزارها بسیار سخت است.

۹ـ۹ شماری از راهکارهای عملی امنیت اطلاعات

۹ـ۹ـ۱ فشرده‌سازی و رمزگذاری روی فایل‌ها (بدون استفاده از نرم‌افزار ویژه)

شاید برای شما این پرسش پیش آمده باشد که چرا سایت‌ها، فایل‌های خودشان در فرمت Zip برای بارگیری (دانلود) قرار می‌دهند؟ خوب پاسخ به این سؤال زیاد سخت نیست. یکی از دلایلش کمبود حجم سایت و شاید راحت‌تر بگوییم، هزینه سنگین فضا (حجم اطلاعات بر روی سرور) برای یک وب سایت است. وب سایت‌ها دسترسی به یک فضا مانند فضای هارد دیسک برایشان مقدور نیست؛ به‌دلیل اینکه باید هزینه زیادی برای داشتن چنین قابلیتی صرف کرد که عاقلانه نیست. به همین دلیل تا جایی که امکان دارد صاحبان وب‌سایت‌ها تا می‌توانند، می‌کوشند حجم اطلاعات خودشان را بر روی وب سرور برای دانلود، تا حد قابل ملاحظه‌ای پایین بیاورند.

نرم‌افزار Winrar یکی از برنامه‌هایی است که وظیفه کم کردن حجم اطلاعات بدون افت کیفیت را بر عهده دارد. دقت داشته باشید که این نرم‌افزار در خود ویندوز هم به صورت پیش فرض وجود دارد و نیاز به نصب نرم‌افزار جانبی نیست، اما نرم‌افزاری که در خود ویندوز وجود دارد، دارای امکانات محدود و کیفیت کمتری است که کاربران بیشتر تمایل دارند از نرم‌افزار جانبی استفاده کنند تا از خود ویندوز.

۹ـ۹ـ۲ روش تهیه نسخه پشتیبان و بازیابی اطلاعات (Backup And Restore)

فایل‌های مهم سیستم عامل و داده‌های شما روی درایوهای دیسک سخت همیشه در معرض آسیب‌های پیش‌بینی نشده و آسیب حذف ناگهانی هستند. به منظور جلوگیری

از حذف اطلاعات مهم در رایانه خود، سیستم عامل ویندوز برنامه‌های سودمند Restore و Backup را در اختیار کاربران خود قرار داده است.

الف) تهیهٔ نسخهٔ پشتیبان (Backup) از اطلاعات

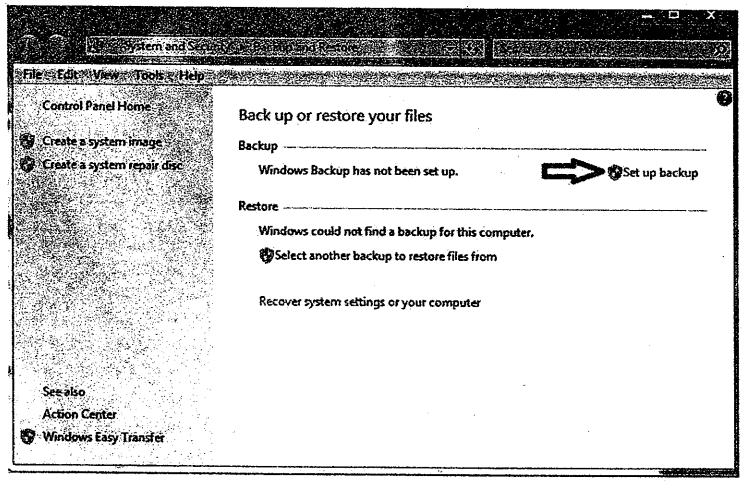
با استفاده از برنامهٔ Backup می‌توانید از پرونده‌ها و پوشه‌های خود، نسخه پشتیبان تهیه کنید. افزون بر این می‌توانید از تنظیم‌های سیستم‌عامل و محتویات رجیستری هم پشتیبان تهیه کنید تا در صورت بروز دشواری در عملکرد سیستم‌عامل، این تنظیم‌ها را به حالت اول برگردانید.

