امنیت فضای تبادل اطلاعات

علیرضا بزرگمهر
Bozorgmehri@persiafava.com

بخش قابل توجهی از وضعیت نامطلوب "امنیت فضای تبادل اطلاعات" کشور (افتا)، بواسطه فقدان زیرساخت هائی از قبیل نظام ارزیابی امنیتی فضای تبادل اطلاعات، نظام صدور گواهی و زیرساختار کلید عمومی، نظام تحلیل و مدیریت مخاطرات امنیتی، نظام پیشگیری و مقابله با حوادث فضای تبادل اطلاعات، نظام مقابله با جرائم فضای تبادل اطلاعات و سایر زیرساخت های امنیت فضای تبادل اطلاعات در کشور می باشد .از سوی دیگر، وجود زیرساخت های فوق، قطعا تاثیر بسزائی در ایمن سازی فضای تبادل اطلاعات دستگاههای دولتی خواهد داشت.

در همین راستا نهاد ریاست جمهوری در مورخ 1383/7/19 طی بخشنامه ای بشماره 39360 به کلیه وزارتخانه ها، سازمانها، موسسات، شرکتهای دولتی، نهادهای انقلاب اسلامی و استانداریها، برنامه امنیت فضای تبادل اطلاعات را ظرف شش ماه به سازمان برنامه و بودجه ارسال نمایند.

در مورد ضرورت و اهمیت پیاده‌سازی سیستم مدیریت امنیت مهمترین نکته اینکه در سند راهبردی امنیت فضای تبادل اطلاعات کشور، پیاده‌سازی سیستم مدیریت امنیت اطلاعات بعنوان یکی از اقدامات اساسی برای راهبردهای امن‌سازی زیرساختهای حیاتی کشور در قبال حملات الکترونیکی و ایجاد و توسعهٔ نظام‌های فنی فرابخشی افتا در نظر گرفته شده است که اجرای آن باید توسط تمام سازمانهای دولتی مد نظر قرار گیرد. ایجاد اعتماد در مشتریان و ارباب رجوع، ایجاد شفافیت، قابلیت پیگیری و حسابرسی، کاهش ریسک‌های فنی، مالی، حقوقی و قضایی ناشی از عدم رعایت مسائل امنیتی از دیگر مزایای پیاده‌سازی این سیستم به شمار می‌روند.

پارامترهای حیاتی برای موفقیت در پیاده سازی سیستم مدیریت امنیت طبق استاندارد عبارتند از:

1- تطابق سیاست‌ها، اهداف و فعالیت‌های امنیت اطلاعات با اهداف سازمان

2- رهیافت و چهارچوبی سازگار با فرهنگ سازمان برای پیاده‌سازی، حفظ، نظارت و بهبود امنیت اطلاعات

3- تعهد و پشتیبانی مؤثر تمام سطوح مدیریتی سازمان

4- درک دقیق نیازمندیهای امنیتی، ارزیابی مخاطرات و مدیریت مخاطرات

5- آگاهی رسانی در مورد سیاست‌های امنیتی، استانداردهای امنیتی و دیگر مسائل امنیتی به تمام مدیران، کارمندان و پیمانکاران

6- تدارک و تأمین بودجهٔ لازم برای فعالیت‌های مدیریت امنیت اطلاعات
7- آموزش مؤثر مبانی پیاده‌سازی و ممیزی سیستم مدیریت امنیت با استفاده از مؤسسات آموزشی و دروس معتبر
8- ایجاد یک روال مؤثر برای مدیریت حوادث امنیتی
9- ایجاد یک سیستم اندازه‌گیری برای ارزیابی کارآیی سیستم مدیریت امنیت اطلاعات و دریافت پیشنهادات برای بهبود سیستم.

در این رابطه دبیرخانه شورای عالی امنیت فضای تبادل اطلاعات کشور یک راهنمای پیاده سازی سیستم مدیریت اطلاعات بر اساس استاندارد ISO/IEC17799 تدوین نمود.

این استاندارد که اولین استاندارد در حوزهء مدیریت امنیت می باشد، در سال 1995 توسط مؤسسه استاندارد انگلیس (BSI) تحت عنوان BS7799 نگرش سیستماتیک به حوزهٔ امنیت اطلاعات مورد توجه قرار گرفت. این استاندارد بعد از بررسی‌های بسیار و تغییرات چندی به جدیدترین استانداردهای بین‌المللی در زمینهٔ امنیت اطلاعات ISO/IEC 17799:2005 و ISO/IEC 27001:2005 تبدیل گردید.

اگر چه تا قبل از تدوین استاندارد ISO 27001 دریافت گواهی بین‌المللی برای پیاده‌سازی سیستم مدیریت امنیت تنها بر اساس استاندارد BS7799:2 امکان‌پذیر بود اما جامعهٔ بین‌المللی شاهد رشد بسیار قابل توجهی در اقدام برای پیاده‌سازی این استاندارد و کسب گواهی مربوطه بود به طوریکه تا کنون بیش از 2000 شرکت موفق به دریافت این گواهی شدند. با فراهم آمدن امکان کسب گواهی تحت عنوان مؤسسه بین‌المللی (ISO) شاهد رویکرد بسیار فزاینده‌ای به سمت پیاده‌سازی این استاندارد می‌باشیم.

برآورده کردن فاکتورهای مندرج در این مقاله در بسیاری از سازمانها نیازمند درک عمیقی از فعالیت‌های سازمان استفاده از متدلوژی‌های معتبر و آزمایش شده برای پیاده‌سازی سیستم مدیریت امنیت اطلاعات (نظیر متدلوژی مؤسسهٔ BSI) می‌باشد. برای استقرار این استاندارد در یک سازمان مراحل زیر بطور معمول طی می گردد :

1- بررسی وضع موجود سازمان طبق چک لیست استاندارد BS7799
2- تدوین طرح مطلوب امنیت فضای تبادل اطلاعات
3- استقرار طرح
4- آزمون نفوذ پذیری و نشت اطلاعات توسط موسسات مورد تایید BSI
5- ممیزی سازمان بر اساس استاندارد ISO/IEC 17799:2005 و ISO/IEC 27001:2005 و اخذ گواهی