حسابرسی

حسابرسی رایانامه

ترجمه و تألیف: ابراهیم ابراهیمی

در نوشتار قبلی به کاربرد رایانامه در حسابرسی پرداخته شد. هم‌چنین عنوان شد شرکت‌ها و سازمان‌ها سعی دارند با بهره‌گیری از رایانامه بهای ارتباط‌گری و اطلاع‌رسانی را نیز به حداقل برسانند. در برخی موارد، رایانامه‌ها جزء مدارک اصلی شرکت محسوب می‌شوند. در نتیجه، کارفرمایان مسئولیت دارند خط‌مشی‌ها و روش‌هایی را برای اطمینان از نگهداری مستندات رایانامه تدوین کنند. در این میان توجه به مسائل امنیتی و مدیریت رایانامه‌ها بیش از پیش ضرورت می‌یابد.

ریسک‌های رایانامه

این حقیقت که مدیریت اطلاعات الکترونیک غالباً زیرنظر مدیران ارشد قرار دارد بدین مفهوم است که در بسیاری از شرکت‌ها و نهادهای دولتی، به انبارش و آرشیو رایانامه، آن طور که سزاوارش است، توجه نمی‌شود. این امر می‌تواند برای بسیاری از شرکت‌ها و سازمان‌ها به ریسک‌های پنهانی منجر شود. مثلاً مدارک رایانامه شواهد مهمی در پی‌گیری و تعقیب‌های عمده بابت اشتباه‌کاری هستند.

رشد سریع استفاده از رایانامه به‌عنوان ابزار ارتباط‌گری و مکاتبات، مدیریت آن را نیز با ریسک‌هایی روبه‌رو می‌کند. رایانامه نقطه‌ی ورودی اصلی ویروس، هرزنامه و نقض حریم خصوصی است. با توجه به برآوردهای صنعت، بین ۶۵ و ۹۵ درصد ویروس‌ها از طریق رایانامه منتقل می‌شوند. ارتباط‌گری خصوصی و محرمانه‌ی عملیات مالی، مذاکرات قراردادی، طرح‌های کسب و کار، موضوعات قانونی، مدارک پزشکی و سایر موضوعات عملیاتی به طور مکرر از طریق سامانه‌های رایانامه بر مبنای روزانه منتقل می‌شوند. به‌علاوه، ارتباط‌گری بی‌سیم، افزایش اتکا به رایانامه مبتنی بر تارنما، احکام خصوصی و سایر روندها کاربردهای آتی رایانامه و شیوه‌ای را که شرکت باید به موضوع ارتباطات الکترونیک واکنش نشان دهد تحت تأثیر قرار خواهد داد.

رایانامه و پایش ارتباطات

استفاده از رایانامه به‌عنوان ابزاری برای ارتباطات و نیز مدارک نمونه علاوه بر این‌که تهدیداتی را به همراه دارد، مسائلی را در زمینه‌ی پایش آن‌ها ایجاد می‌کند. در زمینه‌ی پایش رایانامه‌ها به چند موضوع باید توجه داشت. نخست این‌که بعضاً کارفرمایان با ایجاد شبکه‌ی داخلی و نیز رایانامه‌ی شرکتی، خود را مجاز به آگاهی از محتوای رایانامه‌های کارکنان می‌دانند. باید توجه داشت که به این موضوع هم باید از دید اخلاقی و هم دید مقرراتی- شامل حفظ حریم شخصی و مقررات قانونی ناظر بر آن- نگاه کرد. از طرف دیگر، باید دید که پیام‌های ارسالی از طریق رایانامه، بابت موارد کاری است یا غیرکاری و این‌که آیا این پیام‌ها، مستنداتی برای بنگاه محسوب می‌شوند یا خیر. طبیعی است شرکت‌هایی که در آن‌ها رایانامه‌های ارسالی از سوی کارکنان دارای مشخصات شرکت و حتی در مواردی قالب نامه‌ی شرکتی است، این حق را بر خود محفوظ می‌بینند که رایانامه‌ها را به طور متناوب پایش کنند، چرا که مسئولیت اصلی پیام ارسال شده را متوجه‌ی شخصیت حقوقی شرکت می‌دانند. دوم، در بخش عمومی، رایانامه‌ها باید با توجه به روش‌های مقرر مراجع قانونی مدیریت شود. به عبارت دیگر باید قوانین و مقررات منتشره در این زمینه داشت.

