کنترل‌های ایمنی سایبری از دیدگاه حسابرسان داخلی

شهلا بهتاش*

روند رشد و پیشرفت اینترنت به معنای فضای سایبری آن‌قدر گسترده شده است که تقریباً اکثر انسان‌ها به این فناوری وابستگی پیدا کرده‌اند. در این مقاله، کنترل‌های امنیتی و ایمنی سایبری در حسابرسی داخلی از دو جنبه‌ی کلی شرح داده می‌شود. نخست، برخی از نگرانی‌های امنیتی و ایمنی سایبری است که حسابرسان داخلی باید در بررسی فرایندها و سیستم‌های مبتنی بر فناوری اطلاعات به آن‌ها توجه کنند. از آن‌جا که حوزه‌ی کنترل‌های ایمنی فناوری اطلاعات وسیع است و گاهی به دانش فنی بیشتری از مهارت‌های حسابرسان داخلی نیاز دارد، تمام حسابرسان داخلی باید درکی کلی از رویه‌های کنترل‌های داخلی و خطرهای مربوط داشته باشند. جنبه‌ی دوم، کنترل‌های امنیتی و ایمنی سایبری شامل رویه‌های حسابرسی داخلی است. هدف مقاله، پیشنهاد بهترین روش‌ها برای بهبود حسابرسی داخلی، با وجود متفاوت بودن بخش‌های مختلف حسابرسی داخلی، است.

---

*- دانشجوی دوره‌ی کارشناسی ارشد حسابرسی مؤسسه‌ی آموزش عالی خاتم، نگارنده مایل است از راهنمایی‌های دکتر نظام‌الدین رحیمیان در نگارش این مقاله سپاسگزاری نماید.

ایمنی سایبری

استاندارد ایمنی داده‌های رایانه‌ای و سیستم پشتیبان تصمیم‌گیری[1] را در سپتامبر ۲۰۰۷ **شورای صنعت کارت پرداخت**[2] راه‌اندازی کرد. این گروه صنعتی جهانی را **آمریکن اکسپرس، مسترکارت، ویزا** و دیگران راهبری می‌کرد. استاندارد ایمنی داده‌های رایانه‌ای و سیستم پشتیبان تصمیم‌گیری، استانداردی جهانی است که بر اساس قوانین محلی و ملی گسترده و رهنمودهایی در مورد شرکت‌های کارت اعتباری تصویب شده است. این استانداردها شامل پیکربندی و رهنمودهای حسابرسی است و تمامی دستگاه‌های فناوری اطلاعات را که کارت اعتباری را به عنوان پرداخت قبول می کند پوشش می‌دهد. در حقیقت، استاندارد ایمنی داده‌های رایانه‌ای و سیستم پشتیبان تصمیم‌گیری به ارائه‌ی نمایی کلی از استانداردهای ایمنی سایبری می‌پردازد. نمایه‌ی شماره یک، دوازده الزام اساسی برای اجرای استاندارد ایمنی داده‌های رایانه‌ای و سیستم پشتیبان تصمیم‌گیری و در نهایت هدف نهایی را ممکن می‌سازد. هدف نهایی، پدید آمدن ایمنی سایبری است. بسیاری از بخش‌ها مانند نصب مؤثر فایر وال، استفاده از نرم‌افزار ضد ویروس، اهمیت رویه‌های ایمنی در زمینه‌ی ایمنی شبکه‌ی عمومی مناسب شرح داده می‌شود.

استفاده‌ی مؤثر از این الزامات، به درک عمیق‌تر **کنترل ایمنی سایبری** نیاز دارد. برای نمونه، الزام یازدهم در نمایه شماره یک، نیازمند بررسی فرایندها و سیستم‌های ایمنی به طور منظم است. این مورد شرکت را به رعایت آزمون کنترل‌های امنیتی سالانه، بررسی دقیق داده‌های بیرونی و داخلی هر سه ماه یکبار، اجرای بررسی سالانه بر روی سیستم‌ها، استفاده از ابزار برای بررسی دستورالعمل‌های گروهی و شبکه‌ای و تکمیل رویه‌های نظارتی ملزم می‌سازد. بسیاری از شرکت‌های جهانی می‌کوشند از استاندارد ایمنی داده‌های رایانه‌ای و سیستم پشتیبان تصمیم‌گیری برخوردار باشند. استاندارد ایمنی داده‌های رایانه‌ای و سیستم پشتیبان تصمیم‌گیری، را صنعت کارت اعتباری اجرا می‌کند اما در آینده، صنایع دیگر نیز امکان تدوین این استانداردها را دارند. (مولر، ۲۰۰۹)

نمایه‌ی یک: الزامات استانداردهای ایمنی داده‌های رایانه‌ای و سیستم پشتیبان تصمیم‌گیری

۱. ایجاد و نگهداری شبکه‌ی امن: نصب فایروال برای حفاظت از داده‌ها

۲. ایجاد و نگهداری شبکه‌ی امن: عدم استفاده از پیش‌فرض فروش برای گذرواژه‌ها و دیگر شاخص‌های ایمنی

۳. حفاظت از داده‌های کارت اعتباری: حفظ داده‌ی ذخیره شده و عدم ذخیره‌ی داده‌های غیر ضروری کارت و معاملات آن‌ها

۴. حفاظت از داده‌های کارت اعتباری: ارسال پنهانی داده‌های کارت اعتباری و اطلاعات حیاتی شبکه

۵. نگهداری آسیب‌پذیری مدیریت برنامه‌ها: استفاده از نرم‌افزار ضد ویروس و به‌روز رسانی آن

۶. نگهداری آسیب‌پذیری مدیریت برنامه‌ها: ایجاد و نگهداری سیستم‌های امن و کاربرد آن‌ها

۷. ابزار اساسی برای دسترسی به کنترل: دسترسی محدود به داده‌ها

۸. ابزار اساسی برای دسترسی به کنترل: اختصاص دادن شناسه‌ای واحد به هر فرد برای دسترسی به رایانه

۹. ابزار اساسی برای دسترسی به کنترل: دسترسی فیزیکی محدود به داده‌ها

۱۰. نظارت و آزمون شبکه‌ها به طور منظم: نظارت بر تمام دسترسی‌ها به منابع شبکه و داده‌های حساس

۱۱. نظارت و آزمون شبکه‌ها به طور منظم: آزمون ایمنی سیستم و پردازش‌ها به طور منظم

۱۲. نگهداری رویه‌ی ایمنی اطلاعات: ایجاد و نگهداری اصول ایمنی و رویه‌ها

(1) Payment Card Industry Data Security Standard (PCI_DSS)

(2) the Payment Card Industry (PCI)

اصول ایمنی شبکه‌ی فناوری اطلاعات

در مقابل پیچیده‌تر شدن سیستم‌های فناوری اطلاعات و کنترل بهتر آن‌ها، تهدیدات نیز افزایش یافته‌اند. برای نمونه، هکرها به طور مستقیم می‌توانند داده‌های با ارزش را بدون ردیابی بارگیری کنند. سارق دارایی فناوری اطلاعات ممکن است دارایی‌هایی با ارزشی بیش از وجه نقد به دست آورد. شماره‌های مصوب کارت اعتباری که خریدهای کلان را ممکن می‌سازد، رمز برای دستیابی به سیستم‌های باارزش دیگران یا حتی استفاده از هویت افراد برای معاملات متقلبانه، نمونه‌هایی از این دارایی‌های ارزشمند هستند. گاهی برای عاملان دزدی، دسترسی به سوابق داده‌های باارزش بدون وجود سطح نظارت فعال بسیار آسان است. برای نمونه، در سال ۲۰۰۷ بلافاصله بعد از پایان فصل خرید، یک مجموعه فروشگاه‌های خرده‌فروشی در ایالات متحده با نام شرکت‌های **تی جی ایکس**[1] اعلام کرد که سیستم رایانه‌ای آن‌ها هک شده است و از نسخه‌های بدهی و شماره حساب کارت اعتباری، آدرس مشتریان و داده‌ی شناسایی ۲۰۰۰ تخفیف فروشگاه‌های لباس رونوشت گرفته شده است. هکر (شخص عامل)، با در اختیار داشتن هزار شماره‌ی کارت‌های اعتباری و اطلاعات اشخاص، بدون ردیابی می‌تواند از آنها استفاده کند. سرقت شرکت تی جی ایکس در هفته‌های قبل و بعد از فصل خرید اتفاق افتاد. داده‌ها به وسیله انتقال روزانه‌ی داده‌های فروش از فروشگاه‌های شرکت به سرقت رفته‌اند. این شرکت در ابتدا این نقص را بررسی نکرد زیرا فروش‌های روزانه‌ی فروشگاه از طریق شبکه ارتباطات، انتقال پیدا می‌کرد و به نظر نمی‌رسید مشکلی داشته باشند. هکر از داده‌های فروش شخصی، رونوشتی برای استفاده‌ی خود ایجاد کرده بود. این نمونه‌ای از نقص ایمنی رایانه است که در سراسر دنیا به وجود می‌آید. رفع نواقص، مستلزم بهره‌برداری فنی در سطح گسترده است که در نتیجه‌ی کنترل‌های فنی داخلی خوب پدید می‌آید. حسابرسان داخلی در بسیاری از محیط‌های فناوری اطلاعات، مهارت‌های فنی برای ارزیابی خطرهای ایمنی و ایجاد نظریه‌ی فنی مناسب را ندارند، اما باید از دانش متعارف برای فهم زمینه‌های ایمنی رایانه در حوزه‌ی وسیع بررسی‌های حسابرسی داخلی برخوردار باشند. فقدان رویه‌های حسابرسی داخلی درست، داده‌ها و نرم‌افزار و سخت‌افزار سیستم‌های فناوری اطلاعات را دست‌کم با یکی از موارد تهدیدات اساسی زیر روبه رو می‌سازد:

۱. **انقطاع:** تخریب برنامه، سرقت از قسمت سخت‌افزار یا استفاده‌ی نامناسب از منابع شبکه می‌تواند باعث گم شدن یا غیر قابل استفاده شدن دارایی سیستم شود.

