فرآیند تدوین سیاست‌های امنیت اطلاعات

مهدی فهیمی ، نداسادات میرهاشم

چکیده

نظارت بر عملکرد تجهیزات فناوری‌های اطلاعاتی و ارتباطی، با گذر زمان به تدریج تبدیل به یکی از مشکلات و معضلات جدید و پرچالش سازمان‌ها شده است. با روند روبه‌رشد این فناوری‌ها پردازش داده از مراکز اصلی و متمرکز، به دفتر کار و خانهٔ شخصی افراد منتقل شده است و این تحول، دامنهٔ فعالیت واحدهای IT مدیران امنیت اطلاعات سازمان را بسیار گسترده و پیچیده کرده است. در این شرایط مدیر امنیت اطلاعات سازمان باید طرحی را به سازمان خود معرفی کند که ضمن بکارگیری ضوابط امنیتی برای اطلاعاتی که در محیط کار سازمان در گردش است، در آن عوامل دسترسی، صحت اطلاعات و محرمانه بودن، کاملاً رعایت شده و قابل اطمینان باشد. یک طرح جامع امنیت اطلاعات دارای اجزای مختلفی، از جمله استراتژی امنیت اطلاعات، معماری امنیت، متدولوژی طراحی و اجرا، سیاست‌های امنیت اطلاعات، راهنمای مدیر امنیت اطلاعات، صلاحیت احراز یک مدیر امنیت اطلاعات و در نهایت، فهرست پروژه‌های تشکیل دهنده‌ی یک طرح امنیت اطلاعات است که در این مقاله به فرآیند تدوین سند "سیاست‌های امنیت اطلاعات" به طور اجمال پرداخته خواهد شد.

کلید واژه

امنیت اطلاعات، مدیریت، طرح امنیت، سیاست‌های امنیت اطلاعات، تدوین و اجرا

تعریف‌ها

اطلاعات

اطلاعات از دیدگاه نظری معنای خاصی داشته و با بیان دقیق ریاضی نیز توصیف شده است. اطلاعات در واقع دانش و آموخته‌ها می‌باشد. به این ترتیب که خلاءهای ناشی از ناشناخته‌ها یا ندانسته‌ها با اطلاعات پر می‌شوند. به عبارت دیگر با دریافت اطلاعات دربارهٔ موضوع مشخصی که دربارهٔ آن ابهام داریم، ابهام ما کاهش یافته و در حالت ایده‌آل به دانش و آگاهی کامل دربارهٔ آن موضوع خاص خواهیم رسید]۱[.

امنیت

امنیت مفهومی است که با سه رکن مکمل محرمانگی، صحت و قابلیت دسترسی، مشخص و توصیف می‌گردد. محرمانگی به معنای جلوگیری از انتشار غیرمجاز اطلاعات است. منظور از صحت حفظ محتوی داده‌ها در مقابل تغییرات غیرمجاز یعنی

درستی و صحیح بودن اطلاعات است. به عبارت دیگر در بسیاری از موارد، لزومی به مخفی کردن اطلاعات از دیگران نداریم، ولی آنچه مهم می‌باشد این است که اطلاعات عاری از هرگونه تغییرات عمدی یا سهوی باشند. رکن سوم امنیت به معنای ضمانت در دسترس بودن اطلاعات هنگام نیاز به اطلاعات می‌باشد]۱[.

امنیت اطلاعات

متخصصین مبحث امنیت اطلاعات بر این باورند که اطلاعات تابعی از عناصر زیر است:

(محرمانگی ، درستی ، قابلیت دسترسی) f = اطلاعات

هدف اصلی مدیر امنیت اطلاعات عبارت است از حفاظت از قابلیت دسترسی، محرمانگی و درستی اطلاعات یا منابع اطلاعاتی یک سازمان. بنابراین، از دست دادن، تغییر، حذف و یا اختلال در دسترسی به اطلاعات سازمان، می‌تواند منجر به صدمات مادی و معنوی جدی و خدشه‌دار شدن اعتبار و حیثیت سازمان شود]۲[.