بنا به مطالعه‌ی کوئیک‌تیک، ۴۲ درصد از کارفرمایان، رایانامه‌های شرکتی کارکنان خود را پایش می‌کنند. با این حال، یافته‌ها نشان می‌دهند که تنها ۶۰ درصد از کارفرمایانی که بر رایانامه‌های کارکنانشان پایش دارند، به طور واقعی سیاست مکتوب و به‌جایی دارند. با پایش رایانامه‌ها بدون هشدار دادن به کارکنان، کارفرمایان بی‌تردید حریم خصوصی افراد را زیر پا می‌گذارند و بنابراین در مظان تجاوز به حریم خصوصی دیگران قرار می‌گیرند.

در آمریکا دو قانون فدرال و ایالتی وجود دارد که ناظر بر این عمل است. مطابق قانون فدرال با عنوان "قانون حریم خصوصی ارتباطات الکترونیکی(ECPA)" به شرکت‌ها این اجازه داده می‌شود که زمانی بر رایانامه‌های کارکنان پایشگری کنند که یکی از این سه شرط را داشته باشد: یکی از طرفین رضایت داده باشد، یک دلیل حقانی و قانع‌کننده‌ی تجاری وجود داشته باشد، یا شرکت برای مصونیت از خود مجبور به انجام آن باشد. در جولای ۲۰۰۱ قانون‌گذار، قانون دیگری را با نام "قانون اعلامیه‌ی پایشگری الکترونیک"، وضع کرد که به‌موجب آن کارفرمایان ملزم خواهند شد به کارکنان جدید هرگونه پایش الکترونیک را اعلام کنند و اعلامیه‌ی سالانه‌ای را در اختیار تمام کارکنان قرار دهند. کارفرمایانی که در اطلاع‌رسانی پایش رایانامه به کارکنان قصور کنند، با جریمه‌ی دادخواهی تا سقف ۲۰,۰۰۰ دلار روبه‌رو خواهند شد. با این حال از سپتامبر ۲۰۰۰ به بعد، هیچ اشاره‌ی بیشتری به این قانون نشد.

بنابراین به طور خلاصه می‌توان گفت اگر شرکت هیچ سیاست رایانامه‌ای خاصی را نداشته باشد، کارمند می‌تواند مدعی شود که انتظار معقولی از حریم خصوصی دارد. با این حال اگر شرکت سیاست رایانامه‌ی مکتوبی داشته باشد و کارکنان از احتمال پایشگری رایانامه مطلع باشند، قاعدتاً کارکنان نباید انتظاری از حریم خصوصی داشته‌باشند، و در نتیجه شرکت بابت این مورد از تعقیب و دعوی قانونی در امان بماند.

در کشور ما، قانون جرائم رایانه‌ای تا حدودی ناظر بر این عمل است. البته بیشتر تأکید بر شبکه‌های عمومی است. در این قانون، در ماده‌ی ۱ آمده است که هرکس به طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای مخابراتی که به وسیله‌ی تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد. مجازات‌های دیگری نیز در این قانون برای سایر مصادیق تجاوز به حریم شخصی آورده شده است. اما آنچه در این میان اهمیت دارد، در قانون به وفور از دسترسی غیرمجاز به داده‌های رایانه‌ای استفاده شده است. البته این محدود به ارتباطات عمومی نیست و حتی در برخی مواد، از ارتباطات غیر عمومی نیز نام برده شده است.

این قانون هم‌چنین الزامی را برای نگهداری داده‌ها مقرر می‌کند. مطابق ماده‌ی ۳۲، ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه‌ی اشتراک نگهداری کنند. ماده‌ی ۳۳ نیز بیان می‌دارد که ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش‌ماه پس از خاتمه‌ی اشتراک و محتوای ذخیره شده و داده‌ی ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگهداری کنند.

پیرامون تفتیش پست الکترونیکی نیز موادی در این قانون دیده می‌شود. به طور نمونه تبصره‌ی ماده‌ی ۴۸ عنوان می‌دارد که دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پست الکترونیکی یا پیامک در حکم شنود و مستلزم رعایت مقررات مربوط است.