۲. **جلوگیری:** عوامل برون‌سازمانی مانند یک نفر یا یک برنامه‌ی نرم‌افزاری می‌توانند به دارایی فناوری اطلاعات دسترسی پیدا کند. نمونه‌ای از این نوع تهدیدات، استراق سمع برای به دست آوردن داده‌ها یا استفاده‌ی غیر قانونی از منابع برنامه است.

۳. **اصلاح:** در این قسمت، اختلال غیرمجاز علاوه بر دسترسی به داده‌ها، توانایی ایجاد تغییر در برنامه‌ها و اجزای سخت‌افزاری را ممکن می‌سازد.

---

(1) TJX.CO

۴. جعل: این تهدید، زمانی پدید می‌آید که شخص غیرمجاز معاملات جعلی را به محیط فناوری اطلاعات معرفی می‌کند. انتشار معاملات جعلی در سیستم ارتباطات کاری جدید یا قرار دادن گزارش‌ها در پایگاه داده، نمونه‌ای از تهدیدات است.

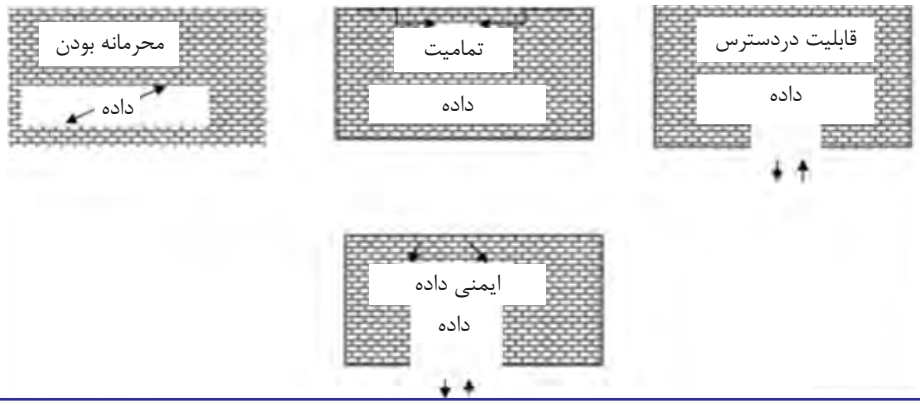
این تهدیدات در اولین روزهای کاربرد سیستم فناوری اطلاعات با جدیت بیشتری مطرح شدند. امروزه این تهدیدات ایمنی با شتاب بسیار افزایش یافته است و دلیل آن، پیشرفت در محیط فعلی اینترنت، ارتباطات بی‌سیم، پایگاه داده‌ی برنامه‌ریزی منابع بنگاه۵ و دستگاه‌های مختلف سیستم‌های پیچیده نسبت به دستگاه‌های دستی کوچک است.

در حال حاضر، حسابرسان داخلی که کنترل‌های داخلی را بررسی می‌کنند باید به تغییرات و تشخیص تهدیداتی آگاه باشند که بیشتر از گذشته اهمیت یافته است. حسابرسان داخلی گاه موفق به اجرای مناسب کنترل‌های امنیتی و ایمنی بر فرایندهای حسابرسی داخلی خود نمی‌شوند و همین امر به خطای ایمنی منجر می‌شود. این خطای ایمنی شامل شکست در مدیریت منابع، کاربرگ محافظت نشده و کنترل ناکافی بر شواهد بااهمیت حسابرسی می‌شود.

(الف) امنیت داده‌ها:

بانک داده‌ها، شامل حساب مصرف‌کننده در مرکز داده‌ی اصلی سیستم برنامه‌ریزی منابع انسانی و حوزه‌ی داده‌ی جمع‌آوری شده بر روی رایانه‌ی دستی شخص است و نیازمند محافظت است. نمایه‌ی شماره دو، بعضی از زمینه‌های اساسی ایمنی داده‌ها را نشان می‌دهد. این نمایه، چهار حالت داده‌ی فناوری اطلاعات نیازمند محافظت را نشان می‌دهد. هریک از این حالت‌ها در تمام وضعیت‌ها ضروری نیست، اما حسابرسان داخلی ممکن است این چهار مورد را در مورد ایمنی داده‌ها مفید بدانند. در برخی ازموارد، داده‌ها ممکن است به برخی محافظت‌های محرمانه‌ی جدی نیاز داشته باشد. بر اساس شکل، کنترل به معنای محرمانه بودن و محافظت کامل در مقابل تهدیدات از طریق دیوارهای محافظتی مطرح نیست و می‌توان اینگونه گفت که کنترل‌های در دسترس منجر به حفاظت داده و برنامه‌ها می‌شود. به علت وجود همیشگی تهدیدات، از داده باید در برابر هر بی‌نظمی و رسوب غیرمنتظره محافظت کرد. تمامیت و درستی، برای هر مخزن داده نگرانی مهم‌تری است. همیشه اشخاص بیرونی (بیرون از سازمان) هستند که سعی در ایجاد شکاف در دیوار حفاظتی داده‌ها را داشته باشند. در مورد شرکت تی جی ایکس، هکر کل داده‌های شرکت را از طریق رونوشت‌های غیر مجاز از بین برد. داده‌ها باید ضمن رعایت جدار محرمانه، در دسترس دیگران باشد. این ورودی دوطرفه است و کنترل رویه‌ها و برنامه‌ها باید داده‌ها را برای افراد مجاز و مناسب، قابل‌دسترس سازد. کنترل گذرواژه در این قسمت بسیار مهم است. مورد پایین در نمایه‌ی دو، سه راهبرد را برای تفهیم محیط امن داده ترکیب می‌کند. دو مفهوم مهم دیگر در اینجا، فایروال و محافظت در برابر ویروس‌ها است. هر چند که این شکل کاملاً ذهنی است، باتوجه به این شکل حسابرسان داخلی باید به ایمنی رایانه در قالب سه مفهوم محرمانه بودن، تمامیت و قابل دسترس بودن داده‌ها فکر کنند.

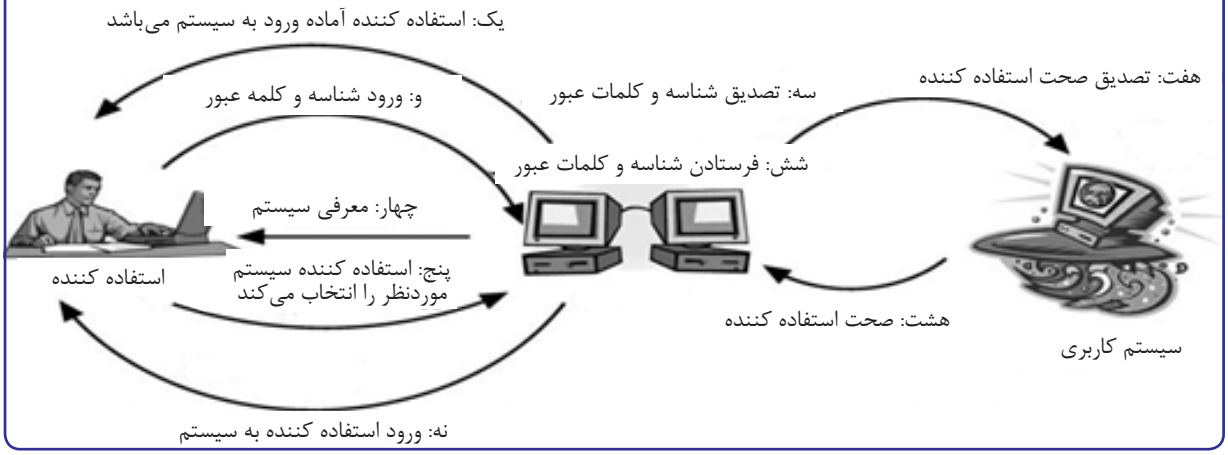
نمایه‌ی دو: مفاهیم امنیت داده‌ها



(ب) اهمیت گذرواژه‌ها فناوری اطلاعات

گذرواژه‌ها، کنترل فناوری اطلاعات هستند که هر کاربر سیستم یا داده باید کد معینی را که تنها برای خودش مشخص است برای دست‌یابی به منابع فناوری اطلاعات به کار ببرد. نمایه‌ی سه تبادلی بین ورود و گذرواژه‌ی فناوری اطلاعات مهم را نشان می‌دهد، هر چند که اشکال پیچیده‌تری هم وجود دارد. کاربر، گذرواژه‌ای را برای پذیرش وارد می‌کند و اگر گذرواژه صحیح نباشد دسترسی به سیستم منتفی می‌شود. حسابرسان داخلی، هنگام بررسی کنترل‌های داخلی در حوزه‌ی کاربرد فناوری اطلاعات، باید به دنبال استفاده‌ی مؤثر از گذرواژه‌ها باشند. زیرا ایمنی فناوری اطلاعات، با استفاده از گذرواژه‌ها معنا پیدا می‌کند. مسئولیت ایجاد گذرواژه‌ها با کاربران است، اما الزامات اجرایی باید به‌گونه‌ای طرح شوند که حدس یا پیش‌بینی آن‌ها برای دیگران دشوار باشد. برای نمونه، هدایت و کنترل باید در جای مناسب خود قرار گیرد تا از استفاده تاریخ تولد یا اسم مستعار کارمند به عنوان گذرواژه جلوگیری کند. گذرواژه باید ترکیبی باشد تا به‌سختی بتوان آن‌ها را حدس زد. برای نمونه، ایمنی فناوری اطلاعات می‌تواند قوانینی بنا نهد که آمیزه‌ای از حروف و اعداد را در گذرواژه ملزم می‌سازد. پردازش‌ها باید در جای مناسب خود قرار گیرند تا تغییر مکرر گذرواژه را الزامی کند. پردازش‌ها باید در جای مناسب خود قرار گیرند تا بر گذرواژه‌ها نظارت داشته باشند. اگر کاربر دوبار به ورود گذرواژه‌ی نامعتبر مبادرت کند، دسترسی شخص به سیستم منتفی می‌شود و اجازه‌ی بازیابی گذرواژه‌ها از طریق رویه‌ی اجرایی را ممکن می‌سازد. در صورت فراموشی گذرواژه، رویه‌ها اجازه‌ی دریافت گذرواژه‌ی مجدد را به کاربر می‌دهد. سیستم نباید اجازه‌ی استفاده از گذرواژه‌های خیلی طولانی یا پیچیده را بدهد، به گونه‌ای که به خاطر آوردن آن‌ها برای استفاده کننده دشوار باشد. اگر گذرواژه‌ها خیلی پیچیده باشند، کاربران برای جلوگیری از فراموشی گذرواژه را در جایی یادداشت می‌کنند و بدین صورت هدف محرمانه بودن گذرواژه‌ها خدشه‌دار می‌شود. باید نحوه‌ی استفاده از گذرواژه را به افراد آموزش داد. به این معنی که باید مانع اشتراک‌گذاری گذرواژه یا نوشتن آن‌ها در محل‌های قابل رؤیت شد.

