پروژه پایانی – چکیده مقاله ۳: بررسی استاندارد BS7799 و ISO 17799

The BS 7799 / ISO 17799

For a better approach to information security

تهیه کننده:

شراره جهانشاه (۸۹۷۱۶۱)

آرمین کامفیروزی (۸۹۱۷۹۳)

استاد راهنما:

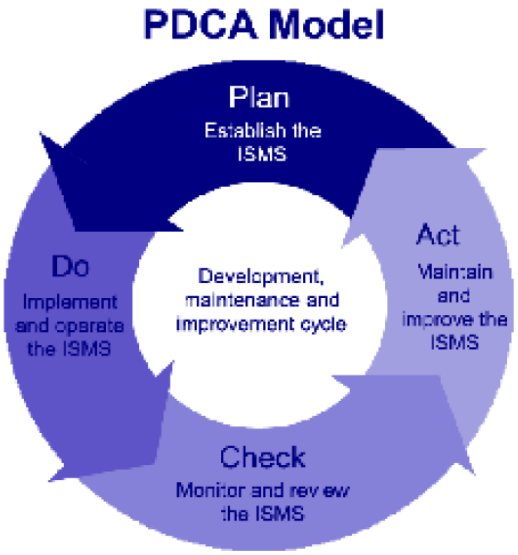
دکتر بوستانی

اسفند ۱۳۹۰

استانداردBS7799

BS7799 استانداردی در جهت بالابردن امنیت اطلاعات در سازمان و شرکتها می باشد. با کمک این استاندارد کلیه دارایی ها لیست و طبقه بندی شده، تهدیدها و نقاط ضعف امنیتی مشخص می شوند و درنهایت کنترل های مختلف برای هریک از این موارد لحاظ می شوند. در واقع BS7799 نیاز سازمان شما را در پیاده سازی یک قالب موفق امنیتی برآورده می سازد.

BS7799 استانداری مطمئن برای ایمن سازی اطلاعات شرکت شماست. این استاندارد از مدل PDCA تبعیت می کند.PDCA الگویی با چهار مرحله زیر است.



PLAN

این فاز در واقع مرحله مشخص شدن **تعاریف اولیه** پیاده سازی ISMS می باشد. تهیه سیاست های امنیتی ،مقاصد ،تعریف پردازشهای مختلف درون سازمانی و روتین های عملیاتی و . . . در این مرحله تعریف و پیاده سازی می شوند.

DO

پیاده سازی و اجرای سیاست های امنیتی ،کنترل ها و پردازش ها در این مرحله انجام می شوند. درواقع این مرحله اجرای کلیه تعاریف فاز اول را طلب می کند.

Check

این مرحله را می توان فاز **ارزیابی** نیز نامید. در این مرحله ارزیابی موفقیت پیاده سازی سیاست های مختلف امنیتی، همچنین تجربه های عملی و گزارش های مدیریتی گردآوری خواهند شد. مرور نتایج ما را در جهت پیدا کردن دیدی بهتر رهنمون می سازد.

ACT

اجرای موارد ترمیمی و بازنگری در نحوه مدیریت اطلاعات،همچنین **تصحیح** موارد مختلف در این فاز انجام می شود.

پس از پایان عملیات فاز چهار دوباره به فاز اول یعنی مرحله PLAN بازگشته و با تعریف سیاستهای جدید مورد نیاز مراحل بعدی را پی می گیریم. باتوجه به تعریفی که در بالا ملاحظه می شود عملیات فوق پروسه ای چرخشی و پویا می باشد که با تغییرات درون سازمانی امکان تصحیح در مدیریت اطلاعات همواره وجود دارد.

BS7799 حفاظت از اطلاعات را در سه مفهوم خاص یعنی قابل اطمینان بودن اطلاعات (Confidentiality) و صحت اطلاعات (Integrity) و در دسترس بودن اطلاعات (Availability) تعریف می کند.

Confidentiality : تنها افراد مجاز به اطلاعات دسترسی خواهند یافت.

Integrity : کامل بودن و صحت اطلاعات و روشهای پردازش اطلاعات مورد نظر هستند.

Availability : اطلاعات در صورت نیاز بطور صحیح در دسترس باید باشد.

