مروری بر بحث امنیت سیستمهای اطلاعاتی

پرسش و دیدگاهتان را در
رابطه با سلسله مطالب ستون
«حسابرسان و فناوری اطلاعات»
از طریق آدرس زیر با ما درمیان بگذارید:
hajian@hesabras.org

حسن حاجیان

برآمد بـاد صبـح و بـوی نـوروز
بـه کـام دوستان و بخت پیروز
مبارک بادت این سال و همه سال
همایـون بادت این روز و همه روز

سـلامی چو بوی خوش آشـنایی به شما سـروران و همراهان گرامی. سـال نو مبارک! سالی سرشـار از موفقیت برایتان آرزو دارم و برقراری سـلامتی و نشاط را برای شما و همه اطرافیان از خداوند مهربان خواستارم.

در سـالی که گذشت، تلاش شـد در این بخش از مجموعه مطالب هر شـماره مجله حسـابرس بـا ارائه مطالـب متنوع با محوریت فناوری اطلاعات در حسابرسی، رضایتمندی شما را در این زمینه نیز به‌دست آوریم. امید است مورد پسند واقع شده باشد و در سال جدید با همکاری شما که همواره موجد انگیزش و مشـوقمان بوده‌اید بتوانیم به کنکاشـهای خـود در این حوزه ادامـه بدهیم. نظرهای شـما همواره چراغ راه بوده و هسـت، پس یاری نموده و از بیان نقطه نظراتتان دریغ نفرمایید.

متأسفانه در روزهای آغازین سال جدید، از خبر درگذشت یکی از همپیشـگان عزیز و ارجمند، آقای **علاءالدین غفاری اقدس** مطلع شـدیم. کسـی که در طول عمر پرثمر خود تلاش کرد تا منشاء اثرات ارزشمندی در آموزش و ارتقای کیفیت حسابرسی در کشور عزیزمان باشد.

چه خوش باشد دراین دنیای فانی
به خوش نامی نمودن زندگانی
که بعد از ما بسی گردش کند چرخ
نمانـد جز نـکونـامـی نشانـی

بـا آرزوی غفـران و رحمت واسـعه بـرای ایشـان و صبر و شـکیبایی برای بازماندگان، این مطلب تقدیم می‌شود به روح پاک آن عزیز همیشه در یاد؛ روحش شاد.

قبل از رفتن به سـراغ مطلب این شماره اجازه می‌خواهم در ابتدا چند پرسش را با شما مطرح کنم.

پرسـش اول: به‌نظر شـما اهمیت اطلاعـات و جایگاه آن در اجتمـاع امروز و نقش فعلی و آینده آن (حتی برای قرن آینده) در تحولات سیاسـی، اجتماعـی، اقتصادی و فرهنگی، به چه میزانی است (ناچیز، کم، زیاد، خیلی زیاد)؟

پرسش دوم: آیا ممکن است کسی نسبت به موضوع پرسش اول اعلام بی‌اطلاعی کند؟

پرسش سوم: به‌نظر شما آیا ممکن است مغایرت جدی بین نظرهای پاسخ‌دهندگان به پرسش اول وجود داشته باشد؟

پرسش چهارم: آیا با توجه به پاسخ پرسش اول، سطح توجه کشور ما نسـبت به ضرورت ایجاد اطمینان نسبت به صحت و اعتبار اطلاعات و برقراری امنیت برای آن مناسب است؟

پرسـش پنجم: آیـا ایجاد امنیـت اطلاعات مسـتلزم ایجاد امنیت در زمینه‌های گوناگون دیگری اسـت؟ اگر هسـت، این زمینه‌ها کدامند؟