نمایه‌ی سه: تبادل بین ورود دو گذرواژه‌ی فناوری اطلاعات



(ج) کد برنامه‌های مخرب و ویروسی

ویروس رایانه‌ای، برنامه‌ی معمولی خیلی کوچکی است که می‌تواند رونوشتی از خود ایجاد کند و رایانه‌ی دیگری را بدون اجازه یا اطلاع کاربر آلوده سازد. واژه‌ی ویروس به این دلیل مورد استفاده قرار می‌گیرد که برنامه‌ای است که می‌تواند خود را به سیستم دیگری برساند و سپس به سیستم‌های دیگر راه پیدا کند. ویروس می‌تواند از رایانه‌ای آلوده به رایانه‌ی سالم انتقال یابد. برای نمونه، به وسیله‌ی کاربری که ویروس را به سراسر شبکه یا اینترنت می‌فرستد یا از طریق حمل آن روی وسیله‌ی قابل حمل مانند دیسک فشرده یا دستگاه‌های یو.اس.بی ویروس‌ها می‌توانند با آلوده‌کردن پرونده‌های روی شبکه، به سیستم رایانه‌هایی گسترش یابند که به بارگیری پرونده‌ی ویروسی پرداخته‌اند.

حسابرسان داخلی باید تشخیص دهند که ویروس، تهدیدی دایمی است. بنابراین باید در سیستم مرکزی فناوری اطلاعات، نرم‌افزار ضد ویروس مؤثر و مناسب را نصب کنند. حسابرس داخلی باید بررسی کند که نسخه‌ی رایج نرم‌افزار حفاظتی نصب شده، به طور منظم به‌روزرسانی و اقدامات لازم برای کشف ویروس‌ها اعمال می‌شود.

نمایه چهار: انواع کدهای برنامه‌های مخرب

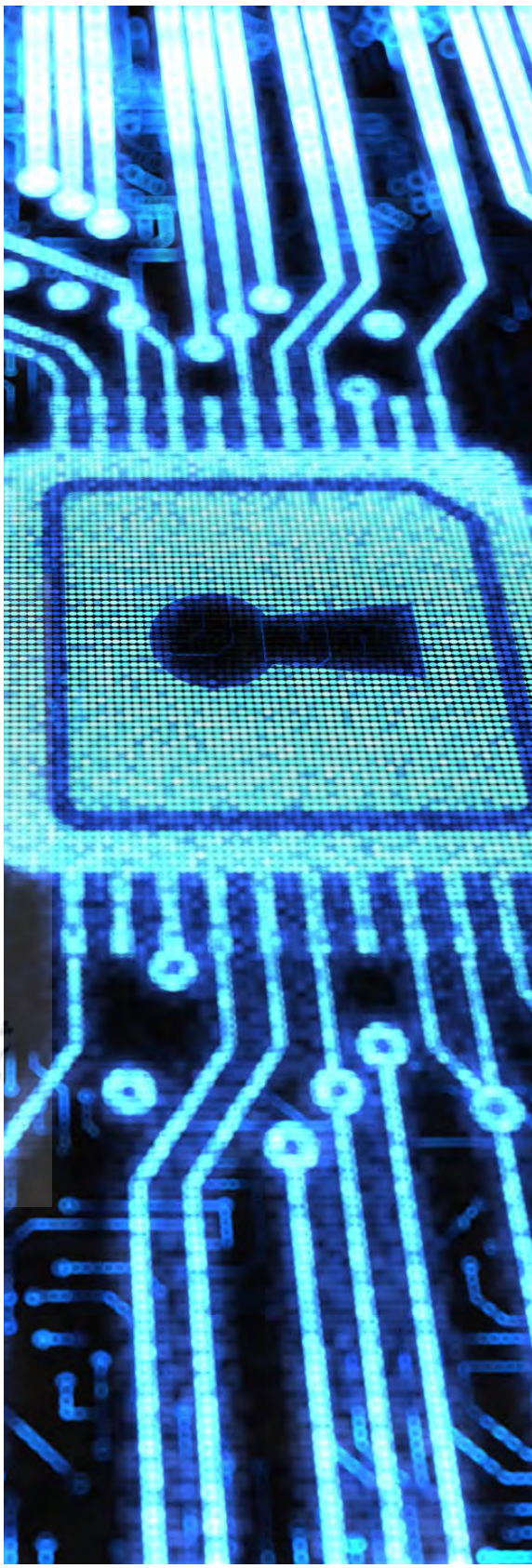
نوع	مشخصات
ویروس(Virus)	خود را به برنامه‌ها ضمیمه می‌کند و رونوشت‌هایی از خود به برنامه‌های دیگر منتشر می‌کند.
تروجان (Trojan horse)	این ویروس قابلیت غیر منتظره بودن دارد که بعد از انجام وظایفی خود را نشان می‌دهد.
بمب منطقی (Logic bomb)	برنامه‌ای‌ست که با رخ دادن رویدادهای مشخصی راه‌اندازی می‌شود.
بمب زمانی(Time bomb)	برنامه‌ای است که در زمان مشخصی راه‌اندازی می‌شود.
در پشتی(Trapdoor)	نرم‌افزاری بدون مدرک شناسایی است که که حفاظت سیستم را مختل می‌کند.
کرم (Worm)	به انتشار نسخه‌هایی از خود از طریق شبکه اقدام می‌کند.
خرگوش (Rabbit)	کد نرم‌افزاری‌ست که بدون محدودیت برای تخلیه‌ی منابع منتشر می‌شود.

(د) سرقت از طریق تارنمای ساختگی و دیگر تهدیدات هویتی

همراه با رشد خرید آنلاین و خرید بانکی، خطرهای ایمنی سایبری به طور گسترده‌ای افزایش یافته‌اند. انگیزه‌های مالی به طراحی روش‌هایی برای فریب کاربران به منظور افشای نام کاربری و گذرواژه‌ها و اطلاعات محرمانه منجر خواهند شد که می‌تواند زمینه‌ی وسیعی برای تقلب هویت افراد ایجاد کنند. هدف معمول، خالی کردن حساب بانکی قربانی است.

سرقت از طریق تارنمای ساختگی به تلاش برای به‌دست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی از طریق جعل تارنما و رایانامه (ای‌میل) گفته می‌شود و فعالیت متقلبانه به عنوان سرقت آن‌لاین شناخته می‌شود. به این صورت که از رایانامه‌ها و تارنماهای ساختگی به عنوان طعمه برای به دست آوردن اطلاعات محرمانه‌ی افراد استفاده می‌شود. کلاهبرداران در این فعالیت‌ها، اقدام به فرستادن رایانامه‌های معتبر به افراد می‌کنند که ادعا دارند از طرف مؤسسات شناخته‌شده هستند. گیرنده، تشویق می‌شود که بر لینک تارنمای موجود در رایانامه کلیک کند و بدین ترتیب به تارنمای ساختگی وارد می‌شود که تشخیص ساختگی بودن آن برای گیرنده ممکن نیست.

در این فرایند، حتی اگر افراد کم‌شماری هم رایانامه و تارنمای ساختگی را معتبر بدانند، کلاهبرداران



مقدار هنگفتی پول می‌توانند به دست آورند. بر اساس یافته‌های کارگروه ضد سرقت آن‌لاین،[1] میانگین طول زمان آن‌لاین برای تارنمای ساختگی چهار روز است. با هزینه‌ی نسبتاً پایین راه‌اندازی تارنما و فرستادن هزاران رایانامه، تنها قربانیان کم‌شماری لازم است که این فرایند سرقت آن‌لاین به طرحی سودآور بدل شود. تاکنون تعداد زیادی از حملات سرقت آن‌لاین گزارش شده است.

سرقت دورنگاری[2]

فرد متقلب در این روش به عنوان تهدید مربوط به احراز هویت، دورنگارهایی را به مشتری سازمانی می‌فرستد و از آن‌ها تقاضای ورود به اینترنت و ارسال نشانی اینترنتی[3] را خواهد داشت. این دورنگار، نسخه‌ای از سرقت آن‌لاین است و سرقت دورنگاری نامیده شده است. کنترل‌های مؤثر لزوماً پیچیده نیستند. برای نمونه، استفاده کنندگان باید با دورنگارها به صورت محتاطانه برخورد کنند. برقراری تماس با فرستنده‌ی فرضی با استفاده از دفترچه تلفن، قبل از پاسخ به‌وسیله‌ی اینترنت کنترل ساده‌ای برای جلوگیری از سرقت دورنگاری است. اگر کسی چنین کنترلی را انجام دهد، می‌تواند از سرقت دورنگاری جلوگیری کند و اطلاعات هویتی یا حساب بانکی خود را حفظ کند.

شناسایی طرح‌های سرقت، از مسئولیت مدیران شرکت است که جامعه‌ی کاربری خود را در برابر چنین تقلب‌هایی آموزش دهد. همچنین حسابرسان داخلی باید از این طرح‌ها آگاه باشند و هشدارهای مورد نیاز را به هنگام نیاز ارائه کنند.

