امنیت اطلاعات
● امنیت پایگاه‌های اطلاعاتی
● ارزیابی وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران

امنیت پایگاه های اطلاعات

شکوه مشهدی تفرشی

چکیده

داده‌های با اهمیت و محرمانه در سرورهای شبکه و یا پایگاه‌های اطلاعاتی همواره در خطر نفوذ و دستیابی از سوی افراد غیرمجاز هستند. بدین جهت، امنیت اطلاعات از مسائل مهم و پیچیده در توسعهٔ پایگاه‌های اطلاعاتی به‌شمار می‌رود. میزان اقدامات امنیتی به حساسیت و اهمیت داده‌ها و میزان اعتماد به کاربران بستگی دارد. به‌طور کلی سه مقوله در کنترل ایمنی داده‌ها مطرح است: ۱) امنیت فیزیکی، ۲) یکپارچه‌سازی پایگاه اطلاعاتی از طریق فنون معتبر، ۳) کنترل معیارها از طریق رمز عبور، کدگذاری، و ارائه به کاربر بر اساس مبانی اصولی. معمولاً پاسخ واحدی به چگونگی ایمن‌سازی پایگاه‌های اطلاعاتی وجود ندارد و همواره بیش از یک لایه محافظ برای امنیت سیستم توصیه شده است. مجراهای گوناگون برای ایجاد امنیت عبارتند از: کنترل دسترسی، یکپارچگی داده‌ها، کدگذاری داده‌های ذخیره شده، کدگذاری داده‌های در حال انتقال، و مانند آن که در این مقاله بدان اشاره خواهد شد.

کلیدواژه‌ها: پایگاه اطلاعاتی. امنیت اطلاعات. کدگذاری. مدیریت اطلاعات.

امنیت پایگاه‌های اطلاعاتی

شکوه مشهدی تفرشی[۱]

تعریف کلی مفهوم امنیت اطلاعات

امنیت اطلاعات و لزوم محافظت از شبکه‌های رایانه‌ای، موضوعی است که امروز اهمیت آن بر کسی پوشیده نیست. امنیت اطلاعات معیارهایی دارد که میزان تضمین هر یک، سطح امنیتی و ضریب نفوذپذیری سیستم را مشخص می‌کند. در این زمینه سازمان‌ها و مراکز مختلفی در سطح جهان معیارها و سطوح ایمنی در دنیای اطلاعات را به صورت استاندارد بیان کرده‌اند. امنیت اطلاعات به معنای حفظ اطلاعات در مقابل آسیب، حمله، نفوذ، و پایداری و قابل اعتماد بودن اطلاعات تعریف شده است. در راهنمای عملی مدیریت امنیت اطلاعات که توسط سازمان بین‌المللی استاندارد (ایزو) تهیه شده، آمده است که اطلاعات سرمایه‌ای است که امنیت آن هم‌چون سایر کالاهای تجاری برای یک سازمان ارزش دارد و حفاظت مطلوب از آن امری ضروری است. هدف امنیت اطلاعات به‌کارگیری مجموعه‌ای از سیاست‌ها، راه‌کارها، سخت‌افزار، و نرم‌افزار به‌منظور فراهم آوردن محیطی عاری از تهدید در تولید، پالایش، و انتقال اطلاعات است. خصوصیات دیگری نیز از قبیل اصالت، محرمانه بودن، تضمین جامع بودن، و ترمیم‌پذیری نیز در سایر تعاریف ارائه شده است (خامدا، ۱۳۸۲، ص ۳ـ۱۵).

۱. دانشجوی دکترای کتابداری و اطلاع‌رسانی دانشگاه آزاد اسلامی، واحد علوم و تحقیقات و عضو هیأت علمی دانشگاه آزاد اسلامی واحد تهران شمال

یک سیستم مناسب امنیتی شامل کنترل مراحل از نظر حفاظت فیزیکی، حفاظت داده‌ها، و دسترسی محدود است. هرچه سازمان‌ها به اطلاعات رایانه‌ای بیشتر متکی باشند، سطح حفاظت بیشتری را می‌طلبند. امنیت اطلاعات با امنیت شبکه در ارتباط و پیوند نزدیکی است ولی با وجود این، قابلیت افزایش سطح امنیتی در نظام‌های اطلاعاتی و شبکه‌های رایانه‌ای در گلوگاهی امنیتی به نام "سیستم عامل" گرفتار شده است. به عبارت دیگر، سیستم عامل زیرین این شبکه‌ها موجب کاهش ضریب امنیتی و افزایش نفوذپذیری به آنها می‌شوند.

داده‌ها ثروتی مهم به‌شمار رفته که نیاز به محافظت دارند. در محیط پایگاه اطلاعاتی ــ جایی که فایل‌های مرکزی قرار دارند ــ امنیت مسئله‌ای جدی است. برای رسیدن به امنیت، مدیریت پشتیبانی سیستم مجبور به طراحی و اجرای سیستمی مناسب برای این امر است. صاحبنظران امنیت را از جهات مختلفی مورد بررسی قرار داده‌اند. گروهی معتقدند که در شش مورد زیر می‌توان امنیت را مورد بررسی قرار داد (اوارد[1]، ۱۹۸۵):

۱. امنیت و دسترسی فیزیکی
۲. امنیت نیروی انسانی
۳. امنیت سیستم عامل
۴. امنیت داده‌ها
۵. امنیت برنامه‌های کاربردی
۶. امنیت شبکه

در بُعد امنیت سیستم چهار بخش قابل تشخیص است:

۱. امنیت
۲. یکپارچگی
۳. محرمانه بودن
۴. سرّی بودن

این چهار بخش با ۶ عامل مورد اشارهٔ بالا در ارتباط است، و در هر جزء آن می‌توان عوامل ششگانه را مورد بررسی قرار داد.

