پژوهش حسابداری
شماره ۷، زمستان ۱۳۹۱

ویروس‌های کامپیوتری تهدیدی برای امنیت سیستم اطلاعات حسابداری

اسفندیار ملکان
دانشیار حسابداری دانشگاه مازندران
رسول سلمانی*
دانشجوی کارشناسی ارشد حسابداری دانشگاه مازندران

چکیده

امروزه اطلاعات به یک دارایی باارزش تبدیل شده است که باید با توجه و دقت از آن نگهداری شود، چرا که بقا و موفقیت در تجارت به شدت به این موضوع بستگی دارد. وابستگی به اطلاعات و سرعت تغییر تکنولوژی، بسیاری از سازمان‌ها را مجبور کرده است که با برنامه‌های امنیتی مناسب، از سیستم اطلاعاتی خود محافظت کنند. اما موفقیت در تأمین امنیت به سطح آگاهی مدیران و کارکنان سازمان‌ها نیز بستگی دارد. امروزه سیستم‌های اطلاعاتی حسابداری در سازمان‌ها، مهم‌ترین رکن یک سازمان محسوب می‌شوند. یکی از فاکتورهای تهدیدکننده سیستم‌های اطلاعاتی ویروس‌ها می‌باشند، ویروس‌های کامپیوتری بدافزارهایی هستند که باعث ایجاد اختلالات متنوعی از جمله از دست دادن اطلاعات و اختلال در فرآیند جاری در سیستم‌های اطلاعاتی حسابداری می‌شوند؛ از سوی دیگر یکی از اهداف اصلی ویروس‌ها سرقت اطلاعات مالی می‌باشد. در این مقاله سعی شده است یکی از عوامل اصلی تهدیدکننده امنیت سیستم‌های اطلاعات حسابداری، یعنی ویروس‌ها، تشریح شود؛ در انتها نیز پیشنهاداتی برای مقابله با این عامل تهدیدکننده ارائه شده است؛ تا بدین وسیله سطح آگاهی مدیران و کارکنان درجهت مقابله با این نوع از تهدیدات ارتقا یابد.

واژه‌های کلیدی: سیستم اطلاعاتی، حسابداری، ویروس، امنیت

* نویسنده‌ی مسئول: rasoulsalmani@yahoo.com

مقدمه

شکست در برقراری و تأمین امنیت اطلاعات و یا دسترسی افراد غیرمجاز به این اطلاعات منجر به خسارات مالی و غیرمالی می‌شود(ابوموسی[۱]، ۲۰۰۲). در معرض مخاطرات کامپیوتری قرار گرفتن، تقریباً اجتناب‌ناپذیر است، مگر آن‌که محافظت کافی صورت گیرد. مفاهیم جرائم کامپیوتری و امنیت اطلاعات از مرزهای جغرافیایی نسبتاً محدود به یک مسئله‌ی جهانی تبدیل شده است. ویلیام بیان می‌کند که هر نوع نقص امنیتی، حتی جزیی، می‌تواند به یک مشکل بزرگ و پرهزینه تبدیل شود(ویلیامز[۲]، ۱۹۹۵). گزارش‌های روزانه‌ی زیادی در نشریات حسابداری و مالی در ارتباط با عواقب خطاهای کامپیوتری، اطلاعات مالی نادرست، تخلف از کنترل‌های داخلی، دزدی، آتش‌سوزی و خرابکاری منتشر می‌شود(کورشی[۳]، ۱۹۹۷)؛ لذا گسترش سیاست برقراری امنیت اطلاعات با بالا بردن سطح آگاهی مدیران و کارکنان در ارتباط با این موضوع، موضوع بسیار بااهمیتی محسوب می‌شود.این مقاله به چندین بخش تقسیم شده است؛ در بخش بعدی به موضوع سیستم و سیستم اطلاعاتی حسابداری پرداخته می‌شود.