تصور نمی‌کنم اگر کسی بگوید قریب به ۱۰۰ درصد پاسخهای دریافتی برای پرسـش‌های دوم و سـوم کلمه خیر خواهد بود، مورد اعتراض شـما قرار گیرد. چراکه در پی تحولات **فناوری اطلاعات** (IT) بعید اسـت کسـی حتی اشـخاص کم‌سواد، به اهمیت نقـش اطلاعات در ابعاد مختلـف زندگی اجتماعی پی نبرده باشـد. امروزه اشتیاق دستیابی سـریع به اطلاعات و نیز رقابت در انتشـار اطلاعات، زمینه‌سـاز عضویت عده زیادی از افراد جامعه در شـبکه‌های اجتماعی با استفاده از ابزار مختلف شـده اسـت. با توجه به همین شـرایط اسـت که اندیشمندان اجتماعـی، جامعه کنونی را در تداوم جریـان نامگذاری جوامع (جامعه کشاورزی و جامعه صنعتی) با عنوان **جامعه اطلاعاتی** (Information Society) مـورد خطاب قـرار می‌دهند و بر ایـن باورند که **فناوری های اطلاعـات و ارتباطات** (ICTs) حکمرانان مطلق این جامعه هستند.

متناسب با این درجه اهمیت برای اطلاعات و ارتباطات، ایجاد قابلیت اتکا و اعتماد به اطلاعات و فناوری‌های مربوط مسـتلزم کنترلهـا و **مراقبتهـای حفاظتـی** (Protection Controls) اسـت. پر واضح است که تنوع‌بخشی و رشـد کیفی این دسته از کنترلها باید هم‌سنگ و گاهی فراتر از رشد فناوری اطلاعات باشد تا امکان برخورداری از اطلاعات سـالم برای بازیگران سیستمها و رویه‌هـای جدیـد (e-mail, e-commerce, e-banking) که در نگارش انگلیسـی با پیشـوند «e» از سیستمها و رویه‌های قبلی قابل تشـخیص هسـتند، فراهم شود. در غیر این صورت، جلـب اعتماد آحـاد جامعه به گونه‌های جدیـد مبادله پول، کالا، اخبار، مسـتندات و ... در عمل غیرممکن اسـت. این موضوعی اسـت که باعث شـده رایانه‌ها و شـبکه‌ها (که بدون آنها شرکتها و سـازمانهای امروزین قابل تصور نیستند) به‌عنوان اصلی‌ترین عامل ریسک برای اطلاعات و مدیریت آن شناخته شوند.

در این مطلب سعی می‌شود جنبه‌های مختلف امنیت اطلاعات با رویکرد آگاهی‌بخشی به حسابرسان، مورد بررسی و توضیح قرار گیرد. امید است با خواندن این مطلب زمینه‌ای هرچند اندک برای ارزیابی قابلیت اتکا به سیسـتمهای مبتنی بـر فناوری اطلاعات واحدهای مورد رسـیدگی، در راستای اسـتانداردهای حسابرسی ۳۱۵ و ۳۳۰ (به‌خصوص هنگام به‌کارگیری تکنیکهای حسابرسی

حسابرسان نباید نسبت به نبود طرح امنیتی اطلاعات بی‌تفاوت باشند بلکه لازم است ضمن اطلاع‌رسانی پیامدهای آن به ارکان راهبری واحد مورد رسیدگی در تعیین راهبرد حسابرسی نیز به این مهم توجه کنند

به کمک رایانه) برای حسابرسان فراهم شود. لازم به ذکر است، ایـن مطلب در ادامـه مطلب مندرج در شـماره ۷۳ حسـابرس با عنـوان «کنترلهـای فناوری اطلاعـات و الزامات اسـتانداردهای حسابرسـی» تهیه شده است، از اینرو مرور مطلب یادشده قبل از مطالعه این مطلب پیشنهاد می‌شود.

تهدیدهای ناشـی از داده‌ها و مدارک جعلی و آثار آن، شتری است که درب خانه هر شخص یا سازمان دارای رایانه متصل به خطوط ارتباطی، دسـتکم برای یکبار خوابیده یا خواهد خوابید. چراکه تهدیدها نسبت به امنیت سیستمهای اطلاعاتی می‌تواند ریشـه در اقدام کاربران، مهاجمـان، تولیدکننـدگان بدافزارها، رقیبان و بسـیاری عوامل دیگر داشـته باشـد و حتـی تغییرات فناوری نیز در شرایط ضعف در سیستمهای امنیتی ممکن است منجر به تهدیدهایی برای اطلاعات شود. همین تعدد در عوامل بروز ناامنی در سیسـتمهای اطلاعاتی بوده که زمینه‌سـاز توجه ویژه مدیران و حسابرسان به بحث امنیت اطلاعات شده است، که شاهد آثار آن در کتابها و مقاله‌های متعدد هستیم.