در این جا هدف پرداختن به موارد حقوقی پایش رایانامه نیست تنها به این موضوع بسنده می‌شود اگر پایش رایانامه‌های سازمانی مجاز باشد، حسابرسی چه نقشی را می‌تواند در این پایش ایفا کند.

همه‌ی مدیران در بخش عمومی و خصوصی باید از موضوعات و مسائلی که در به‌کارگیری رایانامه ایجاد می‌شود آگاه باشند. این موضوعات شامل موارد زیر می‌شود:

- کارایی شبکه، هرزنامه، عدم پذیرش حملات رایانه‌ای و شرنامه
- مسئولیت قانونی، از قبیل بازیابی اطلاعات، یا استفاده از تکذیب‌نامه‌های قانونی در پیام‌های رایانامه‌ای
- امنیت اطلاعات، شامل مصونیت حقوق و ارزش معنوی، محرمانگی و دفاع در برابر ویروس‌ها و یا کدهای بدنهاد.

سازمان باید رهنمودی در این‌باره داشته‌باشد و

این رهنمود باید جزئیاتی درباره‌ی موارد زیر را در برگیرد:

- خط‌مشی بهترین رویه
- خط‌مشی کاربری قابل قبول
- خط‌مشی محرمانگی

شرکت‌ها باید سامانه‌ی رایانه‌ی خود را بهره‌ور نگه دارند و درستی سامانه‌ی خود را حفظ کنند و بنابراین مدیریت باید خط‌مشی کاربرد رایانامه را اجرا و الزام کند و به طور اثربخش این خط‌مشی را به کارکنان اطلاع‌رسانی کند. کارکنان باید این موضوع را درک کنند که کارفرمایشان مسئول هر چیزی است که آن‌ها از طریق رایانامه ارسال می‌کنند، از لطیفه گرفته تا مدارک رسمی کاغذی.

در این حوزه، حسابرسان داخلی می‌توانند به سازمان در حفظ کنترل‌های مورد نیاز بر استفاده از رایانامه کمک‌کنند. اما نظر شما چیست؟ آیا واقعاً انجام حسابرسی رایانامه‌ای توسط حسابرسان داخلی توجیه دارد؟

حسابرسی رایانامه: اهداف و دامنه

هدف از حسابرسی رایانامه را می‌توان چنین برشمرد که معمولاً تعیین این است که:

- آیا سازمان روش‌ها و سیاست‌های کافی(کنترل‌ها) برای پوشش استفاده از رایانامه را دارد؟
- آیا کاربرد کلی سامانه‌ی رایانامه با سیاست شرکت سازگاری دارد؟
- آیا سازمان فرایند کافی و مناسبی برای اطمینان از آن‌که رایانامه‌های مناسب، به‌عنوان مدارک رسمی شرکت تلقی شوند، دارد؟

دامنه‌ی حسابرسی رایانامه نیز باید به تجزیه و تحلیل و ارزیابی استفاده از رایانامه طی یک دوره‌ی زمانی با هدف ساخت پروفایلی از میزان کاربری کارمندان محدود شود. حسابرسان هم‌چنین کنترل‌های مدیریت مربوط به استفاده از رایانامه، شامل سیاست نگهداری، امنیت و کدگذاری، و شیوه‌ی رفتار سازمان با روندهای جاری و آتی پیام الکترونیکی را ارزیابی کند.

برای تجزیه و تحلیل کاربرد رایانامه، حسابرس باید نمونه‌ای از پیام‌های رایانامه‌ای را انتخاب و اطلاعات فرستنده و گیرنده را تجزیه و تحلیل کند تا تعیین کند که آیا این پیام برای اهداف شخصی بوده است یا اهداف کاری. در صورت امکان، پیوست‌ها، سرخط یا عنوان، اندازه و اطلاعات محتوای رایانامه نیز باید تجزیه و تحلیل شود. هم‌چنین توصیه می‌شود حسابرسان با کارمندان آگاه مصاحبه کنند و رهنمودهای مربوطه، شامل دستورالعمل نگهداری مستندات سازمان، را بررسی و بازبینی کنند.

