امنیت داده ها در کامپیوترهای قابل حمل

در زمان استفاده از دستگاه های قابل حملی نظیر کامپیوترهای Laptop علاوه بر رعایت اقدامات احتیاطی در خصوص حفاظت فیزیکی آنان،می بایست یک لایه امنیتی دیگر به منظور ایمن سازی داده ها را ایجاد نمود.

چرا به یک لایه حفاظتی دیگر نیاز داریم ؟

به منظور حفاظت فیزیکی کامپیوترهای Laptop و سایر دستگاه های قابل حمل از روش های متعددی استفاده می گردد . استفاده از هر روشی به منظور حفاظت فیزیکی، عدم سرقت اینگونه دستگاه ها را تضمین نمی نماید . دستگاه های فوق بگونه ای طراحی شده اند که امکان حمل و جابجائی آنان ساده باشد و همین موضوع می تواند احتمال سرقت آنان را افزایش دهد . سرقت یک کامپیوتر حاوی اطلاعات حساس پیامدهای خطرناک امنیتی را بدنبال خواهد داشت . علاوه بر موارد فوق ، هر دستگاهی که به اینترنت متصل می گردد ، دارای استعداد لازم به منظور حملات شبکه ای متعددی است (خصوصا" اگر ارتباط از طریق یک اتصال بدون کابل ایجاد شده باشد).

عملیات لازم به منظور امنیت داده ها

- **استفاده صحیح از رمزهای عبور:** سعی نمائید که برای استفاده از اطلاعات موجود بر روی دستگاه های قابل حمل همواره از رمزهای عبور استفاده نمائید . در زمان درج رمز عبور ، گزینه هائی را انتخاب ننمائید که به کامپیوتر امکان بخاطر سپردن رمزهای عبور را می دهد .از رمزهای عبوری که امکان تشخیص آسان آنان برای افراد غیرمجاز وجود دارد ، استفاده نگردد . از رمزهای عبور مختلفی برای برنامه های متفاوت استفاده نمائید .

• **ذخیره سازی جداگانه داده های مهم :** از امکانات و دستگاه های متعددی به منظور ذخیره سازی داده می توان استفاده نمود . فلاپی دیسک ها ، دیسک های فشرده CD ، DVD و یا درایوهای فلش قابل حمل ، نمونه هائی در این زمینه می باشند . پیشنهاد می گردد اطلاعات موجود بر روی دستگاه های قابل حمل(نظیر کامپیوترهای Laptop) 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 می بایست دارای شرایط مطلوب امنیتی باشد.

• **رمزنگاری فایل ها :** با رمزنگاری فایل ها ، صرفا" 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 ، می بایست تمهیدات لازم در خصوص حفاظت و بخاطر سپردن رمزهای عبور اتخاذ گردد . در صورت گم شدن رمزهای عبور، امکان دستیابی و استفاده از اطلاعات با مشکل مواجه می گردد .

• **نصب و نگهداری نرم افزارهای ضد ویروس :** حفاظت کامپیوترهای قابل حمل در مقابل ویروس ها نظیر حفاظت سایر کامپیوترها بوده و می بایست همواره از بهنگام 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 لارم و پیشگیری اولیه در خصوص دستیابی به سیستم توسط افراد غیرمجاز انجام خواهد شد.

• **Back up گرفتن داده ها :** از هر نوع داده ارزشمند موجود بر روی یک کامپیوتر می بایست back up گرفته و آنان را بر روی CD-ROM ، DVD-ROM و یا شبکه ذخیره نمود. بدین ترتیب در صورتی که کامپیوتر سرقت و یا با مشکل خاصی مواجه شود ، امکان دستیابی به اطلاعات و تشخیص سریع داده های در معرض تهدید وجود خواهد داشت .