برای آغاز فرایند تهیهٔ نسخهٔ پشتیبان یکی از سه روش زیر را به کار بگیرید:

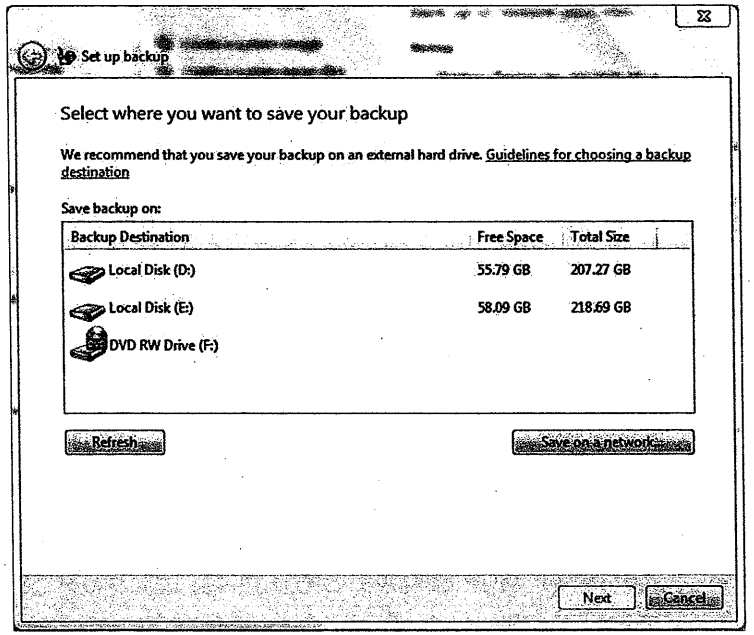
۱. در منوی Start، عبارت Backup را در کادر جستجو و اجرا تایپ کنید و کلید Enter را فشار دهید.

۲. پنجرهٔ Control Panel سیستم‌عامل ویندوز را باز کنید و گزینه‌های آن را با نمایهٔ Small Icon ببینید. سپس روی گزینه Backup and Restore کلیک کنید.

۳. در My computer سیستم‌عامل ویندوز، روی نشانهٔ درایو: C کلیک راست و از منوی میانبر، گزینهٔ Properties را برگزینید. در زبانه Tools روی دکمه ... Backup now کلیک کنید. اکنون برنامه تهیه پشتیبان آشکار می‌شود (شکل ۹ـ۱).



شکل ۹ـ۱

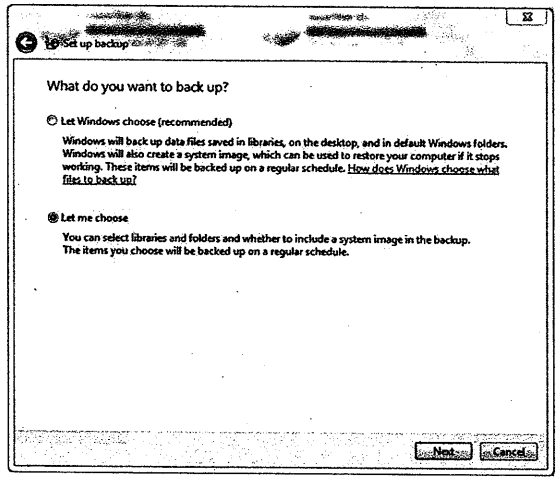


شکل ۹ـ۲

در صورتی که تاکنون از این برنامه استفاده نکرده‌اید، روی عبارت Set up backup کلیک کنید. برنامه ویزارد تهیه نسخه پشتیبان آغاز می‌شود. در مرحلهٔ بعد کادری مانند شکل زیر آشکار می‌شود. در این کادر باید مقصد نگهداری نسخه پشتیبان را معین کنید. توصیه می‌شود که پرونده پشتیبان را روی حافظه جانبی غیر از دیسک سخت (مانند حافظه فلش) ذخیره کنید. با این حال مقصد را می‌توانید از سیاهه (لیست) نشان داده شده، از درایوهای دیسک سخت سامانه نیز برگزینید. در صورت اتصال به شبکه، می‌توانید نسخهٔ پشتیبان را در رایانهٔ دیگر عضو شبکه ذخیره کنید. (شکل ۹ـ۲)

پس از انتخاب درایو مورد نظر، روی دکمهٔ Next کلیک کنید تا کادر what do you want to back up? آشکار شود.

در این مرحله کادری با محتوای شکل زیر آشکار می‌شود. با انتخاب گزینهٔ اول، به سیستم عامل ویندوز اجازه می‌دهید که از پرونده‌ها و پوشه‌های پیش فرض، مانند موردهای موجود در میزکار، پشتیبان تهیه کند و یک دیسک تصویر (Image) به وجود



