استاندارد جدیدی برای مدیریت ایمنی اطلاعات

دکتر کامبیز فرقاندوست حقیقی

این مقاله ره‌آوردی از سمینار حسابرسی سیستمهای اطلاعاتی است که در تیرماه سال ۱۳۸۲ به‌وسیله انجمن امورمالی و حسابداری خبره عمومی (CIPFA) در بیرمنگام برگزار گردید. نویسنده که از شاگردان و پیروان علمی استاد گرانقدر مرحوم دکتر عزیز نبوی است، به‌پاس قدردانی از مقام شامخ استاد در تحول دانش حسابداری در ایران، مقاله را به ایشان تقدیم می‌کند.

سوابق تاریخی

از سالهای ۱۹۷۰ به بعد اندیشه مدیریت ایمنی اطلاعات ایجاد گردید. ظرف ده پانزده سال بعد، این نیاز به همه جا تسری یافت تا آنجا که در حدود سالهای ۱۹۹۰ در انگلستان مجموعه‌ای تحت عنوان «**آیین رفتاری مدیریت ایمنی اطلاعات**»[1] منتشر شد. به‌موازات انتشار این نشریه در انگلستان و همزمان با آن، در اروپا نیز مباحثاتی در مورد ایجاد یک دیدگاه مشترک مشخص در ارتباط با مشکلات ایمنی اطلاعات و راه‌حل‌های احتمالی مرتبط با آنها در جریان بود. این مباحثات منجربه انتشار نشریه‌ای به نام «**کتاب سبز**»[2] گردید. متاسفانه نشریه کتاب سبز بسیار حجیم و غیرقابل استفاده بود.

آیین رفتار حرفه‌ای

صنعت و بازرگانی انگلستان همواره فشاری بر دولت این کشور وارد کرده تا نسبت به تامین محیطی که موجب "**ایجاد اعتماد متقابل بین پایگاههای مختلف کامپیوتری و شرکای تجاری**" گردد، اقدام نماید. این فشارها بویژه در محیط ارتباطی و الکترونیکی بین سازمانها همواره به‌شدت رو به افزایش بوده است.

شاید باورکردنی نباشد که این تلاشها هنگامی صورت می گرفت که بسیاری ازمردم هنوز چیزی در مورد اینترنت نشنیده و تصوری از قابلیتهای کاربردی آن در محیط تجاری نداشتند.

آیین رفتار حرفه‌ای مورد بحث توسط گروهی از نهادهای ذینفع آماده شد. از جمله نهادهایی که در آماده سازی آن دخالت داشتند، می توان دولت، تولیدکنندگان صنعتی، صنعت راه‌آهن، بانکها، مشاوران فناوری اطلاعات، و صنعت ارتباطات را نام برد. بدین ترتیب در تدوین این مجموعه جنبه‌های عملیاتی آن تا حد زیادی مورد نظر قرار گرفته بود. این بدان معنا بود که برای حسابرسان کامپیوتری نیز رویداد درخور ملاحظه‌ای به وقوع پیوسته و بالاخره مرجعی برای مقایسه و شناخت وضعیت کنترلهای مورد نیاز و مستقر در صنعت و تجارت به‌وجود آمده بود. علاوه بر این، مرجع مزبور در مورد بسیاری از سازمانها بدون توجه به بزرگی آنها اعم از بزرگ، متوسط و کوچک قابل اعمال بود. این نشریه آیین رفتار حرفه‌ای بود که در سال ۱۹۹۵ به **استاندارد شماره ۷۷۹۹ انگلستان** (British Standard 7799) تبدیل شد.

کنترلهای اصلی و سایر کنترلها

در محافل بازرگانی و تجاری همواره

مقاومتهایی در قبول این که"**ایمنی بیشتر اطلاعات می تواند به بهبود اوضاع**"منجر گردد، وجود داشته است. البته استثنای چشمگیری هم وجود داشته است. این استثنا را همواره صنایع دفاعی تشکیل می‌داده است. با این حال باید یادآوری کرد که گزارشهای مربوط به تجاوز و سوءاستفاده از سیستمهای اطلاعاتی موید آن است که همواره می باید در راستای ایمنی بیشتر سیستمهای اطلاعاتی گام برداشته شود.

