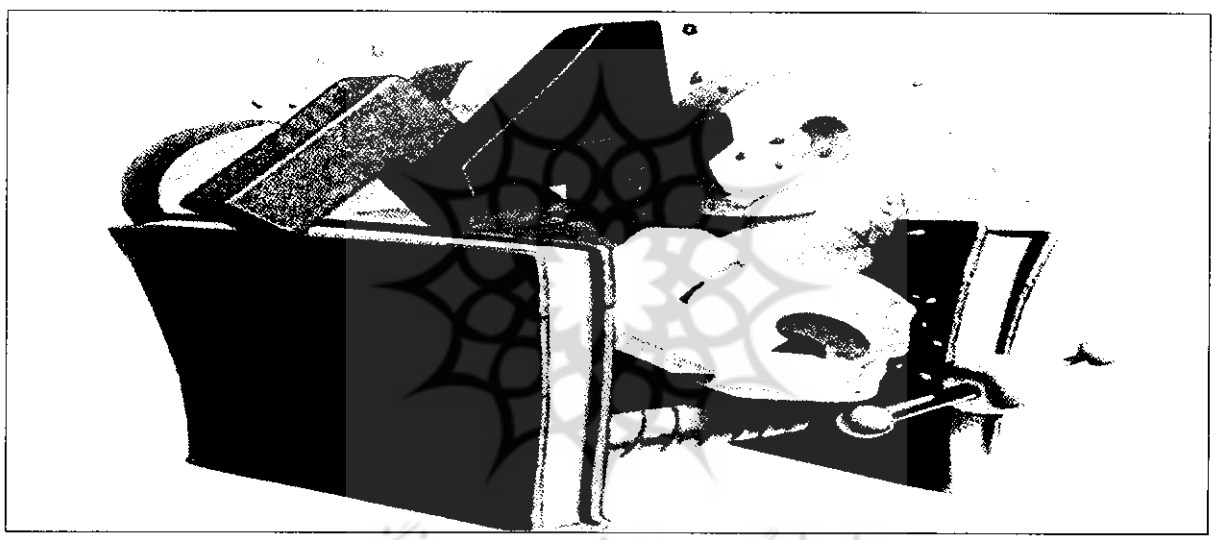
امنیت سیستم‌های اطلاعاتی حسابداری با تاکید بر عوامل زیستی



دکترعلی سعیدی
استادیار گروه حسابداری دانشگاه اصفهان
ناصر رضایی
دانشجوی کارشناسی ارشد حسابداری

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

مقدمه

ساخت، به‌کارگیری و اجرای نرم‌افزاری که بدون در نظر گرفتن مسائل امنیتی ایجاد شده، ممکن است بسیار پرمخاطره باشد. در واقع، این کار مانند راه رفتن روی طناب، بدون وجود تور در زیر آن است. میزان این خطر را می‌توان با مسافت طی شده به‌هنگام سقوط و شدت ضربه بالقوه سنجید. اکثر قسمت‌های نرم‌افزارهای کاربردی امروزی اگر همراه با امنیت لازم ایجاد نشده باشد، در مقابل حملات آسیب‌پذیر است. ترکیب‌کردن رویه‌های امنیتی در طول طراحی سیستم، باعث کاهش هزینه می‌شود، خطر عملیاتی را کم می‌کند، دوام و قابلیت انعطاف عملیات را افزایش می‌دهد و می‌تواند به رعایت الزاماتی که بر نرم‌افزار و فناوری اطلاعات متکی است، کمک کند.

امروزه نرم‌افزار آسیب‌پذیر را می‌توان مانند سرطان مورد هجوم قرارداد و آن را تغییر داد. همچنین، نرم‌افزار آلوده نیز ممکن است تکثیر پیدا کند و در میان شبکه‌ها به‌منظور صدمه رساندن به سایر سیستم‌ها انتقال یابد. این فرایندهای آسیب‌زننده همانند سرطان ممکن است برای شخص غیرمتخصص نامعلوم باشد، ولی متخصصان تصدیق می‌کنند که تهدیدهای آنها رو به‌رشد است. در واقع، هیچ راه کار

مشخصی برای تضمین سطحی معین از امنیت نرم افزار برای سیستم های پیچیده وجود ندارد (Allen, 2007). در این مقاله، کاربردهای بالقوه یک لایه امنیتی فعال زیستی در سیستم‌های حسابداری تشریح می‌شود. لایه مذکور می‌تواند از تهدیدهای مخرب سرویس‌های تشخیص هویت و تعیین اعتبار بکاهد. این مقاله به چهار بخش تقسیم شده است. در بخش ابتدایی، مروری کلی بر فرایند تعیین اعتبار و تشخیص هویت ارائه گردیده و در خصوص خطر و اطمینان و پیامدهای آن و اطمینان وابسته به این فناوری بحث شده است. در بخش دوم، حوزه‌های خاص سیستم‌های اطلاعاتی حسابداری که در آنها به‌کارگیری فناوری زیستی ممکن است افزایش ارزش در پی داشته باشد، مورد تجزیه‌وتحلیل قرار گرفته است. در بخش سوم، چالش‌ها و محدودیت‌های به‌کارگیری لایه امنیتی زیستی برای سیستم‌های اطلاعاتی حسابداری مورد بررسی قرار گرفته و در بخش پایانی نیز نتیجه‌گیری ارایه گردیده است.

