آشنایی با امنیت مجازی و عوامل تهدید کننده آن

مهندس مسعود احمدی- اداره حفاظت اسناد رایانه و داده ها

مفهوم امنیت برای بشر از ابتدا مفهومی کاملا شناخته شده و حیاتی بوده است. امنیت جانی و فیزیکی اساس امنیت برای او به شمار می رفته است. با گسترش جوامع و به وجود آمدن مفاهیم جدید، حوزه امنیت نیز گسترش یافت. امنیت غذایی، امنیت منابع، امنیت ملی، امنیت اقتصادی، امنیت حریم خصوصی و ... نیز به دغدغه های امنیتی او افزوده شدند. در چند سال اخیر ورود تکنولوژی اطلاعات به زندگی بشر، تغییر بسیار زیاد و ملموسی را در مناسبات و معادلات ایجاد نموده است. به تبع این تغییر گسترده، مفهوم جدید امنیت اطلاعات به حوزه های قبلی امنیت اضافه شد به طوری که به دلیل ورود تکنولوژی اطلاعات به بخشهای مختلف زندگی، نادیده گرفتن امنیت اطلاعات می تواند دیگر حوزه های امنیت مانند امنیت اقتصادی، حریم خصوصی و حتی امنیت ملی را به شدت تحت تاثیر قرار دهد.

مفاهیم امنیت در دنیای واقعی با آنچه که در دنیای مجازی وجود دارد شباهت بسیار زیادی دارند ولی ساز و کار پیاده سازی آنها متفاوت است. برای مثال در دنیای واقعی از کلید فلزی برای دسترسی به یک محیط امن نگهداری اسناد استفاده می شود ولی در دنیای مجازی از رمز عبور و شناسه کاربری برای دسترسی به اسناد الکترونیکی استفاده می کنیم. و یا در دنیای واقعی ممکن است از امضای روی چک برای تایید هویت و صحت یک برگ چک استفاده شود در حالی که در دنیای مجازی از امضای دیجیتال که مبتنی بر الگوریتم های رمزنگاری است و همان کار امضای واقعی را با ارائه امنیت بسیار بیشتری انجام می‌دهد استفاده می شود. تهدیداتی که در دنیای واقعی رخ می دهد نیز شباهت بسیاری با حملات مشابه در دنیای مجازی دارد. برای مثال در دنیای واقعی ممکن است کسی به اصطلاح فالگوش بایستد و سخنان شما را از پشت در بشنود و به اطلاعات شما در یک گفتگو دست یابد. نمونه این تهدید را در دنیای مجازی نیز داریم به طوری که کامپیوتر یک هکر می تواند از اطلاعات خروجی کامپیوتر شما در شبکه یک کپی هم برای خودش بر دارد و به این صورت به اطلاعات شما دست پیدا کند. با این حال تفاوتهایی عمده در این میان وجود دارند.

اول اینکه نقض امنیت در دنیای مجازی بسیار سریع اتفاق می افتد یعنی پیش از آنکه متوجه شوید چه اتفاقی رخ داده است و بتوانید جلوی آن را بگیرید کار از کار گذشته است. نمونه آن هم کلاهبرداری اینترنتی است که در آن وجه الکترونیکی در کسری از ثانیه از یک شعبه بانک یا صرافی در یک کشور به بانکی در کشور دیگر منتقل می شود.

دوم اینکه در دنیای مجازی نیاز به حضور فیزیکی برای نقض امنیت وجود ندارد. اگر قبلا شخص برای سرقت پول باید به شعبه می آمد و خطرات بسیاری را می پذیرفت، امروز می‌تواند در هر جایی از دنیا و تنها از طریق اینترنت با اتصال به سیستم های بانکی حتی بدون آنکه شناسایی شود همان کار سارقان قدیمی را با دردسری بسیار کمتر انجام دهد.