۱- مقدمه

امروزه سند سیاست‌های امنیت اطلاعات، بخش مهم و زیربنای ساختار امنیت اطلاعات موسسات پیشرو بشمار می‌آید. از طرفی به دلیل جدید بودن این مبحث در فضای دیجیتال، اکثر سازمان ها با چالش جدی مواجه هستند. به عنوان نمونه، در بررسی‌های اخیر (سال ۲۰۰۴ م) مشخص شده است که ۸۵ درصد سازمان‌ها، حتی در کشورهای پیشرو، فاقد سیاست‌های رسمی و مدون امنیت اطلاعات بوده‌اند. یک سند جامع "سیاست‌های امنیت اطلاعات" باید حداقل پاسخگوی سوال‌های زیر باشد.

۱- آیا سیاست‌های امنیت اطلاعات از جامعیت لازم برخوردار است؟

۲- آیا این سیاست‌ها و رویه‌ها به طور مستمر روزآمد می‌شوند؟

۳- آیا سیاست‌های امنیت اطلاعات به سهولت برای همگان قابل دسترسی هستند؟

۴- آیا کاربران تبعیت لازم از این سیاست‌ها را دارند؟

این سند به عنوان یک راهنمای تخصصی برای همهٔ کارکنان سازمان مورد استفاده قرار گرفته و با راه حل‌های پیشنهادی و ابزارهای یکسان می‌تواند پاسخگوی کلیهٔ افراد مرتبط باشد. در گذشته تصور بر این بود که ساختار و مدیریت امنیت اطلاعات، صرفاً برای سازمان‌های بزرگ مورد نیاز است ولی با گسترش موج اطلاعات و ارتباطات، مشاهده می‌گردد که کلیهٔ سازمان‌ها به منظور بقاء و ادامهٔ حیات در فضای کسب و کار الکترونیک، نیاز به طراحی و اجرای ساختار و سیاست‌های امنیت اطلاعات روزآمد دارند.

سیاست‌های امنیت اطلاعات باید با بهره‌گیری از استانداردها[1] و دستورالعمل‌های سازمانی تهیه شوند، در غیر این صورت ممکن است این سیاست‌ها مورد استفادهٔ کامل قرار نگیرد و یا در مجموعهٔ سازمان نقاط آسیب‌پذیری برای افراد فرصت طلب از داخل یا خارج سازمان فراهم نماید.

طی سال‌های اخیر، بنگاه‌های تحقیقاتی IT ، اقدام به تدوین و نشر سیاست‌های امنیت اطلاعات کرده‌اند که این اسناد می‌تواند به عنوان الگو مورد استفاده قرار گیرد ولی در نهایت هر سازمان باید با تشکیل شورای کارشناسی مورد نیاز، سیاست-های امنیت اطلاعات بومی خود را تدوین، تصویب و اجرا نماید. به عنوان مثال بعضی از اعضای این شورا عبارتند از: نمایندگان ذیصلاح از مجموعه‌های فناوری اطلاعات، مدیریت حراست، دفتر حقوقی، مدیریت نیروی انسانی، مدیریت بازرسی، مدیریت طرح و برنامه و... .

بعضی از سازمان‌ها، سند راهنمای امنیت اطلاعات خود را از طریق تار جهان گستر و به صورت برخط[2] در اختیار کاربران قرار می‌دهند و بعضی از سازمان‌ها، سند فوق را در مجموعه‌های IT سازمان روی رایانه‌های عمومی نصب می‌کنند. در بسیاری

۱- به عنوان نمونه می‌توان از استانداردهای ISO 17799 و BS7799 نام برد.

2 - Online

از سازمان‌ها، کارشناس یا مدیر امنیت اطلاعات باید به صورت پاره وقت در مجموعه حضور داشته باشد و از طرفی، فرد یا واحدی باید در تمام ساعات شبانه روز پاسخگوی نیاز و سئوالات احتمالی کابران باشد. به همین دلیل چنانچه سند سیاست‌های امنیت اطلاعات سازمان بصورت برخط و در طول شبانه روز در اختیار کارکنان سازمان باشد، از بسیاری از مشکلات و حوادث احتمالی پیشگیری خواهد کرد. به عبارت دیگر، برخورداری از سیاست‌های امنیت اطلاعات موجب خواهد شد تا از سرمایه‌های اطلاعاتی و دانش سازمان، مراقبت لازم به عمل آمده، کلیهٔ واحدهای سازمان در تدوین و اجرای این سیاست‌ها هماهنگ باشند و از طرفی کلیهٔ کاربران نسبت به اختیارات و وظایف خود را در قبال تدابیر امنیت اطلاعات سازمان آگاه باشند.

