شماره ثبت: ۷۴۸۰
شماره شناسه ملی: ۱۰۸۶۰۱۶۶۳۲۶

مروری بر مفاهیم امنیت اطلاعات و اصول سه‌گانه‌ی آن

گردآوری و نگارش:

محمدحسین محمدیان سرچشمه، شرکت پیشگامان کی‌پاد

mohammadian@kaipod.ir

چکیده:

در این مقاله، مفاهیم اساسی امنیت اطلاعات شامل تعاریف امنیت، تهدیدات و انواع آن، خدمات امنیتی و انواع آن و اصول سه‌گانه‌ی امنیت اطلاعات به همراه حملات مبتنی بر آن، بیان شده است.

۱. مقدمه

پیرامون زندگی هر بشر امروزی کامپیوترهای شخصی، سیستم‌های متعدد تلفن ثابت و همراه، دستیاران دیجیتالی، کامپیوترهای کیفی، خودپرداز بانک، انواع و اقسام کارت‌های اعتباری، کارت‌های هوشمند و انواع دیگری از این وسایل و ابزار، وجود دارد. وقتی ساختار زندگی سنتی درحال استحاله به الگوهای مدرن باشد، بزهکاری‌های اجتماعی نیز رنگ و بوی مدرنیته به خود می‌گیرد. در سال ۱۹۸۸ یک دانشجوی کارشناسی دانشگاه کرنل، اولین کرم کامپیوتری را به جان کامپیوترها انداخت. هر چند نیت واقعی او صرفاً اثبات برتری هوش و خرد انسان در مقابل ماشین و صرفاً یک تفریح بی مزه‌ی علمی بود ولی سرآغاز ایجاد یک جبهه‌ی جدید علیه اعصاب و روان اجتماع شد که بعداً به دلیل تنیده شدن کامپیوترها در تار و پود زندگی مردم، خسارت‌های مالی و معنوی هنگفتی نیز در پی داشت. تا جایی که در سال ۱۹۹۴ کلاهبرداری اینترنتی یک گروه روس منجر به ۱۰.۴ میلیون دلار خسارت به Citibank شد. پس از سال ۲۰۰۰ نیز تقریباً هر سال بیش از یک میلیون حمله علیه اطلاعات مؤسسات و سازمان‌های دولتی، خصوصی، مراکز مالی و اعتباری، شرکت‌های خدماتی و تجارت الکترونیکی گزارش شده است. این تعداد از حملات فقط آن‌هایی بوده که رسماً اعلام و گزارش شده است، در حالی‌که بسیاری از اخلال‌گری‌ها هرگز در جایی ثبت نمی‌شوند. اگر رخدادهای ناخوشایند و خطرناک را در یکی از رده‌های دسترسی غیرمجاز به داده‌ها، نشت اطلاعات محرمانه، از دسترس خارج شدن خدمات یک سرور، تغییر مخفیانه در اطلاعات، سرقت اطلاعات، نابودشدن اطلاعات، جعل اطلاعات، اختلال در عملکرد صحیح ماشین کاربران و هر نوع تعرض به حریم داده‌های یک ماشین تلقی کنیم، امنیت اطلاعات عبارت است از مجموعه‌ی تمهیدات و روش‌هایی که در یکی از موارد زیر قرار گیرد:

- تمهیداتی که اطمینان می‌دهند رخدادهای ناخوشایند هرگز حادث نمی‌شوند.
- تمهیداتی که احتمال وقوع رخدادهای خطرناک را کاهش می‌دهند.
- تمهیداتی که نقاط حساس به خرابی و استراتژیک را در سطح شبکه توزیع کند.
- تمهیداتی که اجازه می‌دهند به محض وقوع رخدادهای خطرناک، شرایط در اسرع وقت و با کمترین هزینه به شکل عادی برگردد و کمترین خسارت را بر جا بگذارد.

در این مقاله به مروری بر مفاهیم امنیت اطلاعات و به‌ویژه، اصول سه‌گانه‌ی آن خواهیم پرداخت.