علل به خطر افتادن امنیت سیستم (دیدگاه کلی)

با گذر زمان وقوع حوادث الکترونیکی غیر منتظره، ضرورت بذل توجه به مقولهٔ

1. Award

امنیت شبکه‌ها و نظام‌های رایانه‌ای بیشتر می‌شود. وقایعی که تاکنون در شبکه‌های رایانه‌ای سازمان‌ها رخ داده، ناشی از آسیب‌پذیری نوعی سیستم عامل، آسیب‌پذیری کارگزار نامه‌های الکترونیک، و عدم آمادگی کارشناسان مراکز رایانه‌ای سازمان‌ها برای مقابله با یکی دو ویروس یاکرم رایانه‌ای بوده است. ضربه‌پذیری امنیت اطلاعات حاکی از موارد زیر است (لونی[1]، ۲۰۰۱):

۱. عدم توجه به امنیت در فرایند خودکارسازی و رویکرد سازمانی به فن‌آوری اطلاعات، و به دنبال آن فقدان اعتبار لازم برای ایمن‌سازی؛

۲. استفاده از نرم افزارهای رایگان یا فاقد حق مؤلف و عدم توجه به پیامدهای آن؛

۳. اتصال به شبکه‌های محلی یا جهانی، بدون ملاحظهٔ امنیتی و اعتماد کامل به نرم‌افزارهای موجود در سیستم؛

۴. کمبود نیروی انسانی در زمینهٔ امنیت شبکه و کم توجهی مراکز آموزشی عالی به تربیت نیروی انسانی در رشته‌های مرتبط با آن؛

۵. عدم توجه مناسب به حرفهٔ امنیت شبکه به منظور آمادگی برای انجام پروژه‌های مرتبط با امنیت.

عوامل موثر در امنیت پایگاه‌های اطلاعات

همان‌طور که اشاره شد چهار بخش در امنیت اطلاعات مورد توجه است که اینک اهمیت این چهار بخش را مورد بررسی قرار می‌دهیم (اوارد، ۱۹۸۵):

۱. امنیت

امنیت به نوع فن‌آوری سیستم مربوط است. تدابیری است که در سخت‌افزار و سیستم عامل برای محافظت در مقابل خطرات عمدی یا تهدیدات اتفاقی در نظر گرفته شده است.

تحقیقاتی که در سال ۱۹۸۵، در ایالات متحدهٔ امریکا انجام شده است نشان می‌دهد که بیشترین خطرات و آسیب‌ها از طریق خطاهای سهوی و حذف اطلاعات، که معمولاً اتفاقی است، متوجه سیستم است و اغلب این خطاها نیز توسط کاربران صورت گرفته است (اوارد، ۱۹۸۵). تهدیداتی که سیستم را از خارج به خطر می‌اندازد و در ردهٔ آخر قرار گرفته است از نظر میزان آسیب‌رسانی به شکل زیر طبقه‌بندی شده‌اند:

۱. خطا و حذف (پاک کردن)

1. Loney

۲. کارکنان ناراضی و غیرمطمئن
۳. آتش سوزی
۴. حوادث طبیعی
۵. حملات خارجی Hacker ها

با توجه به درک ضرورت توجه به سیستم عامل، IEEE[1] پروژه‌ای را برای تعریف استانداردهای سیستم عامل امن آغاز کرده است. هدف اساسی این پروژه تعریف معیارها و نیازمندی‌های اساسی امنیتی برای سیستم عامل‌های همه منظوره و تجاری است. این استانداردها مبنایی برای ساخت سیستم عامل امن‌تر و با نام (IEEE P 2200) معرفی شده است. در حقیقت، این پروژه تهدیدات بیرونی و ضعف‌های درونی را که به سبب طراحی و مهندسی نامناسب سیستم عامل بروز می‌کند مورد مداقه قرار داده و معیارهای مفیدی را در این باب ارائه می‌دهد (لونی، ۲۰۰۲).

۲. یکپارچگی سیستم

این عامل مربوط به تناسب عملکرد و سخت‌افزار و برنامه است. باید از یکپارچگی داده‌ها و فرم اصلی آن اطمینان حاصل کرد تا به‌طور اتفاقی آشکار شده و از بین نرود و تحت تغییرات ناخواسته قرار نگیرد.

۳. محرمانه‌بودن

این اصطلاح به مفهوم این است که چگونه سازمان باید از دسترسی افراد غیرمجاز به سیستم جلوگیری کند و مانع از انتشار اطلاعات اضافی به بیرون شود.

۴. سرّی بودن

سرّی بودن در وضعیتی خاص مطرح می‌شود که داده‌های حساسی در پایگاه اطلاعاتی وجود دارد که باید محافظت شود. امنیت سیستم مفهومی فنی در حفاظت است، در حالی که محرمانه بودن و سری بودن به چگونگی کاربرد اطلاعات مربوط می‌شود.

