شرکت آب و فاضلاب استان آذربایجان شرقی

امنیت فناوری اطلاعات

دفتر حراست و امور محرمانه شرکت آب و فاضلاب استان آذربایجان شرقی

امنیت الکترونیکی چیست؟

به طور کلی امنیت الکترونیکی عبارت است از هر ابزار، فن، یا فرآیندی که برای حفاظت از سرمایه های اطلاعاتی یک سیستم مورد استفاده قرار می گیرد. امنیت الکترونیکی ارزش یک شبکه را زیاد می‌کند و از زیرساخت های نرم و سخت تشکیل شده است. زیرساخت های نرم عبارتند از سیاست‌ها، فرآیندها، پروتکل‌ها و راهبردهایی که از مورد سوء استفاده قرار گرفتن سیستم و داده‌ها جلوگیری می‌کنند. زیرساخت‌های سخت نیز متشکل از نرم افزار و سخت افزار مورد نیاز برای حفاظت از سیستم و داده‌ها در مقابل تهدیدات امنیتی داخلی و خارجی سازمان می‌باشد.

زیرساخت های حیاتی

زیرساخت حیاتی شبکه ای از سرمایه‌های فیزیکی و سیستم‌هایی است که نقش بسزایی در اقتصاد یا رفاه یک کشور دارند. بعنوان مثال سیستم‌های مالی شامل شبکه‌ی بانک‌ها و ارتباطات جزو زیرساخت‌های حیاتی است. همچنین حوزه‌های انرژی شامل برق و آب نیز جزو زیرساخت‌های حیاتی محسوب می‌شوند. تقریباً در تمامی کشورهای جهان عملیات مدیریت و کنترل شبکه‌های زیرساختی با رایانه‌ها انجام می‌گیرد. مفهوم امنیت زیرساخت به این دلیل مهم است که به روشن شدن اهمیت امنیت رایانه کمک می‌کند، چون امروزه تمام کارهای مرتبط با زیرساخت با رایانه انجام می‌گیرد، بنابراین امنیت رایانه نقش بسیار مهمی در امنیت زیرساخت یک کشور دارد.

دلایل اهمیت تهیه نسخه پشتیبان:

۱- **خطای کاربر:** در استفاده از واسط های گرافیکی کاربر این امکان وجود دارد که یک فایل به صورت سهوی پاک شود.

۲- **نقص در سخت افزار:** سخت افزار مورد استفاده در هر زمان ممکن است دچار خرابی شده و باعث از بین رفتن داده ها شود.

۳- **نقص در نرم افزار:** در برخی مواقع خطای نرم افزاری باعث از بین رفتن داده ها می شود.

۴- **نفوذها و تخریب‌های الکترونیکی:** مهاجمین و ویروس‌های مخرب ممکن است باعث تغییر و یا پاک شدن داده‌ها شوند.

۵- **بلایای طبیعی:** وقوع اتفاقاتی نظیر سیل، زلزله و آتش سوزی اهمیت حفاظت از داده‌ها را بیشتر روشن می‌کنند. در این زمینه نگهداری پشتیبان‌ها در محلی دیگر بسیار مفید خواهد بود.

باج افزار چیست؟

برنامه‌های مخرب و تولیدکننده‌های آن اهداف مختلفی را دنبال می‌کنند. گونه‌ای از برنامه‌های مخرب به اسم باج‌افزار (Ransomware) وجود دارند که در صورت ورود به یک سیستم اطلاعات موجود در سیستم را رمزنگاری کرده و درخواست باج می‌کنند. درخواست کننده‌ی باج معمولاً مبلغ درخواستی را به شکل پول الکترونیک (بیت کوین) درخواست می‌کند که امکان ردگیری توسط نهادهای دولتی وجود نداشته باشد. مشکل باج‌افزارها در حال حاضر افزایش چشمگیری داشته و سازمان‌ها را با خطرات بالقوه‌ای روبرو کرده است که در سال‌های اخیر سازمان‌هایی در کشور بوده‌اند که با مشکل باج‌افزار روبرو شده و هزینه‌های زیادی را متحمل شده‌اند.

روش‌های ورود باج افزار به شبکه عمدتاً از طریق حافظه‌های فلش آلوده و دانلود فایل‌های آلوده‌ی ناشناس از اینترنت می‌باشد که نیازمند توجه در استفاده از فلش‌ها و اینترنت را دارد.

امنیت در پست الکترونیکی:

- قبل از باز کردن ضمیمه‌ی ایمیل اطمینان حاصل کنید که یک فایل اجرایی نیست، به عنوان مثال فایل های .exe و یا .apk نباشند.
- هرگز ضمیمه‌ای که از جانب افراد ناشناس یا ضمیمه‌ی ایمیل‌های تبلیغاتی را باز نکنید؛ مگر اینکه اطمینان حاصل کنید آن نوع فایل نمی‌تواند حاوی کد مخرب باشد.
- رمزهای عبور انتخابی برای پست الکترونیکی را پیچیده انتخاب کنید و به صورت دوره‌ای آن را تغییر دهید.