۲. مفاهیم اساسی امنیت اطلاعات

درتعریفی عام، امنیت اطلاعات یعنی حفاظت از اطلاعات و سیستم‌های اطلاعاتی از فعالیت غیرمجاز. این فعالیت‌ها عبارتند از: دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری. به‌علاوه در تعریف اصطلاح امنیت سیستم و شبکه می‌توان گفت: امنیت، عبارتست از مکانیزم‌های پیشگیری یا کاهش احتمال وقوع رخدادهای خطرناک و جلوگیری از تمرکز قدرت در هر نقطه از سیستم یا شبکه و احیای سیستم یا شبکه در حین وقوع رخدادهای ناخوشایند (وقتی که رخدادهای خطرناک حادث می‌شوند). هر عاملی که به‌طور بالقوه بتواند منجر به وقوع رخدادی خطرناک بشود یک تهدید امنیتی به‌شمار می‌آید. تهدیدهای امنیتی می‌توانند از عوامل زیر ناشی شوند:

- تهدیدات طبیعی: این تهدیدها از عواملی مثل زلزله، سیل و سایر سوانح طبیعی مشابه آن از قوّه به فعل می‌رسند. این تهدیدها همان‌گونه که زندگی را هدف گرفته‌اند، می‌توانند منجر به نابودشدن یا افشای اطلاعات محرمانه و اختلال در سرویس‌دهی مؤلفه‌های اساسی سیستم‌های امنیتی یا شبکه شوند.
- تهدیدات غیرعمد: تهدیدات غیرعمد از اشتباهات سهوی و ناخودآگاه عوامل انسانی (مدیران شبکه، کارکنان و کاربران) ناشی می‌شود و می‌تواند منجر به افشاء یا نابودی اطلاعات یا اختلال در خدمات معمول شبکه و سیستم‌های امنیتی شود.
- تهدیدات عمدی: تهدیدات عمدی(که بیشترین خسارت و دشوارترین راه مقابله را دارند) عبارتست از هرگونه اقدام برنامه ریزی شده جهت افشاء، نابودی یا تغییر در داده‌های حیاتی شبکه و سیستم‌های امنیتی یا ایجاد اختلال در خدمات معمول سرورها. به‌طور عام هرگونه اقدام برنامه‌ریزی شده برای تحقق یک رخداد خطرناک، یک تهدید امنیتی تلقی می‌شود.

در مقابله با تهدیدات امنیتی، اصطلاح خدمات امنیتی وجود دارد که بنا به تعریف، پیاده سازی هر نوع مکانیزم امنیتی و ارائه‌ی آن‌ها به کاربران به نحوی که میزان خطر را به حداقل برساند،

خدمات امنیتی نام دارد. عمده‌ترین خدمات امنیتی در حوزهٔ امنیت اطلاعات که سه مورد اول جزء اصول سه‌گانهٔ امنیت اطلاعات (CIA Triad) نامیده می‌شوند، عبارتند از:

- محرمانه ماندن یا محرمانگی اطلاعات (Confidentiality): به مجموعه‌ی مکانیزم‌هایی که تضمین می‌کند داده‌ها و اطلاعات مهم کاربران از دسترس افراد بیگانه و غیرمجاز دور نگهداشته شود، سرویس محرمانگی اطلاق می‌شود. این سرویس‌ها عموماً با روش‌های رمزنگاری (Cryptography) تحقق می‌یابند. روش‌های مختلف رمزنگاری اطلاعات، زیربنای مابقی سرویس‌های امنیتی است. به بیان ساده‌تر، محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیر مجاز. به عنوان مثال، برای خرید با کارت‌های اعتباری بر روی اینترنت نیاز به ارسال شماره کارت اعتباری از خریدار به فروشنده و سپس به مرکز پردازش معامله است. در این مورد شماره کارت و دیگر اطلاعات مربوط به خریدار و کارت اعتباری او نباید در اختیار افراد غیرمجاز بیفتد و این اطلاعات باید محرمانه بماند. در این مورد برای محرمانه نگهداشتن اطلاعات، شماره کارت رمزنگاری می‌شود و در طی انتقال یا جاهایی که ممکن است ذخیره شود (در پایگاه‌های داده، فایل‌های ثبت وقایع سیستم، پشتیبان‌گیری، چاپ رسید، و غیره) رمزشده باقی می‌ماند. همچنین دسترسی به اطلاعات و سیستم‌ها نیز محدود می‌شود. اگر فردی غیر مجاز به شماره کارت به هر نحوی دست یابد، نقض محرمانگی رخ داده است.

نقض محرمانگی ممکن است اشکال مختلف داشته باشد. مثلاً اگر کسی به هرنحوی اطلاعات محرمانه‌ی نمایش داده شده روی صفحه‌ی نمایش کامپیوتر شما را بخواند، یا فروش یا سرقت کامپیوتر لپ‌تاپ حاوی اطلاعات حساس، یا دادن اطلاعات محرمانه از طریق تلفن، همه موارد نقض محرمانگی است.