امنیت نرم‌افزار

هدف عمده تامین امنیت نرم‌افزار عبارت است از ساخت نرم‌افزاری بهتر و عاری از عیب و نقص تا بتواند به عملکرد صحیح خود در شرایط حملات بدخواهانه، ادامه دهد (McGraw, 2006). امنیت نرم‌افزار به این خاطر مهم است که تعداد زیادی از وظایف و فعالیت‌های حیاتی، وابستگی کاملی به آن دارند. این امر باعث می‌شود تا نرم‌افزار هدفی بسیار با ارزش برای مهاجمانی باشد که انگیزه حملاتشان ممکن است ماهیتی بدخواهانه، جنایت‌کارانه، خصمانه، رقابتی یا تروریستی داشته باشد.

منابع ناامنی نرم‌افزار

تهدیدکننده‌های نرم‌افزار، خواه مدیران پروژه آن‌ها را تشخیص دهند یا ندهند، وجود دارند. اگر مدیران پروژه و مهندسان نرم‌افزار به‌طور معمول در این زمینه آموزش ببینند که چگونه از روی عادت و به‌طور منظم بر ضعف‌های امنیتی نظارت داشته باشند، آنگاه می‌توان درصد بالایی از آنها را در نرم‌افزارها حذف کرد. آماده‌سازی نرم‌افزار به‌همراه امنیت لازم که از همان ابتدا در نظر گرفته می‌شود، از لحاظ درجه اهمیت در مقایسه با تلاش برای ایمن‌سازی نرم‌افزار از طریق آزمون‌های سنجش امنیت، راهکاری موثرتر برای حصول اطمینان از ایمن بودن نرم‌افزار است. دنبال کردن بررسی کدها (برنامه‌ها)، آزمون‌های امنیتی، کنترل دقیق پیکربندی و تضمین کیفیت در طول به‌کارگیری سیستم نرم‌افزاری، دارای اهمیت است؛ چون اطمینان می‌دهد که به‌روزآوری و تعمیر کردن نرم‌افزار باعث افزودن ضعف‌های امنیتی به آن نمی‌شود (Allen, 2007).

پشتیبانی امنیتی سیستم‌های حسابداری

خطاهای غیرعمدی و سهل‌انگاری‌ها، مشکلات اساسی را برای رایانه‌ها ایجاد می‌کنند. هنگامی که طراحی و پیاده‌سازی و اجرا با بی‌دقتی و به‌صورت نامرتب انجام شود، خطاها و غفلت‌ها رایج‌تر است. طراحی سیستم‌های اطلاعاتی حسابداری باید همراه با توجه ویژه‌ای به اقدام‌های امنیتی سیستم صورت پذیرد. دوام اقدام‌های امنیتی به نظارت آگاهانه و دائمی سیستم بستگی دارد که متاسفانه اغلب نادیده گرفته می‌شود. نکته قابل توجه در امنیت سیستم‌ها این است که کلیه ذی‌نفعان، ضرورت امنیت سیستم‌ها و تهدیدهای بالقوه‌ای که سازمان با آن روبه‌رو است را درک کنند.

انجمن حسابداران رسمی امریکا، در ژانویه ۲۰۰۰ فهرست سالیانه خود را در زمینه ده موضوع برتر فناوری منتشر کرد. موضوع‌های امنیت و کنترل اطلاعات، بازیافت حوادث، دسترسی بالا و انعطاف‌پذیری سیستم‌ها، پنج مورد برتر آن فهرست بودند (Luehlfing et al., 2000). موانع توسعه امنیت سیستم‌ها، شامل موانع مالی و فلسفی هستند. امنیت سیستم‌ها اغلب در وضعیتی مشابه با امنیت عینی بررسی می‌شوند. یعنی این که یک‌بار خریداری و برای همیشه مورد استفاده قرار می‌گیرند. متاسفانه روش‌ها، خط‌مشی‌ها و فناوری‌های منسوخ‌شده (برای مثال، ایمنی عینی) سیستم‌ها را در برابر تهدیدهای خارجی و داخلی به‌شدت آسیب‌پذیر می‌سازد.

بیشتر ذی‌نفعان، مخارج مستمر برای امنیت سیستم‌ها را به‌سختی می‌پذیرند؛ به‌خصوص وقتی که اندازه‌گیری منافع آن مشکل باشد. حتی هنگامی که فواید را بتوان اندازه‌گیری کرد، ذی‌نفعان ناآگاه شاید هنوز ضرورت صرف هزینه‌های مستمر در حوزه امنیت سیستم‌ها را نپذیرند. در بسیاری از

موارد، آموزش می‌تواند بر این مانع فلسفی غلبه نماید. متاسفانه فقط آسیب‌های شدید ناشی از یک شکست امنیتی، باعث اقدامی مناسب هرچند با تاخیر می‌شود.

تهدیدهای عمده امنیت رایانه

پنج تهدید اساسی امنیتی عبارت است از بلایای طبیعی، کارمندان نادرست، کارمندان ناراضی، افراد خارج از سازمان، غفلت و اشتباهات ناخواسته. میزان تحقق هر کدام از آنها در **نمایشگر ۱** نشان داده شده است. همان‌طوری که در نمایشگر نشان داده شده، غفلت و خطاهای ناخواسته بیشترین مشکل را برای امنیت رایانه‌ها ایجاد می‌کند.