هنگامی که اطلاعات زیادی در پایگاه اطلاعاتی نگهداری می‌شود، اطلاعات حساس و محرمانه می‌تواند مورد کپی کردن و سرقت قرار گیرد. برای حفاظت از اطلاعات و رفع این‌گونه تهدیدات، طراحان سیستم باید به انباشتگی داده‌ها در سیستم آگاه بوده و به آن دسترسی داشته باشند تا بتوانند هرگونه خطری که سیستم را تحت‌الشعاع قرار می‌دهد پیش‌بینی کنند. طراح سیستم ابتدا سیاهه‌ای از اهداف سیستم

1. Institute of Electrical and Electronics Engineers.

و توانایی‌های رایانه تهیه کرده و ابزارهای امنیتی را پیش‌بینی و معیارهای و سطوح آن را تعیین می‌کند.

پس از آنکه تحلیل صورت گرفت باید معیارهایی برای سطح حفاظت در مورد تهدیدات داخلی و خارجی ارائه گردد. به‌طور کلی چهار سطح برای حفاظت مد نظر قرار می‌گیرد (اوارد، ۱۹۸۵):

الف) شناسایی، ب) کنترل دسترسی، ج) کنترل سمعی، و د) یکپارچگی سیستم.

الف. شناسایی

در زمینهٔ شناسایی می‌توان سه راهکار را به‌کار برد: رمز عبور، کارت شناسایی عکس داری که افرادی که به مرکز می‌آیند شناسایی می‌کند، اثر انگشت یا ظبط صدا که اولی جنبهٔ قانونی دارد و دومّی هم روش دیگر شناسایی سیستم است. با کارت اعتباری سیستم تشخیص می‌دهد که چه کسی می‌خواهد وارد سیستم شود.

ب. کنترل دسترسی

کنترل دسترسی راه‌های مختلفی دارد. یکی استفاده از کارت‌های کددار است که به‌عنوان کلید رمز برای باز کردن در استفاده می‌شود. دیگری کدگذاری داده‌هاست. روش دیگر کنترل بازرسی است که برای انجام این فرایند نرم افزارهای مختلفی وجود دارد که در تمام سطوح مدیریت باید اعمال گردد.

ج. کنترل سمعی

این سطح قبلاً در توضیح شناسایی مورد بحث قرار گرفته است.

د. یکپارچگی سیستم

یکپارچگی سیستم خط سوم دفاعی است که بر عملکرد سخت‌افزار، پایگاه اطلاعاتی، و نرم‌افزار حمایت شده و امنیت فیزیکی و عملکردی تمرکز دارد. ارزشمندترین نرم‌افزارها ممکن است در اثر اشتباه از دست بروند. می‌توان چنین خطراتی را از طریق اجرای موازی در هر مرحله به حداقل رساند. امنیت فیزیکی پایگاه اطلاعاتی را می‌توان از طریق تهیهٔ نسخهٔ پشتیبان[1] افزایش داد. استفادهٔ روزانه از فایل‌های کتابخانه یکی از ویژگی‌های مهم در حفظ امنیت است. این نکته به معنای داشتن نسخهٔ پشتیبان مناسب و کافی و پرسنل مناسب برای ادارهٔ اسناد در زمان مورد نیاز است. نسخهٔ پشتیبانی به معنای نگهداری کپی فایل‌ها در محل مناسب و امن و برای فایل‌های نوری مرحله‌ای عادی جهت نگهداری فایل‌های اصلی پس از روزآمدسازی است.

1. Backup

راه‌های ایمن‌سازی و حفظ امنیت پایگاه اطلاعات

اغلب تدابیر امنیتی مقدماتی مبتنی بر حفظ محیط شبکه است ولی اغلب این کوشش‌ها آسیب‌پذیری داده‌های ذخیره شده در سرورهای شبکه را در نظر نگرفته‌اند؛ زیرا نفوذکنندگان همواره در صدد نفوذ و دسترسی به این اطلاعات هستند. در شبکهٔ اینترنت از دیوارهای آتش[1] استفاده می‌کنند که مانع از نفوذ و تهدیدات داخلی نیست. این تهدیدات می‌تواند از سوی یکی از کارکنان ناراضی سازمان صورت پذیرد. به همین سبب طراحان سیستم از روش کدگذاری برای ایجاد امنیت در پایگاه‌های اطلاعاتی استفاده می‌کنند. اما در طراحی و توسعهٔ سیستم کدگذاری پایگاه‌ها عوامل بسیاری دخیل هستند که باید مورد توجه قرار گیرند تا کارآیی سیستم کدگذاری شده بالا رود. آنچه که مهم است حمایت در عمق است و این به مفهوم وجود بیش از یک دیوار دفاعی است. برجها، دیوارها، آرک‌ها، و مانند آن هریک به تنهایی قادر به حفاظت از سیستم نیستند ولی در جمع با یکدیگر دسترسی به قصر را مشکل می‌سازند.

کدگذاری یکی از لایه‌های محافظ برای پایگاه‌هاست. این روش بدون اجرای سایر معیارهای امنیتی در سیستم غیر موثر و ناکارآمد است. قبل از توضیح دربارهٔ چگونگی اجرای کدگذاری باید از وجود کنترل دسترسی مناسب اطمینان حاصل کرد. علاوه بر افرادی که تهدیدات بیرونی را به پایگاه تحمیل می‌کنند، کارکنانی که به سیستم دسترسی دارند نیز خطرات درون سیستم محسوب می‌شوند. باید سیاستگذاری برای جلوگیری از نمایش و شنود اطلاعات پایگاه انجام گیرد. اگر از تمام امکانات امنیتی مانند کدگذاری، کنترل دسترسی، و استفاده از فن‌آوری شناسایی دقیق کاربران در حفاظت از پایگاه استفاده شده می‌توان تا حدودی به ضریب امنیت پایگاه اطمینان حاصل کرد (کدگذاری[2]، ۲۰۰۳).

