توصیه های حفاظتی در زمینه IT

امروزه امنیت اطلاعات در سیستم های کامپیوتری به عنوان یکی از مسائل مهم مطرح است و باید به مقوله امنیت اطلاعات نه به عنوان یک محصول بلکه به عنوان یک فرآیند نگاه گردد . بدون شک اطلاع رسانی در رابطه با تهدیدات ، حملات و نحوه برخورد با آنان ، دارای جایگاهی خاص در فرآیند ایمن سازی اطلاعات بوده و لازم است همواره نسبت به آخرین اطلاعات موجود در این زمینه خود را به هنگام نمائیم .

بدین دلیل و با توجه به اهمیت اطلاع رسانی در این زمینه ، مطالبی در ارتباط با امنیت اطلاعات ، هشدارهای امنیتی ، ابزارهای برخورد با حملات و تهدیدات امنیتی به اختصار بیان می گردد .

امنیت داده ها در کامپیوترها عملیات لازم به منظور امنیت داده ها

استفاده صحیح از رمزهای عبور :

سعی نمایید که برای استفاده از اطلاعات موجود بر روی دستگاه های قابل حمل همواره از رمزهای عبور استفاده نمائید .

در زمان وارد کردن رمز عبور، گزینه هایی را انتخاب ننمایید که به کامپیوتر امکان به خاطر سپردن رمزهای عبور را بدهد .

از رمزهای عبوری که امکان تشخیص آسان آنان برای افراد غیرمجاز وجود دارد ، استفاده نکنید .

ذخیره سازی جداگانه داده های مهم:

از امکانات و دستگاه های متعددی به منظور ذخیره سازی داده می توان استفاده نمود .
دیسک های فشرده CD، DVD و یا دیسک های قابل حمل پیشنهاد می گردد .

اطلاعات موجود بر روی دستگاه های قابل حمل(نظیر کامپیوترهای Note book) بر روی رسانه های ذخیره سازی قابل حمل و در مکان های متفاوت ، ذخیره و نگهداری گردد .

بدین ترتیب در صورت سرقت و یا خرابی کامپیوتر ، امکان دستیابی و استفاده از داده ها همچنان وجود خواهد داشت .

مکان نگهداری داده ها باید دارای شرایط مطلوب امنیتـی باشد .

رمزنگاری فایل ها :

با رمزنگاری فایل ها ، صرفاً افراد مجاز قادر به دستیابی و مشاهده اطلاعات خواهند بود .
در صورتی که افراد غیر مجاز امکان دستیابی به داده ها را پیدا نمایند ، قادر به مشاهده اطلاعات نخواهند بود .

در زمان رمزنگاری اطلاعات ، باید تمهیدات لازم در خصوص حفاظت و به خاطر سپردن رمزهای عبور اتخاذ گردد .

نصب و نگهداری نرم افزارهای ضد ویروس:

حفاظت کامپیوترهای قابل حمل در مقابل ویروس ها ، نظیر حفاظت سایر کامپیوترها بوده و باید همواره از به هنگام بودن این نوع برنامه ها، اطمینان حاصل نمود .

نصب و نگهداری یک فایروال :

در صورت استفاده از شبکه های متعدد ، ضرورت استفاده از فایروال ها مضاعف می گردد . با استفاده از فایروال ها حفاظت لازم و پیشگیری اولیه در خصوص دستیابی به سیستم توسط افراد غیر مجاز انجام خواهد شد .

Back up گرفتن داده ها :

از هر نوع داده ارزشمند موجود بر روی یک کامپیوتر باید Back up گرفته و آن ها را ذخیره نمود .

بدین ترتیب در صورتی که کامپیوتر سرقت و یا با مشکل مواجه شود ، امکان دستیابی به اطلاعات در معرض تهدید وجود خواهد داشت .

نحوه انتخاب و حفاظت رمزهای عبور:

رمزهای عبور ، روشی به منظور تائید کاربران بوده و تنها حفاظ موجود بین کاربر و اطلاعات موجود بر روی یک کامپیوتر است .

مهاجمان با استفاده از برنامه های متعدد نرم افزاری ، قادر به حدس رمزهای عبور و یا اصطلاحاً "Crack " نمودن آنان هستند .

با انتخاب مناسب رمزهای عبور و نگهداری آنان ، امکان حدس آنان مشکل و بالطبع افراد غیر مجاز قادر به دستیابی اطلاعات شخصی شما نخواهند بود .