نمایشگر ۱

منبع: Allen J., EDPACS, Jul. 2008; 36,1

اگر فرایند طراحی سیستم‌ها به‌طور مناسبی انجام شود، غفلت و خطاها به‌حداقل می‌رسد. ساختار کنترل داخلی اثربخش، جزئی جدایی‌ناپذیر از یک سیستم اطلاعاتی قابل اطمینان است. انگیزه اولیه برای ایجاد کنترل داخلی (خوب طراحی شده)، پشتیبانی از توانایی‌های مدیران و کارکنان شرکت در زمینه مدیریت مالی است. کنترل داخلی نامناسب، ممکن است فعالیت‌های مشکوک و فریبکارانه مدیران و کارمندان را مخفی نگه دارد. حسابداری بی‌نظم و شرایط نامناسب مدیریت مالی که حاصل کنترل‌های داخلی نامناسب است، فشار روانی بیش از حد لزوم ایجاد می‌کند که به‌آسایش روانی مدیران و کارکنان و اثربخشی کارهای آنها آسیب می‌رساند. در حالی که کنترل داخلی قوی، کارمندان درستکار را از سوءظن و تهمت اشتباه حفاظت می‌کند (Luehlfing et al; 2000).

لایه امنیتی زیست‌سنجی در سیستم‌های حسابداری

در این بخش از مقاله، پیامدهای عملی و نظری مربوط به استفاده از لایه‌های امنیتی دارای توانایی زیست‌سنجی در سیستم‌های حسابداری بحث می‌شود که در شناسایی کاربران و کاهش خطر کنترلی یاری می‌رساند. در آغاز مطالعه ماهیت فناوری زیستی، کاربردهایی از این فناوری در رشته‌های علمی مختلف مطرح شده است. البته، استفاده از این فناوری هنوز در ابتدای راه است و جنبه‌های گوناگون پیامدهای آن در امنیت سیستم‌های حسابداری مورد بررسی قرار نگرفته است. فناوری زیست‌سنجی، به‌منظور کاهش خطر کنترل استفاده می‌گردد. باوجود توانایی‌های بسیار، روش زیست‌سنجی دوای همه دردها نیست و وجود مجموعه‌ای از سازوکارهای امنیتی مورد نیاز است تا از منابع اطلاعاتی محافظت شود.

اتفاقات ناخوشایند ۱۱ سپتامبر ۲۰۰۱ در شهر نیویورک، پنسیلوانیا و واشنگتن، تمام کسانی که نگران تکرار این حوادث هستند را وادار کرده تا موارد امنیتی را که شامل موضوع‌های امنیتی سیستم‌های اطلاعاتی است، مورد بازنگری قرار دهند. تقلب‌های رایانه‌ای و کاهش بهره‌وری ناشی از حملات رایانه‌ای، تهدیدهای عمده‌ای در زمینه فعالیت‌های اقتصادی به‌شمار می‌آیند. (Nichols et al., 2000; Pipkin, 2000). علت اصلی چنین خسارت‌هایی، نبود یا ضعف سیستم‌های تشخیص و تایید هویت است (Stallings, 2000). سازوکارهای دقیق تشخیص هویت و تایید، اغلب پیش‌نیازی مبرم برای سبک کردن آثار تهدیدها بر سایر خدمات اساسی امنیتی نظیر قابلیت اعتماد، پذیرش، یکپارچگی داده‌ها و در دسترس بودن داده‌ها است. عامل زیستی، ویژگی رفتاری یا فیزیولوژیکی است که می‌تواند برای تایید و یا تشخیص هویت یک کاربر استفاده گردد (Matyas and Stapleton, 2000). بعضی از روش‌های زیستی شامل اثر انگشت، الگوی صدا، ویژگی‌های فردی عنبیه و شبکیه، دست‌خط، امضا و تجزیه‌وتحلیل چگونگی ضربه زدن به کلیدها است. از زمانی که روش زیستی برای

تشخیص هویت اشخاص استفاده می‌شود، سوءاستفاده اگرچه غیرممکن نشده، ولی سخت‌تر شده است (Chandra and Calderon, 2003).

حرفه حسابداری، چارچوب‌های کنترلی گوناگونی ایجاد کرده است که مخاطرات و اقدامات امنیتی مربوط به منابع اطلاعاتی واحد تجاری و سایر دارایی‌ها را مشخص می‌کند. به‌ویژه، این چارچوب‌های کنترلی از حرفه حسابداری می‌خواهد که سیستم‌های کنترلی را به‌گونه‌ای طراحی و اجرا کند که منابع اطلاعاتی یک موسسه را حفظ نماید. یک سازوکار امنیتی قوی که خطر کنترلی را کاهش می‌دهد و دقت و اعتماد زیادی را در میان کاربران ایجاد می‌نماید، ممکن است ابزار ایده‌آلی برای حسابداران به‌منظور ایفای مسئولیت آنها باشد. فناوری زیستی به‌عنوان روشی قوی پدیدار شده است که به‌طور بالقوه می‌تواند خطر کنترل را در برنامه‌های کاربردی حسابداری و فرایندهای کسب‌وکار کاهش دهد؛ به‌ویژه زمانی که در ارتباط با اقدام‌های کنترلی متداول استفاده شود. در این قسمت، کاربردهای بالقوه لایه امنیتی فعال زیستی در سیستم‌های حسابداری تشریح می‌گردد. لایه مذکور می‌تواند از تهدیدهای مخرب سرویس‌های تشخیص هویت و تعیین اعتبار بکاهد.

