امنیت در فناوری اطلاعات

استفاده از رایانه در کسب و کار از زمانی متحول و فراگیر شد که دسترسی به اطلاعات با سرعت بالا و هزینه کم امکان پذیر گردید. این تحول به شرکت‌هایی که در گذشته از رایانه برای واژه پردازی و یا ذخیره اطلاعات استفاده می کردند، اجازه داد که رایانه های خود را به صورت شبکه درآورند و آن شبکه را به اینترنت متصل کنند. نیروهای رقابتی و شرایط سریع کسب و کار، سازمان‌ها را مجبور ساخته است که برای بقا، شبکه های خود را به روی دیگران باز کنند و تا جایی که ممکن است از راه کارهای الکترونیک برای کسب و کار استفاده کنند درحالی که این تحولات منافع بسیاری در گسترش تجارت امکان کار در خارج از اداره و حمایت نیروهای فروش در خارج از شرکت را برای بسیاری از شرکت‌ها ایجاد می کند. متاسفانه خطراتی مانند ویروس‌های رایانه ای و خرابکاری‌های رایانه‌ای را نیز به همراه خود می آورد.

۱- امنیت اطلاعات

به طورکلی امنیت اطلاعات در سه اصل زیر خلاصه می شود:

- محرمانه بودن: بدین معنی که فقط افراد مجاز حق دسترسی به اطلاعات را داشته باشند.

- صحت و استحکام: بدین معنی که اطلاعات دست نخورده بماند و تغییر در آنها فقط توسط افراد مجاز در صورت لزوم به صورت درست و قابل پیگیری انجام شود.

- دردسترس بودن: بدین معنی که اطلاعات درموقع نیاز به صورت قابل استفاده دردسترس قرار گیرد.

۲- تهدیدها

تهدیدهای امنیتی مربوط به اطلاعات رایانه ای و یا به عبارتی حملات رایانه‌ای شامل مواردی می شود که حداقل یکی از اصول سه گانه امنیت را مخدوش سازد. هدف از یک حمله رایانه ای در کنترل گرفتن یک یا چند رایانه به منظور از کارانداختن، مخدوش کردن یا سوءاستفاده از اطلاعات موجود در آنها ویا به کارگیری آنها برای خرابکاری در رایانه‌های دیگر است.

کسانی که به این حملات دست می‌زنند یا به اصطلاح خرابکارها معمولا" سه دسته هستند:

۱- افراد آماتور که اغلب اطلاعات دقیقی از نحوه کار سیستم های عامل و فناوری اطلاعات نداشته و صرفا" برای تفریح از برنامه‌ها و ابزارهای از پیش تهیه شده برای دسترسی به رایانه‌های محافظت نشده استفاده می‌کنند این افراد را SCRIPT KIDDIES یا SREKCARC می‌نامند.

۲-خرابکاران حرفه ای که معمولا" در ازای دریافت پول اطلاعات ذیقیمت شرکتها را دراختیار رقبای آنها یا گروههای ذینفع قرار می‌دهند و یا در سیستم شرکتهای رقیب خرابکاری می‌کنند. این افراد در امور فناوری اطلاعات وارد بوده واز آسیب‌پذیریهای سیستم های عامل و برنامه‌های مورداستفاده مطلع بوده و قادرند ردپای خود را ناپدید سازند. این افراد را در اصطلاح هکرها (HACKERS) می‌گویند.

۳- کارکنان فعلی شرکتها و یا کارکنان سابق آنها که به نحوی از شرکت مذکور نارضایتی داشته و به قصد انتقامجویی و یا صدمه زدن در سیستم‌های اطلاعاتی شرکت با استفاده از دانش و اطلاعات خود از سیستم‌های موردنظر به خرابکاری دست می زنند.

حملات رایانه ای معمولا" در سه مرحله انجام می شود:

مرحله اول – شناسایی و جمع آوری اطلاعات درمورد رایانه هدف؛

مرحله دوم – یافتن نقاط آسیب پذیر و راههای واردشدن به سیستم به عنوان یک کاربر مجاز؛

مرحله سوم – درصورت امکانپذیر نبودن مرحله دوم تلاش برای دسترسی به رایانه هدف از طریق دیگر و بدون استفاده از مشخصات کاربران مجاز انجام می پذیرد.

۲-۱ انواع تهدیدهای رایانه ای

تهدیدهای رایانه ای به صورت زیر دسته‌بندی می شوند:

۱ – ویروس ها و کرم‌ها : این ها برنامه‌های کوچکی هستند که ازطریق پست الکترونیک و یا نرم افزارهای آلوده به این ویروس ها وارد یک رایانه شده و در آنجا به صدمه زدن و خرابکاری در برنامه ها و یا اطلاعات رایانه مذکور می پردازند.

