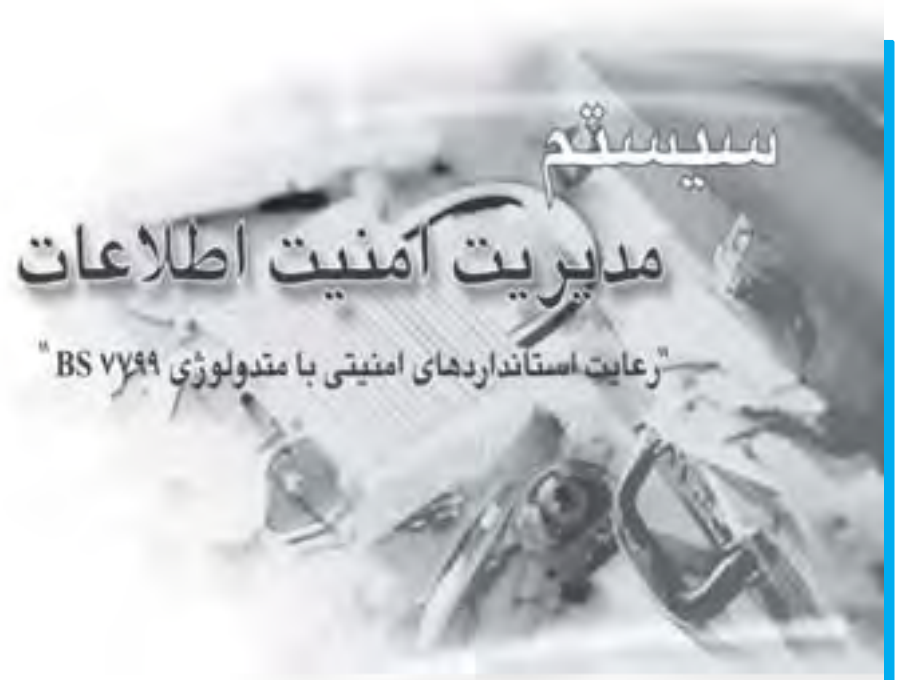


محمدمهدی نوروزی، اداره انفورماتیک بانک

مقدمه:

در حال حاضر وضعیت امنیت فضای تبادل اطلاعات کشور و حتی در برخی مواقع نگهداری فیزیکی اطلاعات بویژه در حوزه دستگاه‌های دولتی، در سطح نامطلوبی قرار دارد، از جمله دلایل اصلی وضعیت موجود را می‌توان به فقدان زیرساخت‌های فنی و اجرایی امنیت و عدم انجام اقدامات موثر در خصوص ایمن‌سازی فضای تبادل اطلاعات دستگاه‌های دولتی اشاره نمود.

زیرساخت‌های امنیتی از قبیل ارزیابی امنیتی فضای تبادل اطلاعات، تحلیل و مدیریت مخاطرات امنیتی، پیشگیری و مقابله با حوادث فضای تبادل اطلاعات، مقابله با جرایم فضای تبادل اطلاعات و ... نقش بسزایی در نا امن بودن فضای تبادل اطلاعات دستگاه‌های دولتی دارد و باعث کاهش اعتبار این دستگاه‌ها شده است.

از این رو تدوین مستندات راهبردی امنیت فضای تبادل اطلاعات کشور و توجه به مقوله ایمن‌سازی فضای تبادل اطلاعات دستگاه‌های دولتی امری اجتناب‌ناپذیر به نظر می‌رسد. علاوه بر این تدوین مستندات راهبردی امنیت فضای تبادل اطلاعات کشور، توجه به مقوله ایمن‌سازی فضای تبادل اطلاعات دستگاه‌های دولتی ضروری بنظر می‌رسد که این امر بر کاهش صدمات و زیان‌های ناشی از وضعیت فعلی امنیت دستگاه‌های دولتی، نقش موثری در فرایند تدوین مستندات راهبردی امنیت فضای تبادل اطلاعات خواهد داشت.