تشخیص هویت در مقابل تعیین اعتبار

تشخیص هویت، یک فرایند تطبیق یک به چند است که وجود یک شخص را در یک پایگاه داده‌ها مشخص می‌کند. این فرایند فقط مشخص می‌کند که آیا این شخص در پایگاه داده‌های مورد نظر وجود دارد یا نه. اگر کنترل‌های دسترسی خبر از وجود یک شخص بدهد، تنها زمانی به این شخص اجازه دسترسی به سیستم داده خواهد شد که مشخص شود شناسه مورد نیاز، در پایگاه داده‌های دارندگان دسترسی وجود دارد. البته، هیچ‌گونه تایید یا گواهی وجود ندارد که شخصی که به او اجازه دسترسی داده شده، واقعاً همان شخصی باشد که فرایند دسترسی را طی کرده است. از سوی دیگر، تعیین اعتبار معین می‌کند شخصی که تشخیص هویت او در پایگاه داده‌ها بررسی شده، به‌درستی همان شخصی است که ادعا می‌کند. تایید اعتبار، یک فرایند تطبیق یک‌به‌یک شخصیت (هویت) مورد ادعا است. سیستم خودکار تشخیص هویت، کل پایگاه داده کاربران را جستجو

فن آوران دانش آسیا

ارائه دهنده نرم افزارهای مالی، اداری و بازرگانی

✓ نرم افزار بامداد

راهکار جامع مالی و اداری شرکتها

✓ نرم افزار آسیا

مناسب کسب و کارهای کوچک

• قابل تطبیق با گردش کار شرکتهای مختلف
• کاربری آسان و راه اندازی سریع
• پویایی و قابلیت تغییر در جهت رفع نیاز مشتریان

www.fdasys.com

تهران: ۸۸۴۰۵۷۱۰-۸۸۴۲۵۹۶۲

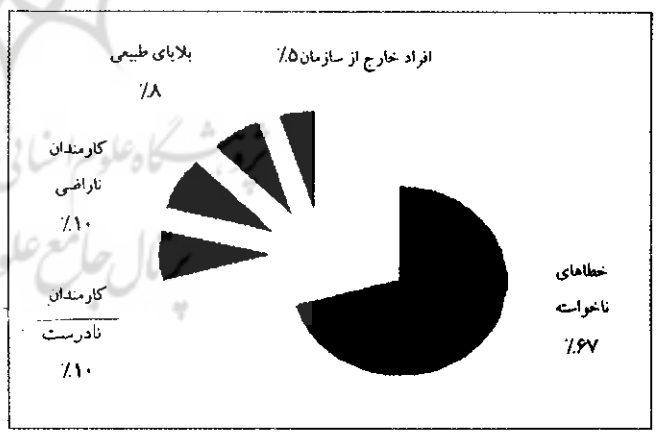
نماینده اصفهان: ۰۹۱۳۳۰۶۱۲۶۱

می‌کند تا یک همتا پیدا کند. از سوی دیگر، فرایند تایید اعتبار، رسیدگی می‌کند که آیا هویت شخص مدعی به همان کاربر تعلق دارد یا نه. این تطبیق، در برابر مرجعی مشخص یا عامل تایید اعتبار مرتبط با هویت مورد ادعا انجام می‌شود.

هرم تایید اعتبار

هرم موجود در **نمایشگر ۲**، سه دسته گسترده از عواملی را نشان می‌دهد که سازمان‌ها برای تایید خودکار اعتبار استفاده می‌کنند. این عوامل عبارت است از مالکیت، دانش و عوامل زیستی. تایید اعتبار ممکن است بر یک عامل (به‌عنوان مثال، رمز عبور، شماره شناسایی شخصی، و یا یک عکس به‌عنوان شناسه) مبتنی باشد. همچنین، این فرایند می‌تواند برمبنای چند عامل (برای نمونه، عکس و رمز عبور، شماره شناسایی شخصی و عکس) باشد. جابجایی عمودی در هرم، به‌صورت افزایش در قدرت فرایند تایید اعتبار است. با جابجایی عمودی در هرم، احتمال آن که هویت (شخصیت) مورد رسیدگی، مالک حقیقی نباشد، کاهش می‌یابد.

نمایشگر ۲ـ تهدیدهای امنیت رایانه



منبع: The CPA Journal; Oct 2000; p.62

در دسته اول، کاربران باید یک ویژگی عینی (مانند یک کلمه رمز یا نشانه) عرضه کنند تا تایید اعتبار شوند. اگرچه ویژگی‌ها قابل رؤیت و معمولاً قابل نقل‌وانتقال هستند، ولی ممکن است گم شوند، سرقت گردند و یا به‌اشتراک گذاشته شوند، تکثیر، فراموش یا خراب شوند. عوامل تایید اعتبار مبتنی بر ویژگی‌ها، این اطمینان را ایجاد می‌کنند که شخص یک کارت یا کلمه رمز معتبر ارائه می‌کند. در زمینه فرایند تایید اعتبار خودکار، این عوامل اطمینان مستقیمی به‌دست نمی‌دهند که کاربر مجاز به دسترسی به سیستم اطلاعاتی، واقعاً همان شخصی است که وی ادعا می‌کند.

در دسته دوم، کاربران اطلاعاتی درباره شناسایی خود (مانند شماره شناسایی شخصی، کلمه عبور، عبارت) ارائه می‌کنند. کلمه عبور و دیگر عوامل تایید اعتبار به‌شدت قابل واگذاری و غیرقابل رویت هستند. همچنین، اغلب می‌توان آنها را تغییر داد و آنها را به‌گونه‌ای طراحی نمود که به‌طور نسبی ایمن باشند. ولی عوامل این گروه نیز ممکن است فراموش یا سرقت شوند، دوباره استفاده شوند، حدس زده شوند و یا به‌اشتراک گذاشته شوند. کلمه عبور این اطمینان را می‌دهد که واردکننده کلمه عبور به سیستم، آن را به‌خوبی می‌داند. اما از سوی دیگر، هیچ اطمینانی وجود ندارد که شخص مذکور، همان فردی است که باید باشد.