مفهوم سیستم و سیستم‌های اطلاعاتی حسابداری

به نقل از ویکی‌پدیا سیستم مجموعه یا گروهی از اشیا مرتبط یا غیر مرتبط است که هدف یا اهدافی خاص را دنبال می‌کنند، به گونه‌ای که واحد پیچیده‌ای را تشکیل می‌دهند؛ سیستم مجموعه‌ای از اجزایی است که با هم کار می‌کنند و هدف معینی را دنبال می‌کنند. سیستم تنها به نوع فیزیکی آن محدود نمی‌شود. مفهوم سیستم را در مورد پدیده‌های مجرد پویا نظیر اقتصاد نیز می‌توانیم بکار بریم. در تعریف علوم انسانی، سیستم را می‌توان مجموعه‌هایی از عناصر که برای انجام مأموریت یا رسیدن به هدف خاصی با کمیت و کیفیت معلوم طراحی و ساخته‌شده و با کمیت و کیفیت معلوم با هم ترکیب‌شده‌اند، تعریف نمود(ویکی پدیا، ۲۰۱۲). سیستم مجموعه‌ای از عناصر است که برای رسیدن به یک هدف مشخص و مشترک گرد هم آمده‌اند، به طوری که

بین این عناصر یک رابطه تعاملی وجود دارد. ویژگی بعدی سیستم، وجود نظم در روابط بین عناصر است؛ به این معنا که هر عنصری دارای یک نقش می‌باشد(سجادی، ۱۳۸۵). حسابداری نیز یک سیستم اطلاعاتی است که به وسیله آن اطلاعات مربوط به فعالیت‌های مالی شناسایی، ثبت، طبقه‌بندی و تلخیص می‌گردد تا به منظور فراهم کردن امکان قضاوت و تصمیم‌گیری آگاهانه در اختیار استفاده‌کنندگان قرار گیرد.

سیستم اطلاعات حسابداری، سیستمی است که از طریق آن می‌توان اطلاعات صورت‌های مالی را گردآوری و تنظیم کرد و در اختیار استفاده‌کنندگان آن قرار داد. لذا کارایی سیستم‌های اطلاعات حسابداری به کیفیت اطلاعات ارائه‌شده آن و به بهره‌برداری مناسب مدیریت از آن بستگی دارد. هر گونه ضعف و نبود کارایی و امنیت در سیستم‌های اطلاعات حسابداری، کاهش کارایی، بازدهی و مشکلات بی‌شماری را در امر برنامه‌ریزی و تصمیم‌گیری به دنبال خواهد داشت(میرمجربیان، ۱۳۸۵).

از آن‌جایی که سیستم اطلاعات حسابداری بر شناخت و درک چگونگی وظایف سیستم حسابداری شامل شیوه‌های گردآوری داده‌های مربوط به فعالیت‌ها و رویدادهای مالی سازمان و شیوه‌ی تبدیل داده‌ها به اطلاعاتی که مدیریت می‌تواند آن‌ها را در سازمان مورد استفاده قرار دهد و شیوه‌ی حصول اطمینان از قابلیت دسترسی و اتکای به آن اطلاعات، تاکید می‌کند، یکی از حیاتی‌ترین و اساسی‌ترین سیستم‌های یک سازمان به شمار می‌رود(دیویس[۴]، ۱۹۹۷).

از سوی دیگر امروزه حسابرسان نقش مهمی را در ایجاد اطمینان برای استفاده‌کنندگان اطلاعات ایفا می‌نمایند. بخشی از اطمینان دهی حسابرسان باید از طریق بررسی امنیت سیستم‌های اطلاعات حسابداری باشد. حسابرسان آگاه‌اند که بدون ایجاد امنیت در سیستم‌های اطلاعات حسابداری، مدیران قادر به ارائه اطلاعات درست و قابل‌اتکا نخواهند بود. زیرا ممکن است گزارش‌های مالی به علت نبود امنیت در سیستم‌های حسابداری مورد تحریف و دست‌کاری قرار گیرد. البته حسابرسان داخلی نیز می‌توانند در برقراری امنیت در سیستم‌های اطلاعات

حســـابداری نقش مهمی داشته باشند، زیرا آن‌ها به طور مستقیم مسئـولیت کمک به مدیریت شـرکت به منظور بهبود کارایی و اثربخشـی ســازمان را بر عهده‌دارند. بخشی از این مسئـولیت، شـــامل کمک به طراحـــی و اجـــرای سیستم‌های اطلاعات حســـابداری است(ودیعی، ۱۳۸۹). در بخش بعدی به موضوع امنیت و انواع خطرهایی که سیستم اطلاعات حسابداری را تهدید می‌کند، پرداخته می‌شود.