سوم اینکه دنیای مجازی، محیط و ابزار بسیار قدرتمندی را در اختیار ناقضان امنیت می‌گذارد. ابزارهایی که امروز در محیط مجازی وجود دارند حتی به غیر حرفه‌ای ها هم اجازه می دهد تا با استفاده از این ابزارهای پیچیده امنیت یک مجموعه را به خطر بیاندازند.

برای درک بهتر امنیت با سه مفهوم بسیار مهم در این حوزه آشنا می شوید. این سه مفهوم، اهداف اصلی در یک طرح امنیتی به شمار می آیند و تمام مکانیزمها، کنترلها، و روالهای امنیتی که سازمانها بکار می برند برای تامین آنهاست. این سه هدف عبارتند از:

۱- محرمانگی : به این معنی که اطلاعات در دسترسی افراد غیر مجاز (چه عمدی و چه غیر عمدی) قرار نگیرد و از آن نسخه برداری نگردد.

۲- یکپارچگی (صحت و تمامیت) : بدین معنی که از اطلاعات در برابر تغییر (جایگزینی و یا حذف بخشی از اطلاعات) توسط افراد غیر مجاز محافظت شود.

۳-در دسترس بودن : بدین معنی که هر وقت به اطلاعات نیاز است بتوان به موقع به آنها دسترسی داشت.

این سه هدف به مانند سه ضلع یک مثلث هستند که نقض هر یک از آنها نقض امنیت است. در یک سیستم نظامی ممکن است محرمانگی و یکپارچگی نقش پررنگتری از دسترسی پذیری اطلاعات داشته باشند و در یک سیستم بانکی بهترین حالت، توجه برابر به این سه هدف است. یعنی محرمانگی و یکپارچگی نباید به اندازه ای زیاد باشد که دسترسی پذیری اطلاعات را کم کند و یا برای آنکه سرویسهای بانکی با سرعت بیشتری ارائه شوند، محرمانگی، صحت و تمامیت اطلاعات را قربانی کنیم. علاوه بر اهداف امنیتی فوق برخی متخصصان دو مفهوم دیگر را نیز جزو اهداف اصلی می دانند. این دو هدف عبارتند از:

تصدیق هویت : بدین معنی که اطمینان حاصل کنیم در یک تبادل اطلاعات طرف مقابل همان است که واقعا باید باشد و خودش را جای کسی دیگر معرفی نکرده است. این فرآیند یکی از مهمترین فرآیندها در یک سیستم امنیتی است.

عدم انکار: اطمینان از این است که طرفین مبادله کننده پیام نتوانند سند و یا پیام فرستاده شده خود را انکار کنند.

نقض هر یک از اهداف امنیتی فوق بوسیله حملاتی بر روی سیستم انجام می شود. یک حمله زمانی رخ می دهد که یک شخص یا گروهی از اشخاص تلاش می‌کنند به سیستم اطلاعاتی دسترسی پیدا کرده، آن را تغییر دهند و یا به آن آسیب برسانند.

کسانی که به سیستم اطلاعاتی حمله می کنند شاید از سر تفریح این کار را انجام دهند یا ممکن است تبهکارانی باشند که قصد سرقت اطلاعات را دارند و یا افراد و گروههایی باشند که به قصد اهداف سیاسی و یا انجام عملیاتی تروریستی این حملات را ترتیب می دهند.

حملات به روشهای مختلف و به دلایل مختلفی رخ می دهند. این حملات عمدتا در سه دسته زیر قرار می گیرند :

۱-حملات دسترسی: حملاتی هستند که در آن سعی می شود به منابع و اطلاعات دسترسی غیر مجاز شود.

هدف این نوع حملات نقض محرمانگی سیستم است. نمونه این نوع حملات می تواند آشغالگردی (جمع آوری اطلاعات از طریق گشتن در زباله ها برای بدست آوردن کاغذ، فلاپی و یا سی دی که حاوی اطلاعات باشد) و یا استراق سمع (شنود اطلاعات عبوری شبکه بوسیله کامپیوتر و یا وسیله ای در شبکه) باشد.