(و) فایروال‌های سیستم فناوری اطلاعات

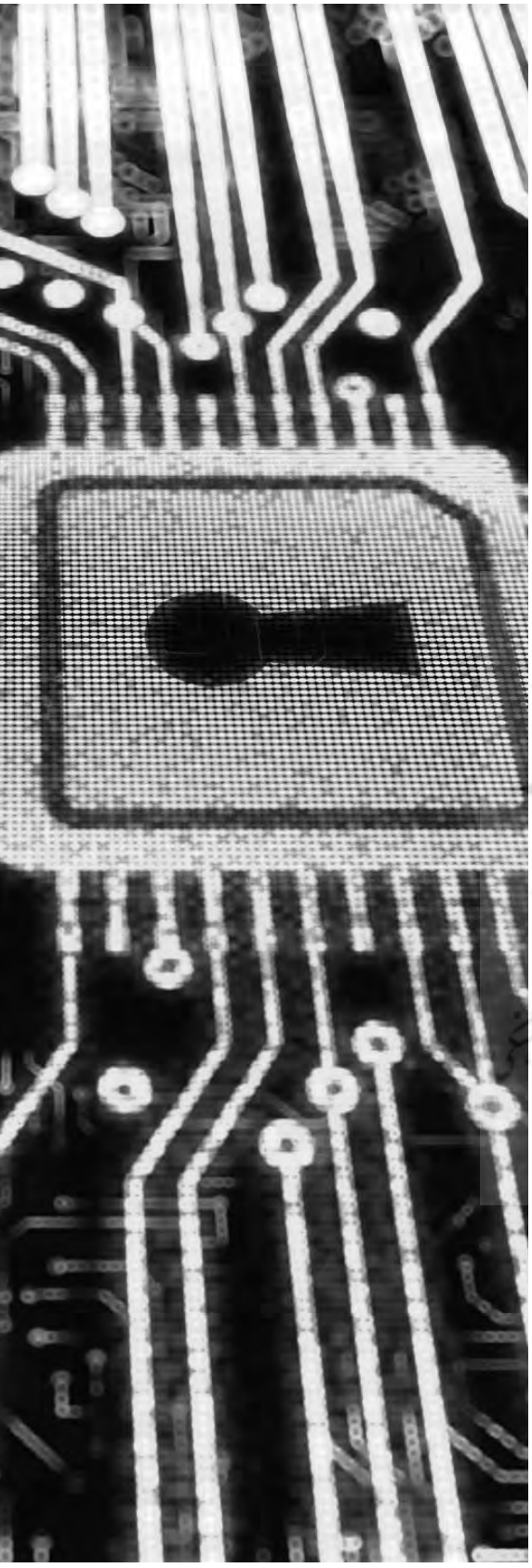
فایروال، ابزاری است که آمدوشد را بین محیط‌های حفاظت‌شده یا قسمت داخلی و محیط‌های کم‌تر محافظت شده یا غیر قابل اطمینان و بیرونی کنترل می‌کند. فایروال، نرم‌افزار تخصصی است که برخی از انواع معاملات را ممکن می‌سازد یا از آن‌ها جلوگیری می کند. شرکت به نصب فایروال بین شبکه‌ی سیستم و دنیای بیرونی از طریق اینترنت یا منابع دیگر نیاز دارد. فایروال، روال نظارت، گذرگاه واسطه‌ای، یا محافظ نامیده می‌شود. حسابرسان داخلی در این زمینه به فهم جزییات فنی نیاز دارند. به نظر حسابرسان داخلی، شرکت‌ها می‌توانند به هنگام راه‌اندازی فهرست قیمت آن‌لاین و ارائه‌ی محصولات، از فایروال‌ها استفاده کنند. فایروال باید از اصلاح قیمت و تولید اطلاعات و دسترسی به پشتیبانی از پرونده‌های در ارتباط با ارائه‌ی محصول توسط کاربران جلوگیری کند. زمانی فایروال مورد استفاده قرار می‌گیرد که شرکت به کارکنان اجازه‌ی دسترسی به برخی از نواحی وب را نمی‌دهد. علاوه بر نظارت بر آدرس‌های شبکه یا آدرس‌های سایت، فایروال می‌تواند بر مفاهیم

(4) enterprise resource planning (ERP)
(5) Universal Serial Bus (USB)
(6) arpanet

خاص در پیغام یا صفحه‌ی وب نظارت کند و همچنین به حسابرسی و گزارش این فعالیت‌ها بپردازد. فایروال باید به طور منظم به‌روزرسانی شود. در صورت کنترل تمام دسترسی‌ها به محیط شبکه، محیط توسط فایروال محافظت شده است. برای نمونه، اگر فایروال برای کنترل دسترسی به شبکه‌ی محلی راه‌اندازی شده باشد، در صورت وجود مودم، امنیت سیستم از بین می‌رود. با وجود این‌که فایروال‌ها کنترل‌های ایمنی قدرتمندی‌اند، گاهی مورد هدف عاملان تقلب قرار می‌گیرند. حسابرسان داخلی باید زمان اجرای بررسی ایمنی داده، محل و ماهیت فایروال‌های نصب شده را درک کنند. علاوه بر آن، حسابرسان داخلی باید به پی‌گیری فعالیت راجع به تخلف گزارش‌های فایروال بپردازد. نکته‌ی مهم این است که فایروال، حفاظت کافی را فراهم آورد و به طور منظم به‌روز شود. استفاده‌ی مؤثر از فایروال، نمونه‌ی خوبی از حسابرسی داخلی مؤثر در بررسی موضوع است. در بسیاری از موارد، حسابرسان داخلی به دانستن ویژگی‌های فنی فایروال نیاز ندارند و تنها باید به طراحی چند سؤال کلی برای ایجاد ایمنی سایبری بپردازند. برای نمونه، حسابرسان داخلی برای بررسی کنترل‌های امنیت سایبری شبکه در بخش اجرایی کوچک، می‌توانند پرسش‌های زیر را از شرکت جویا شوند:

- آیا می‌توانید نموداری از شبکه‌ی فناوری اطلاعات را در اختیار من بگذارید که تمام ارتباطات خارجی و داخلی شبکه را نشان دهد؟
- آیا فایروال برای شبکه نصب کرده‌اید ؟ و در صورت نصب آیا آن‌ها از دسترسی به همه‌ی نقاط حفاظت می کنند؟
- آیا راهی وجود دارد که دستگاه‌های شبکه بتوانند با وسیله‌های دیگر ارتباط برقرار کنند؟
- فایروال چه اقدامات یا مبادلاتی انجام می‌دهد؟
- آیا فایروال به طور منظم به‌روزرسانی می‌شود؟ آخرین به‌روزرسانی مربوط به چه زمانی است؟
- چه نوعی از تلاش‌ها برای دسترسی نامناسب مورد نظارت فایروال است؟
- آیا می‌توانم برخی از اسناد اخیر نقص فایروال را بررسی کنم؟

هیچ کدام از این سؤالات، به دانش فنی حسابرسان داخلی نیاز ندارد. حسابرسان داخلی تشخیص می‌دهند که فایروال‌ها برای کنترل ایمنی مؤثر هستند . البته حسابرسان داخلی همیشه ممکن است با خطر دریافت پاسخ نامفهوم از شخصی مواجه شوند که می‌خواهد بر رویه‌های حسابرسی داخلی اثر گذارد. در این حالت، بهترین راه‌حل نوشتن پاسخ و پیگیری بعدی با منابع فنی است. البته پاسخ‌های عمومی به این سؤال‌ها ممکن است برخی از نقاط قوت و ضعف کنترل داخلی در موضوع مورد بررسی را نشان دهد.



(ی):سایر موضوعات مرتبط با ایمنی رایانه

امروزه، شبکه‌های فناوری اطلاعات باید بسیاری از تهدیدات ایمنی و کدهای مخرب را مورد رسیدگی قرار دهند. روش‌های مقابله شامل گذرواژه‌ها و فایروال‌ها، کنترل‌های اضافی ماهرانه، رمزگذاری هنگام انتقال داده و ایمنی چندسطحی در مدیریت پایگاه داده و بسیاری موارد دیگر است. از نظر حسابرس داخلی، موضوعات مرتبط با ایمنی رایانه بر نیاز به ایجاد حمایت مدیریتی قوی برای برنامه‌های ایمنی فناوری اطلاعات در موقعیت مناسب و برنامه‌های آموزشی برای استفاده کنندگان به منظور کاهش آسیب‌پذیری و تهدیدات متمرکز است. بررسی‌های مداوم کنترل‌های داخلی فناوری اطلاعات به‌وسیله‌ی حسابرسان داخلی، باید شامل رویه‌های کنترل ایمنی سایبری و شبکه باشد. در بسیاری از موارد، این موضوعات دارای پیچیدگی فنی و خطرات بیشترند. حسابرسان داخلی ممکن است متخصصان خبره‌ی ایمنی فناوری اطلاعات نباشند، اما در صورت نیاز آنها باید با متخصصان ایمنی فناوری اطلاعات تماس حاصل کنند. (مولر، ۲۰۰۹)

نگرانی‌های امنیت سیستم فناوری اطلاعات

امروزه در شبکه‌های در حال پیشرفت و پیچیده‌ی متصل به اینترنت، مسئله‌ی ایمنی در بسیاری از سطوح، در حال رشد است و این امر موجب نگرانی در مورد ایمنی می‌شود. در این قسمت در مورد داده‌های شخصی و اطلاعات فردی صحبت می‌شود که شرکت‌ها و مقامات دولتی مجاز به اطلاع از آن‌هاست. به همین ترتیب، از نظر امنیت و ایمنی، شرکت نیز خواستار سطوح کافی حفاظت است. موضوعات مرتبط با فناوری اطلاعات باید در نظارت حسابرس داخلی باشد.

(الف) موضوع امنیتی داده‌های کارکنان

اغلب داده‌ها بدون رضایت از افراد و شرکت‌ها گردآوری می‌شود. برای افراد، داده در سیستم رایانه گردآوری و ذخیره می‌شود و این سیستم دارای مشخصات زیر است:

- صورتحساب‌هایی که با کارت اعتباری پرداخت می‌شوند اثرهایی مانند مقدار و نوع و زمان خرید را در سیستم به جا می‌گذارند.
- استفاده از کارت‌های تخفیف فروشگاه‌های بزرگ که داده‌هایی از تمام خریدها ایجاد می‌کند.
- هنگام گشت‌وگذار در اینترنت و بازدید از تارنماها، اثر قابل‌توجه از افراد به جا می‌ماند.