امنیت اطلاعات عبارت از مجموعه گامهایی است که به دنبال حفظ سه ویژگی محرمانگی بی‌عیبی و در دسترس بودن برای اطلاعات است

امنیت اطلاعات عبارت از مجموعه گامهایی است که به‌دنبال حفظ سـه ویژگیِ محرمانگی، بی‌عیبی و در دسترس بودن برای اطلاعات اسـت. منظور از **محرمانگـی** (Confidentiality)، ارائه اطلاعات، تنها به اشخاص مجاز، آنهم در زمانها و قالبهای از پیش تعیین‌شـده اسـت. **بی‌عیبی** (Integrity) یا به‌عبارتی، یکپارچگـی و صحت، دلالت بر انجام عملیات ویرایش، شـامل ایجاد، تعدیل و حذف اطلاعات (از جمله برنامه‌ها) تنها از سوی افراد مجاز دارد و ویژگی **دردسـترس‌بودن** (Availability) در بردارنده مقاطع دسترسی افراد به اطلاعات و چگونگی این دسترسی است. بایـد توجه داشـت، اولویت‌بندی و اهمیت این سـه ویژگی در محیطها و شـرایط مختلف متفاوت اسـت. براساس تحقیقات انجام‌شـده در امریکا، به‌طور معمول برای شرکتها و سازمانهای بخش خصوصی، ویژگی در دسترس‌بودن اطلاعات در اولویت اول و محرمانگـی در مرتبه آخر اولویت قرار دارد در حالی که در مؤسسه‌ها و سازمانهای دولتی پس از ویژگی بی‌عیبی، به‌ترتیب ویژگی‌های محرمانگی و در دسـترس‌بودن در اولویتهای بعدی هسـتند. از همین رو هنگام ارزیابی ویژگیهای مذکور از سـوی حسابرسـان امنیـت (به‌عنـوان اولین گام) تشـخیص اولویت و اهمیـت این ویژگیها، متناسـب بـا ماهیت فعالیـت واحد مورد رسیدگی، اساسی‌ترین اقدام است.

حسابرسـی امنیـت (Security Audit)، شـاخه‌ای از حسابرسـی فنـاوری اطلاعـات اسـت کـه هـدف آن ارزیابی اثربخشـی کنترلهـای امنیتی اطلاعـات و همچنیـن ارزیابی قابلیـت اتکا بـه فناوریهای پشـتیبان سیسـتمهای اطلاعاتی اسـت. در بحـث امنیت اطلاعات همانند سـایر سیسـتمهای حفاظتـی، آنچه مـورد توصیه متخصصان قـرار دارد ضرورت ایجـاد تعـادل بیـن ریسـک و کنترلهـای کاهنـده آن اسـت. بنابراین مهمترین وظیفه حسابرسـان امنیـت، ارزیابی کارایی و اثربخشـی کنترلهای وضع‌شـده برای کاهش آثـار براوردی ریسـک‌های تهدیدکننده کیفیـت اطلاعات و نیـز اطمینان از

رعایت صرفه اقتصادی در گامهای کنترلی، یعنی ایجاد تناسب بین هزینه‌های برقراری کنترلها با پیامدهای ریسک‌ها است.

در فنـاوری اطلاعات و ارتباطات به آنچه در پوشـش امنیت قرار می‌گیرد، به اصطلاح **داراییهای رایانه‌ای** (Computer Assets) گفته می‌شـود. این داراییها دربرگیرنده سـخت‌افزارها، نرم‌افزارها و داده‌هـا هسـتند. بنابراین گام دوم در حسابرسـی امنیت (پس از گام تشـخیص اولویت‌بنـدی ویژگی‌های امنیت اطلاعات) شناسـایی و تعیین داراییهایی است که در دامنه حسابرسی قرار می‌گیرند. از میان داراییهای یادشـده، داده‌ها بیشـتر از دیگر اقلام در معرض ریسک قـرار دارند ضمن آنکه ارزش عملیاتی آنهـا برای کاربردهای خاص به‌سرعت کاهش پیدا می‌کند.