۲- نمونه‌ای از محتوای یک سند سیاست های امنیت اطلاعات

به عنوان نمونه در این مقاله به سرفصل‌های اصلی یکی از سندهای "سیاست‌های امنیت اطلاعات" اشاره می‌گردد. سرفصل‌های اصلی این سند عبارتند از]۲[:

۱- امنیت سخت‌افزار و تجهیزات
۲- کنترل دسترسی‌ها (اطلاعات و سیستم)
۳- پردازش اطلاعات و اسناد
۴- خرید و نگهداری نرم‌افزارهای تجاری
۵- طراحی و پشتیبانی نرم‌افزارهای غیرتجاری
۶- رویارویی با تهاجمات رایانه‌ای
۷- تبعیت از قوانین و مقررات کشور
۸- برنامه‌ریزی برای بقای کسب و کار در شرایط بحران
۹- امنیت اطلاعات و مدیریت نیروی انسانی در سازمان
۱۰- کسب و کار الکترونیک و امنیت اطلاعات
۱۱- آموزش و آگاه‌سازی کارکنان
۱۲- حفاظت از اماکن سازمان
۱۳- شناسایی و رویارویی با حوادث امنیت اطلاعات
۱۴- طبقه‌بندی اطلاعات و داده
۱۵- واژه نامه تخصصی

۳- مراحل تدوین و اجرای سیاست‌های امنیت اطلاعات یک سازمان

با بررسی‌های به عمل آمده به نظر می‌رسد هفت گام اصلی برای تدوین، تصویب و اجرای سیاست‌های امنیت اطلاعات یک سازمان وجود داشته باشد. این گام‌ها به ترتیب عبارتند از:

گام ۱- انتخاب الگوی کار

بررسی اسناد تخصصی منتشر شده و انتخاب یکی از آنها به عنوان الگو و راهنما[1] . سند منتخب باید ضمن برخورداری از جامعیت لازم به فرهنگ سازمانی و کسب و کار سازمان نزدیک باشد. از طرفی، نباید فراموش کرد که سند (الگوی) انتخابی باید تبعیت لازم از اسناد متدولوژی تدوین و معماری امنیت اطلاعات طرح را داشته باشد.

۱- معمولاً سندهای تخصصی این حوزه بین ۷۰۰ الی ۲۰۰۰ دلار به فروش می‌رسند.

گام ۲- تشکیل گروه کار و مطالعهٔ سند خریداری شده

۲-۱- شورایی متشکل از واحدهای ذینفع سازمان تشکیل گردد. به عنوان نمونه، نمایندهٔ واحدهای فناوری اطلاعات (ترجیحاً کارشناس مرتبط با مبحث امنیت اطلاعات) ، حراست، دفتر حقوقی، بازرسی، طرح و برنامه و نیروی انسانی، می‌توانند از جمله اعضای این شورا باشند. ممکن است بعضی از اعضای این شورا به صورت موردی و بنا به نیاز در جلسات حضور یابند؛ مانند نمایندهٔ واحدهای مالی و آموزش.

۲-۲- مطالعهٔ محتویات سند خریداری شده توسط اعضا و انتخاب فصل‌ها و زیرمجموعه‌هایی که پاسخگوی سازمان شما خواهند بود. به عنوان نمونه، چنانچه سازمان مأموریتی برای تولید نرم‌افزارهای تخصصی خود ندارد، فصل مربوط به نظارت بر تولید و بهره‌برداری از این نرم‌افزارها حذف خواهد شد.

گام ۳- تعریف اصطلاحات تخصصی امنیت اطلاعات

نظر به میان رشته‌ای بودن مبحث "مدیریت امنیت اطلاعات" و بهره‌گیری از اصطلاحات فناوری اطلاعات و ارتباطات، مدیریت و امنیت و از طرفی انتشار تعریف‌های متعدد توسط سازمان‌های مختلف در سطح جهان، نیاز است تا کلیهٔ اصطلاحات تخصصی در قالب یک فرهنگ توصیفی به زبان فارسی تهیه شده تا در هنگام مطالعهٔ سند، مورد استفادهٔ کاربران قرار گیرد و به عبارتی، زبان یکسان بین افراد مختلف سازمان ایجاد کند.