داده‌ها به هنگام اشتراک مجلات، ثبت نام در کتابخانه، عضویت در انجمن‌های حرفه‌ای، تکمیل کارت‌های ضمانت، رأی دادن به نامزد سیاسی، کمک به سازمان‌های مذهبی و خیریه و سرمایه‌گذاری در سهام نیز گردآوری می‌شوند و در پرونده‌های رایانه‌ای ذخیره می‌شوند. بعد از حمله‌ی

تروریستی یازده سپتامبر، دولت ایالات متحده و مقامات اجرایی، تدوین برنامه‌ی آموزشی شرکت هواپیمایی مسافربری را پیشنهاد کردند که داده‌های مورد نیاز آن از پرونده‌های مصرف‌کنندگان گردآوری شد. این پیشنهاد در کنار بحث‌برانگیز بودن آن، قابل‌اجرا نبود اما در سال‌های آینده امکان توسعه‌ی محدود آن وجود دارد. حمایت‌های قانونی برای حفظ حریم خصوصی در ایالات متحده ضعیف هستند. در ایالات متحده در مورد چگونگی نگهداری داده‌ها و ادغام، محدودیت‌هایی وجود دارد. در حالی که در کشورهای عضو اتحادیه‌ی اروپا، کانادا،

زلاندنو و استرالیا قوانین قوی‌تری وجود دارد. در واقع، به دلیل وجود داده‌های نامحدود و منابع متعدد نقص ایمنی در محیطی ممکن می‌شود که در آن چند محدودیت قانونی در مورد چگونگی استفاده داده‌ها و ادغام وجود دارد و در نتیجه آزادی‌های مدنی پایمال می‌شود. حسابرسان داخلی باید درکی کلی از این موارد داشته باشند.

(ب) حریم خصوصی آن‌لاین در مسایل مربوط به تجارت الکترونیک

تهدیدات حریم شخصی کاربران اینترنت، امری عادی است. دانستن این موضوع الزامی است که اینترنت به عنوان وسیله‌ی ارتباطات ذاتاً ناامن طراحی شده است و هکرها اغلب نشان داده‌اند که آن‌ها می‌توانند به امن‌ترین امکانات نهادهای مالی و نظامی نفوذ پیدا کنند. علاوه بر این، شرکت‌ها روش‌های متعددی برای ردیابی کاربران وب طراحی کرده‌اند به این عنوان که آن‌ها از تمام تارنماهای اینترنت بازدید کند و به خرید می‌پردازند. سارقان هویت می‌توانند در فروشگاه آن‌لاین، به صورت ناشناس از هویت اعتباری دیگران استفاده کنند و کارگزاران اطلاعات مبتنی بر وب، داده‌های شخصی افراد را ارزان بفروشند.

(ج) شناسایی فرکانس رادیویی

هنگامی که مراجعه‌کنندگان به پمپ‌های گاز می روند و متناسب با مقدار مصرفی گاز پول می پردازند، از فناوری فرکانس رادیویی[1] استفاده می کنند. فناوری شناسایی فرکانس رادیویی اغلب برای کارت‌های ورودی استفاده می‌شود. برای نمونه، افراد با استفاده از کارت شناسایی می‌توانند به ساختمان یا دفتر داخلی ساختمان وارد شوند. بسیاری از کارت‌های شناسایی کارکنان با استفاده از فناوری شناسایی فرکانس رادیویی مورد استفاده قرار می‌گیرند. به دلیل آن‌که استفاده از این کارت‌ها تنها به تکان دادن آن‌ها در فاصله‌ی چند اینچی از کارت‌خوان خلاصه می‌شود. این کارت‌ها، کارت‌های از راه دور و بدون تماس نامیده می‌شوند. هر فرد به خوبی از هر برچسب شناسایی فرکانس رادیویی و هربار آگاهی دارد که قابل دسترس باشد. اما برچسب‌های شناسایی فرکانس رادیویی کوچک هستند و در مواردی می‌توانند چنان جاسازی شوند که نامرئی باشند و همین‌طور دستگاه‌های خواندن برچسب‌ها نیز می‌توانند نامرئی باشند. در آینده دستگاه‌های خواندن شناسایی فرکانس رادیویی در دکل‌های چراغ‌های خیابان جاسازی خواهند شد و امکان دارد که برچسب شناسایی فرکانس رادیویی مرتبط با فرد در گواهینامه‌ی او جاسازی شود و تمام تراکنش‌های فرد را که در طول روز با آن‌ها درگیر است ضبط کند. برای نمونه، خرید روزنامه از دستگاه سکه‌ای، ورود به فروشگاه و خرید مواد غذایی، استفاده از وسایل حمل‌ونقل عمومی، ورود به محل کار و از این قبیل کارهای روزانه که شناسایی فرکانس رادیویی قادر خواهد بود در آینده همه‌ی آن‌ها را ضبط کند. اگر برچسب‌های شناسایی فرکانس رادیویی در گواهی‌نامه‌های رانندگان جاسازی می‌شدند که اکثر مردم در بیش‌تر مواقع آن‌ها را با خود حمل می‌کنند ناشناس‌ماندن و حریم خصوصی دیگر وجود نخواهد داشت و به تاریخ خواهد پیوست. آیا چنین سناریویی ممکن است اتفاق بیفتد؟ بسیاری از مردم به‌سختی می‌توانند تصور کنند که چنین استفاده‌هایی از شناسایی فرکانس رادیویی بتواند رخ دهد.

(7) (IBM) Corporation) International Business Machines

(د) نبود قوانین حفاظت داده‌ها

شهروندان کشورهای توسعه‌یافته در سراسر جهان به احیای حقوق از طریق قوانین حفاظت داده‌ها علاقه‌مندند. در بسیاری از کشورهای وسیع یا در میان توده‌ی مردم، قوانین حفاظتی داده چگونگی استفاده از اطلاعات شخصی به وسیله‌ی نمایندگی‌های دولت مانند نهادهای بخش‌های تجاری کنترل می‌کند. با توجه به این قوانین استفاده از اطلاعات شخصی معمولاً برای تصمیم‌گیری‌های شخصی است. به عبارت دیگر، اطلاعات شخصی افراد برای بازاریابی استفاده نمی‌شود مگر آن‌که افراد راضی باشند. ایالات متحده این قوانین را ندارد، اما قوانینی وجود دارد که بخش‌های صنعتی معینی را پوشش می‌دهد. برای نمونه، قانون حفاظت از کاربر تلفن، قانون گزارش اعتباری منصفانه، قانون نقل‌وانتقال و مورد اطمینان بودن بیمه و دیگر قوانین ایمنی مالی مطرح است. کاستی‌های مطرح شده در این قسمت، استفاده از داده‌های شخصی حفاظت نشده است. حق انتخاب خارجی رویکرد ایمنی مورد استفاده است که در ایالات متحده به آن اشاره می شود. برای نمونه، اطلاعات شخصی افراد برای فرستادن پست الکترونیک تبلیغاتی استفاده می‌شود و در صورت عدم تمایل افراد به دریافت این پست‌های الکترونیکی، آن‌ها می‌توانند ازطریق صنعت بازاریابی خدمات دریافت پست الکترونیک از فرستادن پست الکترونیک جلوگیری به عمل آورند. (مولر، ۲۰۰۹)

حسابرسی حریم خصوصی و امنیت فناوری اطلاعات

حسابرسان داخلی باید به اجرای بررسی‌های فناوری اطلاعات یا کنترل‌های ایمنی سایبری و همچنین انطباق با رویه‌های ایمنی توجه کنند. همان‌طور که بحث شد، رویه‌ی ایمنی شبکه می‌تواند فنی و پیچیده باشد، بنابراین حسابرسان داخلی با آموزش تخصصی و فنی محدود و بررسی محدود ضمنی ایمنی سایبری نمی‌توانند به صورت کارا عمل کنند. حسابرسان داخلی دارای مهارت‌های فنی، می‌توانند در برنامه‌ریزی و اجرای حسابرسی مفید واقع شوند. نمایه‌ی پنج، مهم ترین رویه‌های حسابرسی کنترل‌های داخلی ایمنی سایبری را توضیح می‌دهد.

حسابرسان داخلی باید سطح درک خود را از کنترل‌ها و خطرات موضوعات مهم رشد دهند. به دلیل وجود جهان به‌هم‌پیوسته، بنگاه‌های اقتصادی به ایجاد و گسترش کنترل‌های ایمنی سایبری مؤثر و قوی نیاز دارند. حسابرسان داخلی ممکن است افراد فنی نباشند اما در کلی از خطرات و مسایل مربوط به کنترل در این حوزه‌ها باعث کمک مؤثری برای مدیریت بنگاه اقتصادی است. (مولر، ۲۰۰۹)

۱. انواع کنترل‌های امنیتی شبکه

الف) بررسی وضعیت شبکه برای حداقل سازی اتصالات به شبکه‌های دیگر و سیستم‌های رایانه‌ای

ب) محدود ساختن اتصالات به اینترنت و استفاده از آن در موارد لزوم

ج) ارزیابی میزان اتصالات بی سیم و تعیین ایمن بودن اتصالات

د) بررسی میزان اتصالات شماره‌گیری در محل و بررسی ایمن بودن اتصالات به وسیله نظارت

۲. کنترل‌های دسترسی به سیستم شبکه

الف) ارزیابی کفایت کنترل‌های ایمنی فنی در مراکز داده اصلی

ب) بررسی هرگونه امکانات از راه دور مانند سایت‌های آزمایشگاهی تحقیقاتی و تعیین این که آیا آن‌ها زیر نظر پردازش فناوری اطلاعات مرکزی هستند؟

ج) بررسی وضعیت برای اطمینان از امنیت بخش‌های کاری مرتبط با شبکه

د) ارزیابی مناسب بودن حفاظت‌های فیزیکی شامل سخت افزار، تجهیزات مخابراتی، کابل‌ها

۳. بررسی میزان و پوشش رویه‌های ایمنی سایبری فعلی

الف) نظارت بر اطلاعات نیروهای استخدامی جدید

ب) کنترل‌های اساسی اسناد و حفاظت اطلاعات

ج) رویه‌های دسترسی به سیستم و گذرواژه

د) استفاده از امکانات برای موارد کسب‌وکار و محدودیت استفاده‌ی شخصی از منابع سیستم

هـ)کشف اطلاعات حساس

۴. کنترل‌های متقابل و پیشگیری

الف) بررسی سیاست همه‌جانبه‌ی گذرواژه برای تعیین وجود رویه‌هایی برای نظارت موارد تخلف گذرواژه‌ها و الزام تغییرات منظم آن

ب) تشخیص مؤثر بودن سیاست تنظیم مجدد گذرواژه‌ها در صورت فراموشی رمز.