اولین قدم تعریف یک سیاست مدیریت ایمنی در سطح سازمان است بدیهی است که گستردگی این سیاستگذاری تابعی از اندازه و بزرگی سازمان و حساسیت عملیات کامپیوتری در محیط آن خواهد بود

در زمینهٔ انگیزش مدیران ارشد و تسهیل شناخت آنها از موضوع ایمنی، در آیین رفتار حرفه‌ای موصوف ده نکته کلیدی ذکر شده بود.

این ایده برای معرفی و انتشار بسیار موثر واقع شد. بویژه آنکه در میان این ده نکته، دو نکته وجود دارد که به طور مشخص همواره مشکلاتی را از نظر عملیاتی و حقوقی برای سازمانها ایجاد کرده است. این دو موضوع عبارت است از ویروسهای کامپیوتری‌وسرقت نرم‌افزارها.

ده نکته یاد شده به شرح زیر بود:

- مستندسازی خط مشی و سیاستهای مربوط به ایمنی اطلاعات،
- فرایند و برنامه تداوم عملیات تجاری،
- تعیین مسئولیتهای مرتبط با ایمنی اطلاعات،
- اعمال کنترل بر نسخه برداری از نرم‌افزارهای ویژه متعلق به هر سازمان،
- آموزش و اشاعه مفاهیم ایمنی اطلاعات،
- حفاظت از سوابق سازمان،
- گزارش رویدادهای مرتبط با ایمنی اطلاعات،
- حفاظت اطلاعات (در ارتباط با اطلاعات مرتبط با اشخاص)،
- کنترل ویروسها،
- رعایت خط مشی ها و سیاستهای ایمنی و متابعت از آنها.

در پشت این ده نکته کلیدی این فرض مستتر بوده که هر گاه سازمانی به نحو رضایت بخشی بتواند قابلیت لازم برای رعایت آنها را نشان دهد، قابلیت آن را که ضوابط مناسبی برای ایمنی اطلاعات به مورد اجراء بگذارد نیز خواهد داشت.

رویدادهای درخور ملاحظه بعدی

اقدام بعدی، تقویت آثار آیین رفتار حرفه‌ای مزبور بود. به عبارت دیگر ایجاد یک ضمانت اجرایی برای این آیین رفتار حرفه‌ای. بدین ترتیب بخش دومی برای آن تهیه شد. این بخش دوم در سال ۱۹۹۸ انتشار یافت. بخش دوم بسیار بارزتر به نظر

می رسید، زیرا که در آن مراتب لازم برای اعطای گواهینامه رسمی به سازمانها در ارتباط با رعایت استانداردهای ایمنی اطلاعات پیشبینی شده بود.

اگرچه این موضوع ممکن است فرایندی طولانی به نظر آید، اما موضوع بخش دوم استانداردهای مدیریت ایمنی سیستمهای اطلاعاتی را ضوابطی تشکیل می داد که شرکتها می باید برای دریافت گواهینامه رسمی رعایت استانداردهای مدیریت ایمنی اطلاعات، آنها را در شرکت خود معرفی می کردند و زمینه های اجرای موفقیت آمیز آنها را کاملاً فراهم می نمودند. به نظر می رسد مهمترین جنبه های این فرایند، این واقعیت را منعکس می سازد که مدیریت ارشد سازمان باید موضعی کاملاً جدی در پشتیبانی از مدیریت ایمنی اطلاعات داشته باشد در حالی که قبل از این رویدادها، اغلب ایمنی، موضوعی حاشیه‌ای و فرعی تلقی می شد و هرگز جزء یکی از اولویتهای مدیریت ارشد سازمانها به حساب نمی آمد.