دلیـل قـرار داشـتن داده‌ها در معرض ریسـکهای بیشـتر، دسترسـی بـه آنهـا از سـوی گروههـای مختلـف (کاربران، تحلیلگران و برنامه‌نویسـان) در مقایسـه با داراییهای دیگر و همچنیـن مواجه‌بودن داده‌ها با تهدیدهای یکسـان ناشـی از هریـک از آن گروهها اسـت. گزارش‌ها حاکی از آنسـت که از خسـارتهای واردشده به شـرکتها به‌دلیل ضعف امنیتی، حدود ۵ درصد به‌طورمسـتقیم مربوط به سـخت‌افزارها، نرم‌افزارها و دیگـر تجهیزات رایانه‌ای بوده و ۹۵ درصد مابقی از سـرقت اطلاعات، دسـتکاری اطلاعـات و به‌هم‌ریختگـی اطلاعات ناشی شده اسـت که براورد آثار این سـری از خسارتها به‌دلیل گسـتردگی پیامدهای آنها (از دسـت دادن مزیتهـای رقابتی، دعـاوی کیفری، لطمه‌های اعتباری و ...) به آسـانی امکانپذیر نیسـت. طول عمر عملیاتی سـخت‌افزارها حدود ۴ تا ۵ سـال و بـرای نرم‌افزارهـا در بهتریـن حالـت بیـن ۱۰ تا ۱۲ سـال براورد می‌شـود و با توجه به سـهولت جایگزینی این داراییها، تحمل خسـارت ناشـی از آنها چندان مشـکل نیست، درحالی کـه خسـارتهای مربوط بـه اطلاعات (سـرقت، دسـتکاری، به‌هم‌ریختگی) در بیشتر موارد می‌تواند غیرقابل‌تحمل و حتی جبران‌ناپذیر باشد.

تهدیدهـای امنیتی فناوری اطلاعات و ارتباطات براسـاس منشاء آنها در سـه گروه تصادفی، طبیعی و عمدی دسته‌بندی می‌شـوند. **تهدیدهای تصادفی** (Accidental Threats) شـامل خطاهـای انسـانی، خرابی تجهیـزات، قطعـی برق، جریانهـای الکترومغناطیسـی و دیگـر مـوارد مشـابه اسـت.

تهدیدهای طبیعی (Natural Threats) می‌تواند به دلایل مختلفی همچون آتش‌سـوزی، سـیل، طوفـان، زمین‌لرزه و دمای بالای هوا بروز کند. **تهدیدهای عمدی** (Intentional Threats) عبـارت از صدمه‌هـای هدفمنـد بـه سیسـتمهای اطلاعاتی و یا اطلاعات آن اسـت. از جمله این موارد سـرقت اطلاعـات، ایجاد اخلال‌ها و نَشـتی‌های عمده و غیرعمده در سیسـتمها و اطلاعات و اقدام متقلبانه اسـت. اقـدام متقلبانه شامل متأثرکردن سیستمهای اطلاعاتی با داده‌های جعلی و یا با رویه‌های تحریف‌کننده نتایج به‌منظور کسب منافع شخصی است.

راهـکار مقابله با تهدیدهـای امنیتی، برقـراری **کنترلهای امنیتـی** (Security Controls) اسـت. هـدف از کنترلهای امنیتی، کاهش ریسـک اسـت. کنترلهای امنیتـی که در بحث سیستمهای رایانه‌ای به آن **اقدام متقابل** (Countermeasure) نیـز گفته می‌شـود عبارت از تـدارک کارکردهـای کنترلی در یک سیستم یا محصول نرم‌افزاری با هدف ارتقا و بهبود سطح امنیت است. توجه به این مهم ضروری است که داراییهای رایانه‌ای، در شرایط زمانی و مکانی مختلف از قابلیتهای آسیب‌پذیری متنوعی برخوردار هسـتند که آثار تهدیدهـای گوناگون در هر یک از آن شرایط می‌تواند بسیار متفاوت باشد.