برقراری کنترل دسترسی نیازمند پیکره‌بندی نحوهٔ تعامل استفاده‌کنندگان از پایگاه است. ساختار کنترل و مکانیزم آن از طریق پایگاه، بهترین مفهوم برای یک دسترسی کنترل شده است. وقتی که در جای مناسب یک دسترسی کنترل شده وجود داشته باشد می‌توان کدگذاری را انجام داد. این ممنوعیت اضافی در زمانی که دسترسی کنترل شده شکسته شده باشد می‌تواند مفید واقع شود. وقتی که نفوذکنندگان نخستین درهای دسترسی کنترل شده را می‌شکنند، کدها دومین مانع در راه‌یابی آنها به سیستم تلقی می‌گردد.

1. Firewall
2. Encryption

به‌طور مثال، می‌خواهیم در محیط ویندوز با استفاده از کدگذاری فایل‌های سیستم یک مدرک مهم و سرّی را در سیستم داشته و امنیت دسترسی به آن را حفظ کنیم. اولین قدم باید (NTFSA) باشد که دسترسی اشخاص غیر مجاز را به فایل ممنوع کند. البته این دیواره چندان قابل اعتماد نیست و نقاط ضعف بیشماری دارد؛ مانند به‌دست آوردن کنترل سیستم اجرایی توسط حمله‌کنندگان به سیستم یا دریافت مجوّز عبور از طریق دور زدن سیستم و boot کردن سرور. در هر حال، کدگذاری یک روش پیشنهادی منطقی و در عین حال نامطلوب برای پاسخ به نیاز امنیت سیستم است. نامطلوب است زیرا نمی‌تواند مانع پاک شدن اطلاعات شود و همچنین نمی‌تواند مانع تغییر و اصلاحات غیرمجاز گردد. به همین سبب حتماً باید از اطلاعات موجود فایل پشتیبان تهیه شود تا در موقع لزوم مورد استفاده قرار گیرد. به‌طورکلی، روش‌های ایمن‌سازی در زمینهٔ کنترل دسترسی به سیستم به شرح ذیل است:

۱. کدگذاری مبتنی بر رمز ورود،[1] که بر اساس استاندارد PKCS#5 انجام می‌شود.

۲. کارت هوشمند یا رمزگذاری با نشانه‌های مبتنی بر الگوریتم عمومی کلیدی یا فن‌آوری هماهنگ با زمان، که تا حدودی ایمنی قوی‌تری را به‌وجود می‌آورد. این شیوه مبتنی بر کاربر است. استفاده از این کارت‌ها برای کاربران نهایی بسیار ساده است، به‌خصوص در نظام‌های پیچیده با نقش‌های مختلف و مسئولیت‌های متعدد که نیاز به دسترسی به کلید رمز و استفاده از اطلاعات حساس دارد. هم‌چنین هنگامی که در سیستم کلید رمزهای متعدد به‌کار گرفته شده است این کارت‌ها کاربری دارد.

۳. روش بایومتریک. این روش مبتنی بر اثر انگشت یا صدا و سیستم‌های بیولوژیکی است.

حال پس از بحث پیرامون مدیریت دسترسی کنترل شده به مقولهٔ کدگذاری از دیدگاه عمیق‌تر می‌نگریم. در زمینهٔ کدگذاری داده‌ها در پایگاه‌های اطلاعاتی دو مقوله مطرح می‌شود. یکی کدگذاری داده‌ها در زمان انتقال[2] و دیگری کدگذاری داده‌ها در مخزن پایگاه[3].

کدگذاری داده‌ها در حال انتقال. کدگذاری بدین صورت است که همان‌طور که اطلاعات در طول شبکه از پایگاه به کاربر و بالعکس حرکت می‌کند اطلاعات را پنهان می‌کند. این روش ترافیک حرکتی، شبکه‌های محلی و اینترنت و حتی شبکه‌های بی‌سیم را محافظت می‌کند. استانداردهای مختلفی در این زمینه وضع شده است.

1. Password Based Encryption
2. Data in motion
3. Data at rest

مثل (SSL)[1]، (TLS)[2]، یا (TPSEC)[3] و ISO/IEC 17799 . اغلب کارگزاران و وندورهای پایگاه‌های اطلاعاتی از سیستم SSL استفاده می‌کنند.

از طریق تونل SSL مجموعه‌ای از RSA و RC4 و DES و سایر الگوریتم‌های هل من[4] را به‌کار می‌برند. این کدگذاری به منظور جلوگیری از قطع ارتباط در ترافیک رفت و برگشت داده‌ها بین کاربر و پایگاه به‌کار می‌رود. شبکهٔ ارتباطات در زمان انتقال از طریق سیم‌ها کدگذاری شده و در زمان رسیدن به مقصد دوباره کدها باز می‌شوند.