امنیت و انواع تهدیدها

امروزه اداره‌ی موفق واحدهای تجاری، بدون بهره‌گیری از ابزار اطلاعاتی مانند گزارش‌ها و اطلاعات حاصل از سیستم‌های اطلاعاتی حسابداری، در عمل غیرممکن است. به منظور موفقیت و تعالی سازمان در عرصه‌ی رقابت، سیستم‌های اطلاعاتی مورد نیاز است. حسابداری به عنوان یک سیستم اطلاعاتی، داده‌های واحد تجاری را شناسایی، جمع‌آوری، پردازش و تلخیص می‌کند. سیستم اطلاعات حسابداری داده‌های مالی را به اطلاعات مالی تبدیل می‌کند و این اطلاعات به گروه وسیعی از تصمیم‌گیرندگان ارائه می‌شود(ودیعی،۱۳۸۷). اطلاعات، مهم‌ترین منبع تصمیم‌گیری است، پس باید در آن سیستم امنیت نیز برقرار گردد. کارشناسان حسابداری فناوری اطلاعات در نشست مشترک خود امنیت اطلاعات را به عنوان مهم‌ترین فناوری که باید مورد توجه قرار گیرد، برگزیده‌اند. این گزینش بر اساس نتایج حاصل از هفدهمین نظرخواهی سالانه‌ی ۱۰ فناوری برتر به وسیله‌ی انجمن حسـابداران رسمی آمـریکا صورت گرفته است؛ به گونه‌ای که در فهرست۱۰ فناوری برتر سال ۲۰۰۶، فناوری کشف و انهدام نرم‌افزارهای جاسوسی به چشم می‌خورد. این فناوری، برنامه‌هایی را که به صورت پنهان و بدون اطلاع و اجازه در پی جمع‌آوری و انتقال اطلاعات محرمانه بهره‌برداران سیستم‌های اطلاعاتی است، کشف و منهدم می‌کند(صفار، ۱۳۸۵).

ودیعی بیان می‌کند که همزمان با افزایش پیچیدگی سیستم‌های اطلاعاتی، شرکت‌ها و سازمان‌ها با تهدیدهایی روبه رو هستند. بیشتر تهدیدهایی که شرکت‌ها و سازمان‌ها با آن روبه رو هستند، به شرح زیر است:

۱. ایجاد، تغییر و دست‌کاری در اطلاعات

۲. کپی‌برداری غیرمجاز و یا سرقت اطلاعات

۳. منتشر کردن اطلاعات

۴. تخریب پایگاه‌های اطلاعاتی

۵. تهدیدهای مربوط به پایگاه‌های کامپیوتری فعال در امور مالی و اقتصادی(ودیعی، ۱۳۸۹).

ویروس‌ها، انواع و تخریب‌های بالقوه

تشخیص نوع حملات توسط ویروس‌ها کاری دشوار است. ماهیت حملات ویروس‌ها در چند سال قبل تغییر کرده است. مثلاً در گذشته بیشتر حملات ایجادشده توسط هکرها با نیت خرابکاری صورت می‌گرفت ولی در حال حاضر بیشتر هجوم‌ها باهدف سوءاستفاده‌های مالی صورت می‌گیرد. مثلاً زمانی که شما قصد دانلود یک موسیقی را دارید ممکن است هدف حملات هکرها قرار بگیرید و زمانی که شما در حال شنیدن این موسیقی هستید چه بسا ممکن است ویروس‌ها بر روی سیستم شما تکثیر یافته و اطلاعات شما به سرقت رود.به عنوان مثال، فلیم[۵](آتش) جدیدترین ویروسی است که توسط سیستم‌های امنیتی غربی علیه جمهوری اسلامی ایران طراحی شده است، بر خلاف استاکس نت[۶] که فقط برای جاسوسی و جمع‌آوری اطلاعات طراحی شده است؛ این ویروس از صفحه‌ی نمایشگر رایانه عکس می‌گیرد و میکروفون رایانه را روشن می‌کند تا مکالمات محیط ضبط شود. سپس اطلاعات گردآوری‌شده به منبع منتشرکننده ویروس منتقل می‌شود. یک ویروس کامپیوتری، برنامه‌ای کامپیوتری محسوب می‌شود که می‌تواند خود را تکثیر نماید و کامپیوتر را آلوده کند. واژه‌ی ویروس به غلط درباره برخی از بدافزارها، ابزارهای تبلیغاتی مزاحم که قدرت تکثیر ندارد نیز اطلاق می‌شود. یک ویروس کامپیوتری به همان شکل اولیه یا با