گام ۴- تدوین نسخهٔ بومی از سند امنیت اطلاعات

معمولاً اسناد تخصصی منتشر شده در زمینهٔ امنیت اطلاعات به صورت جامع بوده و نیاز اکثر سازمان‌ها را پوشش می‌دهند. اما بدیهی است که یک سند خارجی بر اساس قوانین و مقررات ملی هر کشور (مانند قوانین جرایم رایانه‌ای) و آیین‌نامه‌های داخلی هر سازمان تنظیم می‌گردد. بنابراین محتوای سند و روند تدوین آن باید به عنوان الگو مورد استفاده قرار گرفته ولی محتوای بعضی از فصل‌ها و زیرمجموعه‌های آن باید به صورت بومی و بر اساس نیاز سازمان تدوین گردد. در این گام تعامل و همکاری سازمانی فعال بین واحدهای پیش گفته، به کیفیت و غنای سند خواهد افزود.

گام ۵- ضمانت اجرائی سند

بنابر تناسب هر سازمان و فرهنگ سازمانی حاکم، سند سیاست‌های امنیت اطلاعات باید به تصویب مسئولین مربوط رسیده تا از ضمانت اجرائی لازم برخوردار باشد.

به عنوان مثال، ممکن است سندی برای استفاده دز یکی از زیرمجموعه‌های وزارت‌خانه باشد و بنابراین تصویب و ابلاغ آن توسط واحد فناوری اطلاعات وزارت‌خانه کافی باشد.

ولی گاهی اوقات ممکن است این اسناد پوشش فراسازمانی داشته باشند (مانند نیروهای مسلح) . در این گونه موارد سند نهایی باید به تصویب ذینفعان طرح جامع IT (مانند: وزارت دفاع، ستاد کل نیروهای مسلح، موسسهٔ تحقیقات، شرکت ایزایران و...) رسیده و سپس ابلاغ گردد.

روزآمدسازی سند نیز با نظارت مسئولین پیش‌گفته انجام خواهد شد تا ضمانت اجرایی لازم را در کلیهٔ سازمان‌های عضو داشته باشد.

گام ۶- انتشار و ابلاغ سند

در این مرحله سیاست‌های امنیت اطلاعات با حضور شورای تشکیل شده مورد بحث و بررسی، تدوین و تصویب قرار گرفته است و اکنون باید به کلیهٔ کارکنان سازمان الاغ گردد.

یکی از مخاطبین اصلی این ابلاغیه مدیریت نیروی انسانی سازمان خواهد بود که باید ملاحظات حفاظتی لازم را در عقد قراردادها و عزل و نصب کارکنان مورد توجه قرار دهد.

گام ۷- هماهنگی در اجرا

درنهایت تدابیر لازم به منظور اجرای سیاست‌ها، هماهنگی مجموعه با این سیاست‌ها و تبعیت از مصوبات انجام شده مورد نیاز است. سیاست‌های امنیت اطلاعات به طور گسترده‌ای وارد حوزه‌های مختلف امنیت اطلاعات در لایه‌های مختلف سازمان شده است. از طرفی، اعمال این سیاست‌ها به صورت روش‌های اجرایی و کاربردی در فعالیت‌های روزمرهٔ کارکنان، خود یک چالش مدیریتی به شمار می‌رود. به عبارت دیگر، بر اساس سیاست‌های ابلاغ شدهٔ فوق، هر واحد باید بنا به تناسب، رویه‌های مورد نیاز هر سیاست را تدوین و ابلاغ نماید. همچنین اجرای بعضی از سیاست‌ها منتهی به تعریف و اجرای پروژه‌های فنی خواهد شد تا زنجیرهٔ طرح امنیت سازمان کامل شود. از جملهٔ این پروژه‌ها می‌توان به مواردی مانند: دیواره‌های آتش، طبقه-بندی اطلاعات، نرم‌افزارهای ضد ویروس و... اشاره کرد.

در ادامه نمونه ای از سند سیاست‌های امنیت اطلاعات احتمالی، آورده شده است.

ماده ۶-۱-۹- دفاع در مقابل حملات ویروسی

سیاست پیشنهادی

بدون استثناء نرم افزارهای ضد ویروس بایستی بر روی تمامی رایانه های شخصی نصب شده و به طور مستمر روزآمدشود. دائماً سرورها، رایانه های شخصی و رایانه های قابل حمل توسط این نرم افزارهاکنترل و بررسی شود.

یادداشت توضیحی

می‌توان احتمال آلودگی به ویروس را با بکارگیری نرم افزارهای ضدویروس تایید شده و روزآمدسازی مستمر فایل واکسن-های مرتبط با آن، به حداقل رساند. اغلب شرکت ها و تهیه کنندگان نرم‌افزارهای ضدویروس، یک چنین روزآمدسازی را از طریق وب‌گاه خود فراهم می کنند.