۲ – اسب تروا (TROJAN HORSE) :برنامه‌هایی هستند که ظاهرا" ماهیت خرابکاری نداشته به صورت برنامه‌های بازی و یا کمکی وارد سیستم شده و سپس در خفا به کارهای غیرمجاز و کنترل رایانه و سرقت اطلاعات محرمانه و یا شخصی کاربر می‌پردازند.

۳ – از کارانداختن (DENIAL OF SERVICE) : این عمل با ایجاد تعداد زیادی تقاضای سرویس از یک سیستم انجام شده و درنتیجه سیستم مذکور کارایی خود را از دست داده و یا از کار می افتد. درنتیجه سیستم نمی تواند خدمات لازم را به مشتریان واقعی خود ارائه کند. نظیر مشغول کردن یک تلفن.

۴ – شنود اطلاعات : در این مورد در مسیر ارتباطات ازطرق گوناگون اطلاعات مبادله شده سرقت و یا شنود می شوند.

۵ – وب سایت های تقلبی (PHISHING) : در این مورد یک وب سایت تقلبی با شکل و قیافه و امکانات کاملا" مشابه به یک وب سایت واقعی طراحی و دراختیار کاربران قرار می‌گیرد و بدین‌وسیله اطلاعات شخصی و محرمانه کاربران را به سرقت می برند.

۳- محافظت

برای محافظت از سیستم‌های اطلاعاتی رایانه‌ای شناسایی قسمتهای مختلف سیستم و آسیب پذیریهای موجود در آن ضروری است. پس از شناسایی و رفع آسیب پذیریهای سیستم باید مرتباً مواظب بود که آسیب پذیریهای جدید به وجود نیاید و به طور متناوب سیستم را بررسی کرد تا از امنیت آن مطمئن شد درحالی که هیچگاه نمی‌توان صددرصد از امنیت یک سیستم مطمئن بود ولی با اقدامات زیر می توان تا حد بسیار بالایی امنیت وحفاظت از یک سیستم را فراهم ساخت:

۱ – تهیه نقشه و راهنمای سیستم: این کار شامل شناسایی رایانه ها و شبکه‌های متصل و غیرمتصل به اینترنت و به خط تلفن و یا بی سیم، نرم افزارها و سیستم های عامل مورداستفاده نرم افزارهای ضدویروس و محافظ و اطلاعات و برنامه های حساس تجاری خواهدشد؛

۲ – تهیه سیاست امنیتی: این کار شامل تعریف سیاستهای مربوط به استفاده از رایانه‌ها توسط کارکنان و روشهای مورداستفاده در امنیت و حفاظت اطلاعات است. این سیاست چارچوبی را برای حفاظت از شبکه‌های رایانه‌ای و منابع اطلاعاتی موجود در آنها تعیین می‌کند. این سیاست باید به سادگی برای مدیران و کارکنان قابل درک بوده و تمامی نکات و موارد مربوط به امنیت را دربرگیرد. ازجمله مطالب مهم این سیاست عبارتند از:

تعریف استفاده مجاز، چگونگی احراز هویت و انتخاب کلمه رمز، مسئولیت به روز کردن نرم افزارهای موجود در هر رایانه اقدامات لازم درهنگام بروز یک حمله و یا ویروس رایانه ای و مسئولیتهای افراد دراین مورد.

معمولاً سیاست امنیتی در دو شکل تهیه می‌گردد. یکی به صورت ساده وکلی که برای عموم کارکنان قابل استفاده باشد و دیگری با جزئیات بیشتر که معمولاً محرمانه است و برای استفاده مدیران و کارشناسان فناوری اطلاعات و امنیت است.

۳ – محکم کاری در نرم افزارهای مورداستفاده: این قسمت شامل شناسایی نرم افزارهای موجود در سیستم و به روز کردن آنهاست. زیرا معمولا" آخرین مدل یک نرم افزار آسیب پذیریهای کمتری نسبت به مدلهای قدیمی تر آن دارد. ازجمله کارهای دیگر دراین قسمت حذف برنامه های آزمایشی و نمونه و برنامه‌هایی که ازنظر امنیتی مطمئن نیستند از سیستم های مورداستفاده است.

۴ – کاهش تعداد نقاط دسترسی و کنترل نقاط باقیمانده: این مرحله شامل بررسی نقشه سیستم و شناسایی نقاط اتصال به اینترنت و دسترسی از راه دور به منظور کاهش نقاط دسترسی به حداقل ممکن و کنترل نقاط باقیمانده ازنظر دسترسی و ورود و خروج اطلاعات است.

۵ – شناسایی نقاط ورود پنهان: شناسایی و حذف مودم ها و نقاط دسترسی غیرمعمول که احتمالا" از نظرها پنهان می ماند ولی بعضی از کارکنان آنها را مورداستفاده قرار می دهند.