- تضمین صحت یا جامعیت اطلاعات (Integrity): مجموعه‌ی مکانیزم‌هایی که از هرگونه تحریف، دستکاری، تکرار، حذف یا آلوده سازی داده‌ها پیشگیری می‌کنند یا حداقل باعث کشف چنین اقداماتی می‌شوند، سرویس تضمین صحت یا جامعیت اطلاعات نامیده می‌شود. به بیان ساده‌تر، جامعیت یا یکپارچه بودن یعنی جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دستکاری غیر مجاز اطلاعات. یکپارچگی وقتی نقض می‌شود که اطلاعات در حین انتقال بصورت غیرمجاز تغییر داده می‌شود. سیستم‌های امنیت اطلاعات به‌طور معمول علاوه بر محرمانه بودن اطلاعات، یکپارچگی آنرا نیز تضمین می‌کنند.

- قابل دسترس بودن (Availability): اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند. این بدان معنی است که، باید از درست کار کردن و جلوگیری از اختلال در سیستم های ذخیره و پردازش اطلاعات و کانال های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد. سیستم‌های با دسترسی بالا در همه حال حتی به علت قطع برق، خرابی سخت‌افزار، و ارتقاء سیستم در دسترس باقی می‌ماند. یک از راه‌های از دسترس خارج کردن اطلاعات و سیستم اطلاعاتی درخواست بیش از طریق خدمات از سیستم اطلاعاتی است که در این حالت چون سیستم توانایی و ظرفیت چنین حجم انبوده خدمات دهی را ندارد از سرویس دادن به‌طور کامل یا جزیی عاجز می‌ماند.

- احراز هویت (Authentication): مجموعه‌ی مکانیزم‌هایی که این امکان را فراهم می‌کنند که بتوان مبدأ (صاحب) واقعی یک پیام، سند یا تراکنش (Transaction) را بدون ذره‌ای تردید یا ابهام مشخص کرد، سرویس احراز هویت نامیده می‌شود. به بیان ساده‌تر، احراز هویت، تشخیص هویت کسی یا چیزی است. این هویت ممکن است توسط فرد ادعا شود و یا ما خود تشخیص دهیم. اگر یک فرد می‌گوید : "سلام، نام من علی است" این یک ادعا است. اما این ادعا ممکن است درست یا غلط باشد. قبل از این که به علی اجازه‌ی دسترسی به اطلاعات حفاظت شده داده شود، ضروری است که هویت این فرد بررسی شود که او چه کسی است و آیا همانی است که ادعا می‌کند یا خیر.
- غیرقابل انکارساختن پیام‌ها (Non-Repudiation): مجموعه‌ی مکانیزم‌هایی که به پیام‌ها وتراکنش‌ها، پشتوانه‌ی حقوقی می‌بخشد و اجازه نمی‌دهد که فرستنده به هر طریق ارسال پیام خود را انکار کند و یا گیرنده منکر دریافت آن شود به سرویس غیرقابل انکارساختن پیام‌ها شهرت دارد.
- کنترل دسترسی (Access Control): مکانیزم‌هایی که دسترسی به کوچکترین منابع اشتراکی شبکه را تحت کنترل درآورده و هرمنبع را بر اساس سطح مجوز کاربران و پروسه‌ها در اختیار آن‌ها قرار می‌دهد، کنترل دسترسی خوانده می‌شود. به بیان دیگر برای حفظ امنیت اطلاعات، باید دسترسی به اطلاعات کنترل شود. افراد مجاز باید و افراد غیرمجاز نباید توانایی دسترسی داشته باشند. دسترسی به اطلاعات حفاظت شده باید به افراد، برنامه های کامپیوتری، فرآیندها و سیستم‌هایی که مجاز به دسترسی به اطلاعات هستند، محدود باشد. این مستلزم وجود مکانیزم‌هایی برای کنترل دسترسی به اطلاعات حفاظت شده می‌باشد. پیچیدگی مکانیزم‌های کنترل دسترسی باید مطابق با ارزش اطلاعات مورد حفاظت باشد. اطلاعات حساس‌تر و با ارزش‌تر نیاز به مکانیزم کنترل دسترسی قوی‌تری دارند. اساس مکانیزم‌های کنترل دسترسی بر دو مقوله‌ی احراز هویت و تصدیق هویت است. در سیستم‌های کامپیوتری امروزی، نام کاربری رایج‌ترین شکل احراز و

کلمه‌ی عبور رایج‌ترین شکل تصدیق هویت است. نام کاربری و کلمه‌ی عبور به اندازه‌ی کافی به امنیت اطلاعات خدمت کرده‌اند اما در دنیای مدرن با سیستم‌های پیچیده‌تر از گذشته، دیگر کافی نمی‌باشند. نام کاربری و کلمه‌ی عبور به تدریج با روش‌های پیچیده‌تری جایگزین می‌شوند.

