استانداردهای حوزه امنیت اطلاعات

* ترجمه: رقیه خبیری
دانشجوی دکترای تخصصی مدیریت خدمات بهداشتی و درمانی گروه علوم مدیریت و اقتصاد بهداشت، دانشکده بهداشت، دانشگاه علوم پزشکی تهران

استاندارد ISO/ BS۷۷۹۹ ۱۷۷۹۹ ، استاندارد سیستم‌های مدیریت اطلاعات است که هدف آن فراهم سازی پایه و اساسی برای توسعه استانداردهای امنیت سازمانی و مدیریت کارای امنیت اطلاعات و به وجود آوردن اعتماد در فعالیت‌های درون سازمانی است.

هم اکنون از این استاندارد به عنوان یک مستند مرجع برای دریافت گواهینامه مدیریت امنیت اطلاعات در بسیاری از کشورها استفاده می‌شود. این استاندارد می‌تواند برای هر سازمانی اعم از خصوصی یا دولتی که مسئولیت حفظ و نگهداری یک سری اطلاعات مهم و محرمانه را در سیستمهای داخلی یا خارجی به عهده داشته یا مایل است میزان امنیت اطلاعاتش را در مقایسه با یک استاندارد بین المللی مورد سنجش و ارزیابی قرار دهد، مورد توجه قرار گیرد.

سازمان‌های بیمه، موسسات مالی و سایر سازمان‌های دولتی که ریسک آسیب پذیری اطلاعات در آنها بسیار بالاست توجه زیادی به دریافت گواهینامهء تطبیق با این استاندارد نشان می‌دهند.

دریافت گواهینامه استاندارد BS۷۷۹۹ از یک گروه یا سازمان معتبر بین المللی نمایانگر قابلیت‌های اجرایی و توانمندی مدیریت وکنترل وتضمین وجود سه عنصر محرمانگی، صحت، و در دسترس بودن اطلاعات می‌باشد. این گواهینامه می‌تواند به یک سازمان، بخشی از یک سازمان یا حتی یک سایت اینترنتی اعطا شود و سپس به مرور در سازمان گسترش یافته و سایر بخش‌ها را نیز پوشش دهد.

تاریخچه استانداردهای مربوط به حفظ امنیت و محرمانگی اطلاعات

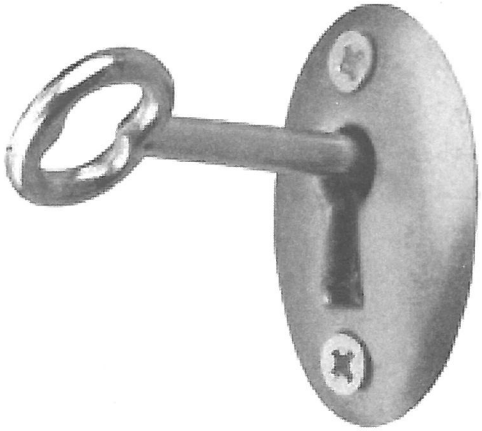
استاندارد ISO ۱۷۷۹۹ اولین بار در دسامبر سال ۲۰۰۰ از سوی سازمان بین المللی استانداردسازی. (International Organizationof Standardization, www.iso.ch)به عنوان استانداردی جهت حفظ امنیت و محرمانگی اطلاعات معرفی گردید. این استاندارد از استاندارد مدیریت امنیت اطلاعات BS۷۷۹۹ که از سوی موسسه استاندارد بریتانیا (BSI) معرفی شده بود، مشتق گردیده است.

در پاسخ به تقاضای روزافزون صنایع، در سال ۱۹۹۰ یک گروه کاری برای مطالعه در زمینه امنیت اطلاعات تشکیل شد. این گروه در سال ۱۹۹۳ یک دستورالعمل کاری در زمینه مدیریت امنیت اطلاعات منتشر ساخت و همین مجموعه، زمینه ای برای تعریف اولین نسخه استاندارد BS۷۷۹۹ شد که در سال ۱۹۹۵ معرفی گردید.

در اواخر سال ۱۹۹۵ در پی درخواست‌های مکرر سازمان‌های گوناگون، موسسه استاندارد بریتانیا، برنامه ای برای ممیزی و اعتبار بخشی شرکت‌ها و سازمان‌ها طراحی کرد که به برنامه c:cure معروف بود. در ادامه یک کمیته پایش و ارزیابی نیز تشکیل شد که یک نسخه به روز شده از استاندارد BS۷۷۹۹ را در سال ۱۹۸۸ و ۱۹۹۹ منتشر ساخت.

درحال حاضر این استاندارد شامل دو قسمت است. بخش اول آن دستورالعمل‌های کاری و بخش دوم آن اختصاصات مربوط به سیستم‌های مدیریت امنیت اطلاعات می‌باشد.