۶ – نصب دیواره آتش (FIREWALL): این سیستم برای جداسازی و محافظت سیستم داخلی از اینترنت و همچنین کنترل دسترسی به سایت های اینترنتی به خصوص سایت‌های غیرمربوط به کار نصب می گردد. در مواردی می‌توان رایانه‌های مشخصی را جهت استفاده از اینترنت اختصاص داد. درصورت نیاز تغییر پورت های اتصال و آموزش کارکنان درمورد راههای درست دسترسی حائزاهمیت است.

۷ – نصب سیستم‌های تشخیص و جلوگیری از ورود غیرمجاز (INTRUSION DETECTION AND PREVENTION SYSTEMS): این سیستم‌ها به مانند دزدگیر عمل کرده و ورود و دسترسی غیرمجاز به سیستم را ثبت و اطلاع می‌دهد و یا از انجام آن جلوگیری می‌کند. حتی در مواردی که عبور غیرمجاز از دیواره آتش انجام پذیرد با استفاده از این سیستم می توان آن را شناسایی و از بروز مجدد آن جلوگیری کرد. همچنین با بررسی به موقع لیست ثبت شده توسط سیستم IDP وشناسایی تلاشهای انجام شده برای دسترسی غیرمجاز به سیستم می‌توان از خطرات آتی جلوگیری کرد.

۸ – نصب نرم‌افزارهای ضدویروس: نصب نرم افزارهای ضدویروس در دروازه های ورودی سیستم و در رایانه‌ها برای شناسایی و جلوگیری از ورود ویروس های رایانه های به سیستم و احیاناً مرمت سیستم های آلوده به ویروس ضروری است. این نرم افزارها باید مرتباً به روز درآیند تا همواره از آخرین اطلاعات مربوط به ویروس‌های رایانه‌ای استفاده گردد.

۹ – بررسی متناوب عملکرد سیستم و رفع اشکالات آن: این بررسی ها به مدیریت این امکان را می دهد تا با درنظر گرفتن خطرات امنیتی موجود و نیاز به انجام عملیات تجاری، ضمن رفع اشکالات شناخته شده سیاست و برنامه امنیتی متناسب و متوازنی را اتخاذ کند.

۱۰ – آموزش کارکنان: کارکنان باید باتوجه به نیاز آنها در سطوح مختلف درباره مسائل امنیتی و حفاظت از اطلاعات رایانه ای آموزش دیده و آگاهی های لازم را پیدا کنند. ازجمله آموزش سیاست امنیتی مدارس و موسسات آموزشی از ضروریات است.

۴- استانداردهای بین المللی برای امنیت اطلاعات

دررابطه با امنیت اطلاعات و داده ها و حفاظت از اطلاعات حساس، استاندارد انگلیسی ۷۷۹۹BS به وجود آمده که بعداً به صورت استاندارد بین المللی ۱۷۷۹۹ISO درآمد. این استانداردها ایجاد ۱۰ کنترل کلیدی را ملزم ساخته که عبارتنداز:

۱ – تهیه یک سیاست امنیتی مدون؛

۲ – مشخص کردن مسئولیتهای امنیتی در سازمان؛

۳ – آموزش درموارد امنیت اطلاعات؛

۴ – گزارش به موقع تهدیدات امنیتی و نحوه برخورد با آنها؛

۵– جلوگیری و کنترل ویروس‌های رایانه‌ای؛

۶– برنامه ادامه تجارت درصورت بروز خطرات امنیتی؛

۷ – کنترل تکثیر و کپی کردن نرم‌افزارهای دارای حقوق محفوظ؛

۸ – ایجاد فرایند مناسب برای مدیریت ثبت اطلاعات حساس؛

۹ – حفاظت از اطلاعات شخصی و خصوصی افراد؛

۱۰ – بررسی متناوب پیروی از استانداردها.

این ۱۰ کنترل، اطلاعات الکترونیک و غیرالکترونیک و همچنین نحوه ذخیره الکترونیک و فیزیکی آنها را شامل می‌شود.

باتوجه به اینکه مقوله امنیت اطلاعات و بخصوص مطابقت با یک استاندارد قابل قبول بین المللی هم ازنظر شرکتها و تولیدکنندگان و هم ازنظر مشتریان و خریداران خدمات این شرکتها حائزاهمیت است و بادرنظر گرفتن اینکه رعایت استانداردهای امنیتی شرکتها را در زمینه مسئولیتهای قانونی آنها حمایت می‌کند توجه به استانداردهای بین‌المللی امنیت اطلاعات و پیروی از آنها در بازار جهانی امروز از اهمیت بیشتری برخوردار گشته است.