یکی از بهترین روش های حفاظت از اطلاعات ، حصول اطمینان از این موضوع است که صرفاً افراد مجاز قادر به دستیابی به اطلاعات می‌باشند.

فرآیند تایید هویت و اعتبار کاربران در دنیای مجازی شرایط و ویژگی های خاص خود را داشته و شاید بتوان ادعا کرد که این موضوع به مراتب پیچیده تر از دنیای غیرمجازی است .

در صورتی که شما رمزهای عبور را به درستی انتخاب نکرده و یا از آنان به درستی مراقبت ننمایید ، قطعاً پتانسیل فوق جایگاه و کارایی واقعی خود را از دست خواهد داد .

تعداد زیادی از سیستم ها و سرویس ها صرفاً به دلیل عدم ایمن بودن رمزهای عبور با مشکل مواجه شده و برخی از ویروس ها با حدس و تشخیص رمزهای عبور ضعیف ، توانسته اند به اهداف مخرب خود دست یابند .

چگونه یک رمزعبور خوب تعریف کنیم ؟

اکثر افراد از رمزهای عبوری استفاده می نمایند که مبتنی بر اطلاعات شخصی آنان است ، چراکه بخاطر سپردن این نوع رمزهای عبور برای آنان ساده تر می باشد .

بدیهی است به همان نسبت ، مهاجمان نیز با سادگی بیشتری قادر به تشخیص و کراک نمودن رمزهای عبور خواهند بود .

این نوع رمزهای عبور دارای استعداد لازم برای حملات از نوع "دیکشنری "، می باشند .

به منظور تعریف رمزعبور ، موارد زیر پیشنهاد می گردد :

عدم استفاده از رمزهای عبوری که مبتنی بر اطلاعات شخصی هستند زیرا این نوع رمزهای عبور به سادگی حدس و تشخیص داده می شوند.

عدم استفاده از کلماتی که می توان آنان را در هر دیکشنری پیدا نمود .

پیاده سازی یک سیستم و روش خاص به منظور به خاطرسپردن رمزها استفاده از حروف بزرگ و کوچک در زمان تعریف رمز عبور استفاده از ترکیب حروف ، اعداد و حروف ویژه نحوه حفاظت رمزهای عبور پس از انتخاب یک رمزعبور که امکان حدس و تشخیص آن مشکل است ، باید تمهیدات لازم در خصوص نگهداری آنان پیش بینی گردد .

در این رابطه موارد زیر پیشنهاد می گردد :

از دادن رمز عبور خود به سایر افراد جداً اجتناب گردد .

از نوشتن رمز عبور بر روی کاغذ و گذاشتن آن بر روی میز محل کار ، نزدیک کامپیوتر و یا چسباندن آن بر روی کامپیوتر ، جداً اجتناب گردد .

افرادی که امکان دستیابی فیزیکی به محل کار شما را داشته باشند ، به راحتی قادر به تشخیص رمز عبور شما خواهند بود .

هرگز به خواسته افرادی که به بهانه های مختلف از طریق تلفن و یا نامه از شما درخواست رمز عبور را می نمایند ، توجه ننمائید .

در صورتی که مرکز ارائه دهنده خدمات اینترنت شما ، انتخاب سیستم تائید (Authentication) را برعهده شما گذاشته است، سعی نمائید یکی از گزینه هایChallenge/response یا Public encryption key را در مقابل رمزهای عبور ساده ، انتخاب نمائید.

بسیاری از برنامه ها امکان به خاطر سپردن رمزهای عبور را ارائه می نمایند ، برخی از این برنامه ها دارای سطوح مناسب امنیتی به منظور حفاظت از اطلاعات نمی باشند .

برخی برنامه ها نظیر برنامه های سرویس گیرنده پست الکترونیکی ، اطلاعات را به صورت متن (غیر رمزشده) در یک فایل بر روی کامپیوتر ذخیره می نمایند . این بدان معنی است که افرادی که به کامپیوتر شما دستیابی دارند ، قادر به کشف تمامی رمزهای عبور و دستیابی به اطلاعات شما خواهند بود .

بدین دلیل ، همواره به خاطر داشته باشید زمانی که از یک کامپیوتر عمومی، استفاده می نمائید، عملیات logout را انجام دهید .

برخی از برنامه ها از یک مدل رمز نگاری مناسب به منظور حفاظت اطلاعات استفاده می نمایند که ممکن است دارای امکانات ارزشمندی به منظور مدیریت رمزهای عبور باشند .