استاندارد BS7799 دارای ۱۰ گروه کنترلی می باشد که هرگروه شامل چندین کنترل زیرمجموعه است بنابراین در کل ۱۲۷ کنترل برای داشتن سیستم مدیریت امنیت اطلاعات مدنظر قراردارد. این ده گروه کنترلی عبارتند از :

۱- سیاستهای امنیتی

۲- امنیت سازمان

۳- کنترل و طبقه بندی دارایی ها

۴- امنیت فردی

۵- امنیت فیزیکی

۶- مدیریت ارتباط ها

۷- کنترل دسترسی ها

۸- روشها و روالهای نگهداری و بهبود اطلاعات

۹- مدیریت تداوم کار سازمان

۱۰- سازگاری با موارد قانونی

نمونه هایی از استانداردهای موجود:

- تفکیک و کلاسه کردن در شبکه (۹,۴,۶A.)
- کنترل ارتباطهای شبکه (۹,۴,۷A.)
- کنترل های مسیر یابی شبکه (۹,۴,۸A.)
- امنیت ابزارهای انتقال اطلاعات (۸,۶A.)
- رد و بدل کردن اطلاعات و نرم افزار بین شرکتهای مختلف(۸,۷A.)
- قرارداد انتقال اطلاعات بین شرکت ها (۸,۷,۱A.)
- امنیت اطلاعات در ترانزیت (۸,۷,۲A.)
- امنیت تجارت الکترونیک (۸,۷,۳A.)
- امنیت نامه های الکترونیکی یا e-mail (۸,۷,۴A.)
- امنیت سیستم های موجود در شرکت (۸,۷,۵A.)
- صحت اطلاعات (۸,۷,۶A.)

فوائد استاندارد BS7799 **و لزوم پیاده سازی**

استاندارد BS7799 قالبی مطمئن برای داشتن یک سیستم مورد اطمینان امنیتی می باشد. در زیر به تعدادی از فوائد پیاده سازی این استاندارد اشاره شده است:

اطمینان از تداوم تجارت و کاهش صدمات توسط ایمن ساختن اطلاعات و کاهش تهدیدها

اطمینان از سازگاری با استاندارد امنیت اطلاعات و محافظت از داده ها

قابل اطمینان کردن تصمیم گیری ها و محک زدن سیستم مدیریت امنیت اطلاعات

ایجاد اطمینان نزد مشتریان و شرکای تجاری

امکان رقابت بهتر با سایر شرکت ها

ایجاد مدیریت فعال و پویا در پیاده سازی امنیت داده ها و اطلاعات

بخاطر مشکلات امنیتی اطلاعات و ایده های خود را در خارج سازمان پنهان نسازید

مراحل ایجاد سیستم مدیریت امنیت اطلاعات :

ایجاد و تعریف سیاست ها:

در این مرحله ایجاد سیاستهای کلی سازمان مدنظر قراردارد. روالها از درون فعالیت شرکت یا سازمان استخراج شده و در قالب سند و سیاست امنیتی به شرکت ارائه می شود. مدیران کلیدی و کارشناسان برنامه ریز نقش کلیدی در گردآوری این سند خواهند داشت.

تعیین محدوده عملیاتی :

یک سازمان ممکن است دارای چندین زیرمجموعه و شاخه های کاری باشد لذا شروع پیاده سازی سیستم امنیت اطلاعات کاری بس دشوار است . برای جلوگیری از پیچیدگی پیاده سازی ، تعریف محدوده و Scope صورت می پذیرد. Scope می تواند ساختمان مرکزی یک سازمان یا بخش اداری و یا حتی سایت کامپیوتری سازمان باشد. بنابراین قدم اول تعیین Scope و الویت برای پیاده سازی استاندارد امنیت اطلاعات در Scope خواهد بود. پس از پیاده سازی و اجرای کنترل های BS7799 و اخذ گواهینامه برای محدوده تعیین شده نوبت به پیاده سازی آن در سایر قسمت ها می رسد که مرحله به مرحله اجرا خواهند شد.