در دسته سوم، سیستم ویژگی‌های زیست‌سنجی قابل تمیز و خصیصه‌های رفتاری کاربران را به‌کار می‌گیرد تا او را تایید اعتبار کند و به او اجازه دسترسی به‌منابع اطلاعاتی را بدهد. فناوری‌زیستی به‌این دسته تعلق دارد. دزدیدن یا شبیه‌سازی ویژگی‌های زیستی بسیار سخت است، زیرا به‌طور مستقیم فقط و فقط به کاربر تعلق دارند. افزون بر این، آنها فراموش نمی‌شوند و یا در جای نادرست به‌کار گرفته نمی‌شوند و شبیه اطلاعات مربوط به شناسایی در دسته دوم، صفت ذاتی همان کاربر هستند. ویژگی غیرقابل انتقال بودن (مگر فقط با جراحی در اتاق عمل)، هویت‌هایی را به‌دست می‌دهد که به‌کمک عوامل زیستی، امتیازی بی‌مانند در زمینه خدمات مربوط به ایجاد اطمینان به کاربر و اعتماد در تشخیص هویت و تایید اعتبار به‌شمار می‌آید.

برخی از ویژگی‌های مورد استفاده در دسته سوم عوامل مورد استفاده در تایید خودکار اعتبار، عبارت است از منحنی‌های دست؛ بررسی امضا، از طریق پی‌بردن به این‌که شخص چگونه اسم خود یا حروف را می‌نویسد؛ اثر انگشت، به‌کمک مطابقت دادن کوچکترین جزئیات، طرح یا خطوط انگشت که این امر، در محیط‌های کنترلی بسیار متداول است؛ بررسی صدا، به‌کمک بررسی طول موج و فرکانس صدا؛ بررسی عنبیه، از طریق بررسی عنبیه چشم و تبدیل کردن آن به ارقام جهت بررسی و مطابقت و شناسایی

نمایشگر ۳ـ راهکارهای تایید اعتبار در الگوی تایید اعتبار یک عاملی

منبع: Chandra A., and T.G. Calderon Journal of Information Systems, Fall 2003, 17,2, pp.51-70

هویت؛ بررسی شبکیه چشم، از طریق تصویر دیجیتالی که از شبکیه چشم ایجاد می‌شود و شدت نوری که عبور می‌کند؛ بررسی صورت، به‌کمک بررسی منحنی‌های گونه و لب و فک جهت شناسایی.

کاربردهای حسابداری

فناوری زیستی در هر جایی که رسیدگی و تایید هویت واقعی یک شخص اهمیت دارد، به‌کار گرفته می‌شود. رشته حسابداری، حوزه‌ای مستعد برای بهره‌گیری از عوامل زیستی به‌شمار می‌آید تا در نتیجهٔ استفاده از آن، تقلب، اشتباه، خطا و خطر کنترل کاهش یابد. حرفه حسابداری به‌طور بالقوه می‌تواند از مزایای فناوری زیستی در چهار سطح مشخص استفاده کند: ۱ـ طراحی سیستم‌ها، ۲ـ خدمات اطمینان‌بخشی، ۳ـ یکپارچه کردن کنترل‌ها و ۴ـ تمامیت و یکپارچگی داده‌ها در سطح پایگاه داده‌ها.

۱ـ طراحی سیستم‌ها: در طراحی سیستم‌های اطلاعاتی، می‌توان از ابزار امنیتی دارای توانایی زیستی استفاده نمود. از این ابزار می‌توان برای حصول اطمینان از معتبر بودن کاربران در طول مراحل تشخیص هویت و تایید اعتبار و دادن اجازه برای ورود به سیستم‌ها، استفاده کرد.

۲ـ خدمات اطمینان‌بخشی: حسابداران، تخصص لازم را در انجام خدمات اطمینان‌بخشی برای اشخاص ثالث، دارا هستند. اگر چه حسابداران ممکن است مهارت‌های فنی مورد نیاز برای انجام خدمات اطمینان‌بخشی برای یک سیستم امنیتی کاملاً زیستی را به‌هیچ‌وجه دارا نباشند، ولی انتظار می‌رود به‌علت توانایی سنتی و اعتبار آنها به‌عنوان ارائه‌کنندگان خدمات اطمینان‌بخشی، بتوانند خدماتی را در زمینه ارزیابی مستقل از قابلیت اعتماد فرایند ثبت، پایش و نظارت بر پایگاه داده‌های زیستی، امنیت مجاری ارتباطی و رسیدگی به این موضوع که نرخ خطاهای سیستم در سطحی قابل قبول است، انجام دهند. در مجموع، خدمات ارائه شده توسط حسابداران باید به‌دنبال فراهم آوردن این اطمینان باشد که عوامل زیستی می‌توانند سطح مطلوب امنیت را به‌ویژه در محیط‌های شبکه‌های توزیعی، به‌اجرا بگذارند.

۳ـ یکپارچگی کنترل: اثربخشی محیط کنترلی سازمان را می‌توان با ترکیب عوامل زیستی و مجموعه سازوکارهای تعیین اعتبار و تشخیص هویت موجود و مورد استفاده در سیستم‌های حسابداری، افزایش داد. برای مثال، عوامل زیستی را می‌توان با کلمه عبور ترکیب کرد تا سازوکار تایید اعتبار چند عاملی ایجاد شود و از این طریق، از داده‌ها و اطلاعات بسیار حساس مانند شماره تامین اجتماعی کارکنان، اطلاعات محرمانه مشتریان و فرایندهای اختصاصی کسب‌وکار حفاظت شود. از دیدگاه کلی، حرفه حسابداری اغلب عهده‌دار مسئولیت امنیت دارایی‌های سازمان است. از سوی دیگر، اطلاعات بخشی از دارایی‌های پیش‌گفته محسوب می‌شود. این مسئولیت، به طور مفصل در گزارش **کمیسیون تردوی**[1] (COSO, 1992) مطرح شده است.