مراحل حسابرسی

۱- شناسایی رهنمود استفاده‌ی کارکنان از رایانامه

- آیا دستورالعمل، از قبیل محدودیت‌های استفاده از رایانامه، برای سطوح شغلی، عناوین و سطح امنیتی اطلاعات وجود دارد؟
- آیا این دستورالعمل، سوءاستفاده را تعریف می‌کند؟
- آیا دستورالعمل، پایش و تعقیب سوءاستفاده را مشخص می‌کند؟

۲- شناسایی و بررسی دستورالعمل شرکت از بابت شناخت و آرشیو مستندات رسمی

۳- شناسایی و بازبینی الزامات قانونی یا مقرراتی مربوط برای استفاده از رایانامه و نگهداری

۴- ارزیابی دستورالعمل و رهنمودهای موجود درباره‌ی استفاده از رایانامه

۵- تعیین این‌که کدام رایانه‌ها دادگان رایانامه را مدیریت می‌کنند و در کجا واقع شده‌اند

۶-کسب یا تهیه فلوچارتی از سامانه‌ی رایانامه

۷- تعیین الزامات آرشیو برای سرورهای رایانامه

۸- بررسی گزارش‌های داخلی قبلی و گزارش‌های بازرسی، به منظور شناسایی یافته‌ها و پیشنهادهایی که مربوط به این موضوع هستند

۹- تعیین این‌که آیا روش‌های به‌جایی برای پایش فعالیت‌های کاربرد رایانامه وجود دارد، از قبیل ضبط اطلاعات مربوط به ترافیک رایانامه، بررسی فایل‌ها در رایانه‌ها یا استفاده از نرم‌افزار برای اسکن محتوای رایانامه‌ها در شبکه.

- آیا شرکت فعالیت‌های رایانامه را پایش نکرده است، به چه دلایلی؟
- آیا رایانامه‌ها را فیلتر می‌کند؟
- چه کسی اختیار دریافت و ارسال مستندات و پیام‌ها از طریق رایانامه را دارد؟ آیا این اختیار بر مبنای وظایف کاری است؟

۱۰- مصاحبه با افراد مطلع برای شناسایی هرگونه تخلفات از دستورالعمل‌های رایانامه که منجر به کژرفتاری شده است.

۱۱- پرس و جو درباره‌ی کنترل‌های حاکم بر رمز عبور.

- آیا سامانه‌ی رایانامه رمز عبورهای پیش‌فرضی را به کاربران جدید، بر مبنای مشخصه‌های معمول تخصیص می‌دهد؟
- آیا فرایندی برای اجازه دادن به کاربر در تغییر رمز عبور با اولین ورود به سامانه وجود دارد؟
- چند وقت یک‌بار تغییر رمز عبورها الزامی است؟
- آیا رمز عبورهای بین مشتری و سرورهای رایانامه، کافی و مناسب هستند؟(رابطه‌ی اطمینان بین آن‌ها چیست؟)

۱۲- تعیین کاربردهای جاری و مورد انتظار از رایانامه و ظرفیت آن.

۱۳- تعیین بهای برنامه، ظرفیت سامانه و ملاحظات امنیتی.

۱۴- ارزیابی کاربرد رایانامه کارکنان برای تعیین این‌که تا چه اندازه‌ای سیاست‌های جاری می‌تواند تقویت شود. میزان استفاده از رایانامه در فعالیت‌های کاری و غیرکاری، از طریق دریافت لوگ‌های رایانامه و تجزیه و تحلیل ارسال‌کنندگان و نشانی‌ها و سایر اطلاعات مربوط از لوگ‌ها تعیین شود.

- شناسایی و بررسی پیام‌های غیرکاری. بهتر است حسابرس هفت روز را در ماه گذشته انتخاب کند تا از معرف بودن نمونه از هر روز هفته اطمینان یابد. نمونه‌ای آماری از پیام‌ها از هفت روز را انتخاب و محتوای رایانامه‌های

واقعی را بررسی کند.

• شناسایی سطح و بهای مربوط به استفاده‌ی غیرکاری از رایانامه(در صورت امکان)

۱۵- مصاحبه با افراد مطلع، شامل مشاور حقوقی

۱۶- تعیین این‌که آیا امنیت رایانامه‌ها کافی است.