کدگذاری داده‌ها در مخزن پایگاه. این کدگذاری به منظور تغییر شکل داده‌ها در پایگاه اطلاعاتی صورت می‌گیرد به شکلی که فقط افراد مجاز قادر به خواندن اطلاعات باشند. این روش مانع از مورد حمله قرار گرفتن اطلاعات در نقطه پایانی نیست؛ زیرا اغلب حمله‌ها معمولاً به جایی که داده‌ها برای مدت طولانی در آن قرار می‌گیرند صورت می‌پذیرد. درک این مسئله سوء تفاهماتی در زمینهٔ کدگذاری ایجاد کرده است. اغلب متخصصان، کدگذاری داده‌های در حال انتقال را به‌شکل گسترده‌ای انجام می‌دهند؛ ولی اغلب در زمینهٔ پایگاه‌هایی که نیاز به مدیریت امنیت دارند کدگذاری داده‌ها در پایگاه انجام نگرفته است و این نشان از عدم امنیت پایگاه اطلاعاتی دارد.

کدگذاری یک پایگاه می‌تواند در سطوح مختلف در سیستم انجام شود. به‌طور مثال، از سیستم عامل می‌توان آغاز کرد. این روش چون نمی‌تواند به دلخواه بخشی از داده‌ها را کدگذاری کند لذا کل فایل را کدگذاری می‌کند و این امر سبب ایجاد مسائل جدی در خواندن اطلاعات از پایگاه‌ها می‌شود.

در این روش بدون توجه به اینکه آیا همهٔ داده‌ها نیاز به حفاظت دارند یا خیر از همه محافظت می‌شود و در نتیجه سبب بالا رفتن هزینه‌های خواندن فایل و سایر هزینه‌ها می‌گردد. به‌طور مثال، می‌توان به EFS[5] اشاره کرد که در محیط ویندوز ورودی کل فایل‌های پایگاه توسط مایکروسافت کد گذاشته شده است. نقاط ضعف بیشتری نیز در این سیستم وجود دارد. به‌طور مثال، در زمان بازیابی نمایه‌ها و سایر ساختارهای داخلی مشکلاتی را ایجاد می‌کنند. دیگر اینکه وقتی که یک فایل یا ضمیمه‌ای به پایگاه اضافه می‌شود فقط کد فایل بدست آمده باید به داده‌های وارد شده تعلق بگیرد؛ در حالی که باید کل پایگاه رمزگشایی شده و سپس داده‌ها وارد شوند. اشکال دیگر این است که داده‌ها نمی‌توانند به‌طور جداگانه کدگذاری و کلید رمز جدا داشته باشند.

1. Secure Socket layer (SSL)
2. Transport Layer Security (TLS)
3. Secure Internet Protocol (TPSEC)
4. Hellman
5. Encryption File System (EFS)

معمولاً همهٔ داده‌ها از نظر اهمیت اطلاعاتی در یک سطح نیستند. کدگذاری باید در سطوح مختلف صورت گیرد. به‌طور مثال، شمارهٔ کارت اعتباری مسئله‌ای کاملاً سری است که نباید کسی به آن دسترسی داشته باشد، ولی نام و نام خانوادگی و یا تحصیلات نیاز به چنین حفاظتی ندارند. هم چنین ممکن است پایگاهی دارای اطلاعات فروش و پرسنلی باشد. بخش مدیریت منابع انسانی باید به بخش پرسنلی دسترسی داشته باشد نه به فایل اطلاعات فروش، و همین‌طور مدیریت فروش نیاز بـه دسـترسی بـه فـایل فروش دارد نه اطلاعات پرسنلی. استفاده از کدگذاری لایه‌ای فایل‌ها قادر نیست که بخش به بخش عمل کند و کل داده‌ها در سیستم دارای یک کد می‌شوند. کدگذاری مبتنی بـر فایل‌ها فقط داده‌ها را از حمله‌کنندگان به سیستم عامل محافظت می‌کند. راه مؤثرتر و کارآمدتر برای کدگذاری اطلاعات در پایگاه، کدگذاری بر سطرها و ستون‌هاست. به‌طور مثال، می‌توان فقط روی شمارهٔ کارت اعتباری کد گذاشت یعنی کدگذاری سطرها و یا ستون‌ها بسیار مهم و حساس که در واقع منجر به حداقل رساندن عملیات می‌شود.

یکی دیگر از مسائلی که کدگذاری آن را حل می‌کند، حفاظت از داده‌هـا در مـقابل مدیران سیستم است. اینکار از طریق کد دادن به بخش‌های ویژه که باید مخفی بمانند انجام می‌شود. در واقع، برای حفاظت یک فایل با دادهٔ سری از دید مدیریت سـیستم صورت می‌گیرد.

با توجه به نیاز به دسترسی سریع و مکان بازیابی، در کدگذاری باید بسیار دقت کرد. بنابراین، یک پایگاه نمی‌تواند برای هر بـخشی از داده‌هـای مـورد کـاوش کـدگذاری و رمزگشایی کند؛ لذا در هر حال کدگذاری یک ستون از اطلاعات که ضرورت سرّی ماندن دارد شانس بالا بردن سرعت پایگاه را افزایش داده و سرعت جست‌وجو را زیاد می‌کند.