◆ ◆ ◆

سیستم مدیریت امنیت اطلاعات

ارایه یک راه کار جامع و مناسب برای امن‌سازی سیستم‌های اطلاعاتی یک سازمان نیازمند بررسی دقیق تمامی سیستم‌های اطلاعاتی، مدیریتی و عملیاتی آن سازمان است. علاوه بر این رشد تکنولوژی منجر به بروز تهدیدات جدید می‌شود. ارائه یک راه کار مقطعی، هر چند که مشکلات زمان مربوط را حل می‌کند، ولی یک انتخاب مناسب برای مدیران ژرف‌نگر و دوراندیش نیست. نکته درستی که باید در امن‌سازی دقت نمود این است که امن‌سازی یک فرآیند است و نه یک وظیفه‌ای در یک مقطع زمان. حال به این نکته باید توجه شود که برای استقرار فرآیند چه رهیافت‌ها و مکانیسم‌هایی وجود دارد و به طور کلی آیا می‌توان یک روند متدولوژیک و استاندارد را برای رسیدن به این مطلوب طی نمود.

مروری بر استانداردهای مدیریت امنیت اطلاعات

استانداردهای مدیریتی ارایه شده در خصوص امنیت اطلاعات و ارتباطات سازمان‌ها عبارتند از:

-استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس

-استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد

- گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد

تاریخچه استاندارد BS7799 موسسه استاندارد انگلیس

استاندارد BS7799 اولین استاندارد مدیریت امنیت اطلاعات است که نسخه اول آن (BS7799:1) در سال 1995 منتشر شد. نسخه دوم این استاندارد (BS7799:2) که در سال 1999 ارایه شد، علاوه بر تغییر نسبت به نسخه اول، در دو بخش ارایه گردید. آخرین نسخه این استاندارد، (BS7799:2002) نیز در سال 2002 و در دو بخش منتشر گردید.

بخش اول

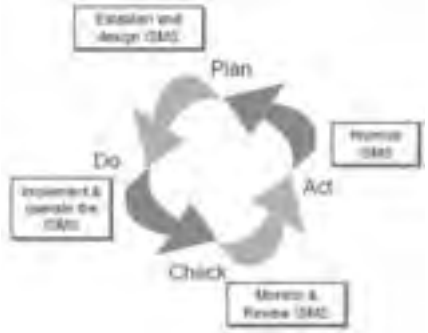
در این بخش از استاندارد، مجموعه کنترل‌های امنیتی مورد نیاز سیستم‌های اطلاعاتی و ارتباطی هر سازمان، در قالب ده دسته‌بندی کلی شامل موارد زیر، ارایه شده است:

۱-تدوین سیاست امنیتی سازمان
۲-ایجاد تشکیلات تامین امنیت سازمان
۳-دسته بندی سرمایه‌ها و تعیین کنترل‌های لازم
۴-امنیت پرسنلی
۵-امنیت فیزیکی و پیرامونی
۶-مدیریت ارتباطات
۷-کنترل دسترسی
۸-نگهداری و توسعه سیستم‌ها

۹-مدیریت تداوم فعالیت سازمان
۱۰-پاسخگویی به نیازهای امنیتی

بخش دوم:

در این بخش از استاندارد برای تامین امنیت اطلاعات و ارتباطات سازمان ،مطابق شکل (۱)یک چرخهٔ ایمن‌سازی شامل ۴ مرحلهٔ طراحی، پیاده‌سازی، تست و اصلاح ارایه شده و جزییات هر یک از مراحل به همراه لیست و محتوای مستندات مورد نیاز جهت ایجاد سیستم مدیریت امنیت اطلاعات سازمان، ارایه شده است.



شکل(۱): مراحل ایمن‌سازی بر اساس استاندارد BS7799:2002

چرا در میان استانداردها، BSV۹۹ معروف است؟

بیشتر صحبت‌های امروزه در مورد BS7799-2 است که در سال ۱۹۹۹ منتشر شده است. دلیل محبوبیت این استاندارد در سال‌های اخیر اهمیت بسیار زیاد حفاظت اطلاعات می‌باشد.

امروزه دسته‌بندی و درجه‌بندی اهمیت دارایی‌های با ارزش سازمان توسط مدیریت سازمان مشخص می‌شود. هرچقدر این دسته‌بندی و اطلاعات کامل باشد پیشبرد اهداف امنیتی یک سازمان آسانتر صورت خواهد پذیرفت.

BS7799-2 یکی از معدود روش‌هایی است که اطلاعات و امنیت آنها را با جزییات کامل بیان می‌کند. در واقع چگونگی مدیریت امنیت اطلاعات توسط BS7799 بیان شده است.

سازگاری: سازگاری با BS7799 سازمان را مجبور می‌سازد سیستم امنیت اطلاعات را اجرا نموده و مستند نماید و همچنین بندهای کنترلی مختلف در آن سازمان اجرا شود.