برآورد دارایی ها و طبقه بندی آنها:

برای اینکه بتوان کنترل های مناسب را برای قسمت های مختلف سازمان اعمال کرد ابتدا نیاز به تعیین دارایی ها می باشیم. در واقع ابتدا باید تعیین کرد چه داریم و سپس اقدام به ایمن سازی آن نماییم. در این مرحله لیست کلیه تجهیزات و دارایی های سازمان تهیه شده و باتوجه به درجه اهمیت آن طبقه بندی خواهند شد.

ارزیابی خطرات:

با داشتن لیست دارایی ها و اهمیت آن ها برای سازمان ، نسبت به پیش بینی خطرات اقدام کنید. پس از تعیین کلیه خطرات برای هر دارایی اقدام به تشخیص نقاط ضعف امنیتی و دلایل بوجود آمدن تهدیدها نمایید و سپس با داشتن اطلاعات نقاط ضعف را برطرف سازید و خطرات و تهدیدها و نقاط ضعف را مستند نمایید.

مدیریت خطرات :

مستندات مربوط به خطرات و تهدید ها و همچنین نقاط ضعف امنیتی شما را قادر به اتخاذ تصمیم درست و مؤثر برای مقابله با آنها می نماید.

انتخاب کنترل مناسب :

استاندارد BS7799 دارای ۱۰ گروه کنترلی می باشد که هرگروه شامل چندین کنترل زیرمجموعه است بنابراین در کل ۱۲۷ کنترل برای داشتن سیستم مدیریت امنیت اطلاعات مدنظر قراردارد. با انجام مراحل بالا شرکت یا سازمان شما پتانسیل پیاده سازی کنترل های مذکور را خواهد داشت.

این ده گروه کنترلی عبارتند از :

۱- سیاستهای امنیتی

۲- امنیت سازمان

۳- کنترل و طبقه بندی دارایی ها

۴- امنیت فردی

۵- امنیت فیزیکی

۶- مدیریت ارتباط ها

۷- کنترل دسترسی ها

۸- روشها و روالهای نگهداری و بهبود اطلاعات

۹- مدیریت تداوم کار سازمان

۱۰- سازگاری با موارد قانونی

تعیین قابلیت اجرا:

جمع آوری لیست دارایی ها، تعیین تهدیدها ، نقاط ضعف امنیتی و در نهایت ایجاد جدول کنترل ها مارا در به دست آوردن جدولی موسوم به SOA یا Statement Of Applicability یاری می رساند. این جدول لیستی نهایی از کلیه کنترل های مورد نیاز برای پیاده سازی را ارائه می دهد. با مطالعه این جدول و مشخص کردن کنترل های قابل اجرا و اعمال آنها ،سازمان یا شرکت خودرا برای اخذ استاندارد BS7799 آماده خواهید ساخت.

فوائد اجرا و گرفتن گواهینامه BS7799 **به شرح زیرمی باشد:**

اطمینان از تداوم تجارت و کاهش صدمات توسط ایمن ساختن اطلاعات و کاهش تهدیدها

اطمینان از سازگاری با استاندارد امنیت اطلاعات و محافظت از داده ها

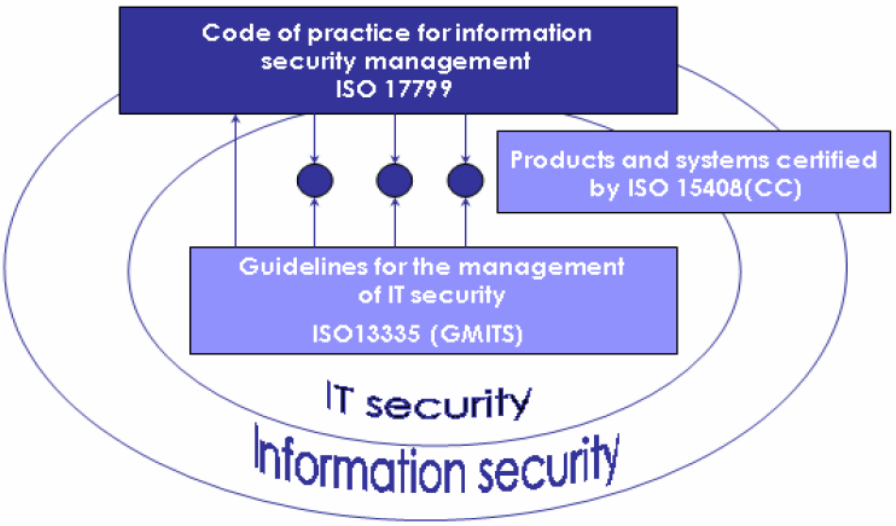
قابل اطمینان کردن تصمیم گیری ها و محک زدن سیستم مدیریت امنیت اطلاعات