قبل از پرداختن به فرایند درونی که هر سازمان باید آن را در پیش گیرد، بد نیست نگاهی به عنوانهای تصریح شده در بخش دوم انداخته شود تا برداشتی از دامنه این استانداردها به دست آید.

محتوای بخش دوم استاندارد شماره ۷۷۹۹

علاوه بر دامنه تسری استانداردها و تعاریف مرتبط با آن، دو موضوع دیگر وجود دارد که محتوای اصلی بخش دوم را تشکیل می دهد. این دو موضوع عبارتند از «ویژگیهای سیستم مدیریت ایمنی اطلاعات» و «عناصر کنترلهای تصریح شده در بخش دوم» عناصر مرتبط با کنترلها به شرح زیر است:

۱- سیاست و خط مشی های ایمنی اطلاعات،
۲- سازمان ایمنی،
۳- طبقه بندی و کنترلهای داراییها،
۴- ایمنی کارکنان،
۵- ایمنی فیزیکی و محیطی،
۶- مدیریت کامپیوتر و شبکه ها،
۷- کنترلهای دسترسی به سیستم،
۸- ایجاد و نگاهداری کنترلها،
۹- برنامه تداوم فعالیت،
۱۰- رعایت.

همانطور که مشاهده می شود این عنوانها کلیه مواردی را که می تواند در حسابرسی کامپیوتری مورد نظر قرار گیرد، یا باید مورد نظر باشد، شامل می گردد. همین قدر کافی است که گفته شود، رعایت نکردن هر کدام آنها، نیاز به توجیه کافی خواهد داشت. برای مثال، باید تصریح شود که به جای کنترل مورد نظر، کنترل جبرانی دیگری استقرار دارد یا آنکه ممکن است کنترلی در شرایط یک شرکت اصلاً مورد نداشته باشد. به عبارت دیگر، فرایند تفکر نه تنها باید از تمامیت لازم برخوردار باشد، بلکه ضرورت دارد که مستند و قابل ارائه به دیگران نیز باشد.

فرایند داخلی استقرار سیستم مدیریت ایمنی

نشان دادن این که بنگاهی از شرایط لازم برای کسب **گواهی سیستم مدیریت ایمنی**[۳] برخوردار است، متضمن آن است که نشان داده شود سیستمی رسمی برای استقرار و مدیریت ایمنی مزبور در شرکت وجود دارد. استاندارد در این مورد کمک می کند تا گامهای لازم، مشخص گردد و برداشته شود.

مدیریت ارشد سازمان باید موضعی کاملاً جدی در پشتیبانی از مدیریت ایمنی اطلاعات داشته باشد
اغلب ایمنی موضوعی حاشیه ای و فرعی تلقی می شد و هرگز جزء یکی از اولویتهای مدیریت ارشد سازمانها به حساب نمی آمد

۱ - به عنوان حسابرس، انتظار می رود که اولین گام در سطح مدیریت ارشد (بالاترین

سطح مدیریتی بنگاه) برداشته شود. در واقع، اولین قدم تعریف یک سیاست مدیریت ایمنی در سطح سازمان است. بدیهی است که گستردگی این سیاستگذاری تابعی از اندازه و بزرگی سازمان و حساسیت عملیات کامپیوتری در محیط آن خواهد بود.

۲ - در راستای ایجاد معیارهای لازم برای سنجش و نظارت در فرایند کسب گواهینامه ایمنی، سازمان باید تعریفی از داراییهای مرتبط با تکنولوژی اطلاعات و سیستم ایمنی اطلاعات را به دست دهد. در این راستا باید توجه شود که داراییهای مرتبط با تکنولوژی اطلاعات منحصر به کامپیوترها و مدارک پشتیبان آنها نیست و داراییهای به مراتب بیشتری را دربر می گیرد.