۴ـ تمامیت داده‌ها: وظیفه متداول حسابداری، نگهداری داده‌های شرکت است. ذخیره داده‌های زیستی، یکی از چالش‌های مورد بحث جامعه فناوری اطلاعات است. این موضوع، حوزه مستعدی را برای حسابداری فراهم می‌کند تا از فرصت استفاده نماید و برای طراحی و ذخیره پایگاه داده‌های زیستی که مطابق با راهبرد شرکت باشد، کمک کند.

چالش‌ها و توسعه در آینده

استفاده از عوامل‌زیستی به‌عنوان یکی از روش‌های امنیت اطلاعات، روش جدیدی است. از طرف دیگر، به‌دلیل چالش‌ها و مسایل زیادی که وجود دارد، طراحان سیستم‌ها باید خود را با دانش زیست‌سنجی مجهز کنند. سازوکار امنیتی، یکی از عامل‌های مهم در کاهش خطر کنترل است. این چالش‌ها و کاربردهایی که در این بخش ارائه شد، فرصت‌هایی را برای پژوهش‌های آینده فراهم می‌کند (Chandra and Calderon, 2003).

موقعیت سازمان‌ها در زمینه عوامل زیستی

تلاش‌های زیادی برای گسترش فناوری‌های جدید بر اساس باورهای تصمیم‌گیرندگان اصلی که تحت‌تاثیر تازگی و رواج فناوری هستند، انجام شده است (Swan and Newell 1994; Rogers 1995). به‌نظر می‌رسد که حسابداران و طراحان سیستم باید تمرکز خود را روی موقعیت سازمان‌ها و سایر عوامل وابسته قرار دهند تا سازمان‌ها را به سمت استفاده از سیستم‌های امنیتی زیستی سوق دهند. ولی در حال حاضر، درباره عوامل‌پذیرش و تسهیل اجرای موثر این فناوری نو، ادبیاتی وجود ندارد. برای شناخت این موضوع‌ها به‌پژوهش نیاز است.

زیرساخت‌های مورد نیاز

سازمان‌هایی که می‌خواهند از عوامل زیستی استفاده کنند، باید از زیرساخت‌های مطمئنی برای حمایت از این فرایند

برخوردار باشند. این در حالی است که ممکن است سازمانی به‌آسانی این قبیل زیرساخت‌ها را در محدوده سازمان خود فراهم کند، ولی احتمال دارد که گسترش این زیرساخت‌ها به شرکای تجاری و مشتریان، به چالش‌های عمده‌ای ختم شود. در حال حاضر، زیرساخت‌هایی جهت اطمینان از امنیت و یکپارچگی فرایندها، به‌خصوص در محیط شبکه‌های توزیعی، وجود ندارد. ادبیات موجود، بینش اندکی درباره موضوع‌های عملی و نظری مربوط به‌ایجاد چنین زیرساخت‌هایی ارئه داده است. بنابراین، اقدام به انجام پژوهش‌هایی در این زمینه، در آینده ضروری به‌نظر می‌رسد.

موانع اجتماعی

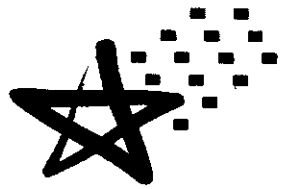
استفاده از ویژگی‌های رفتاری و فیزیولوژیکی، به موضوعی ستیزه‌جویانه مبدل شده است. به‌عنوان مثال، بعضی سازمان‌ها مدعی شده‌اند که تعیین هویت افراد از طریق ویژگی‌های زیستی، بیم و هراس زیادی را ایجاد می‌کند (Stanley and Steinhardt, 2002). عوامل موثر بر نفوذ و پذیرش سیستم‌های زیستی، در سازمان‌ها هنوز ناشناخته است. افزون بر این، نگرانی کاربران در مورد حریم خصوصی و اثر آن برفناوری زیستی و واکنش‌های لازم در مقابل برنامه‌های به‌خطر افتاده مربوط به زیست‌سنجی، شایسته توجه بیشتر در ادبیات پژوهشی سیستم‌های اطلاعاتی حسابداری است.

جنبه‌های گوناگون امنیت و اطلاعات

لایه امنیتی یک سیستم زیست‌سنجی، راه چاره کلی برای سیستم‌های حسابداری نیست. سیستم‌های امنیت اطلاعات باید از قابلیت اعتماد، در دسترس بودن، جامعیت، تعیین اعتبار و قابلیت پذیرش برخوردار باشند (Kaufman et al., 2002; Stallings, 2000; AICPA, 2002). امنیت اطلاعات، جنبه‌های گوناگونی دارد، به‌گونه‌ای که لایه امنیتی دارای توان زیستی نمی‌تواند به‌تنهایی تمام اهداف اساسی امنیت اطلاعات را براورده نماید. افزون بر این، طراحی یک سیستم امنیتی زیستی برای حفاظت از سیستم اطلاعات حسابداری، به بررسی فزونی منافع بر مخارج نیاز دارد. با وجود این که ممکن است لایه امنیتی زیستی، موجب تقویت برخی از کنترل‌های عمومی و برنامه‌های کاربردی شود، ولی

