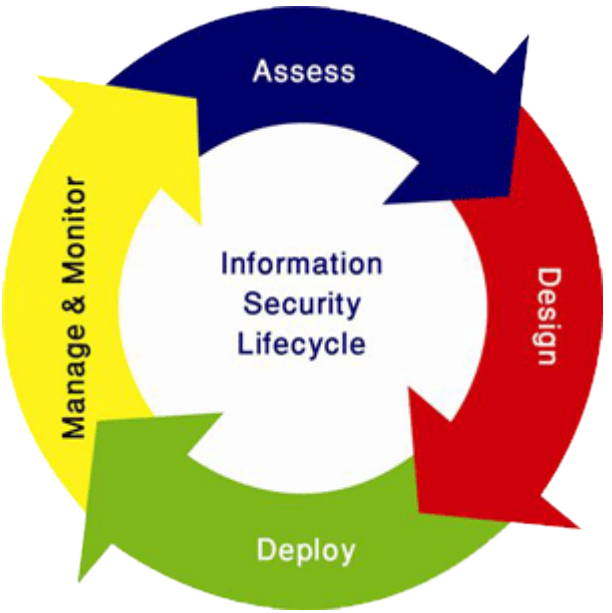
معرفی و بررسی استانداردهای فاوا



فهرست

آغاز

اطلاعات در حال حاضر مهمترین گنجینه به حساب می آید. در بعضی سازمان ها و حتی در موارد شخصی از بین رفتن اطلاعات و حتی آسیب دیدن اطلاعات منجر به صرف زمان و نیروی کار غیر قابل تصور جهت دسترسی به آنها می شود و حتی در برخی موارد اصول کاری یک سازمان را مورد تهدید قرار می دهد.

تکنولوژی اطلاعات(IT) یک سکه دو روست ؛ هم فرصت است و هم تهدید! اگر به همان نسبتی که به توسعه و همه گیری اش توجه و تکیه می کنیم به " امنیت " آن توجه نکنیم می تواند به سادگی در کسری از ثانیه تبدیل به یک تهدید و مصیبت بزرگ شود

بنابراین ITبه همان نسبتی که باعث رفاه و افزایش توانمندی های ما می شود می تواند خطرناک بوده و سازمان ، ارگان و یا کشور را فلج نماید. لذا جهت حفظ اطلاعات و مدیریت آنها و جلوگیری از هر گونه سوء استفاده می بایست بر اساس آخرین دستاورد های روز دنیا و استاندارد های مربوطه اقدام نمود.

برای پیشگیری از تهدید های امنیتی ، متد ها و استاندارد های مختلفی تا به حال ارائه شده است که در ادامه به طور مختصر به بررسی تعدادی از این استانداردها می - پردازیم.

استانداردهایISO17799 و ISO27001

ایزو ۱۷۷۹۹ به رسمیت شناخته شده ترین استاندارد امنیتی است که مسا ئل امنیتی را تا حد زیادی پوشش داده و شامل تعداد قابل توجهی از کنترل های ضروری و بسیار پیچیده می باشد. این استاندارد تفصیلی در ده بخش اصلیکه هرکدام محدوده‌ی متفاوتی را دربر می گیرد سازماندهی شده است. اصلی‌ترین کنترل‌های مورد بررسی در این استاندارد عبارتند از:

- برنامه ریزی دوام کسب وکار
- کنترل دسترسی به سیستم
- توسعه و نگهداری سیستم
- امنیت فیزیکی و محیطی
- پذیرش
- امنیت کارکنان
- سازماندهی امنیت
- مدیریت کامپیوتر و شبکه
- کنترل و طبقه بندی دارایی ها
- سیاست گذاری امنیتی
- مدیریت امنیت فیزیکی و محیطی به موارد زیر می پردازد:

- بکار بردن زمینه های امنیتی برای محافظت از تاسیسات
- استفاده از امنیت فیزیکی محیطی برای حفاظت از مناطق
- استفاده از کنترل های فیزیکی ورود برای محافظت از مناطق امنیتی
- امن سازی دفاتر ، اتاقها و امکانات سازمان
- حفاظت از امکانات در برابر خطرات طبیعی و انسانی
- استفاده از دستورالعمل های کاری برای حفاظت از مناطق امنیتی
- جداکردن و کنترل نقاط دسترسی عمومی
- حفاظت از تجهیزات
- جانمایی تجهیزات و استفاده از استراتژی های حفاظتی
- اطمینان از قابل اعتماد بودن ابزارهای پشتیبان
- ایمن سازی برق و کابلهای مخابراتی
- نگهداری از تجهیزات سازمان
- محافظت از تجهیزات برون سازمانی
- کنترل تجهیزات در اختیار و استفاده مجدد
- کنترل استفاده از دارایی های برون سازمانی

هر چند این استاندارد حوزه‌های مختلف امنیتی را پوشش می‌دهد، رویکرد اصلی آن فنی است و توجه کمتری به عوامل انسانی در حوزه‌ی امنیت دارد. به عنوان مثال اگرچه در کنترل‌های این استاندارد به موضوع دارایی‌های انسانی سازمان و فرهنگ‌سازی به صورت کلی اشاره شده، ولی به موضوع مهمی همچون مهندسی

اجتماعی که وزن بسیار بالایی در حوادث امنیتی به وقوع پیوسته برای سازمان‌ها دارد، پرداخته نشده است.

نکته‌ی قابل توجه دیگر، تراز تهدید است، تهدیدها و وقایع ضد امنیتی در دو حوزه‌ی جرم و جنگ قابل بررسی است. اگرچه برخی از ابزارهای مقابله با جرم در زمینه‌ی مقابله با جنگ نیز می‌توانند مؤثر باشند، اما بسیاری از آن‌ها در حوزه‌ی مقابله با جنگ ناکارآمد هستند.

باید توجه داشت که کنترل‌های این استاندارد و سایر استانداردهای مشابه آن تنها برای برقراری امنیت در مقابل جرایم طراحی شده است.

استاندارد NIST800[1]

طبق این استاندارد، پیاده سازی کنترل های امنیتی مناسب برای یک سیستم اطلاعاتی و ارتباطی وظیفه‌ی مهمی است که می‌تواند اثرات عمده‌ای بر عملکرد و دارایی‌های سازمان داشته باشد. کنترل امنیت، محافظتیا مقابله‌ی مدیریتی، عملیاتی و تکنیکی در نظر گرفته شده برای یک سیستم اطلاعاتی و ارتباطی به منظور محافظت از محرمانگی، یکپارچگی و در دسترس بودن سیستم و اطلاعات آن است.

بر اساس این استاندارد به چند سوال مهم باید توسط مس ؤلین سازمان در زمان پرداختن به ملاحظات امنیتی سیستم‌های اطلاعاتی و ارتباطیپاسخ داده شود:

- برای حفاظت کافی از سیستم های اطلاعاتی و ارتباطی که عملیات و دارایی های سازمان را به منظورپشتیبانی از انجام ماموریت ه‌ا، محافظت از سرمایه ها، انجام مس ؤلیت‌های قانونی، ادامه‌ی

[1]National Institute of Standards and Technology

فعالیت‌های روزانه و حمایت از افراد ، تسهیل می کنند چه کنترل‌های امنیتی مورد نیاز است؟

- آیا کنترل امنیتی انتخاب شده قابل اجراست؟ به عبارت دیگر یک طرح واقع بینانه برای اجرای آن وجود دارد؟
- کنترل‌های امنیتی انتخاب شده پس از اجرا ، چه سطح اطمینانی را برای سازمان فراهم می کنند؟

در این استاندارد یک برنامه‌ی امنیتی فناوری اطلاعات و ارتباطات م ؤثر شامل موارد زیر است:

- ارزیابی ریسک دوره‌ای
- سیاست‌ها و رویه هایی بر اساس ارزیابی ریسک برای اطمینان از سطح قابل قبول امنیت در مراحل مختلف
- برنامه‌های فرعی برای تأمین امنیت اطلاعات کافی و مناسب برای امکانات و تجهیزات، شبکه‌ها و سیستم‌های اطلاعاتی
- آموزش و اطلاع رسانی به تمامی کارکنان در مورد ریسک های امنیت اطلاعات مرتبط با فعالیت ها و مسؤولیت آنها و م نطبق با سیاست‌های سازمانی و روش های طراحی شده برای کاهش این خطرات
- آزمون و ارزیابی متناوب در خصوص مؤثر بودن سیاست‌های امنیت اطلاعات و ارتباطات ، رویه ها و کنترل های امنیتی که متناسب با ریسک تکرار شده اند.

- یک فر آیند برای برنامه ریزی، پیاده سازی، ارزیابی و مستندسازی فعالیت‌هایی که به به‌بود هر گونه کمبود در سیاست های امنیت اطلاعات، رویه‌ها و شیوه‌های سازمان می‌انجامد.
- رویه‌هایی برای تشخیص، گزارش‌دهی و پاسخ به حوادث امنیتی.
- طرح‌ها و رویه هایی برای اطمینان از تداوم عملیات سیستم های اطلاعاتی و ارتباطی که پشتیبان عملیات و دارایی های سازمان هستند.

اگرچه این استاندارد نیز مانند استاندارد قبلی، می‌تواند کاربردهای زیادی در تأمین امنیت فیزیکی داشته باشد، اما نقاط ضعف مهمی از منظر پدافند غیرعامل در آن مشهود است.

این استاندارد نیز مانند استانداردهای خانواده ISO 27000 به مخاطرات ناشی از عوامل انسانی توجه کافی نداشته است.از طرف دیگر کنترل‌هایی برای مقابله در حوزه‌ی جنگ در آن تعریف نشده است.

استانداردهای FIPS[1]

استاندارد FIPS199 کنترل‌هایی را برای طبقه بندی سیستم‌های فناوری اطلاعات و ارتباطات به عنوان تاثیر کم، متوسط یا بالا، در اثر نقض محرمانگی، یکپارچگی و یا در دسترس بودن سیستم، انتشار داده است. استاندارد FIPS200 حداقل امنیت مورد نیاز را در چندین بخش امنیتی زیر تنظیم می کند.

- کنترل دسترسی
- آگاهی و آموزش
- ممیزی و مسئولیت‌پذیری
- صدور گواهینامه، مجوز رسمی و ارزیابی امنیتی
- مدیریت تنظیمات
- برنامه‌ریزی آتی
- شناسایی و تایید هویت
- پاسخ به حوادث
- نگهداری
- محافظت از رسانه‌ها
- برنامه‌ریزی حفاظت فیزیکی و محیطی
- امنیت کارکنان
- ارزیابی ریسک

[1] Federal Information Processing Standard

- مالکیت سیستم و خدمات
- محافظت از سیستم و ارتباطات
- یکپارچگی سیستم و اطلاعات

در این دو استاندارد هم مانند سایر استانداردهای مورد بحث مبحث مهندسی اجتماعی کمتر مورد توجه قرار گرفته است. از طرف دیگر حداقل قابل قبول امنیت در موضوعات مورد بحث استاندارد FIPS200 بر اساس تراز تهدید جرم تعریف گردیده است.

پیاده‌سازی کامل این استانداردها منجر به مخاطراتی می‌شود. از آن‌جا که بسیاری از سازمان‌ها و مراکز کلیدی برای پیاده‌سازی استاندارد به برون‌سپاری روی می‌آورند، زمینه برای جمع‌آوری اطلاعات تجمیع شده در خصوص نقاط ضعف و آسیب‌پذیری‌های سازمان و درز آن به بیرون از سازمان فراهم می‌گردد.