در حین کدگذاری سیستم جهت حفظ امنیت و بالا بردن دقت لازم است به سؤالات زیر پاسخ داده می‌شود:

۱. چند کلید رمز مورد نیاز است؟
۲. چگونه باید این کلیدهای رمز را مدیریت کرد؟
۳. کلیدهای رمز کجا باید نگهداری و حفاظت شوند؟
۴. چگونه باید از دسترسی به کلیدها توسط اشخاص غیر مجاز جلوگیری کرد؟
۵. چندگاه یکبار باید این کلیدها تغییر کند؟
۶. چه داده‌هایی باید رمزگذاری شود؟ همهٔ ستون‌ها؟ فقط یک ستون یا بیشتر؟

استانداردهای ایمنی

در اینجا ضروری است که مختصری در زمینهٔ استاندارد امنیت اطلاعات توضیح داده شود.

این استاندارد (BS 77991) در اوایل سال ۱۹۹۰ در نتیجهٔ درخواست‌های صنایع، دولت، و تجارت برای دستیابی به یک الگوی امنیت اطلاعات گسترش یافته است. سازمان‌ها احساس می‌کردند که در مبادلات تجاری نیاز به اطمینانی دارند تا بتوانند در سایهٔ آن مشترک عمل نمایند و همچنین برای شرکای تجاری خود نیز امنیت ایجاد نمایند. این استانداردها جنبه‌هایی از برنامهٔ حفاظت اطلاعات را که برای رفع نیازهای تجاری و صنعتی لازم است مشخص می‌سازد. این حفاظت برای اطمینان از یکپارچگی و درستی داده‌ها، در دسترس بودن، محرمانه بودن اطلاعات با ارزش حقوقی صورت می‌گیرد.

این اطمینان از طریق کنترل‌هایی که مدیریت درون سازمان ایجاد و یا حفظ می‌کند به دست می‌آید. استاندارد SSL و TLS و TPSEC که در بخش گذشته به آن اشاره شد در زمینهٔ کنترل و حفظ امنیت داده‌ها در هنگام اتصال در شبکه به‌کار می‌روند. IEEEP2200 استانداردی است که برای معیارهای ویژگی‌های امنیتی در سیستم عامل به‌کار می‌رود.

راهنمای حفظ امنیت سیستم از تجاوز، تقلب، و استفادهٔ غیرمجاز

این راهنما شامل هفت گزینه است (اوارد، ۱۹۸۵):

۱. برنامه‌های طبقه‌بندی شده باید فقط توسط رمز عبور صحیح اجرا شوند؛

۲. در اطاق رایانه باید همیشه حداقل دو نفر حضور داشته باشند؛

۳. اشکال خاص و مهم مثل چک‌ها، اسناد بهادار باید در محل مناسب نگهداری شوند؛

۴. کنترل نهایی برنامه‌ها سبب می‌شود که فقط برنامه‌های مناسب جایگزین شوند؛

۵. به‌طور متناوب باید دیسک برنامه‌ها کنترل شود تا از کپی شدن روی سایر رسانه‌ها مطمئن شوید؛

۶. نرم‌افزارهای کتابخانه‌ای را متناوباً کنترل کنید تا از وجود یک سری کامل از منابع و هدف‌های برنامه و عملکرد اسناد موجود برای کاربران اطمینان حاصل نمایید؛

۷. نسخهٔ پشتیبان را از کل برنامه‌های مورد نیاز سیستم و اطلاعات ذخیره شده و روزآمد شده ایجاد و نگهداری کنید.

راهنمای حفظ امنیت فیزیکی

حفظ امنیت فیزیکی پایگاه شامل گزینه‌های زیر است:

۱. گیرنده‌هایی برای آگاهی سریع از گرما، آتش، دود و مانند آن روی سخت‌افزار نصب کنید؛

۲. نصب ابزارهای آتش نشانی در نزدیک مکان‌های نصب سیستم‌ها و سایر امکانات تأمینی برای این کار؛

۳. وجود خط ارتباطی مستقیم بین محل قرار گرفتن سیستم‌ها و ایستگاه پلیس یا آتش‌نشانی؛

۴. یک مخزن یا گاوصندوق ضد حریق برای نگهداری داده‌ها، نوارها، و سایر انواع مواد اطلاعاتی تهیه شود؛

۵. ابزارهای اطفاء حریق در محل مناسب و در مقابل دید قرار گیرد؛

۶. کپی‌های فایل‌های رایانه‌ای، نرم‌افزار، اسناد و تنظیمات سخت‌افزاری باید در محلی خارج از محوطهٔ سیستم‌ها قرار گرفته و نگهداری شود؛

۷. لوله‌های آب باید در جایی دور از محل قرارگرفتن رایانه‌ها و مخزن آنها قرار گیرد؛

۸. ساختمان باید در محلی مرتفع برای جلوگیری از نفوذ آب باران و غیره به داخل آن قرار گیرد؛

۹. دیوارها و سقف‌ها باید در مقابل نفوذ آب باران ایزوله شوند.

