

## ایمنی و امنیت اطلاعات دیجیتالی ۳



کنترل محیط زیست: همه محصولات الکترونیک و دیجیتال بسیار پیچیده است و به محیط زیست سالم نیاز دارند. مرحله اول یک سیستم تهویه مطبوع مناسب برای حفظ محصولات دیجیتال و اطلاعات برای استفاده طولانی مدت ضروری است و همچنین باید از آتش، گرد و غبار و نفوذ آبت نیز دوری شود.

کنترل فیزیکی: کنترل دسترسی فیزیکی نقش مهمی در امنیت اطلاعات را دارد. لازم است این اطمینان ایجاد شود که هیچ فردی نمی تواند به سیستم های اطلاعات دیجیتال و رسانه های ذخیره سازی و همچنین به سیستم شبکه، سرور و یا هر سیستم مشتری آسیب برساند. شناسایی و تصدیق هویت از کاربران که تمایل به دسترسی به اطلاعات دیجیتال نیز بخشی از کنترل فیزیکی می باشد. اثر انگشت و یا انگشت شست سیستم های تشخیص احساس بهترین مثال از به رسمیت شناختن کاربران می باشد. استقرار نگهبان، قفل کابل، قفل درها، سیستم های آتش نیز بخشی از سیستم کنترل فیزیکی می باشد. فایل های دیجیتال باید به طور کامل مراقبت شوند. و در فواصل زمانی معین تجدید و در محیط مناسب حفظ شوند.

برای محافظت اطلاعات از هکر ها، دیوار آتش بهترین راه خل و برای محافظت شبکه کردن کافی است. به منظور حفاظت از ویروس ها و سازمان های حمله هرزنامه دارای دروازه ضد ویروس و ضد هرزنامه می باشد. برای دسترسی به اطلاعات دیجیتال موجود در اینترنت و خود سازمان های امنیتی فیلتر کردن محتوای وب را دارند، و برای توقف اطلاعات ناخواسته ایمیل، فیلتر کردن اسپم ها انجام می شود. در نهایت، ما می توانیم به عبارت دیگر بگوییم که دستگاه های مدیریت تهدید متحد تمام این توابع را در خود دارد. مدیریت تهدید متحد شامل تمام عناصر مهم امنیتی مانند فایروال، آنتی ویروس، آنتی اسپم، فیلتر URL، IDS/IPS می باشد.

کنترل اداری: برای توسعه سیاست مانند سیاست های امنیتی، استخدام، انضباطی و همچنین توسعه استانداردهای امنیت داده ها برای دسترسی به اطلاعات دیجیتال عملکردهای کنترل اداری وجود دارد.

به عنوان مثال وزارت فناوری اطلاعات دولت هند تکنولوژی اطلاعات را به عنوان واقعیت در سال ۲۰۰۰ برای توجه به امنیت اطلاعات در سراسر کشور معرفی کرده است.

عوامل عیب اوراق بهادار

عوامل طبیعی و محیط زیست

پدیده های طبیعی در طول این زمان تلفات سنگینی به انسان و اموالشان وارد کردند. این پدیده ها به طور عمده: طوفان، سیل، زلزله، سونامی و ... سونامی در ۲۶ دسامبر ۲۰۰۴ بود که بسیاری از کشورها از جمله هند را تحت تاثیر قرار داده و از تجزیه و تحلیل های پیگیری شده از لیست سازمان ملل متحد در مجموع ۲۹۸۶۶ نفر از دست داده که شامل ۱۸۶۹۸۳ کشته و ۴۲۸۸۳ گم شده می باشند. منطقه اتحادیه از پوندکری در هند بسیاری از مراکز اطلاع رسانی و کتابخانه هایش را از دست داده بود. عوامل محیطی نیز نقش مهمی برای حفظ اطلاعات دیجیتالی دارد. تمام زیرساخت های مرتبط با کامپیوتر نیاز به منطقه ای با درجه حرارت مناسب، بدون رطوبت و گرد و غبار است.

عوامل انسانی

مرد عامل بسیار قابل اطمینان و خطرناک است. اگر تصور از یک مرد مثبت باشد، هیچ صدمه ای به اطلاعات و زیرساخت های اطلاعاتی وجود ندارد،

اما وقتی که تصور اشتباه باشد اطلاعات می توانند آسیب ببینند، دزدیده، حذف، خراب و یا سوء استفاده شوند. بی دقتی کاربر همچنین می تواند به اطلاعا آسیب برساند.

عوامل فنی برنامه

با کمک برنامه های کوچک، برنامه نویسان به توسعه نرم افزار و پروس و سعی برای هک و یا صدمه به اطلاعات دیجیتالی را می کنند. گاهی اوقات برنامه نویسان نیز اطلاعات زشت و ناپسند برای بهم زدن اطلاعات دیجیتالی منتشر می کنند.

مسایل امنیتی

حملات و پروسی، وپروس از اینترنت،

ویروس از پست الکترونیکی

تراوش اطلاعات و محرمانگی آنها

ایمیل های هاخواسته از ایمیل

هکرهای جاسوس، سرقت رمز های عبور،

هکرهای سیاه

فساد اطلاعات، امنیت اطلاعات

تجارت آنلاین

امنیت شبکه

سوء استفاده از اینترنت، امنیت آنلاین و

امنیت مرتبط با اینترنت و ...

فن کنترل مسائل امنیتی

کنترل برنامه نویسی/فنی: کامپیوترها دسترسی به نیازها را فقط از طریق برنامه های تحت کنترل ایجاد می کنند. هر برنامه ای تحت کنترل و یا با نام یک کاربر عمل می کند. روش های مدیریت دسترسی هنگامی که کاربران خود را شناسایی کردند آغاز خواهد شد. تایید هویت و پس از آن تایید اعتبار کاربران، تایید آنچه که آنها واقعا به آن ادعا می کنند. پس از اعتبار سنجی کاربران می توانند به دسته های خاص اختصاص داده شوند. در این فرایند کاربران به برخی از ابزارهای برنامه نویسی آشنا می شوند. این تکنیک ها عبارت اند از: رمز، آنتی اسپم، آنتی ویروس، ارزیابی آسیب پذیری، خدمات مدیریت امنیت، مدیریت تهدید متحد و ... . مدیریت تهدید متحد: مدیریت تهدید متحد همچون یک راه حل کامل برای بسیاری از نگرانی های امنیتی با پوشش بسیاری از جنبه های یک راه حل واحد می آید. این می تواند عملیاتی از قبیل فیلتر کردن هرزنامه ها، تشخیص مزاحمت ها و ضد ویروس ها را انجام دهد. که به طور سنتی توسط سیستم های مختلف بکار گرفته شده است.