موارد امنیت اطلاعات که بایستی در این زمینه در سیاستگذاری ها مورد توجه قرارگیرد، عبارتنداز:

هنگامی که طرح تهیه شده فاقد پاسخگویی لازم باشد، عکس العمل کاربران، مسئولین فناوری اطلاعات و مدیران سلیقه‌ای و احتمالاً ناکارآمد خواهد بود. در نتیجه امکان دارد یک حادثه جزیی و قابل کنترل به مشکلی جدی تبدیل شود.

فقدان استانداردهای توافق شده یا به کارگیری ناهماهنگ نرم‌افزارهای ضد ویروس، منجر به افزایش ریسک آلودگی، انتشار و خرابی خواهد شد.

کوتاهی در زمینه روزآمدسازی فایل‌های شناسایی ویروس در فواصل منظم، منجر به افزایش ریسک آلودگی نسبت به انواع ویروس‌هایی می‌شود که سازمان واکسن مورد نیاز آنها را ندارد. این امر خسارات جبران ناپذیری را به همراه خواهد داشت.

کوتاهی در زمینه کنترل و بررسی تمامی فایل‌های اطلاعاتی موجود بر روی سرور در فواصل منظم؛ امکان شناسایی و درمان ویروس را، قبل از آن که فایل توسط یک کاربر گشوده شود و از خود اثری بر روی سیستم برجای گذارد، کاهش خواهد داد.

فقدان آگاه‌سازی به کاربران در زمینه ریسک گشودن نامه‌های الکترونیک از طرف فرستنده‌های ناشناس، منجر به انتشار آلودگی به ویروس در سراسر سازمان خواهد شد.

***استانداردهای مرتبط با این سیاست در ISO 17799 و BS 7799 عبارتند** از:*

فصل ۸-۳-۱ کنترل علیه نرم‌افزارهای نفوذ و تهاجم

۴- نتیجه‌گیری

با ظهور موج اطلاعات و ارتباطات و دسترسی کارکنان و مراجعین سازمان به بسیاری از اطلاعات موجود، ایجاد چتر امنیت اطلاعات در یک سازمان، نیاز به رویکردی جامع دارد و با مشارکت کلیهٔ مجموعه‌های ذینفع حاصل خواهد شد. بنابراین باید

سازمان یکی از الگوهای پیشرو و جامع را مورد استفاده قرار داده و سیاست‌های امنیت اطلاعات خود را بصورت بومی و با مشارکت کلیهٔ زیرمجموعه‌های مرتبط، مانند فناوری اطلاعات، حراست، نیروی انسانی، دفتر حقوقی، بازرسی، طرح و برنامه و... تدوین و ابلاغ نماید.

۵- مراجع

]۱[دانشگاه صنعتی مالک اشتر، مجتمع دانشگاهی برق و الکترونیک، راهنمای تدوین سند راهبردی امنیت اطلاعات، ویراست دوم، تابستان ۱۳۸۳.ص ۵۲

]۲[طرح جامع امنیت اطلاعات، گزارش مطالعاتی، موسسهٔ روشنگران اندیشه، زمستان ۱۳۸۳ .

]۳[راهنمای پیاده‌سازی سیستم مدیریت امنیت اطلاعات، خالقی محمود، دبیرخانهٔ شورای عالی امنیت فضای تبادل اطلاعات کشور.

[4] Security Planning & Disaster Recovery, Maiwald Eric, Sieglein William, 2002.
[5] Asset Protection & Security MGT Handbook, Walsh James, 2003.
[6] Information Security Management Handbook -, by Harold F. Tipton, 2004
[7] Information Security Management Handbook 4th Edition, Tipton and Krause Micki, 2000.
[8] JISC Committee on Authentication & Security, Developing an Information Security Policy, Feb 2001, www.jisc.ac.uk/index
[9] Site Security Handbook, ed. B. Fraser, 1997, http://www.cis.ohio-state.edu/htbin/rfc/rfc2196.html
[10] What Do I Put in a Security Policy?, W. Farnsworth, 2000, http://www.sans.org/infosecFAQ/policy/policy.htm
[11] Develop Your Company's First Security Baseline Standard, G. Livingstone,2000, http://www.sans.org/infosecFAQ/policy/baseline.htm