۳ - با توجه به آنچه در بند ۲ بالا تشریح شد، ضرورت انجام اقدامات لازم برای ارزیابی مخاطرات، آسیب پذیریها و آثار آنها بر داراییهای مرتبط با تکنولوژی اطلاعات تصریح شده در مفاد بند بالا، آشکار به نظر

بدین ترتیب در درازمدت مستنداتی در اختیار حسابرسان کامپیوتری قرار خواهد گرفت که به عنوان معیاری در راستای قابلیت سنجش مدیریت ایمنی سیستمهای اطلاعاتی در محیط صاحبکار یا در بخشهایی از محیط صاحبکار قابلیت کاربرد خواهد داشت

می رسد. در اینجاست که سازمان لازم است به دقت تعیین کند که آمادگی پذیرش چه میزان مخاطره (ریسک) را دارد و یا برعکس به چه سطح اطمینانی می خواهد دست یابد.

۴- به تناسب مخاطرات شناسایی شده، بنگاه باید در مورد تناسب اهداف کنترلی تعریف شده، برای رسیدن به هدفهای کنترلها و به حداقل رساندن مخاطرات، تصمیمگیری کند. مرحله بعدی، انتخاب کنترلهای مرتبط و مناسب از مجموعه استانداردهای شماره ۷۷۹۹ و هرنوع کنترل اضافی دیگری است که ممکن است از خارج از چارچوب استاندارد مزبور باید اجرا شود.

۵- پس از طی کلیه مراحل بالا، که در مورد برخی از مدیران می تواند نوعی شوک را تداعی کند (تجربیات گذشته این موضوع را تایید می کند)، لازم است یک تقاضای **صدور گواهینامه**[4] تنظیم گردد. در این فرم تقاضا باید کلیه اهداف کنترلی و کنترلهای مرتبط با آنها، دلایل انتخاب آن کنترلها و موارد استثنا شده از مجموعه کنترلهای تصریح شده در استاندارد، همراه با مستندات مربوط ارائه شود. همین فرم بعداً در راستای ارزیابی نحوه پیاده سازی و کارایی مدیریت ایمنی اطلاعات در بنگاه، مورد استفاده واقع شده و مبنای ارزیابیهای بعدی را تشکیل خواهد داد.

۶- بدین ترتیب مشاهده می شود که لازم است کلیه فرایندها با مستندات رسمی برای کلیه اقدامات انجام شده و خط مشی های مصوب، مستندسازی شده باشند. این وضعیت در مورد مستندات مرتبط با کنترلها و مستندات مرتبط با مراحل بعدی نگاهداری سیستم نیز تسری خواهد یافت.

و بالاخره نگاهی به آینده

در کشور انگلستان، فرایند دریافت گواهینامه مزبور آغاز شده است. در کشور هلند فرایند دریافت گواهینامه استاندارد شماره ۷۷۹۹ از مدتها قبل به اجرا گذاشته شده اما باید در نظر داشت که مستندات و فرمهای این استاندارد به گونه ای تنظیم و تدوین شده است که کاربرد آنها می تواند کاملاً جنبه جهانی و بین المللی داشته باشد و به هیچ وجه منحصر به دو کشور پیشگفته و یا تنها قاره اروپا نباشد.

بدین ترتیب، در درازمدت، مستنداتی در اختیار حسابرسان کامپیوتری قرار خواهد گرفت که به عنوان معیاری در راستای قابلیت سنجش مدیریت ایمنی سیستمهای اطلاعاتی، در محیط صاحبکار یا در بخشهایی از محیط صاحبکار قابلیت کاربرد خواهد داشت.

پانوشت ها:

1- A Code of Practice for Information Security Management
2- The Green Book
3- Information Security Management System
4- A Statement of Applicability

منابع:

- تقریر و تحریر و جزوات دریافت شده در سفر هیئت مامور از سازمان حسابرسی برای شرکت در سمینار حسابرسی سیستمهای کامپیوتری برگزار شده در تیرماه سال ۱۳۸۲ در کشور انگلستان
- A New Standard in Information Security Management, Vol. #1, Glyn Richard (Dick) Price, December 15, 1998
- Information Mangement Systems, Biju Mukund, Indian Express Group, 2002