پس از آن‌که فرد، برنامه یا کامپیوتر با موفقیت احراز و تصدیق هویت شد، سپس باید تعیین کرد که او به چه منابع اطلاعاتی و چه اقداماتی روی آن‌ها مجاز به انجام است (اجراء، نمایش، ایجاد، حذف، یا تغییر). این عمل را صدور مجوز گویند. صدور مجوز برای دسترسی به اطلاعات و خدمات کامپیوتری با برقراری سیاست و روش‌های مدیریتی آغاز می‌شود. سیاست دسترسی تبیین می‌کند که چه اطلاعات و خدمات کامپیوتری می تواند توسط چه کسی و تحت چه شرایطی دسترسی شود. مکانیسم‌های کنترل دسترسی سپس برای به اجراء درآوردن این سیاست‌ها نصب و تنظیم می‌شوند. رویکردهای کنترل دسترسی مختلفی وجود دارند. سه رویکرد شناخته شده وجود دارند که عبارتند از: رویکرد صلاحدیدی، غیرصلاحدیدی و اجباری. در رویکرد صلاحدیدی خالق یا صاحب منابع اطلاعات قابلیت دسترسی به این منابع را تعیین می‌کند. رویکرد غیر صلاحدیدی تمام کنترل دسترسی متمرکز است و به صلاحدید افراد نیست. در روش اجباری، دسترسی به اطلاعات و یا محروم کردن بسته به طبقه بندی اطلاعات و رتبه فرد خواهان دسترسی دارد. تمام خدمات امنیتی (شامل محرمانگی، احراز هویت، غیر قابل انکار بودن و صحت پیام‌ها) با این فرض طراحی و پیاده‌سازی می‌شوند که تهدیدهای چهارگانه‌ی زیر همیشه علیه آن‌ها وجود دارند و هر لحظه ممکن است اتفاق بیفتد:

- استراق سمع (Interception): هرگاه یک شخص غیرمجاز به هر نحو بتواند نسخه‌ای از داده‌های در حال جریان بین مبدأ و مقصد را به نفع خود شنود کند، حمله‌ی استراق سمع به‌وقوع پیوسته است.
- دستکاری (Modification): هرگاه داده‌های در حال جریان بین مبدأ و مقصد توسط شخص غیرمجاز به هر نحو دستکاری یا تحریف شود، حمله‌ی دستکاری داده‌ها رخ داده است.
- جعل (Fabrication): هرگاه یک شخص غیرمجاز اقدام به تولید پیام‌های ساختگی کرده و ارسال آن‌ها را به شخص مجاز دیگری نسبت بدهد حمله‌ی جعل و ارسال داده‌های ساختگی به‌وقوع پیوسته است.
- وقفه (Interruption): هرگاه کسی بتواند سیستم یا سرویسی را در شبکه از کار بیندازد حمله‌ی وقفه رخ داده است.

« استراق سمع»، تهدیدی علیه سرویس محرمانگی اطلاعات (Confidentiality)، « دستکاری» تهدیدی علیه سرویس صحت یا جامعیت اطلاعات (Integrity)، « جعل» تهدیدی علیه سرویس

احراز هویت (Authentication) و « وقفه» تهدیدی علیه قابلیت دسترسی دائم (Availability) به‌حساب می‌آید.

در جدول زیر می‌توان کلیات اصول سه‌گانهٔ امنیت اطلاعات را در موارد کاربر، شبکه و داده مشاهده کرد :

	قابل دسترس بودن	محرمانگی	جامعیت
کاربر	تصدیق هویت	کنترل‌های دسترسی نقش محور	احراز هویت
شبکه	کنترل‌های دسترسی اجباری	دیواره آتش،لایه سوکت امن (SSL)	آنتی‌ویروس،مدیریت کنترل تغییر
داده	کنترل‌های دسترسی احتیاطی	رمزنگاری	–

منابع:

1. Kinamik Whitepaper: The CIA triad: Have you thought about Integrity?
۲. امنیت داده‌ها، دکتر علی ذاکرالحسینی، مهندس احسان ملکیان، انتشارات نص.