نتایج تحقیق مؤسسه **ارنست و یانگ** (Ernst & Young) با عنوان امنیت اطلاعات نشـان‌دهنده آمار جالبی است. بیش از ۳۴ درصد سـازمانها پاسـخ داده‌انـد که توانایـی کافی برای تشخیص اینکه آیا سیستمهایشان مورد حمله قرار گرفته یا خیر ندارند و بیش از ۳۳ درصد اقرار کرده‌اند که توانایی عکس‌العمل مناسب در مقابل رخدادهای امنیتی را ندارند. براساس تحقیق یادشـده به‌رغم اینکه ۹۰ درصد سـازمانها امنیت اطلاعات را عنصری اساسـی برای دسـتیابی به هدفهای کلی خود عنوان داشته‌اند و بیشتر آنها هدف اصلی برای تأمین امنیت اطلاعات را کاهش مخاطرات مطـرح کرده‌اند ولی ۵۶ درصد آنها بودجه ناکافـی را به‌عنـوان مانع اصلـی در توجه مؤثر بـه تهدیدهای امنیت اطلاعات برشمرده‌اند.

بـرای خنثی‌کردن تهدیدهـا، به‌کارگیـری کنترلهای امنیتی متعـدد و مختلفی ضروری اسـت که در ادامه بـه آنها پرداخته خواهد شـد. قبل از پرداختن به کنترلهای امنیتی، اشاره به این

نکته ضروری است که برخی کنترلها، به‌رغم هم‌موضوعی، ولی به دلیل تفاوت در مکانیزم استقرار و محیط اجرا (کار در محیط انزوا یا در محیط تعامل با دیگران) دارای عملکردهای متفاوتی هستند که این موضوع هنگام ارزیابی اثربخشی آنها باید مورد توجه حسابرسان قرار گیرد.

کنترلهای امنیتی بر حسب شیوه عمل و ماهیت در گروههای مختلفی دسته‌بندی می‌شوند. گروه‌بندی این کنترلها برحسب شیوه عمل، عبارت از کنترلهای پیشگیرانه، کنترلهای کشف‌کننده، کنترلهای اصلاح‌کننده و کنترلهای ترمیمی است و گروه‌بندی آنها بر حسب ماهیت نیز عبارت از کنترلهای قانونی، کنترلهای مدیریتی، کنترلهای فیزیکی و کنترلهای فنی است.

کنترلهای پیشگیرانه (Preventive Controls)، تلاش در کاهش احتمال مواجهه با تهدیدهای معین دارد. برای مثال، استفاده از روتین‌های کنترل دسترسی، که مانع استفاده از منابع حساس یا داده‌های خاص به‌وسیله کاربران غیرمجاز می‌شود یا استفاده از **دیوارهای آتش** (Firewalls) جهت ممانعت از دسترسی به برخی آدرسها در محیط شبکه یا ایجاد محدودیت در تبادل اطلاعات، نمونه‌هایی از این نوع کنترلها است.

کنترلهای کشف‌کننده (Detective Controls)، با شناسایی حملات و صدور هشدار، سیستم را در اقدام به‌موقع برای کاهش خسارت یاری می‌کند. استفاده از کدهای اعتبارسنجی مبتنی بر ارزیابی چینش اجزای داده هنگام بروز رویدادهای تغییر در داده‌ها که با استفاده از توابعی موسوم به **توابع دَرهَم سازی**(Hash Functions) انجام می‌شود از جمله این کنترلها است.

کنترلهای اصلاح‌کننده (Correction Controls)، پس از عملکرد کنترلهای کشف‌کننده وارد عمل می‌شوند و اقدامهای تعیین‌شده را نسبت به حملات اتفاقی یا تعمدی به مرحله اجرا درمی‌آورند. غیرفعال کردن کارت بانکی هنگام وارد کردن اشتباه رمز در سه بار پی‌درپی نمونه‌ای آشنا از این نوع کنترل است.