تجربه ای نو
با
سیستم یکپارچه مالی سپهر۳

عملکرد عالی
کیفیت مطلوب
پشتیبانی فنی مستمر
سادگی، کارایی و انعطاف فوق العاده
قابلیت انطباق با نیازهای مشتری
گارانتی عملکرد
قیمت مناسب
اجرا شده در صنایع و کاربردهای مختلف
نسخ استاندارد، حرفه ای و پیشرفته



info@setarehsepehr.com
www.setarehsepehr.com
تهران، خیابان ملاصدرا، بعدازچهار راه شیراز
ساختمان سارا، پ ۲۰ طبقه ۳ واحد۱۳
تلفن: ۸۸۰۳۹۸۵۵ - ۸۸۰۳۹۴۴۸

هنوز هم باید اجزای کنترل‌های داخلی را حفظ نمود و فعالیت‌های کنترلی پایه مانند تفکیک وظایف، نظارت و اختیارات، تصویب، مغایرت‌گیری، رسیدگی و تایید معاملات و رویدادها را اجرا کرد (Chandra and Calderon, 2003).

خلاصه و نتیجه‌گیری

فناوری زیستی، برای برنامه‌های کاربردی حسابداری نویدهایی دارد. این فناوری، افزایش امنیت در زمینه تشخیص هویت و تایید اعتبار کاربران را در پی دارد و همچنین، از توانایی کاهش خطر کنترل در کسب‌وکار و سیستم‌های اطلاعاتی حسابداری برخوردار است. به‌دلیل این‌که رمزهای عبور و کلمه‌های رمز به شخصی خاص مقید نیستند، آسیب‌پذیر هستند و ممکن است در مواقعی که استفاده می‌شوند، به‌دست‌کم گرفتن خطر کنترل منجر گردند. از طرف دیگر، عوامل زیستی شخصیت واقعی کسی راکه در حال استفاده از سیستم است، تایید می‌کنند. از لحاظ نظری، عوامل پیش‌گفته می‌توانند بدون ابهام مورد استفاده قرار گیرند تا منبع فناوری اطلاعات را به شخصی خاص منحصر سازند. ولی همه فرایندهای کسب‌وکار و برنامه‌های کاربردی، برای حفاظت شدن نیازمند عوامل زیستی نیستند. علاوه براین، مسائل و چالش‌های حل‌نشده بسیاری وجود دارد که نیازمند پژوهش‌های بیشتر است.

به‌منظور ساختن یک لایه امنیتی دارای توانایی زیستی برای سیستم‌های اطلاعاتی حسابداری، لازم است تا چندین موضوع نظری و اجرایی از دید دانشگاهیان و اشخاص حرفه‌ای، مورد توجه قرار گیرد. برای اجرای سیستم‌ها و فرایندهای با توان زیست‌سنجی، باید تعامل بین عوامل فناوری، شناختی، رفتاری، فنی و قانونی مورد بررسی قرار گیرد. پس ضروری است که شاغلان در حرفه و متخصصان هر دو گروه، در مسیری مناسب گام بردارند. نوید مورد ادعای عوامل زیستی بر این فرض استوار است که یک وضعیت کسب‌وکار دقیق و بی‌خطر ایجاد گردد، سیستم به‌درستی اجرا و استفاده شود و به‌طور اثربخش عمل کند. برای موفقیت عوامل زیستی در سیستم‌های اطلاعاتی حسابداری، باید فرض‌ها، چالش‌ها و محدودیت‌های این فناوری در وضعیت کنونی را در نظر گرفت. برای کاوش در زمینه این موضوع‌ها، پژوهش‌های بیشتری مورد نیاز است.

پی‌نوشت:

1- Committee of Sponsoring Organizations of the Treadway Commission

منابع:

1- Allen J., **Why is Security a Software Issue?**, EDPACS, 36, 1, pp. 1-12, 2007

2- Chandra A., Calderon T. G., **Toward a Biometric Security Layer in Accounting Systems**, Journal of Information Systems, 17, 2, pp. 51-71, 2003

3- Kaufman C., Perlman R., Spencer M., **Network Security: Private Communication in a Public World**, Upper Saddle River, NJ: Prentice Hall, 2002

4- Luehlfing M. S., Daily C. M., Phillips T. J., Smith L. M., **Defending the Security of the Accounting System**, The CPA Journal, 70, 10, pp. 62-65, 2000

5- Matyas S. M., Stapleton J., **A Biometric Standard for Information Management and Security**, Computers & Security 19: pp. 428-441, 2000

6- McGraw G., **Software Security: Building Security In**, Boston, MA: Addison-Wesley, 2000

7- Nichols R. K., Ryan D. J. Ryan J. J. C. H., **Defending Your Assets**, New York, NY: McGraw-Hill, 2000

8- Pipkin, D., **Information Security**, Upper Saddle River, NJ: Prentice Hall, 2000

9- Stallings W., **Network Security Essentials: Application & Standards**. Upper Saddle River, NJ: Prentice Hall, 2000

10- Stanley J., Steinhardt B., **Drawing a Blank: The Failure of Facial Recognition Technology in Tampa**, Florida, An ACLU Special Report, Available at: http://arehive.aciu.org

11- Swan J. A., and S. Newell, **Managers' Beliefs About Factors Affecting the Adoption of Technological Innovation**, A Study Using Cognitive Maps, Journal of Managerial Psychology 9, 2, pp.3-11, 1994