تغییرات ایجاد کرده در خود، از کامپیوتری به کامپیوتر دیگر از طریق اینترنت، یواس بی[۷] و یا دیسک‌های جانبی انتقال می‌یابد. ویروس‌ها می‌توانند شانس خود را در گسترش به دیگر کامپیوترها با آلوده کردن فایل‌ها در یک سیستم یا شبکه افزایش دهند.

ویروس‌ها هم مشابه همه‌ی برنامه‌های دیگر از منابع سیستم مانند حافظه و فضای دیسک سخت[۸]، توان پردازنده‌ی مرکزی و سایر منابع بهره می‌گیرند و می‌توانند اعمال خطرناکی را انجام دهند. به عنوان مثال فایل‌های روی دیسک را پاک کرده، پشتیبان‌های تهیه‌شده توسط سیستم اطلاعات حسابداری را از بین برده و یا کل دیسک سخت را با تمامی اطلاعات پاک نماید.

انواع ویروس‌های رایج را می‌توان به دسته‌های زیر تقسیم‌بندی نمود:

بوت سکتور[۹]: که هنگام آغاز به کار سیستم‌عامل شروع به فعالیت می‌کند.

ماکرو[۱۰]: که از زبان‌های برنامه‌نویسی ماکرویی مانند ورد و اکسل استفاده می‌کند.

ویروس‌های فایل‌های اجرایی[۱۱]: هنگام اجراشدن برنامه‌های موجود از جمله سیستم‌های اطلاعاتی حسابداری در کامپیوتر شروع به فعالیت می‌کنند.

ویروس‌های چند شکلی[۱۲]: این ویروس‌ها در هر فایل آلوده به شکلی ظاهر می‌شوند. با توجه به اینکه از الگوریتم‌های کد گذاری استفاده می‌کند و ردپای خود را نیز پاک می‌کند، آشکارسازی و تشخیص این‌گونه ویروس‌ها دشوار است.

ویروس‌های مخفی[۱۳]: این ویروس‌ها سعی می‌کنند خود را از سیستم‌عامل و نرم‌افزارهای ضد ویروس پنهان نگه‌دارند.

سایر برنامه‌های مختل‌کننده امنیت: اسب تروا[۱۴]، کرم ها[۱۵] و بمب‌های منطقی[۱۶] در این گروه قرار می‌گیرند، این برنامه‌ها هم بسیار خطرناک بوده و هم می‌توانند خساراتی جدی به سیستم‌های کامپیوتری وارد نمایند.

سیاست‌های امنیتی و راه‌های پیشنهادی پیشگیری از خطرات ویروس‌ها

سازمان‌های بزرگ و کوچک نیازمند ایجاد سیاست‌های امنیتی لازم در خصوص استفاده از کامپیوتر و ایمن‌سازی اطلاعات و شبکه‌های کامپیوتری می‌باشند. سیاست‌های امنیتی، مجموعه قوانین لازم به منظور استفاده از کامپیوتر و شبکه‌های کامپیوتری بوده که در آن وظایف تمامی کاربران دقیقاً مشخص و در صورت ضرورت، هشدارهای لازم به کاربران در خصوص استفاده از منابع موجود در شبکه داده می‌شود. دانش تمامی کاربرانی که به تمام و یا بخشی از شبکه دستیابی دارند، می‌بایست به صورت منظم و با توجه به سیاست‌های تدوین‌یافته، به هنگام گردد(آموزش مستمر و هدفمند با توجه به سیاست‌های تدوین‌شده). برخی از این نوع سیاست‌ها و راه‌های پیشگیری از خطرات ویروس‌ها به شرح زیر می‌باشد:

پذیرش مسئولیت به عنوان یک شهروند سایبر[۱۷] **:** در صورتی که از اینترنت استفاده می‌نمائید، شما به عنوان عضوی از جامعه جهانی و یا شهروند سایبر، محسوب شده و همانند یک شهروند معمولی، دارای مسئولیت‌های خاصی بوده که می‌بایست پذیرای آنان باشید.