ج) بررسی محل و هدف فایروال‌های نصب‌شده و ارزیابی مناسب آن‌ها

د) بررسی فعالیت فایروال و پیشنهاد فعالیت‌های اصلاحی در صورت نیاز

ه) بررسی کفایت رویه‌های حفاظتی برای جلوگیری از تقلب

د)ارزیابی کفایت رویه‌های رمزگذاری

۵. روش‌های رسیدگی و نظارت ایمنی

الف) بررسی اینکه آن‌ها رویه‌های رسیدگی و گزارش‌های رویدادی معمول‌اند.

ب) بررسی مناسب برنامه‌های اقدامی برای اجرا در هنگام وقوع نواقص ایمنی

ج) بر اساس یک آزمون، بررسی اقدامات انجام‌شده بر رویدادهای مشکوک گزارش‌شده نشان می‌دهد که اقدامات اصلاحی قابل‌اجرا انجام شده است.

د) بررسی مهارت‌ها، آموزش و اقدامات مستند در پاسخ‌های رویدادی برای ارزیابی مؤثر آن‌ها

هـ) تشخیص کفایت هماهنگی با سازمان‌های اجرای قانون در حمایت از موضوعات ایمنی سایبری

۶. آموزش ایمنی سایبری

الف) تشخیص این‌که تمام کارکنان تحت تأثیر آموزش در حوزه‌ی مسائل و خطرهای ایمنی سایبری هستند.

ب) جست‌وجوی برنامه‌ی آموزشی امنیتی برای افزایش آگاهی و برجسته‌سازی خطرهای بالقوه

امنیت و حریم خصوصی در حسابرسی داخلی

حسابرسان داخلی به عنوان عاملی در بنگاه اقتصادی نیاز به گسترش ایمنی و امنیت رویه‌ها و اتخاذ بهترین روش‌ها را دارند. حسابرسان داخلی به طور منظم سایت‌ها را می‌بینند و اطلاعات را در سخت‌افزار یا نرم‌افزار ذخیره و بررسی خود را در مورد موضوع کامل می‌کنند و اطلاعات دیگران را هم از سایت حسابرسی‌شده به دست می‌آورند. بر اساس ماهیت بررسی‌ها، شواهد حسابرسی به دست آمده را باید به صورتی امن و محرمانه نگهداری کرد.

امروزه اکثر واحدهای حسابرسی داخلی، به جای ثبت اطلاعات در کاربرگ‌ها با استفاده از مداد و کاغذ و داشتن گزارش‌های حجیم، به استفاده از رایانه رو آورده‌اند. در سال‌های گذشته، حسابرسان داخلی نتایج کار خود را در کاربرگ‌ها نگه‌داری می‌کردند و بعد از اتمام حسابرسی موارد ویژه، کاربرگ‌های تأیید شده را در بخش‌های حسابرسی نسبتاً امن نگه‌داری می‌کردند. در گذشته همیشه خطر گم شدن کاربرگ‌ها وجود داشت و در مقابل در عصر سیستم‌های رایانه‌ای ممکن است خطرهای ایمنی و امنیتی بیشتری را برای حسابرسان داخلی ایجاد کند. (مولر، ۲۰۰۹)

(الف) امنیت و کنترل برای سیستم‌های رایانه‌ی حسابرسان

هنگامی که روش حسابرسی پیشرفته مورد استفاده قرار می‌گیرد، استفاده‌ی حسابرسان از سیستم رایانه‌ای، امری طبیعی و اساسی است. بر اساس نرم‌افزار سیستم اجرایی مایکروسافت، برای ثبت گزارش‌های حسابرسی از نرم‌افزار واژه‌پردازی، نرم‌افزار صفحه گسترده و ارتباط با دیگران در گروه حسابرسی از طریق پست الکترونیک و اینترنت استفاده می‌شود.

حسابرسان داخلی، رایانه‌ی دستی خود را همراه با خود حمل می‌کنند. برای نمونه، حسابرسان داخلی هنگام پرواز از سیستم رایانه‌ای خود برای رسیدگی به حسابرسی‌ها استفاده و به تارنماهای صاحب‌کار خود مراجعه می‌کنند. به دلیل اینکه سیستم رایانه‌ای حسابرسان، حاوی پرونده و اطلاعات مهم است، دستگاه دارای ارزش ذاتی است. حمل رایانه‌ی دستی در سالن‌های فرودگاه یا حمل آن در صندلی عقب اتومبیل‌های کرایه‌ای، آن را در معرض سرقت قرار می‌دهد. هزینه‌ی اصلی هر رایانه‌ی دستی، از دست دادن داده‌های حسابرسی داخلی در پرونده‌های سیستم است. برخی از روش‌های مهم برای حفاظت رایانه‌ی دستی حسابرس عبارتند از:

مسئولیت شخصی حسابرسان برای رایانه‌ی دستی: باید به حسابرسان داخلی دارای رایانه‌ی دستی از طریق آموزش، استانداردهای بخش حسابرسی و رهنمودهای مؤثر خاطر نشان کرد که مسئولیت ایمنی رایانه‌ی دستی با حسابرسان داخلی است. این نوع از استانداردها شامل رهنمودهای ساده‌ی رها نکردن رایانه دستی در صندلی اتومبیل، حفظ آن در کیف قفل شده و اجازه ندادن به اعضای خانواده برای استفاده ار رایانه دستی است.

روش‌های تهیه‌ی نسخه‌ی پشتیبان: بخش پشتیبان سایت در مرکز راهبری دفتر حسابرسی داخلی، باید به طور منظم به تهیه‌ی نسخه‌ی پشتیبان مبادرت کند. امروزه دستگاه‌های ذخیره‌سازی مخصوصاً دستگاه‌های گذرگاه پیاپی همگانی، بسیار ارزان و در اختیار همگان است. باید رویه‌هایی برای حسابرسان داخلی ایجاد شود که کپی‌برداری روزانه از سیستم‌ها را ملزم می‌سازد. در این قسمت نیاز به ذخیره‌ی نسخه‌های متعدد نیست، زیرا نسخه‌ی پشتیبان فعلی به طور معمول کافی است. اگر کپی‌گرفتن برای حفاظت از داده‌ها در مقابل سرقت و یا آتش‌سوزی است، محل ذخیره‌سازی نباید نزدیک سیستم رایانه باشد؛ بلکه باید جایی باشد که در مقابل این مشکلات از حفاظت کامل برخوردار است. ولی اگر تهیه‌ی نسخه‌ی پشتیبان فقط برای بازیابی داده‌های پاک‌شده یا تغییر کرده صورت می‌پذیرد، باید محل آن طوری انتخاب شود که دسترسی به آن آسان باشد یک راه‌حل این است که حسابرسان داخلی، پشتیبانی‌های کامل را در یک محل امن و پشتیبانی‌های اضافی را در محلی نزدیک قرار دهند. راه دیگر این است که جدیدترین پشتیبان تهیه شده از داده‌ها را در دسترس و نسخه‌های قدیمی‌تر را در محل‌های امن‌تر بگذارند. بعضی افراد از پشتیبان‌ها دو نسخه تهیه می‌کنند و نسخه‌ای را دردسترس و دیگری را دور

از دسترس قرار می‌دهند. (سادوسکای و همکاران، ۱۳۸۴)

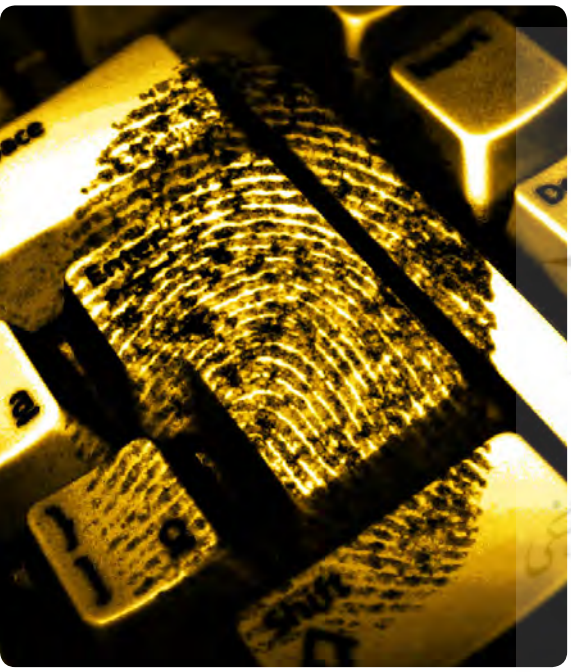
قفل‌های فیزیکی و سازوکار آن‌ها: دستگاه‌های کوچک متعددی، مشابه زنجیر قفل دوچرخه هستند که می‌توانند رایانه‌ی دستی را به میز یا وسیله‌ی دیگری متصل کنند که جابه‌جایی آن را دشوار می‌سازد. این قفل‌ها نسبتاً ارزان هستند و مدیران حسابرسان داخلی باید آن‌ها را برای استفاده‌ی حسابرسان داخلی به کار گیرند.

نرم‌افزار ضد ویروس و ابزارهای دیگر: نرم‌افزار ضد ویروس باید در تمام رایانه‌های دستی حسابرسان داخلی نصب شود. رایانه‌ی دستی حسابرسان داخلی اغلب مخزنی برای گزارش‌های حسابرس، نسخه‌هایی از اسناد و دیگر شواهد اساسی حسابرسی است. روش‌های امنیتی مناسب باید برای حفاظت منابع حسابرسی داخلی ایجاد شود حتی زمانی که مقامات حسابرسان داخلی از رایانه‌ی دستی استفاده نکنند و تنها به ماشین‌های رومیزی اکتفا کنند، باید روش‌های مشابه امنیتی حسابرسی نصب شود.