کنترلهای ترمیمی (Recovery Controls)، مأموریت بازیابی سیستم اطلاعاتی به وضعیت قبل از صدمه را دارند. تهیه نسخ پشتیبان در قالب راهبردهای مشخص، نمونه‌ای از کنترلهای ترمیمی است. درخصوص راهبردهای تهیه نسخ پشتیبان از اطلاعات، مطلبی در صفحه ۵۱ شماره ۶۴ حسابرس ارائه شد که در صورت تمایل می‌توانید به آن مراجعه کنید.

کنترلهای قانونی (Legal Controls)، الزامات پیش‌بینی‌شده از سوی مراجع قانونی برای حفظ امنیت سیستمهای اطلاعاتی و اطلاعات مؤثر در اجرای بهینه قوانین را شامل می‌شود. الزامات مربوط به توزیع بانکهای اطلاعاتی، حفاظت از اطلاعات شخصی افراد و امضای الکترونیک، نمونه‌های مرسوم از این گروه کنترلها است.

کنترلهای مدیریتی (Administrative Controls)، بر پایه اصول حاکم بر محیط کنترلی (از جمله اجزای پنجگانه نظام کنترل داخلی) طراحی و استقرار می‌یابند. تدوین سیاستها و روشهای پیاده‌سازی و بهبود کنترلها و ایجاد ضمانت اجرایی برای آنها، جداسازی مسئولیتها، اتخاذ سیاستهای طبقه‌بندی اطلاعات، تعیین الزامات سابقه‌نگاری حمله‌ها به اطلاعات و سیستمهای اطلاعاتی و به‌طور کلی برقراری نظام مدیریت امنیت، در این گروه قرار می‌گیرد.

کنترلهای فیزیکی (Physical Controls)، به‌منظور مقابله با تهدیدهای بیرون از محیط سیستم اطلاعاتی که منجر به صدمه فیزیکی به منابع می‌شود، وضع می‌شوند. از جمله این کنترلها، استفاده از تجهیزات الکتریکی و الکترونیکی برای مقابله با نارساییهای سیستم تأمین برق، آتش‌سوزی، سیل، جریانهای الکترومغناطیسی، خرابکاری و سرقت است.

کنترلهای فنی (Technical Controls)، تلاش در حفاظت از نرم‌افزارها (بنیانی و کاربردی) و داده‌ها دارند. این اقدام کنترلی، هم در بستر سخت‌افزاری و هم در بستر نرم‌افزاری قابل پیاده‌سازی است. طی دو دهه گذشته تحقیقات زیادی در این زمینه به‌عمل آمده که منجر به طرحهای امنیتی متعددی شده است مانند طرحهای **کنترل دسترسی** (Access Control Models)، **طرحهای کنترل جریان داده** (Data Flow Control Models)، طرحهای **رمزنگاری** (Cryptosystems)، سیستمهای امضای الکترونیکی برای انتقال داده‌ها و ... که تمامی آنها تأثیر بسیاری در تغییر روشهای درک امنیت اطلاعات داشته است.

اطلاع از تهدیدها و کنترلهای امنیتی، در نبود یک سیاست امنیتی تقریباً بی‌فایده است. همان‌گونه که ذکر شد تهدیدهای امنیتی می‌تواند ریشه داخلی و بیرونی داشته باشد و بیشتر حمله‌ها به سیستمهای اطلاعاتی، هدفهای غیرقانونی و غیراخلاقی را دنبال می‌کند. برای ایجاد سیاست امنیتی، لازم است میزان آسیب‌پذیری فرایندهای داخلی و هدفهای سازمان تخمین زده شود. به این منظور سابقه‌نگاری حمله‌ها از طریق جمع‌آوری اطلاعات زیر توصیه شده است:

- زمان وقوع حمله،
- مشخصات مهاجم،
- چگونگی حمله و مسیر اجرایی آن،
- بدترین پیامدها و خسارتهای حمله،
- نظر متخصصان در مورد حمله،
- آموزشهای داده‌شده به کارکنان در زمینه حمله و شیوه‌های مقابله با آن،
- عملکرد نقطه تماس (برای اخذ پیامهای کارکنان هنگام وقوع حمله و گزارش وقایع به مدیریت)،
- هدفهای تعیین‌شده برای مقابله،
- طرحهای ترمیمی به اجرا گذاشته شده، و
- هزینه واکنشهای به‌عمل‌آمده.