استفاده از نرم‌افزارهای ضد ویروس[۱۸]**:** یک ویروس کامپیوتری، برنامه‌ای است که می‌تواند به کامپیوتر شما نفوذ کرده و صدمات فراوانی را باعث گردد. نرم‌افزارهای ضد ویروس به منظور حفاظت اطلاعات و کامپیوترها در مقابل ویروس‌های شناخته‌شده، طراحی‌شده‌اند. با توجه به این که روزانه شاهد عرضه‌ی ویروس‌های جدید می‌باشیم، می‌بایست برنامه‌های ضد ویروس به صورت منظم و مرتب بهنگام گردند. برای دریافت خدمات کامل و موثرتر از جانب شرکت‌های تولیدکننده ضد ویروس هیچ‌گاه از ضد ویروس‌های تکثیر یافته به صورت غیرمجاز استفاده ننمایید.

عدم فعال نمودن نامه‌های الکترونیکی ارسال‌شده توسط منابع نامشخص و گمنام: نامه‌های الکترونیکی ارسالی توسط منابع ناشناس را می‌بایست همواره حذف نمود. به فایل هائی که به عنوان ضمیمه همراه یک نامه‌ی الکترونیکی ارسال می‌گردند، توجه گردد؛ حتی در صورتی که این نوع از نامه‌های الکترونیکی را از طریق دوستان و آشنایان خود دریافت می‌نمائید(خصوصاً اگر دارای انشعاب exe. باشند). برخی فایل ها مسئولیت

توزیع ویروس‌ها را بر عهده داشته و می‌توانند باعث بروز اشکالات فراوانی نظیر حذف دائم فایل ها گردند.

از رمزهای عبوری که تشخیص آنان مشکل می‌باشد، استفاده نموده و آنان را محرمانه نزد خود نگه‌دارید. تعداد زیادی از کاربران کامپیوتر دقت لازم در خصوص نگهداری رمز عبور خود را نمی‌نمایند و همین امر می‌تواند مشکلات متعددی را متوجه آنان، نماید. رمزهای عبوری که تشخیص و یا حدس آنان آسان است، گزینه‌های مناسبی در این رابطه نمی‌باشند. در فواصل زمانی مشخص و به صورت مستمر، اقدام به تغییر رمز عبور خود نمائید. هرگز رمز عبور خود را در اختیار اشخاص دیگری قرار ندهید. برای انتخاب یک رمز عبور از ترکیب اعداد، حروف و علائم استفاده گردد تا حدس و ردیابی آنان توسط افراد غیرمجاز، مشکل شود.

استفاده از دیوار آتش[۱۹] به منظور حفاظت کامپیوترها : نصب و پیکربندی یک دیوار آتش کار مشکلی نخواهد بود. یک دیوار آتش، امکان دستیابی و کنترل سیستم توسط مهاجمان را سلب نموده و پیشگیری لازم در خصوص سرقت اطلاعات موجود بر روی کامپیوتر را انجام می‌دهد.

پشتیبان گرفتن[۲۰] منظم از اطلاعات ارزشمند موجود بر روی کامپیوتر: در فواصل زمانی مشخص و بر اساس یک برنامه خاص از اطلاعات ارزشمند موجود بر روی کامپیوتر و سیستم اطلاعات حسابداری و اطلاعات مالی پشتیبان گرفته شود و آنان را بر روی رسانه‌های ذخیره‌سازی نظیر لوح‌های فشرده ذخیره نمایید.

دریافت و نصب منظم بهنگام شده مربوط به نقایص امنیتی: نقایص امنیتی به صورت مرتب در سیستم های عامل و برنامه‌های کاربردی کشف می‌گردند. شرکت‌های تولیدکننده نرم‌افزارها از جمله سیستم‌های اطلاعات حسابداری، به سرعت اقدام به ارائه‌ی نسخه‌های بهنگام شده‌ای با نام آپدیت[۲۱] نموده که کاربران می‌بایست آنان را دریافت و بر روی سیستم خود نصب نمایند. در این رابطه لازم است به صورت منظم از سایت های مربوط به تولیدکنندگان نرم‌افزار بازدید به عمل آمده تا در صورت ارائه‌ی آپدیت، آن را دریافت و بر روی سیستم نصب نمود.