شکل ۹ـ۳

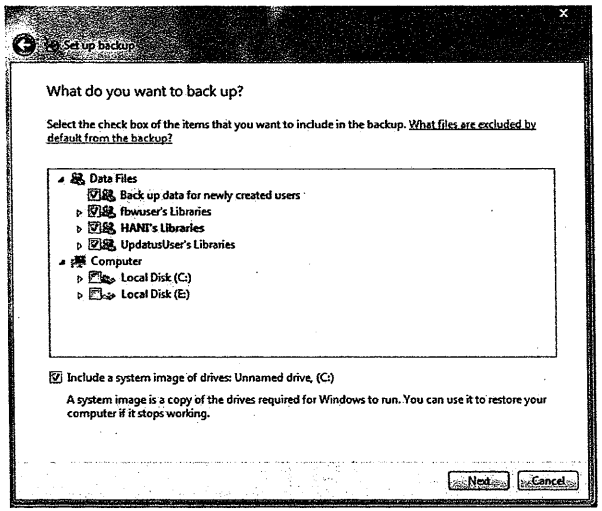
آورد. این موردها برای پشتیبان دوره‌ای، زمان‌بندی خواهد شد. در صورتی که مایل هستید موردهای پشتیبان را خود برگزینید، گزینهٔ دوم با عنوان Let me choose را انتخاب و روی دکمهٔ Next کلیک کنید. (شکل ۹ـ۳)

در این مرحله کادری مانند شکل زیر آشکار می‌شود و شما می‌توانید پوشه‌ها و پرونده‌های مورد نظر برای تهیه پشتیبان را برگزینید. پس از انتخاب روی دکمهٔ Next کلیک کنید. در مرحلهٔ بعد پیش از تهیهٔ پشتیبان، باید موردهای انتخابی را تأیید کنید (شکل ۹ـ۴).

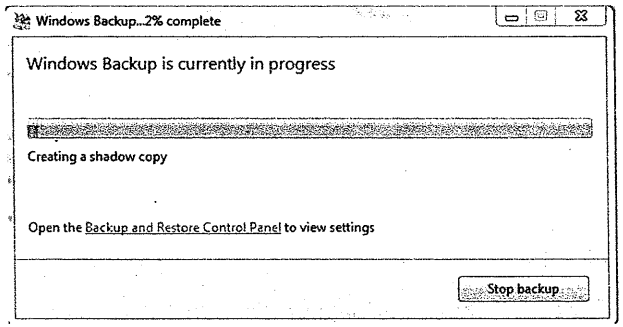
در این مرحله کادری جدید آشکار می‌شود. در این کادر می‌توانید دوره‌های زمانی تهیه پشتیبان را زمان‌بندی کنید. با انتخاب روز، ماه و سال روی دکمه OK کلیک کنید تا وارد مرحله بعد شوید.

در مرحله بعد با نمایش کادری فرایند تهیه پشتیبان آغاز می‌شود. برای دیدن جزئیات کپی شدن اطلاعات، روی دکمه View Details کلیک کنید تا پیشرفت کار را ببینید (شکل ۹ـ۵).

در پایان، پرونده پشتیبان در محل مورد نظر ذخیره خواهد شد. برای برگرداندن کافی است روی آن دوبار کلیک کنید.



شکل ۹ـ۴

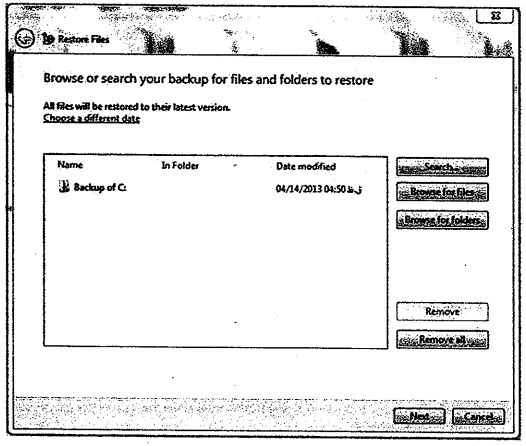


شکل ۹ـ۵

ب) بازیابی (Restore) اطلاعات از نسخهٔ پشتیبان

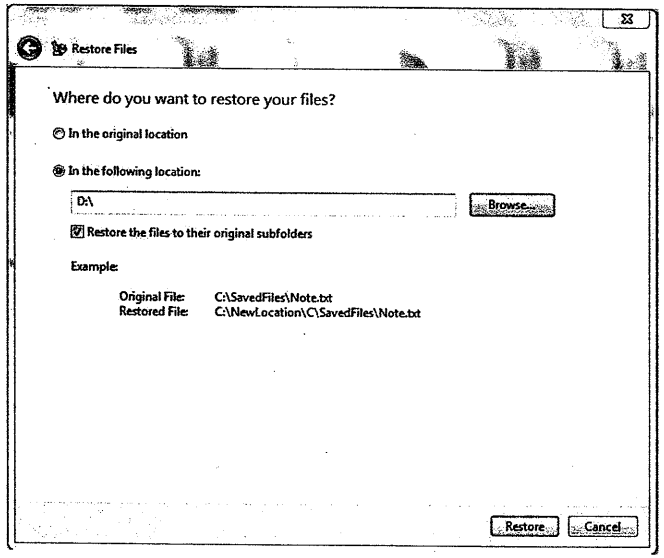
برای بازیابی داده‌های ذخیره‌شده در فایل پشتیبان، تنها کافی است روی فایل پشتیبان که در مرحلهٔ پیش ساخته شده است، دوبار کلیک و مرحله‌های گزینه Restore my files را برگزینید.