گردآوری اطلاعات مذکور، سازمان را در موقعیت طراحی یک طرح امنیتی شامل روشهای مقابله با تهدیدها و طرحهای ترمیم، قرار می‌دهد. حسابرسان نباید نسبت به نبود طرح امنیتی اطلاعات بی‌تفاوت باشند بلکه لازم است ضمن اطلاع‌رسانی پیامدهای آن به ارکان راهبری واحد مورد رسیدگی، در تعیین راهبرد حسابرسی نیز به این مهم توجه کنند. یک طرح امنیتی مناسب باید قادر به پاسخگویی به پرسشهای زیر باشد:

- کدام داراییهای رایانه‌ای نیاز به حفاظت ویژه دارند؟
- چه عواملی امنیت آن داراییها را تهدید می‌کند؟
- تا چه میزان تلاش و منابع مالی برای تأمین امنیت داراییها، توجیه‌پذیر تلقی شده است؟
- آیا روشهای عکس‌العمل سریع نسبت به حمله‌ها تعریف شده‌اند؟
- آیا رویه‌ها، صریح، قابل فهم و به‌روز هستند؟
- آیا تمهیدات لازم برای ترمیم صدمه‌ها به‌خصوص موارد ناشی از بلایای طبیعی پیش‌بینی شده است؟
- آیا منابع و تجهیزات کافی برای واکنشهای مناسب نسبت به تهدیدها تدارک دیده شده است؟
- آیا دستورعملهای لازم برای چگونگی تماس با کارشناسان امنیت تهیه شده است؟
- آیا نحوه عمل در شرایط نبود دستیابی به کارشناسان امنیت و چگونگی اطلاع‌رسانی مشکل به مدیریت مشخص است؟
- آیا روشی برای مطلع‌نمودن مدیران ارشد (به‌خصوص مدیر ارشد اطلاعات) از وقوع حوادث احتمالی تعریف شده است؟
- آیا روالی برای تماس با افراد خارج از سازمان (شامل شرایط و زمان تماس) به‌منظور درخواست کمک در نظر گرفته شده است؟

- آیا کارکنان کلیدی برای اجرای روشهای برخورد با حمله‌ها مشخص شده‌اند و آموزش لازم را دیده‌اند؟
- آیا مناسبات مدیران سیستمها و گروههای امنیتی روان است؟
- آیا ابزار لازم برای کشف حمله بر روی سیستمها نصب و فعال شده است؟
- آیا ابزار شناسایی حمله، قادر به کشف حمله‌های ناشناخته و عملیات ناشناس می‌باشد؟
- آیا امکان ردیابی و تعقیب حمله‌ها بر روی شبکه وجود دارد؟
- آیا براساس ممیزی رسمی امنیت، تمامی سیستمها دارای کنترل امنیتی کافی هستند؟

اگرچه تهیه طرح امنیتی نقشی اساسی در کاهش تهدیدهای

امنیتی و پیامدهای آن دارد ولی باید توجه داشت که به‌تنهایی کافی نبوده و جاری‌سازی فرایند نظارتی بر اجرای آن از اهمیت ویژه‌ای برخوردار است. هدف اصلی از چنین نظارتی کسب اطمینان از اجرای صحیح و کامل طرح و ارزیابی اثربخشی اقدام است. کلید موفقیت در امنیت سیستمهای اطلاعاتی، تشخیص تمامی تهدیدهای ممکن علیه سیستم و آمادگی دفاعی در مقابل حمله‌ها است.