ایجاد اطمینان نزد مشتریان و شرکای تجاری

امکان رقابت بهتر با سایر شرکت ها

ایجاد مدیریت فعال و پویا در پیاده سازی امنیت داده ها و اطلاعات

بخاطر مشکلات امنیتی اطلاعات و ایده های خود را در خارج سازمان پنهان نسازید.



سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه

سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه، متناسب با دسته‌بندی انجام شده روی سرمایه‌های فضای تبادل اطلاعات دستگاه، عبارتند از:

- سیاست‌های امنیتی سرویس‌های فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی سخت‌افزارهای فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی نرم‌افزارهای فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی اطلاعات فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی ارتباطات فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی کاربران فضای تبادل اطلاعات دستگاه

معماری شبکه ارتباطی

در این بخش، لازم است معماری شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- ساختار شبکه ارتباطی
- ساختار آدرس‌دهی و مسیریابی
- ساختار دسترسی به شبکه ارتباطی

تجهیزات شبکه ارتباطی

در این بخش، لازم است تجهیزات شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- محافظت فیزیکی
- نسخه و آسیب‌پذیریهای نرم‌افزار
- مدیریت محلی و از راه دور
- تصدیق هویت، تعیین اختیارات و ثبت عملکرد سیستم، بویژه در دسترسی‌های مدیریتی
- ثبت وقایع
- نگهداری و به‌روزنمودن پیکربندی
- مقابله با حملات علیه خود سیستم، بویژه حملات ممانعت از سرویس

سرویس‌های شبکه ارتباطی

در این بخش، لازم است سرویس‌های شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- سیستم عامل سرویس‌دهنده
- سخت‌افزار سرویس‌دهنده، بویژه رعایت افزونگی در سطح ماجول و سیستم
- نرم‌افزار سرویس
- استفاده از ابزارها و مکانیزم‌های امنیتی روی سرویس‌دهنده‌ها

طرح امنیت :

پس از تحلیل مخاطرات امنیتی شبکه ارتباطی دستگاه و دسته‌بندی مخاطرات امنیتی این شبکه، در طرح امنیت، ابزارها و مکانیزم‌های موردنیاز به منظور رفع این ضعفها و مقابله با تهدیدها، ارائه می‌شوند. در طرح امنیت، لازم است کلیه ابزارها ومکانیزم‌های امنیتی موجود، بکار گرفته شوند. نمونه‌ای از این ابزارها عبارتند از:

۱- سیستم‌های کنترل جریان اطلاعات و تشکیل نواحی امنیتی

- فایروال‌ها
- سایر سیستم‌های تامین امنیت گذرگاه‌ها

۲- سیستم‌های تشخیص و مقابله یا تشخیص و پیشگیری از حملات،شامل:

- سیستم‌های مبتنی بر ایستگاه
- سیستم‌های مبتنی بر شبکه

۳- سیستم فیلترینگ محتوا (بویژه برای سرویس E-Mail)

۴- نرم‌افزارهای تشخیص و مقابله با ویروس

۵- سیستم‌های تشخیص هویت، تعیین حدود اختیارات و ثبت عملکرد کاربران

۶- سیستم‌های ثبت و تحلیل رویدادنامه‌ها

۷- سیستم‌های رمزنگاری اطلاعات

۸- نرم‌افزارهای نظارت بر ترافیک شبکه

۹- نرم‌افزارهای پویشگر امنیتی

۱۰- نرم‌افزارهای مدیریت امنیت شبکه

طرح مقابله با حوادث امنیتی و ترمیم خرابیها

طرح مقابله با حوادث امنیتی، با هدف پیشگیری، تشخیص و مقابله با حوادث امنیتی فضای تبادل اطلاعات، ارائه می‌گردد. محتوای این طرح، حداقل شامل موارد زیر می‌باشد:

۱- دسته‌بندی حوادث

۲- سیاست‌های مربوط به هر یک از سرویس‌های مقابله با حوادث امنیتی

۳- ساختار و شرح وظایف مربوط به تیم مقابله با حوادث امنیتی دستگاه

۴- سرویس‌های پیشگیری و مقابله با حوادث که توسط تیم مقابله با حوادث امنیتی دستگاه ارائه می‌گردد

۵- روالهای اجرائی مربوط به هر یک از سرویس‌ها

۶- متدولوژی مقابله با حوادث امنیتی

- آماده‌سازی تیم
- تشخیص و تحلیل حوادث
- محدودسازی، ترمیم و ریشه‌کنی حوادث
- فعالیت‌های بعد از حوادث
- چک لیست مقابله با حوادث

۷- الگوی مقابله با حوادث امنیتی

برنامه آگاهی‌رسانی امنیتی

برنامه آگاهی‌رسانی امنیتی، با هدف برنامه‌ریزی نحوه آگاهی رسانی به کاربران شبکه دستگاه ارائه می‌گردد و باید حاوی موارد ذیل باشد:

۱- اهداف آگاهی‌رسانی

۲- راهبردها

۳- برنامه اجرائی آگاهی‌رسانی

۴- مفاد دوره‌های آگاهی‌رسانی از قبیل:

- اعلام حیطه حریم خصوصی کاربران
- اعلام وظایف، مسئولیتها و مواردی که کاربران باید پاسخگو باشند
- اعلام مواردی که کاربران باید نسبت به آن حساسیت داشته باشند (از قبیل اعلام حوادث به تیم مقابله با حوادث)
- ارائه اطلاعات در زمینه آسیب‌پذیری سیستم‌ها و مواردی که کاربران باید دقت بیشتری لحاظ نمایند.

برنامه آموزش پرسنل تشکیلات امنیت

برنامه آموزش امنیتی، با هدف توانمند سازی پرسنل تشکیلات امنیت دستگاه ارائه می‌گردد و باید حاوی موارد ذیل باشد:

۵- اهداف آموزش

۶- راهبردها

۷- برنامه اجرائی آموزش

۸- مفاد دوره‌های آموزشی

تشکیلات تامین امنیت فضای تبادل اطلاعات دستگاه

اجزاء و ساختار تشکیلات امنیت

بر اساس استانداردهای مدیریت امنیت اطلاعات و ارتباطات، هر دستگاه به منظور تامین امنیت اطلاعات و ارتباطات خود، لازم است تشکیلات تامین امنیت به شرح زیر، ایجاد نماید.

اجزاء تشکیلات امنیت :

تشکیلات امنیت شبکه، متشکل از سه جزء اصلی به شرح زیر می باشد:

- در سطح سیاستگذاری: کمیته راهبری امنیت فضای تبادل اطلاعات دستگاه
- در سطح مدیریت اجرائی: مدیر امنیت فضای تبادل اطلاعات دستگاه
- در سطح فنی: واحد پشتیبانی امنیت فضای تبادل اطلاعات دستگاه

علاوه بر موارد فوق، واحدهای "مشاوره و طراحی" و "نظارت و بازرسی" نیز لازم است. لیکن این واحدها الزاما در داخل دستگاه و چارت سازمانی، تشکیل نخواهند شد.

ساختار تشکیلات امنیت :

ساختار تشکیلات امنیت شبکه دستگاه، عبارتست از:

اعضاء تشکیلات امنیت فضای تبادل اطلاعات دستگاه عبارتند از:

۱- اعضاء کمیته راهبری امنیت:

۲- مدیر امنیت :

مدیریت واحد پشتیبانی امنیت شبکه را به عهده دارد و توسط مدیر فن‌آوری اطلاعات دستگاه تعیین می‌شود.

۳- تیم‌های پشتیبانی امنیت :

شامل تیم‌های زیر بوده و اعضاء آن مستقیما توسط مدیر امنیت شبکه دستگاه تعیین می‌شوند:

- تیم پشتیبانی حوادث
- تیم نظارت و بازرسی
- تیم نگهداری امنیت
- تیم مدیریت تغییرات
- تیم بررسی پاسخگوئی به نیازهای امنیتی