آرپا
نرم افزاری متفاوت

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

ارایه نرم افزار به صورت آزمایشی یک ماهه
یک سال خدمات پشتیبانی رایگان
ارایه آموزش نامحدود به صورت رایگان
اعمال تغییرات و پیشنهادات مشتری در برنامه در حداقل زمان
معرفی و راه اندازی کدینگ مالی
انجام خدمات حسابداری مشاوره ای و حضور مستمر در شرکت مربوطه
انجام خدمات پشتیبانی به صورت ۲۴ ساعته و در کمترین زمان ممکن

تهران - خیابان قرنی - بالاتر از طالقانی - کوچه سوسن - پلاک ۴ - طبقه ۲ - واحد ۲۲
تلفکس: ۸۸۸۹۱۳۹۸-۰۲۱
وب سایت: www.arpa-co.ir

موسسه آموزشی و پژوهشی اتاق بازرگانی
و صنایع و معادن ایران

انجمن حسابداران خبره ایران

دوره‌های حسابداری و مدیریت مالی موسسه آموزشی و پژوهشی

اتاق بازرگانی و صنایع و معادن ایران

با همکاری انجمن حسابداران خبره ایران

دوره‌های حسابداری و مالی کوتاه‌مدت و بلندمدت:

کد دوره	نام دوره	مدت دوره	شهریه /ریال	پیش‌نیاز
۴۰۱	حسابداری مالی (۱)	۶۰ ساعت	۱,۱۰۰,۰۰۰	حداقل دیپلم
۴۰۲	حسابداری مالی (۲)	۶۰ ساعت	۱,۲۵۰,۰۰۰	۴۰۱
۴۰۵	حسابداری صنعتی (۱)	۶۰ ساعت	۱,۲۰۰,۰۰۰	۴۰۲
۴۰۶	حسابداری صنعتی (۲)	۵۰ ساعت	۱,۳۰۰,۰۰۰	۴۰۵
۴۰۷	حسابداری مدیریت	۴۰ ساعت	۲,۰۰۰,۰۰۰	۴۰۶
۴۰۸	مدیریت مالی	۳۰ ساعت	۱,۰۰۰,۰۰۰	۴۰۲
۴۰۹	حسابداری تلفیقی	۲۰ ساعت	۳,۰۰۰,۰۰۰	لیسانس حسابداری یا مرتبط
۴۱۰	حسابرسی داخلی و عملیاتی	۴۰ ساعت	۱,۳۰۰,۰۰۰	۴۰۲
۴۱۲	قانون مالیاتهای مستقیم	۳۵ ساعت	۹۰۰,۰۰۰	۴۰۲
۴۱۳	مدیریت مالی برای مدیران غیرمالی	۴۰ ساعت	۱,۵۰۰,۰۰۰	۳ سال سابقه مدیریت
۴۱۴	مدیریت سرمایه‌گذاری در بورس اوراق بهادار و مهندسی مالی	۳۰ ساعت	۲,۰۰۰,۰۰۰	لیسانس حسابداری یا مرتبط
۴۱۶	تجزیه وتحلیل و طراحی سیستمهای حسابداری	۲۰ ساعت	۱,۲۵۰,۰۰۰	لیسانس حسابداری یا مرتبط
۴۱۷	اصول برنامه‌ریزی و بودجه	۳۰ ساعت	۱,۰۰۰,۰۰۰	لیسانس حسابداری یا مرتبط
۴۱۸	صورت جریان وجوه نقد	۱۸ ساعت	۱,۲۰۰,۰۰۰	لیسانس حسابداری یا مرتبط
۴۱۹	تهیه و ارائه صورت‌های مالی (استانداردهای حسابداری ۱، ۲، ۶ و ۱۴)	۲۰ ساعت	۱,۳۰۰,۰۰۰	لیسانس حسابداری یا مرتبط
۴۲۰	صورت مالی نمونه	۱۲ ساعت	۱,۰۰۰,۰۰۰	لیسانس حسابداری
۴۲۰	استفاده از نرم‌افزارهای حسابداری	۴۰ ساعت	۱,۲۰۰,۰۰۰	۴۰۲
۵۰۱	دوره عالی حسابداری و مدیریت مالی	۲۶۰ ساعت	۷,۵۰۰,۰۰۰	لیسانس حسابداری یا مرتبط
۵۰۲	دوره تکمیلی و امور مالی (۱)	۲۶۰ ساعت	۶,۰۰۰,۰۰۰	۴۰۲
۶۰۱	حسابداری مالی به زبان انگلیسی	۶۰ ساعت	۱,۶۰۰,۰۰۰	حداقل لیسانس مرتبط
۶۰۲	حسابداری صنعتی و مدیریت مالی به زبان انگلیسی	۶۰ ساعت	۱,۸۰۰,۰۰۰	۶۰۱
۷۰۱	کاربرد Excel در حسابداری	۳۰ ساعت	۱,۲۰۰,۰۰۰	۴۰۱ و ۴۰۲
۷۰۲	کاربرد Access در حسابداری	۴۰ ساعت	۱,۲۰۰,۰۰۰	۴۰۱ و ۴۰۲

در صورت نیاز به اطلاعات بیشتر می‌توانید با موسسه آموزشی و پژوهشی اتاق بازرگانی به آدرس زیر مراجعه یا با تلفن‌های مرکز تماس حاصل فرمایید.

خیابان انقلاب، میدان فردوسی خیابان شهید موسوی (فرصت جنوبی) شماره ۳۶

تلفن ۵-۸۸۸۱۰۵۳۴ - ۸۸۸۱۴۰۴۰ نمابر ۸۸۸۲۸۷۸۷