درحالی که بسیاری از سازمان‌ها از استاندارد مذکور استفاده می‌کردند با این حال تقاضاهای زیادی در سطح جهان برای معرفی یک استاندارد بین المللی که در همه جای دنیا به رسمیت شناخته شود مطرح بود. در همین راستا سازمان بین المللی استاندارد سازی بخش اول استاندارد BS۷۷۹۹ را با انجام یک سری اصلاحات به عنوان استاندارد ISO۱۷۷۹۹ در سپتامبر سال ۲۰۰۰ به عنوان استاندارد جامع و جهانی مدیریت امنیت اطلاعات معرفی نمود.



حفظ امنیت اطلاعات پزشکی کامپیوتری:

• محرمانگی به این معنی است که اطلاعات و داده هایی که یک بار توسط بیماران افشا می‌شوند، بدون اجازه منشا اطلاعات (شخص) به اشتراک گذاشته نخواهند شد. به اشتراک گذاشتن اطلاعات شخصی به کسانی محدود می‌شود که مجاز به داشتن آن اطلاعات می باشند. در مراقبتهای بهداشتی و درمانی، افراد حجم زیادی از اطلاعات محرمانه را با متخصصین در میان می‌گذارند. متخصصین و سازمانهای مراقبتهای بهداشتی و درمانی یک مسئولیت اخلاقی دیرینه و عمیق برای حفظ این اطلاعات محرمانه دارند.

• کمیته E۳۱ سازمان ASTM (American Society for Testing and Materials) در مورد انفورماتیک بهداشتی، استانداردها و دستورالعمل‌های متعددی را در ارتباط با امنیت داده‌ها و سیستم منتشر نموده است. سایر سازمان‌ها از قبیل انجمن مدیریت اطلاعات بهداشتی امریکا و انجمن انفورماتیک پزشکی امریکا نیز انتشاراتی داشته اند که هدف آنها کمک به افراد و سازمان‌ها می‌باشد تا تعهد خود را در حق محرمانگی گیرنده خدمت و ارائه کننده خدمت حفظ کنند.

می‌گویند تا به حال هیچ کس به خاطر افشاء و انتشار نادرست مدارک و اطلاعات پزشکی اش نمرده است اما سالانه هزاران هزار نفر تنها به دلیل آنکه دسترسی سریع به اطلاعات پزشکی آنها ممکن نیست، زندگی خود را از دست می‌دهند. بنابراین باید بین نیاز به حفظ جنبه محرمانه اسناد و مدارک پزشکی و نیاز به دسترسی سریع به این اطلاعات تعادل مناسبی برقرار شود.

عناصر امنیت:

در مورد عناصر امنیت اطلاعات به تقسیم بندی‌های مختلفی اشاره شده است اما آنچه میان همه تعاریف و طبقه بندی‌ها مشترک شناخته شده عبارت است از:

• تصدیق یا تایید هویت کاربران (Authentication)
• به رسمیت شناسی اختیارات کاربران(Authorization)
•پاسخگویی (Accountability)
• موجود بودن اطلاعات مورد نیاز (Availability)
• ممیزی (Audition)
• یکپارچه سازی اطلاعات(Integration)
• کنترل میزان دسترسی ورمز گذاری

از سه عنصر اول تحت عنوان ۳A یاد می‌شود وبه عناصر اصلی حفظ امنیت اطلاعات معروفند که امروزه در زمینه حفظ محرمانگی و کنترل سطوح دسترسی در تجارت الکترونیک از اهمیت چشمگیری برخوردار می‌باشند. یکپارچه سازی اطلاعات (Integrity) نیز به معنای کسب اطمینان از این مساله مهم است که انجام اصلاحات لازم در مورد اسناد، مدارک واطلاعات توسط افراد مجاز صورت گرفته و این امر با استفاده از رویه‌ها و فرایندهای مجاز و تعریف شده صورت پذیرفته و همخوانی و سازگاری درونی و بیرونی آنها حفظ می‌شود.

معمولا برای تعریف سطح اختیارات افراد برای دسترسی به اسناد و اطلاعات از روشهای مختلفی استفاده می‌شود که برخی از آنها عبارتند از:

• روش مبتنی بر کاربر(User-Based)
• در این روش، سطح دسترسی برحسب این که کاربر مورد نظر چه کسی بوده و از چه هویتی برخوردار می‌باشد، تعریف می‌شود.
• روش مبتنی بر نقش کاربر(Role-Based)
• در این شیوه سطح اختیارات بر حسب نوع نقشی که کاربر ایفا می‌نماید تعریف می‌شود.
• روش مبتنی بر موقعیت(Context-Based)
• در این شیوه تعریف سطح دسترسی و اختیار یک فرد بر حسب ترکیبی از عوامل مختلف صورت می‌پذیرد و این ترکیب به این صورت است که:

فرد مورد نظر چه کسی است + کجا است + چه نقشی دارد + در چه زمانی قرار دارد.

منابع:

Carlson. Tom, "Information Security Management: Understanding ISO ۱۷۷۰۰", Lucent Technologies Worldwide Service, ۲۰۰۰. Available at http://www.netbotz.com/library/ISO_۱۷۷۹۹.pdf