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 می باشند . مهاجمان با بکارگیری برنامه های متعدد نرم افزاری ، قادر به حدس رمز های عبور و یا اصطلاحا" "کراک" نمودن آنان می باشند . با انتخاب مناسب رمزهای عبور و نگهداری ایمن آنان ، امکان حدس آنان مشکل و بالطبع افراد غیر مجاز قادر به دستیابی اطلاعات شخصی شما نخواهند بود.
چرا به یک رمز عبور نیاز است ؟
انسان عصر اطلاعات در طی مدت زمان حیات خود و متناسب با فعالیت های روزانه خود نیازمند استفاده از رمزهای عبور متفاوتی می باشد . بخاطر سپردن شماره کد دستگاه موبایل خود ، شماره کد دستگاههای متفاوتی نظیر دستگاهایATM برای دریافت پول ، شماره کد لازم به منظور ورود به یک سیستم کامپیوتری ، شماره کد مربوط به برنامه های کامپیوتری نظیر برنامه های پست الکترونیکی ، امضای دیجیتالی درون یک بانک Onlineو یا فروشگاههای مجازی و موارد بسیار دیگر ، نمونه هائی در این زمینه می باشند . نگهداری این همه عدد ، حرف و شاید هم ترکیب آنان، کاربران را مستاصل و گاها" نگران می نماید . مهاجمان با آگاهی از رمز عبور شما قادر به برنامه ریزی یک تهاجم بزرگ و دستیابی به اطلاعات شما می باشند.
یکی از بهترین روش های حفاظت از اطلاعات ، حصول اطمینان از این موضوع است که صرفا" افراد مجاز قادر به دستیابی به اطلاعات می باشد . فرآیند تائید هویت و اعتبار کاربران در دنیای سایبر شرایط و ویژگی های خاص خود را داشته و شاید بتوان این ادعا را داشت که این موضوع بمراتب پیچیده تر از دنیای غیرسایبر است . رمزهای عبور یکی از متداولترین روش های موجود در خصوص تائید افراد می باشد . در صورتی که شما رمزهای عبور را بدرستی انتخاب نکرده و یا از آنان بدرستی مراقبت ننمائید ، قطعا" پتانسیل فوق جایگاه و کارآئی واقعی خود را از دست خواهد داد . تعداد زیادی از سیستم ها و سرویس ها صرفا" بدلیل عدم ایمن بودن رمزهای عبور با مشکل مواجه شده و برخی از ویروس ها و کرم ها با حدس و تشخیص رمزهای عبور ضعیف ، توانسته اند به اهداف مخرب خود دست یابند.

چگونه می توان یک رمزعبور خوب را تعریف کرد ؟

اکثر افراد از رمزهای عبوری استفاده می نمایند که مبتنی بر اطلاعات شخصیآنان می باشد ، 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 . به عنوان نمونه ، یک رمز عبور چهار حرفی را در نظر بگیرید . ممکن است این عدد ارتباطی با تاریخ تولد شما داشته و یا چهار شماره آخر شماره دانشجوئی و یا کارمندی و شماره تلفن باشد . این نوع رمزهای عبور دارای استعداد لازم برای حملات از نوع "دیکشنری " ، می باشند . مهاجمان در این نوع از حملات با توجه به کلمات موجود در دیکشنری ، سعی در حدس و تشخیص رمزهای عبور می نمایند.
با این که تایپ نادرست برخی کلمات نظیرdaytt در مقابل استفاده ازdate ممکن است مقاومت بیشتری در مقابل حملات از نوع دیکشنری را داشته باشد ، یک روش مناسب دیگر می تواند شامل استفاده از مجموعه ای کلمات و بکارگیری روش هائی خاص به منظور افزایش قدرت بخاطر سپردن اطلاعات در حافظه باشد . مثلا"در مقابل رمز عبور "hoops"، از "IITpbb" ، استفاده نمائید. (بر گرفته شده از کلمات عبارت ILike To : Play Basketball) . استفاده از حروف بزرگ و کوچک و ترکیب آنان با یکدیگر نیز می تواند ضریب مقاومت رمزهای عبور را در مقابل حملات از نوع "دیکشنری" تا اندازه ای افزایش

دهد . به منظور افزایش ضریب مقاومت رمزهای عبور ، می بایست از رمزهای عبور پیچیده ای استفاده نمود که از ترکیب اعداد ، حروف الفبائی و حروف ویژه ، ایجاد شده باشند.
پس از تعریف یک رمز عبور مناسب ، برخی از کاربران از آن به منظور دستیابی به هر سیستم و یا برنامه های نرم افزاری استفاده می نمایند.(کلید جادوئی !) این نوع از کاربران می بایست به این نکته توجه نمایند که در صورتی که یک مهاجم رمز عبور شما را حدس و تشخیص دهد ، وی به تمامی سیستم هائی که با این رمز عبور کار می کنند، دستیابی پیدا می نماید . به منظور تعریف رمزعبور ، موارد زیر پیشنهاد می گردد :

- عدم استفاده از رمزهای عبوری که مبتنی بر اطلاعات شخصی می باشند . این نوع رمزهای عبور بهسادگی حدس و تشخیص داده می شوند .
- عدم استفاده از کلماتی که می توان آنان را در هر دیکشنری و یا زبانی پیدا نمود .
- پیاده سازی یک سیستم و روش خاص به منظور بخاطرسپردن رمزهای عبور پیچیده
- استفاده از حروف بزرگ و کوچک در زمان تعریف رمزعبور
- استفاده از ترکیب حروف ، اعداد و حروف ویژه
- استفاده از رمزهای عبور متفاوت برای سیستم های متفاوت

نحوه حفاظت رمزهای عبور

پس از انتخاب یک رمزعبور که امکان حدس و تشخیص آن مشکل است ، می بایست 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 جدا" 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 ، جدا" اجتناب گردد . افرادیکه امکان دستیابی فیزیکی به محل کار شما را داشته باشند ، براحتی قادر به تشخیص رمز عبور شما خواهند بود .

- هرگز به خواسته افرادیکه (مهاجمان) 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 را برعهده شما گذاشته است ، سعی نمائید یکی از گزینه های Kerberos, challenge/responseو یا public keyencryption را در مقابل رمزهای عبور ساده ، انتخاب نمائید .
- تعداد زیادی از برنامه ها امکان بخاطر 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(غیررمزشده)در یک فایل بر روی کامپیوتر ذخیره می نمایند . این بدان معنی است کهافرادیکه به کامپیوتر شما دستیابی دارند، قادر به کشف تمامی رمزهای عبور و دستیابی به اطلاعات شما خواهند بود . بدین دلیل ، همواره بخاطر داشته باشید زمانی که از یک کامپیوتر عمومی (در کتابخانه ، کافی نت و یا یک کامپیوتر مشترک در اداره) ، استفاده می نمائید ، عملیاتlogout را انجام دهید . برخی از برنامه ها از یک مدل رمزنگاری مناسب به منظور حفاظت اطلاعات استفاده می نمایند . این نوع برنامه ها ممکن است دارای امکانات ارزشمندی به منظور مدیریت رمزهای عبور باشند .