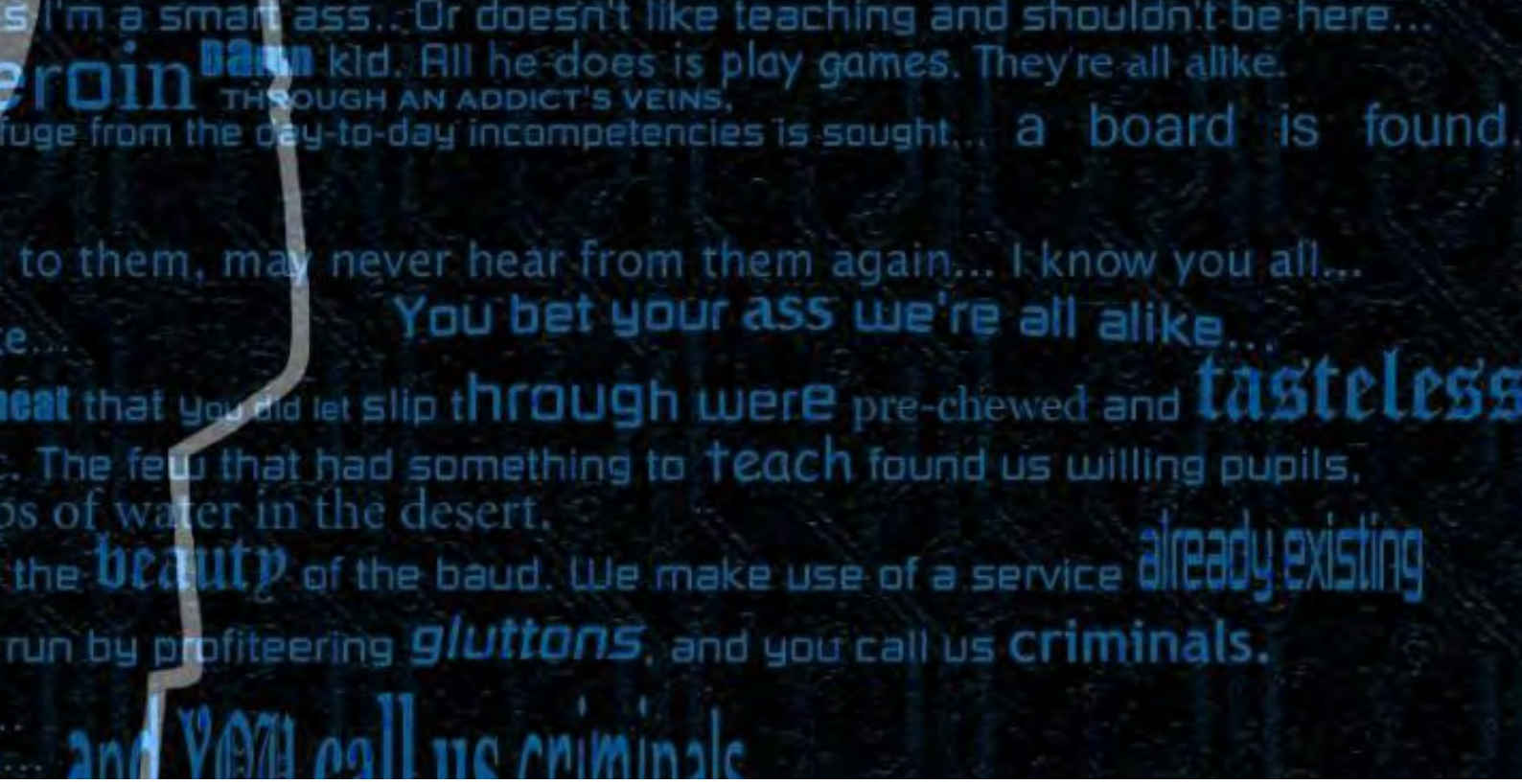
(ب) امنیت کاربرگ‌ها

کاربرگ‌ها، اسناد اساسی هستند که شواهد حسابرسی و نتیجه‌ی کار حسابرسی داخلی را نشان می‌دهند. در این بخش، ایمنی بخش حسابرسی بیشتر از کاربرگ‌ها دارای اهمیت است. قانون ساربینز آکسلی، نگه‌داری کاربرگ را برای دوره‌ی هفت ساله به عنوان شواهد حسابرسی ملزم می‌سازد. همچنین در موقعیت دادخواهی، کاربرگ‌های حسابرسی داخلی می‌توانند شواهد دادرسی مدنی یا حتی شواهد دادگاه جنایی باشند.

در محیط امروز، مستندسازی کاربرگ می‌تواند ترکیبی از نسخه‌های نرم‌افزاری و سخت‌افزاری باشند. حسابرسان داخلی به رویه‌ای قوی برای فهرست‌بندی، ذخیره‌سازی و ایمنی کاربرگ‌های حسابرسی داخلی نیاز دارند. مدیر اجرایی حسابرسی در راه‌اندازی چنین برنامه‌ای باید بداند که هفت سال زمانی طولانی است و در طول این مدت تغییرات زیادی در شرکت و واحدهای اجرایی آن می‌تواند ایجاد شود. هدف اصلی فرایند شماره‌گذاری کاربرگ‌ها، اجازه‌ی بررسی آن‌ها توسط مردم است. استفاده از کاربرگ‌ها باید به کارکنان حسابرسی داخلی و حسابرسی مستقل در صورت درخواست محدود شود. شماره‌ی پی‌گیری اسناد باید برای شناسایی محل کاربرگ‌های بررسی شده در هر زمانی نگهداری شود. حسابرسان همیشه نگران امنیت کاربرگ‌ها هستند. همواره اطلاعات موجود در کاربرگ‌ها در اشکال سخت‌افزاری و نرم‌افزاری ذخیره می‌شوند. رویه‌ها باید به گونه‌ای باشند که تهیه‌ی نسخه‌ی پشتیبان و حفاظت از کاربرگ‌ها را فراهم کنند. مستندات سخت‌افزاری باید در محلی امن و محافظت شده و با دسترسی محدود نگهداری شود. زیرا تجمع هفت‌ساله‌ی اطلاعات موجب پیدایش حجم زیادی از محتویات و توافقات می‌شود که به دنبال آن باید کاربرگ‌های قدیمی‌تر به مخازن اسناد امن منتقل شوند. نمایه‌ی شش، مواردی از بهترین روش‌های امنیتی کاربرگ حسابرسان داخلی را دسته‌بندی کرده است. امنیت کاربرگ‌ها به عنوان مهم‌ترین مستندات از این رو قابل توجه است که تمام فعالیت‌های حسابرسی داخلی را توصیف می‌کند. اعضای دیگر گروه حسابرسی همیشه اجازه‌ی بررسی کاربرگ‌های قدیمی برای پیگیری برنامه‌ها و روش‌های حسابرسی ایجاد شده را دارند. بعد از تصویب مستندات حسابرسی و انتقال قانونی هرگونه جلوگیری از تغییر در کاربرگ نیاز به



توجه ویژه‌ای دارد. همواره خطر وجود افراد متقلب در گروه حسابرسی داخلی وجود دارد. به همین دلیل شواهد در کاربرگ گردآوری می‌شود و به‌وسیله‌ی نسخه‌های سخت‌افزاری و نرم‌افزاری از اعمال تغییرات جلوگیری به عمل می‌آید به نحوی که تنها خواندن آن‌ها مجاز باشد.



نمایه شش: بهترین روش‌ها برای ایمنی کاربرگ‌های حسابرسی داخلی

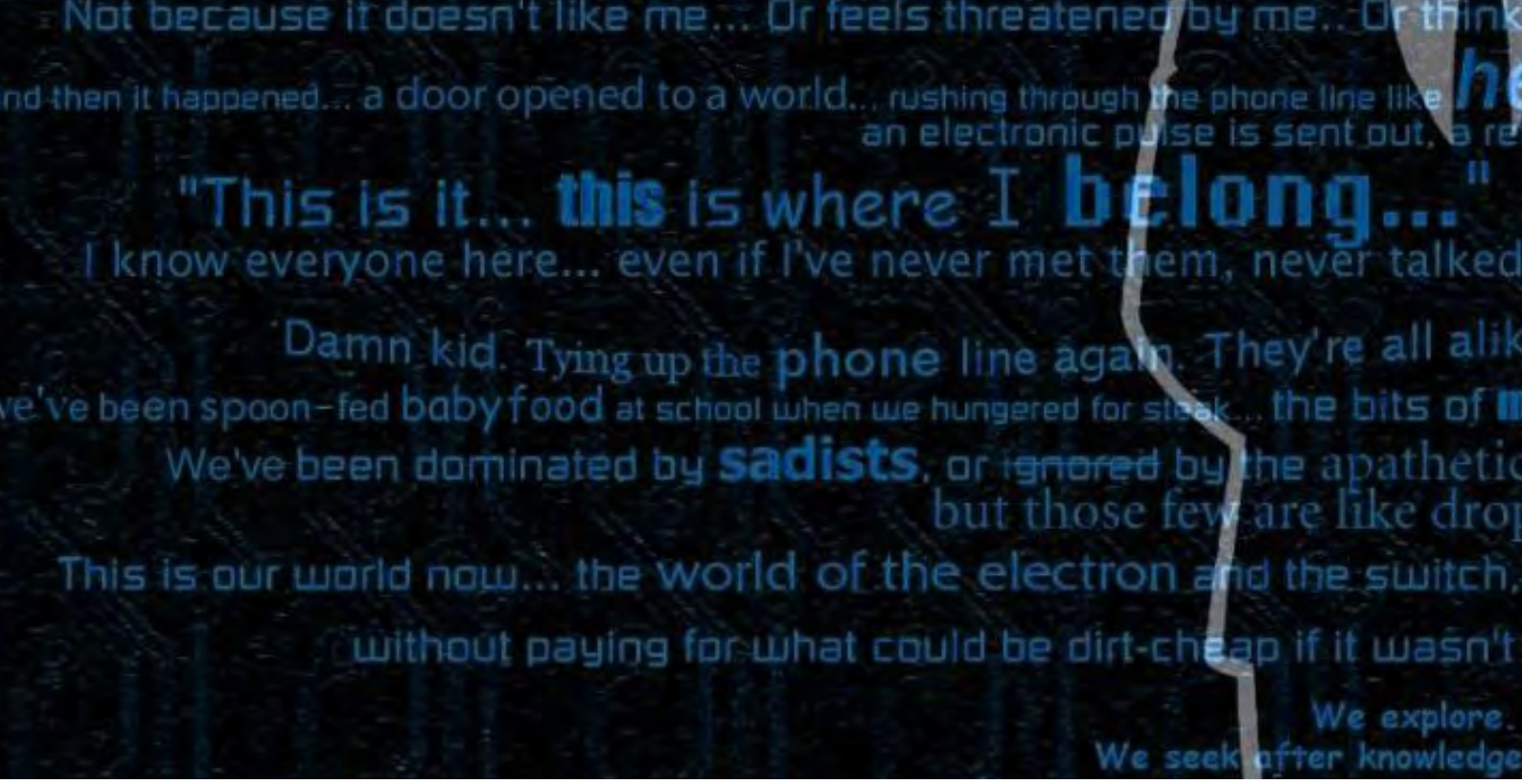
- ایجاد استانداردهایی برای کاربرگ‌های بخش حسابرسی داخلی برای موضوعات مشخصی مانند گردآوری شواهد حسابرسی، ضبط شواهد حسابرسی و دیگر موارد.
- ایجاد رویه‌های عمومی برای آماده‌سازی کاربرگ‌ها و ذخیره‌ی آن‌ها در سخت‌افزارهایی مانند کاغذ یا برنامه‌های آفیس در نرم‌افزار و ایجاد رهنمودهایی برای موارد استفاده‌ی هریک از سخت افزارها و نرم‌افزارها
- ایجاد سیستم‌هایی به صورت نمایه یا شماره‌گذاری برای تمام کاربرگ‌هایی که موجب شناسایی واحد تجاری و نوع حسابرسی و سال حسابرسی می شود.