با کلیک روی این دکمه، کادری به صورت شکل زیر نمایان می‌شود و از شما می‌خواهد، موردهای بازیابی را برگزینید (شکل ۹ـ۶).



شکل ۹ـ۶

برای انتخاب پرونده‌های مورد نظر برای بازیابی، روی دکمه Browse for files کلیک کنید. به منظور انتخاب پوشهٔ مورد بازیابی، دکمهٔ Browse for folders را برگزینید. پس از انتخاب فایل‌ها، دکمه Next را بزنید. سپس کادری مانند شکل ۹ـ۷ آشکار می‌شود.



شکل ۹ـ۷

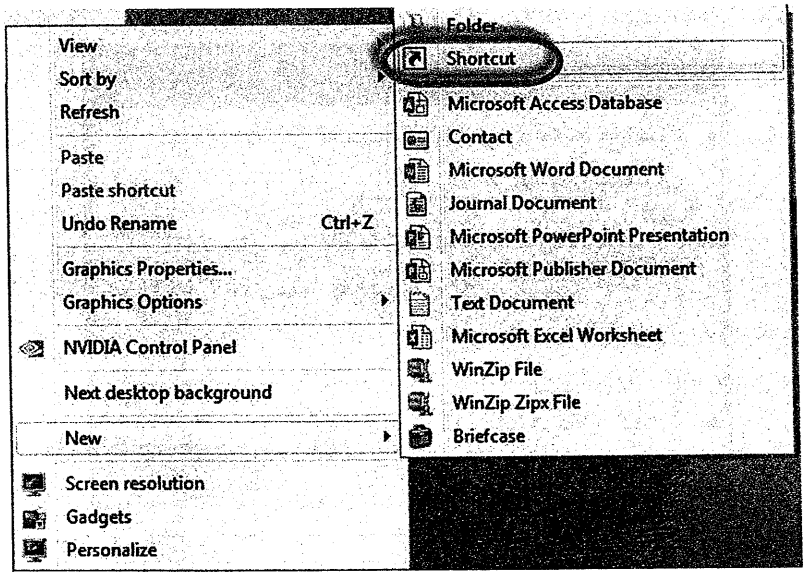
در این کادر با انتخاب In the original location بازیابی پرونده‌ها در محل اصلی پشتیبان‌گیری انجام می‌شود. در صورت انتخاب گزینهٔ In the following location می‌توانید پرونده‌ها را در مسیر مشخص‌شده بازیابی کنید. همچنین می‌توانید با کلیک روی دکمهٔ Browse... مسیر دلخواهی را انتخاب کنید. نشان‌دار بودن گزینهٔ Restore the files to their original subfolders سبب می‌شود پرونده‌های موجود در زیرفهرست‌ها در مسیر اولیه خود بازیابی شوند.

با کلیک روی دکمه Restore کادری باز خواهد شدکه پیشرفت بازیابی را نمایش خواهد داد.

۹ـ۹ـ۳ قفل کردن رایانه

شاید تا به حال به فکر یافتن راهی بوده‌اید که رایانه خود را آسان‌تر از آنچه متداول است در حالت Lock قرار دهید.

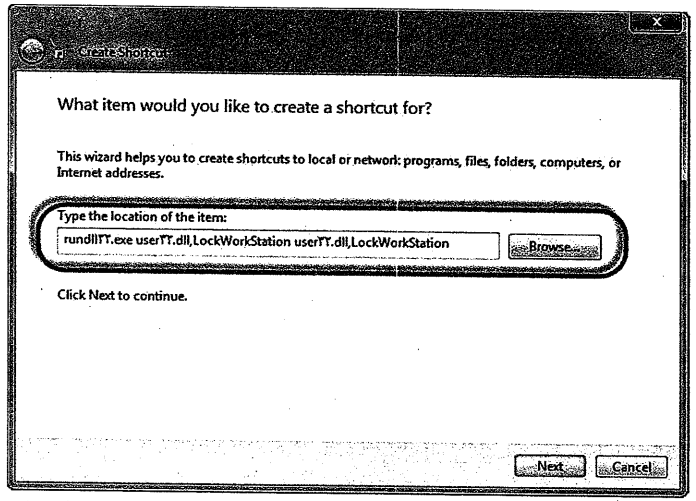
این کار بسیار ساده است و با طی کردن مرحله‌های زیر شما می‌توانید یک Icon به دسکتاپ یا Quick Launch بیفزایید که با یک ضربه ماوس بر روی آن سامانهٔ شما در حالت Lock قرار می‌گیرد.