چند عادت خوب امنیتی انسان عصر اطلاعات باید در کنار استفاده از فن آوری های متعدد ، سعی نماید برخی عادات و حرکات پسندیده را برای خود اصل قرار داده و با تکرار مدوام آنان ، امکان و یا بهتر بگوئیم شانس خرابی اطلاعات و یا کامپیوتر را کاهش دهد .

دستـیابی به یک کامپیوتر به دو صورت فیزیکی و از راه دور ، امکان پذیر است . شما می توانید به سادگی افرادی را که قادر به دستیابی فیزیکی به سیستم شما هستند را شناسایی نمایید .

آیا شناسایی افرادی که قادرند از راه دور به سیستم شما متصل گردند ، نیز امری ساده است؟

پاسخ سوال فوق ، منفی است و شناسایی افرادی که از راه دور به سیستم شما متصل می شوند ، به مراتب مشکل تر خواهد بود .

اگر شما کامپیوتر خود را به یک شبکه متصل نموده اید ، قطعاً در معرض تهدید و آسیب خواهید بود .

استفاده کنندگان کامپیوتر و کاربران شبکه های کامپیوتری (خصوصاً اینترنت) ، می توانند با رعایت برخی نکات که می بایست به عادت تبدیل شوند ، ضریب مقاومت و ایمنی سیستم خود را افزایش دهند .

در ادامه به برخی از این موارد اشاره می گردد :

قفل نمودن کامپیوتر زمانی که از آن دور هستیم :

شما با قفل نمودن کامپیوتر خود ، عرصه را برای افرادی که با نشستن پشت کامپیوتر شما قصد دستیابی بدون محدودیت به اطلاعات شما را دارند ، تنگ خواهید کرد .

قطع ارتباط با اینترنت زمانی که از آن استفاده نمی گردد :

پیاده سازی فناوری هایی نظیر DSL و مودم های کابلی این امکان را برای کاربران فراهم نموده است که همواره به اینترنت متصل و اصطلاحاً online باشند . این مزیت دارای چالش های امنیتی خاص خود نیز می باشد . با توجه به این که شما بطور دائم به شبکه متصل می باشید ، مهاجمان و ویروس ها فرصت بیشتری برای یافتن قربانیان خود خواهند داشت . در صورتی که کامپیوتر شما همواره به اینترنت متصل است . باید در زمانی که قصد استفاده از اینترنت را ندارید ، اتصال خود را غیر فعال نمایید . فرآیند غیرفعال نمودن اتصال به اینترنت به نوع ارتباط ایجاد شده ، بستگی دارد . چنانچه اطلاعات شما اهمیت زیادی دارد از اتصال سیستم به اینترنت اجتناب کنید .

بررسی تنظیمات امنیتی :

اکثر نرم افزارها نظیر برنامه های مرورگر و یا پست الکترونیکی ، امکانات متنوعی را به منظور پیکربندی سفارشی متناسب با شرایط و خواسته استفاده کنندگان ، ارائه می نمایند . در برخی موارد همزمان با فعال نمودن برخی از گزینه ها از یک طرف امکان استفاده از سیستم راحت تر شده و از طرف دیگر ممکن است احتمال آسیب پذیری شما در مقابل حملات ، افزایش یابد . در این رابطه لازم است تنظیمات امنیتی موجود در نرم افزار را بررسی نموده و گزینه هایی را انتخاب نمائید که علاوه بر تأمین نیاز شما ، آسیب پذیری سیستم شما در مقابل حملات را افزایش ندهد .

در صورتی که یک Patch و یا نسخه جدیدی از یک نرم افزار را بر روی سیستم خود نصب می نمائید ، ممکن است تغییراتی را در تنظیمات انجام شده اعمال نماید ، باید بررسی مجدد در خصوص تنظیمات امنیتی را انجام داده تا این اطمینان حاصل گردد که سیستم دارای شرایط مناسب و مقاوم در مقابل تهدیدات است.

از دانلود کردن نرم افزارهای موجود در بازار و نصب کپی نرم افزار ها بر روی سیستم خودداری نمایید .

به منظور افزایش مقاومت سیستم در مقابل خرابی و از دست دادن اطلاعات ، باید به ابعاد دیگری نیز توجه داشت .

برخی مواقع تهدید اطلاعات و در معرض آسیب قرار گرفتن آنان از جانب افراد نبوده و این موضوع به عوامل طبیعی و فنی دیگری بستگی دارد. با اینکه روشی برای کنترل و یا پیشگیری قطعی این نوع از حوادث وجود ندارد ولی می توان با رعایت برخی نکات میزان خرابی را کاهش داد .