• آیا سامانه‌ی امنیتی می‌تواند کارمند را از وارد شدن به صندوق پیام رایانامه‌ی شخص دیگر باز دارد؟

• آیا پیام‌های حیاتی می‌تواند رمزگذاری شود؟

• آیا دسترسی به سامانه‌ی رایانامه، از دسترسی به سایر سامانه‌ها جدا است؟

• آیا شبکه نسبت به ویروس‌ها، کرم‌های اینترنتی یا هر نوع تهدید امنیتی دیگر آسیب‌پذیر است؟

• آیا برنامه‌های آنتی ویروس فعال‌اند؟

• آیا کنترل‌های حاکم بر دسترسی از راه دور کافی است؟

بر مبنای نتایج حاصل از حسابرسی، باید تعیین شود که اگر سازمان سیاست‌ها و روش‌های(کنترل‌های) کافی بر استفاده از سامانه‌ی رایانامه ندارد، فرایندی مناسبی که اطمینان‌دهد رایانامه‌ها به‌عنوان مستندات رسمی شرکت هستند یا استفاده‌ی کارکنان از سامانه‌ی رایانامه مطابق با دستورالعمل مکتوب شرکت نباشد، چه پیامدهایی خواهد داشت.

اگر اثرات، قابل ملاحظه هستند چه تغییراتی باید اعمال شود؟ باید به مدیریت پیشنهادهای مناسب داده شود. حسابرسی رایانامه آشکار می‌سازد که کارکنان چگونه از رایانامه استفاده یا سوءاستفاده می‌کنند. به علاوه، حسابرسی نقاط ضعف در نگهداری رایانامه‌ها به‌عنوان مستندات را شناسایی خواهد کرد. حسابرسی به مدیریت این امکان را خواهد داد که به جای استفاده از نرم‌افزار فیلتر، سیاست رایانامه‌ای قوی تدوین و کارکنان را به منظور هماهنگی با سیاست‌ها آموزش‌دهد. این رویکرد کنش‌گرایانه می‌تواند ریسک‌های رایانامه را کاهش‌دهد، بهره‌وری را افزایش دهد، و در نهایت از رعایت قوانین و مقررات اطمینان دهد و دارایی شرکت را مصون کند.

منابع

۱- قانون مجازات جرائم رایانه‌ای.

2-Anderson W.Alan.2011.The Pros and Cons of E-Mail Use During the Audit. Anderson›s Audit Express series. Available at www.kscpa.org

3- Moody, Robert, and Beth Serepca, 2003.Auditing Employee Use of E-mail. Information Systems Control Journal, Volume 1.

4- Overly Michael. 1999. E-Policy - . SciTech Publishing.

5- Spykerman,Mike.2004. Is email monitoring legal?.. Red Earth Software; available at www.policypatrol.com

ابراهیم ابراهیمی: دانشجوی دکتری دانشگاه تهران

نرم افزار های یکپارچه مالی اداری

کاکتوس

ابزاری کارآمد در دست مدیران

نسل جدید برنامه حسابداری کاکتوس از راه رسید!

- کاربری آسان (استفاده کامل از صفحه کلید ...)
- تنظیم دلخواه گزارشات
- اجرای برنامه تحت وب
- سرعت پردازش بالا
- تنوع گزینه ها (جستجوی قوی، مدیریت کاربران، مدیریت بانک اطلاعاتی و ...)
- برنامه چند زبانه (فارسی، انگلیسی و ...)
- امکانات ویژه (گزارشات مدیریتی و ...)
- ظاهری آراسته
- استفاده از فناوری های جدید :

.Net 4.0, SQL 2008, SSRS, SSAS

لیست نرم افزارهای یکپارچه کاکتوس

حسابداری	سرویس مشتری و خدمات
انبارداری	پس از فروش
خرید و فروش	پخش مویرگی
چک	پیمانکاری
صندوق	تعاونی و سهام
حقوق و دستمزد	حمل و نقل باری
قیمت تمام شده	دبیرخانه و بایگانی
وام و قرض الحسنه	بانک اطلاعاتی قراردادها
کنترل موجودی تولید	بانک اطلاعاتی اشخاص و ...

شرکت کاکتوس کامپیوتر

۸۸۴۵۳۶۹۳ - ۸۸۴۵۰۱۰۲
۰۹۱۲۳۲۲۳۸۰۳

تهران، سهروردی شمالی، مقابل پمپ بنزین، پلاک ۳۱۷، طبقه هفتم، واحد شرقی

www.cactus.ir