عناصر راهبردی در حفاظت از اطلاعات

توفیق در ایمن‌سازی اطلاعات منوط به حفاظت از اطلاعات و نظام‌های اطلاعاتی در مقابل حملات است. بدین منظور، از خدمات امنیتی متعددی استفاده می‌شود. خدمات انتخابی می‌بایست توانایی لازم در خصوص ایجاد یک سیستم حفاظتی متناسب، تشخیص به‌موقع حملات، و واکنش سریع را داشته باشند. بنابراین، می‌توان محور راهبرد انتخابی را بر سه مؤلفهٔ حفاظت، تشخیص، و واکنش استوار ساخت. حفاظت مطمئن، تشخیص به موقع، و واکنش مناسب از جمله مواردی است که می‌بایست همواره در ایجاد یک سیستم امنیتی رعایت گردد. سازمان‌ها و مؤسسات،

علاوه بر یکپارچگی بین مکانیزم‌های حفاظتی می‌بایست همواره انتظار حملات اطلاعاتی را داشته و خود را به ابزارهای تشخیص و روتین‌های واکنش سریع مجهز کنند تا زمینهٔ برخورد مناسب با مهاجمان و بازیافت اطلاعات در زمان مناسب فراهم گردد. یکی از اصول مهم استراتژی "دفاع در عمق" برقراری توازن میان سه عنصر اساسی: انسان، فن‌آوری، و عملیات است (کدگذاری، ۲۰۰۳). حرکت به سمت فن‌آوری اطلاعات بدون افراد آموزش دیده و روتین‌های عملیاتی که راهنمای آنان در نحوهٔ استفاده و ایمن‌سازی اطلاعات باشد محقق نخواهد شد.

الف. انسان

موفقیت در ایمن‌سازی اطلاعات با پذیرش مسئولیت و حمایت مدیریت‌های یک سازمان (معمولاً در سطح مدیریت ارشد اطلاعات) و بر اساس شناخت مناسب از تهاجمات حاصل می‌گردد. نیل به موفقیت با پیگیری سیاست‌ها، روتین‌های مربوط، تعیین وظایف و مسئولیت‌ها، آموزش منابع انسانی حساس (کاربران، مدیران سیستم)، و توجیه مسئولیت‌های شخصی کارکنان حاصل می‌گردد. دراین راستا، لازم است یک سیستم امنیتی فیزیکی و شخصی به‌منظور کنترل و هماهنگی در دستیابی به هریک از عناصر حیاتی در محیط‌های مبتنی بر فن‌آوری اطلاعات نیز ایجاد گردد. ایمن‌سازی اطلاعات از جمله مواردی است که می‌بایست موفقیت خود را در عمل و نه در حرف نشان دهد. بنابراین، لازم است که پس از تدوین سیاست‌ها و دستورالعمل‌های مربوط، پی‌گیری مستمر و هدفمند جهت اجرای سیاست‌ها و دستورالعمل‌ها دنبال گردد. بهترین استراتژی تدوین شده در صورتی که امکان تحقق عملی آن فراهم نگردد هرگز امتیاز مثبتی را در کارنامهٔ خود ثبت نخواهد کرد. با توجه به جایگاه خاص منابع انسانی در ایجاد یک محیط ایمن مبتنی بر فن‌آوری اطلاعات لازم است به موارد زیر توجه گردد (مدیریت شبکه[1] ۲۰۰۴):

- تدوین سیاست‌ها و رویّه‌ها
- ارائهٔ آموزش‌های لازم جهت افزایش دانش
- مدیریت سیستم امنیتی
- امنیت فیزیکی
- امنیت شخصی
- تدابیر لازم در خصوص پیشگیری

1. Net management

ب. فن‌آوری

امروزه از فن‌آوری‌های متعدد به منظور ارائهٔ خدمات لازم در باب ایمن‌سازی اطلاعات و تشخیص مزاحمان اطلاعاتی استفاده می‌گردد. سازمان‌ها و مؤسسات می‌بایست سیاست‌ها و فرایندهای لازم به منظور استفاده از یک فن‌آوری را تشخیص داده تا زمینهٔ انتخاب و به‌کارگیری درست فن‌آوری در سازمان ذیربط فراهم گردد. در این رابطه، می‌بایست به مواردی چون سیاست امنیتی، اصول ایمن‌سازی اطلاعات، استانداردها و معماری ایمن‌سازی اطلاعات، استفاده از محصولات مربوط به ارائه‌دهندگان شناخته شده و خوش نام، راهنمای پیکربندی، پردازش‌های لازم برای ارزیابی ریسک سیستم‌های مجتمع و به‌هم مرتبط توجه گردد. در این راستا موارد زیر پیشنهاد می‌گردد:

- دفاع در چندین محل. مهاجمان اطلاعاتی (داخلی یا خارجی) ممکن است یک هدف را از چندین نقطه مورد تهاجم قرار دهند. بنابراین، لازم است از روش‌های حفاظتی متفاوت در چندین سطح استفاده شود تا زمینهٔ عکس‌العمل لازم در مقابل انواع متفاوت حملات فراهم گردد. لذا باید به موارد زیر توجه شود:
  - دفاع از شبکه‌ها و زیرساخت. لازم است شبکه‌های محلی یا سراسری حفاظت گردند (حفاظت در مقابل حملات اطلاعاتی از نوع عدم پذیرش خدمات)
  - حفاظت یکپارچه و محرمانه برای ارسال اطلاعات در شبکه (استفاده از کدگذاری و کنترل ترافیک به منظور واکنش در مقابل مشاهدهٔ غیرفعال)
  - دفاع در محدوده‌های مرزی (به‌کارگیری دیوارهٔ آتش و سیستم‌های مزاحم‌یاب به منظور واکنش در مقابل حملات اطلاعاتی از نوع فعال)
  - دفاع در محیط‌های محاسباتی (کنترل‌های لازم به منظور دستیابی به میزبان‌ها و سرویس‌دهنده به‌منظور واکنش لازم در مقابل حملات از نوع خودی، توزیع، و مجاور)
- دفاع لایه‌ای. بهترین محصولات مربوط به ایمن‌سازی اطلاعات دارای نقاط ضعف ذاتی مربوط به خود هستند. بنابراین، همواره مهاجمان اطلاعاتی برای نفوذ در نظام‌های اطلاعاتی زمان لازم در اختیار خواهند داشت. بدین ترتیب، لازم است قبل از سوءاستفادهٔ اطلاعاتی متجاوزان، اقدامات مناسبی صورت پذیرد. یکی از روش‌های مؤثر پیشگیری در این خصوص، استفاده از دفاع لایه‌ای در مکان‌های بین مهاجمان و اهداف مورد نظر آنان است. هریک از مکانیزم‌های انتخابی می‌بایست قادر به ایجاد