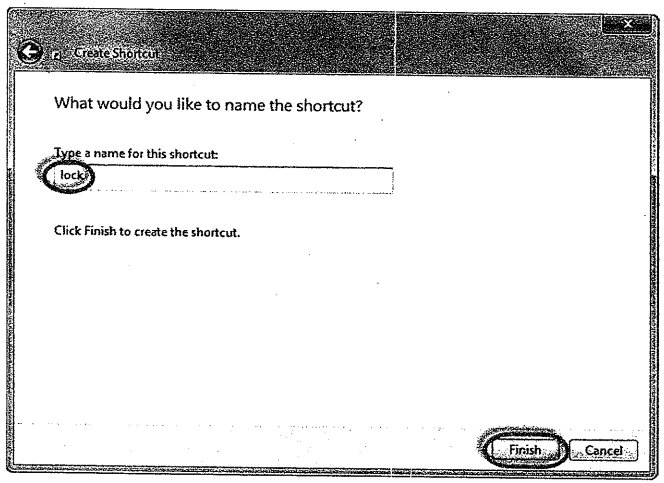
۱. بر روی صفحه نمایش خود Right-Click کنید و از Shortcut، New را برگزینید.

۲. در پنجره‌ای که آشکار شده در بخش Type the location of the item فرمان زیر را بنویسید:

rundll32.exe user32.dll,LockWorkStation user32.dll,LockWorkStation



۳. بر روی Next کلیک کنید و نام Shortcut را وارد کنید و کلید Finish را بزنید.



برای آسانی بیشتر پیشنهاد می‌شود که میانبر (Shortcut) ایجاد شده را با ماوس به یک بخش از فضای خالی Quick Launch بکشید تا از این پس در هنگام نیاز با زدن یک کلید دستگاه شما در حالت Lock قرار گیرد.

۹ـ۱۰ نتیجه‌گیری

اگر چه بیشتر سازمان‌ها تمایل به داشتن شبکه‌های ایمن دارند، ارائه تعریفی واحد از امنیت که همهٔ نیازهای شبکه را تأمین کند ممکن نیست؛ در عوض، هر سازمان باید ارزش اطلاعات خود را ارزیابی کند و سپس یک خط‌مشی امنیتی برای مواردی مشخص کند که باید حفاظت شوند. برای نمونه روش‌های تصدیق هویت زیست‌سنجی از نظر قدرت و در دسترس بودن، در حال بهبود هستند، اما اکنون با نوعی دودلی با آنها برخورد می‌شود و این تردید ناشی از هزینه‌های به نسبت بالا و دشواری‌های مرتبط با دغدغه‌های حفظ حریم خصوصی است. البته نظرهایی وجود دارند که به سبب آنها می‌توان از ترکیب فناوری‌های متنوع امنیتی، برای تشکیل فناوری‌های امنیتی قوی در زمینهٔ امنیت اطلاعات استفاده کرد. برای نمونه، در آینده نزدیک با ترکیب دیوار آتش، نظام‌های آشکارساز نفوذی و فناوری‌های 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 کنند. به علاوه، ارائهٔ این طبقه‌بندی از فناوری‌ها، زمینه‌ساز پژوهش جدیدی خواهد بود.

پرسش و پژوهش

۱. امنیت اطلاعات چیست؟
۲. چند مورد از راهکارهای عملی امنیت اطلاعات را بیان کنید؟
۳. انواع ویروس‌ها و آسیب‌پذیری‌ها و تهدیدهای امنیتی که رایانه را مورد حمله قرار می‌دهند را بررسی کنید
۴. اصول امنیت اطلاعات چیست؟
۵. گام های پیاده‌سازی امنیت اطلاعات را بیان کنید؟
۶. بررسی: باج افزار (Ransomware) چیست؟
۷. بررسی: حمله‌ها از کار انداختن سرویس پخش‌شده (DdoS) چیست؟
۸. بررسی: تفاوت دو پروتکل SSL و TLS چیست؟ سه حمله به پروتکل SSL را نام ببرید؟