در ارتباط با این موضوع با مرور در سوابق مرتبط با بحث امنیت سیستمهای اطلاعاتی در کشورمان، به سند راهبردی انجمن صنفی امنیت فضای تولید و تبادل اطلاعات (افتا) که در پی ابلاغ سیاستهای کلی نظام در این حوزه تنظیم شده می‌رسیم. در این سند، ضرورت پیاده‌سازی **سیستم مدیریت امنیت اطلاعات** (Information Security Management System (ISMS)) در دستگاههای اجرایی کشور مورد اشاره قرار گرفته و ۶ راهبرد به‌شرح زیر برای آن تعیین شده است:

۱- امن‌سازی زیرساختهای حیاتی کشور در قبال حمله‌های الکترونیکی،

۲- ایجاد و توسعه نظامهای فرابخشی امنیت فضای تبادل اطلاعات،

۳- تأمین سلامت و جلوگیری از مخاطرات ناشی از محتوا در امنیت فضای تبادل اطلاعات،

۴- تقویت صنعت و توسعه خدمات و محصولات امنیت فضای تبادل اطلاعات،

۵- حمایت از تحقیق، ارتقای سطح آگاهی، دانش و مهارتهای مرتبط با امنیت فضای تبادل اطلاعات، و

۶- افزایش سطح همکاری‌های منطقه‌ای و بین‌المللی در زمینه امنیت فضای تبادل اطلاعات.

سوابق نشان‌دهنده آنست که دو طرح با عنوانهای «طرح امن‌سازی زیرساختهای حیاتی کشور و منابع ملی در برابر حمله‌های الکترونیکی» و «طرح ایجاد نظام مدیریت امنیت زیرساختهای حیاتی در دستگاههای مرتبط» در راستای راهبرد اول تنظیم شده است.

در سال ۱۳۸۶ معاون اول ریاست جمهوری وقت، طی بخشنامه‌ای تحت شماره ۱۳۷۱۱-۸۶/م/۳۸۵۰۵ به تاریخ ۱۳۸۶/۸/۱۰ تمامی دستگاههای بهره‌مند از شبکه‌های رایانه‌ای را موظف به تهیه طرح سیستم مدیریت امنیت اطلاعات تا پایان سال ۱۳۸۶ ساخت و همچنین مقرر داشت که تمامی دستگاهها با همکاری واحد حراست، حداکثر ظرف دو ماه نسبت به ایجاد حراست فناوری اطلاعات خود اقدام نمایند. در همین راستا شرکت فناوری اطلاعات کشور مسئول بررسی و ممیزی سامانه‌های راه‌اندازی‌شده شد و مقرر گردید گواهی سامانه مدیریت امنیت اطلاعات از سوی این شرکت به دستگاهها ارائه شود.

در تداوم تأکیدها در این زمینه، در قانون برنامه پنجساله پنجم توسعه، مهلت دریافت گواهی پیاده‌سازی سیستم مدیریت امنیت اطلاعات که مدت اعتبار آن ۲ سال است، تعیین و مقرر شد دستگاههای حیاتی و حساس و مالی کشور ظرف دو سال اول برنامه، گواهی مذکور را اخذ کرده و دیگر دستگاهها تا پایان برنامه حداقل یکبار نسبت به دریافت آن گواهی اقدام کنند که امید است این‌کار را با جدیت انجام داده باشند.

آنچه مشخص است، بحث امنیت اطلاعات و فضای تبادل اطلاعات، با توجه به تهدیدها و گونه‌های مختلف حمله و پیامدهای مخرب آن بحثی جدی در سطح امنیت ملی است و بی‌توجهی به آن همان‌گونه که متأسفانه در ماجرای ویروس‌های «Flame» و «Stuxnet» تجربه شد، خاطرات تلخی را به‌جا خواهد گذاشت. چنانچه حسابرسان در جریان ارزیابی کنترلهای داخلی، به‌خصوص کنترلهای حفاظتی داراییها در شرکتها و سازمانهای بزرگ، گوشه چشمی نیز به کنترلهای حاکم بر داراییهای رایانه‌ای و صد البته داده‌ها و فضای تبادل آنها داشته باشند، می‌توانند با هشدارهای به‌موقع نقش مهمی در مقابله با تهدیدهای یادشده ایفا کنند.

موفق باشید

منابع:

- **راهنمای امنیت فناوری اطلاعات**، انتشارات دبیرخانه شورای‌عالی اطلاع‌رسانی، ۱۳۸۴
- مرکز اطلاع‌رسانی اینترنتی انجمن صنفی امنیت فضای تولید و تبادل اطلاعات: www.aftta.ir
- Pathak J., **Information Technology Auditing; an Evolving Agenda**, Springer, 2005