موانع لازم در ارتباط با مهاجمان اطلاعاتی (حفاظت) و تشخیص به موقع حملات باشد. بدین ترتیب، امکان تشخیص مهاجمان اطلاعاتی افزایش و از سوی دیگر شانس آنها به منظور نفوذ در سیستم و کسب موفقیت کاهش خواهد یافت. استفاده از دیواره‌های آتش تو در تو (هر دیواره در کنار خود از یک سیستم تشخیص مزاحم نیز استفاده می‌نماید) در محدوده‌های داخلی و خارجی شبکه، نمونه‌ای از رویکرد دفاع لایه‌ای است. دیوارهٔ آتش داخلی ممکن است امکانات بیشتری را در رابطه با فیلترسازی داده‌ها و کنترل دستیابی به منابع موجود ارائه نمایند.

● تعیین میزان اقتدار امنیتی هریک از عناصر موجود در ایمن‌سازی اطلاعات (چه چیزی حفاظت شده و نحوهٔ برخورد با تهاجم اطلاعاتی در محلی که از عنصر مربوط استفاده شده به چه صورت است؟). پس از سنجش میزان اقتدار امنیتی هریک از عناصر مربوط، می‌توان از آن در جایگاهی که دارای حداکثر کارآیی باشد استفاده کرد.

● استفاده از مدیریت کلید مقتدر و زیرساخت کلید عمومی، که قادر به حمایت از تمام فن‌آوری‌های مرتبط با ایمن‌سازی اطلاعات بوده و دارای مقاومت مطلوب در مقابل یک مهاجم اطلاعاتی باشد.

● به‌کارگیری زیرساخت لازم به منظور تشخیص مزاحمان، و آنالیز و یکپارچگی نتایج به منظور انجام واکنش‌های مناسب در رابطه با نوع تهاجم. زیرساخت مربوط بایستی به پرسنل عملیاتی راهنمایی لازم را در مواجه با سؤالاتی نظیر: آیا من تحت تهاجم اطلاعاتی قرار گرفته‌ام؟ منبع تهاجم چه کسی است؟ به چه فرد دیگری تهاجم شده است؟ راه‌حل‌ها و راهکارهای من در این رابطه چیست؟ را ارائه نماید.

ج. عملیات

منظور از عملیات، مجموعه فعالیت‌های لازم به منظور نگهداری وضعیت امنیتی یک سازمان است. در این رابطه به موارد زیر توجه گردد:

● پشتیبانی ملموس و به‌هنگام‌سازی سیاست‌های امنیتی؛

● اصل تغییرات لازم با توجه به روند تحولات مرتبط با فن‌آوری اطلاعات. در این رابطه محاسبات داده‌های مورد نظر جمع‌آوری تا زمینهٔ تصمیم‌سازی مناسب برای مدیریت فراهم گردد (تأمین اطلاعات ضروری برای مدیریت ریسک).

● مدیریت وضعیت امنیتی با توجه به فن‌آوری‌های استفاده شده در رابطه با ایمن‌سازی اطلاعات (نصب patch امنیتی، به‌هنگام سازی ویروس‌یاب‌ها، پشتیبانی

لیست‌های کنترل دستیابی)؛

- ارائهٔ خدمات مدیریتی اساسی و حفاظت از زیر ساخت‌های مهم (خصوصاً زیرساخت‌هایی که برای یک سازمان منتهی به درآمد می‌گردد)؛
- ارزیابی سیستم امنیتی؛
- هماهنگی و و اکنش در مقابل حملات جاری؛
- تشخیص حملات و ارائهٔ هشدار و پاسخ مناسب به منظور ایزوله کردن حملات و پیشگیری از موارد مشابه؛
- بازیافت و برگرداندن امور به حالت اولیه (بازسازی).

مآخذ

خامدا، زهرا (۱۳۸۲). "ارزیابی وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی شهر تهران». پایان نامهٔ کارشناسی ارشد کتابداری و اطلاع‌رسانی. دانشگاه تهران، دانشکده علوم تربیتی.

Award, Elios, M. (1985). *System Analysis and Design*. [2nd ed], U.S.A. : Irwin.inc.

"Encryption of data at rest: database encryption" (2003). [on-line] Available: http://www.Appsecinc.com.

"Developing a database encryption strategy" (2002). [on-line] Availabe: http:// www. rsasecurity.com.

Loney, Matt (2002). "Your worrst security treat: Employees". [on-line] Available: http://nsc.sharif.edu/amn.

"Net management" (2004). [online] Available: http://www.nsc.sharif.edu/amn