برای کاربرگ‌های موجود در نسخه‌های نرم‌افزاری

- ایجاد پرونده و پوشه‌هایی حاوی پرونده‌های سازگار که آخرین تغییرات را شناسایی می‌کنند.
- به‌روز سازی کنترل‌های امنیتی
- تهیه‌ی نسخه‌های پشتیبان برای داشتن پرونده‌هایی امن به طور مداوم
- ایجاد رویه‌هایی برای به‌روزرسانی کاربرگ‌ها مانند به‌روزرسانی خودکار
- ایجاد رونوشت از کاربرگ‌هایی که نتایج کامل حسابرسی را نشان می‌دهند.

برای کاربرگ‌هایی که در سخت افزار (کاغذی) ذخیره می‌شوند

- ایجاد قوانین ایمنی برای کاربرگ‌های سنتی (کاغذ) در طول فرایند حسابرسی به منظور جلوگیری از دسترسی غیر مجاز افراد به کاربرگ‌های موجود درمیز حسابرس و غیره.
- تدوین رویه‌های سازگار برای انتقال داده‌های کاربرگ
- ایجاد استاندارد حسابرسی و رهنمود در مورد تغییرات صحیح کاربرگ‌ها به دلیل ردیابی دشوار تغییرات مفاهیم موجود در کاربرگ
- قرار دادن کاربرگ‌های فعلی در مخازن ایمن
- توافق برای حفظ تمام کاربرگ‌های قدیمی در مخازن ذخیره‌سازی انبوه.
- ساخت پایگاه داده‌ی وسیع برای برقراری ارتباط میان تمام کاربرگ‌های حسابرسی‌شده و گزارش‌ها و کشف‌های مهم.
- در رونوشت‌های سخت‌افزاری و نرم‌افزاری: ایجاد روش‌هایی برای بررسی کاربرگ‌های سازگار برای شناسایی زمان بررسی‌های نظارتی



(ج) حفظ حریم خصوصی و گزارش‌های حسابرسی

گزارش‌های حسابرسان داخلی، اطلاعاتی هستند که به توصیف فعالیت‌های حسابرسی داخلی برای طرح حسابرسی برنامه‌ریزی شده، روش‌های انجام‌شده، یافته‌ها و توصیه‌نامه‌ها، پاسخ‌های مدیریت به یافته‌ها در طول برنامه برای اقدامات اصلاحی می‌پردازند.

با توجه به ماهیت گزارش‌های حسابرسی متوجه می‌شویم که آن‌ها مستنداتی برای توزیع گروهی نیستند. آن‌ها تنها باید با توافق مدیریت صاحب‌کار، مدیریت ارشد بنگاه اقتصادی، حسابرس مستقل و کمیته‌ی حسابرسی به اشتراک گذاشته شوند. عدم اظهارنظرهای اضافه‌شده به مستندات گزارش حاکی از آن است که مستنداتی کپی نشده یا به اشتراک گذاشته نشده‌اند. اعضای گروه حسابرسی باید به طور منظم بر نیاز به محرمانه بودن این مستندات تأکید کنند.

مباحث مورد بحث در کاربرگ‌ها روی مسایل امنیتی مربوط متمرکز است. یافته‌های گزارش حسابرسی داخلی می‌تواند به اعتبار حرفه‌ای بخش‌های بنگاه اقتصادی و اعضای هیأت مدیره صدمه بزند. گزارش‌های حسابرسی منتشرشده امنیت را به‌خوبی افزایش داده است. باید از گزارش‌های حسابرسی در برابر دسترسی افراد غیرمجاز حفاظت کرد.

(د) آموزش و استانداردهای ایمنی و امنیتی حسابرسی داخلی

دیدگاه ما در مورد روش‌های ایمنی و امنیتی حسابرسی داخلی، برخی از بهترین روش‌ها را نشان می دهد که باید مسئولان حسابرسی داخلی بدون توجه به بزرگی آن‌ها، صنعت یا مکان جغرافیایی خود آن‌ها را در نظر بگیرند. در حالی‌که توافق و اجرای این رویه‌ها، موضوعی برای مهندسی به کمک رایانه است، تمام حسابرسان داخلی باید به طور مداوم از این روش‌ها آگاه باشند.

حسابرسان داخلی باید استانداردهای اداری را برای ایمنی و امنیت کاربرگ‌ها ایجاد کنند. توافقات برای مخازن رسمی کتابخانه (محل نگهداری کاربرگ) باید در داخل بنگاه‌های اقتصادی ایجاد شود. این توافقات به طور معمول با مهندسی به کمک رایانه و مرکز فرماندهی بنگاه اقتصادی ایجاد می‌شوند. برای بنگاه اقتصادی بزرگ و مقام حسابرسی داخلی بزرگ‌تر، مخازن کتابخانه‌های چندگانه یا خارج سازمان می‌توانند ایجاد شود. مکان اختصاص‌یافته به اعضای هیأت اداری باید از طریق کنترل همه‌جانبه‌ی اداری امن باشد. با الزامات نگهداری مداوم هفت‌ساله‌ی کاربرگ‌ها در مخازن سخت‌افزاری و نرم‌افزاری و کتابخانه‌ها، بازرسی‌های بعدی نسبتا آسان خواهد شد.

استانداردهای ایمنی و امنیتی بخش حسابرسی شامل استانداردهای بخش حسابرسی و آموزش می‌شود. به طور خاص، همان‌طور که بحث شد، هر عضو از گروه حسابرسی باید تقاضای به رسمیت شناختن نیازهای حفاظتی و ایمنی اختصاص یافته به رایانه را داشته باشد. اگرچه در بسیاری از موضوعات حسابرسی، حسابرسان داخلی توصیه‌های مربوط به ایمنی و امنیت را برقرار می‌کنند. (مولر، ۲۰۰۹)

نتیجه‌گیری

حسابرسان داخلی برای برقراری کنترل‌های امنیتی و ایمنی سایبری به دانش فناوری اطلاعات نیاز دارند و به دلیل پیشرفت روزافزون آن، نیاز به فهم کلی از رویه‌های کنترل داخلی و خطرهای مربوط احساس می‌شود. همچنین آنان باید بر الزامات استاندارد ایمنی داده‌ی رایانه و سیستم پشتیبان تصمیم‌گیری تسلط کافی داشته باشند. البته پیش‌نیاز آن، درک بیش‌تر کنترل ایمنی سایبری است. حسابرسان داخلی با دانستن اهمیت گذرواژه‌ها، آشنایی با برنامه‌های مخرب، نصب و به‌روز کردن منظم نرم‌افزار حفاظتی و درک ماهیت فایروال‌های نصب شده می‌توانند فعالیت‌های خود را بهبود بخشند. البته باید به این نکته توجه کرد که فقدان رویه‌های حسابرسی داخلی درست، داده‌ها و نرم‌افزار و سخت‌افزار سیستم‌های فناوری اطلاعات را با تهدیدات اساسی روبه‌رو می‌سازد.

منابع

الف) منابع فارسی

- جاود، بهراد(۱۳۹۱). مزاحمت سایبری چیست و چگونه با ان مقابله کنیم؟ قابل دسترسی در: http://d4fteam. com
- سلاجقه، ایمان(۱۳۹۲). ابعاد مختلف دنیای سایبر. قابل دسترسی در: bidaricyberi.blogfa.com
- سادوسکای، جورج. اکس دمپزی، جیمز. گرن برگ، آلن. شوارتز، آلن. جی مک، باربارا. (۱۳۸۴). راهنمای امنیت فناوری اطلاعات. مترجمان مهدی. میردامادی، زهرا شجاعی، محمدجواد صمدی. چاپ اول، دبیرخانه شورای عالی اطلاع رسانی.
- صدیق بنای، هلن(۱۳۸۵). فضای سایبر. قابل دسترسی در: /http://hamshahrionline. ir
- نورمن، کنت ال. (۱۳۹۱) روان شناسی سایبری. ترجمه: فاطمه وحدت نیا. ویراستار: بهاره فیروزه. تهران: نشر آسیم، .

ب) منابع انگلیسی

-Moeller, Robert. (2006) Seventh Edition. John Wiley & Sons, Inc. Brink's Modern Internal Auditing

-the Anti-Phishing Working Group (APWG) "Phishing special report: What to expect for 2007," available in:http://www. antiphishing. org/sponsors technical papers/rsaPHISH2 WP 0107. pdf