گواهینامه : BS7799 در صورت مستند بودن کلیه موارد امنیتی یک سازمان و همچنین به اجرا در آمدن صحیح آنها به سازمان تعلق می‌گیرد. در واقع پیاده‌سازی کلیه کنترل‌های BS7799 شرط دریافت گواهینامه می‌باشد.

قبل از تطابق و حرکت در مسیر داشتن این استاندارد موارد زیر مدنظر هستند:

۱-دانستن وسعت و گستردگی کنترل‌های مختلف استاندارد.
۲-مشخص کردن کنترل‌های وابسته به سازمان
۳-سنجیدن فواید استاندارد با توجه به هزینه‌ها و زمان
۴-نیازمندی‌های قانونی
۵-نیازمندی‌های تنظیمی
۶-ساختار ساختمان

ممکن است در این ارزیابی اولیه خیلی از سازمان‌ها به نتیجه برسند که نیاز برای اجرای کامل استاندارد وجود ندارد و تنها به استانداردسازی بخشی از سازمان اکتفا نمایند.

آیا باید گواهینامه گرفت؟

تصمیم‌گیری در این مورد کاملاً خصوصی است و به موارد زیر و میزان اهمیت در یک سازمان بستگی دارد.

۱-محدوده امنیتی مشخص شود.
۲-مستندات و اجرا با کنترل‌های مصوب در استاندارد سازگاری داشته باشد.
۳-استثنی‌ها مشخص و توجیه منطقی شوند.

بعد از این مراحل می‌توان برای دریافت گواهینامه BS7799 اقدام کرد لذا نیاز به حضور ارزیاب و کارشناسان BS7799 پیدا خواهد شد.

اجرای پیش نیازها پروسه پر زحمت و مداومی را طلب می‌کند که باید با دقت و کاملاً دقیق اجرا شود. برای اجرای این پیش‌نیازها نیاز به مرور دوره‌ای توسط ارزیاب‌های BS7799 می‌باشد که در صورت اخذ مدرک BS7799 این بازدید توسط ارزیابان BS7799 هرسه سال یکبار تکرار خواهد شد. در آخر، نتایج اخذ این مدرک و مفید بودن آن در پیشبرد اهداف سازمان باید کاملا مدنظر قرار گیرد. البته اعتباری که یک سازمان در نتیجه اخذ این مدرک خواهد گرفت باید مورد توجه قرار گیرد.

تفکر اینکه اخذ این گواهینامه ۱۰۰٪ اطلاعات یک سازمان را امن می‌کند کاملا اشتباه است و تنها سازمان قادر می‌شود خطرات را تا حد زیادی پیش‌بینی کرده، قانونمند نموده و خنثی نماید.

چه مواردی برای اخذ گواهینامه مورد نیاز است؟

برای دریافت این گواهینامه می‌بایست کلیه سازگاری‌ها با بندهای استاندارد صورت پذیرد و همچنین نیاز به بازدیدهای دوره‌ای توسط ارزیاب‌های BS7799 می‌باشد. پس از محقق شدن کلیه مراحل و ارزیابی‌های مختلف و سازگاری کامل، شخص گواهینامه‌دهنده از شرکت معتبر BSI جهت بازدید نهایی و اعطای گواهینامه مراجعه خواهد کرد. در صورت عدم تطابق بیش از یک کنترل مهم اعطای گواهینامه به آینده و بازدید بعدی منوط خواهد شد.

نتیجه : BS7799-2 استانداردی مدیریتی برای حفاظت از اطلاعات و دارایی‌های با اهمیت یک سازمان می‌باشد. و اگر هر سازمان نیازمند امنیت فضای تبادل اطلاعات است BS7799 نظر سازمان را تامین خواهد کرد. لازم به ذکر است سازمان‌ها جهت خنثی کردن مخاطرات امنیتی هزینه‌ای پرداخت نمی‌کنند، بلکه سرمایه‌گذاری می‌نمایند. چنانچه مدیران یک سازمان نگرش سرمایه‌گذاری یا پرداخت هزینه جهت پیاده‌سازی استانداردهای امنیتی داشته باشند در قبول پیاده‌سازی این استانداردها در سازمان نقش بسزایی خواهد داشت.

---

* ISMS: Information Security Management System

منابع :

www.sgnet.net
www.Itiran.com