دیگر نمونه جالب از این نوع حملات، حمله موسوم به مهندسی اجتماعی است که در این نوع حمله، شخص حمله کننده سعی می کند از طریق ایجاد دوستی یا روابط عاطفی و احساسی با افراد دارای حق دسترسی مجاز، به اطلاعات سیستم دسترسی پیدا کند. در این نوع حملات، حمله کننده سعی می کند مخفی باشد. بنابراین کشف این نوع حملات کار مشکلی است.

۲-حملات تغییر و انکار: هدف از این حملات نقض یکپارچگی سیستم است.

حمله تغییر شامل پاک کردن ، اضافه کردن و یا تغییر اطلاعات مبادله شده می باشد به صورتی که برای گیرنده کاملا واقعی و درست به نظر برسد. نمونه معمول این نوع حملات تغییر صفحه اصلی وب سایت ها است. تغییر رقم یک چک در یک شبکه بانکی نیز در این دسته از حملات قرار می گیرد.

حملات انکار در این نوع حملات، شخص، انجام تمام و یا بخشی از عملیاتی را که انجام داده است انکار می کند. برای مثال یک مشتری بانک را در نظر بگیرید که قبول نمی کند به صورت آنلاین بخشی از وجه را از حساب خود انتقال داده و ادعا می‌کند این اشتباه بانک بوده است. این نوع حملات معمول ترین نوع حملات در سیستم های مالی به حساب می آیند.

۳-حملات مختل کننده سرویس: حملاتی هستند که در آن سعی می شود سرویس های ارائه شده را قطع کنند و یا از دسترسی فرد مجاز به اطلاعات جلوگیری بعمل آورند. هدف از این نوع حملات نقض دسترسی پذیری سیستم است. جلوگیری از ارائه سرویس می تواند با خرابی نرم افزار، سخت افزار و یا حتی خرابی شبکه مخابراتی انجام شود. در این نوع حمله نیازی نیست تمام منابع مختل شوند بلکه خرابی بخشی از منابع برای انجام آن نیز کافی می باشد. برای مثال جهت اختلال در عملیات خدمات اینترنتی ارائه شده از سوی یک بانک، خرابی صفحه اصلی سایت کافی است و دیگر نیازی به حمله به سخت افزار و یا نرم افزار وجود ندارد. در نمونه دیگر از این نوع حملات، در خواستهای بسیار زیادی به سوی کامپیوترهای خدمات دهنده سرویس ارسال می‌کنند تا عملا این کامپیوترها را از ارائه خدمات به درخواستهای دیگر باز دارند. در ساده ترین حالت، این حمله از طریق یک کامپیوتر انجام می شود. در حمله بزرگتر و پیچیده تری که موسوم به حمله اختلال سرویس توزیع شده می باشد چند کامپیوتر همزمان به کامپیوتر مقصد حمله می کنند. سرعت و حجم آسیب این نوع حمله بسیار بالاست. این حمله را که موسوم به DDOS است در مقاله قبلی که در همین مجله چاپ شده تشریح کرده ایم.

به خاطر داشته باشید که علاوه بر این حملات، حملاتی نیز وجود دارند که از ترکیب حملات فوق ایجاد می شوند و برای سادگی مطلب به آنها اشاره ای نشده است.

در این مقاله سعی شد تا به دسته بندی و شناخت کلی حملات اشاره شود. برای پیشگیری و یا مقابله با این حملات راه کارهای مختلفی از جمله رمزنگاری، کنترل فیزیکی، کنترل پرسنلی، کنترل حق دسترسی، افزونگی و .... وجود دارد. انتخاب و پیاده سازی این کنترل ها با توجه به نیاز سازمان، نوع کسب و کار آن و تهدیدات گسترده و متنوعی که متوجه آن سازمان است، نیاز به یک سیستم مدیریت جامع امنیت اطلاعات دارد. انشاء ا... در مقالات بعد به برخی روشهای برخورد با این تهدیدات اشاره خواهیم کرد.