بررسی و ارزیابی دوره‌ای امنیت کامپیوتر: وضعیت امنیتی کامپیوتر خود را در مقاطع زمانی مشخصی، بررسی نموده و در صورتی که خود نمی‌توانید این کار را انجام دهید از کارشناسان ذی‌ربط استفاده نمایید.

غیرفعال نمودن ارتباط با اینترنت در زمان عدم استفاده: اینترنت نظیر یک جاده دو طرفه است. شما اطلاعاتی را دریافت و یا ارسال می‌نمائید. غیرفعال نمودن ارتباط با اینترنت در مواردی که به آن نیاز نمی‌باشد، امکان دستیابی سایرین به کامپیوتر شما را سلب می‌نماید.

عدم اشتراک منابع موجود بر روی کامپیوتر با کاربرانی که هویت آنان نامشخص است: سیستم‌عامل نصب‌شده بر روی یک کامپیوتر، ممکن است امکان به اشتراک گذاشتن برخی منابع موجود نظیر فایل ها را با سایر کاربران شبکه، فراهم نماید. ویژگی فوق، می‌تواند زمینه‌ی بروز تهدیدات امنیتی خاصی را فراهم نماید. بنابراین می‌بایست نسبت به غیرفعال نمودن ویژگی فوق، اقدام لازم صورت پذیرد.

- **استفاده مناسب از حافظه‌های جانبی:** حافظه‌های جانبی یکی از اصلی‌ترین راه‌های انتقال ویروس می‌باشد، در استفاده کردن از آن‌ها باید دقت نمود.

استفاده از خدمات کارشناسان: از خدمات کارشناسان ماهر حوزه‌ی امنیت استفاده کنید.

نتیجه‌گیری

امروزه اداره‌ی موفق یک واحد تجاری بدون در نظر گرفتن نقش اساسی اطلاعات در عمل غیرممکن است. اطلاعات مالی یک واحد تجاری دارایی ارزشمندی محسوب می‌شود. اجرای امنیت به عنوان سازوکار حمایت از اطلاعات، جزئی لاینفک در اداره‌ی موفق سازمان است. امروزه ویروس‌های کامپیوتری یکی از عوامل مهم آسیب‌رسان به مقوله امنیت می‌باشند. در این بین سرقت اطلاعات مالی یکی از اهداف مهم ویروس‌ها می‌باشد. عدم توجه به خطرات بالقوه‌ی ویروس‌ها و عدم رعایت اصول پیشگیرانه در این موضوع، ممکن است مشکلات غیرقابل جبرانی

را ایجاد کند. جنبه‌ی دیگری که باید مورد توجه قرار گیرد، موضوع حسابرسی است. بخشی از اطمینان دهی حسابرسان باید از طریق بررسی امنیت سیستم‌های اطلاعات حسابداری باشد. حسابرسان آگاه‌اند که بدون ایجاد امنیت در سیستم‌های اطلاعات حسابداری، مدیران قادر به ارائه‌ی اطلاعات درست و قابل‌اتکا نخواهند بود. این امر اهمیت موضوع امنیت را دوچندان می‌کند. در پیشنهادهای مطرح‌شده بیان شد که باید به عنوان یک کاربر، قوانین حاکم بر اینترنت را رعایت نماییم؛ از ضد ویروس‌های مناسب برای جلوگیری از آلوده شدن کامپیوتر استفاده کنیم؛ ایمیل‌های ناشناس را حذف نماییم؛ از رمزهای عبور مناسب برای تعیین سطح دسترسی استفاده کنیم؛ دیوار آتش مناسبی را برای عدم دسترسی مهاجمان طراحی کنیم؛ به صورت ادواری از اطلاعات نسخه پشتیبان تهیه کنیم؛ سیستم‌های اطلاعاتی خود را به‌روز نماییم؛ وضعیت امنیت کامپیوتر را به صورت دوره‌ای بررسی نماییم؛ در زمانی که به اینترنت نیازی نداریم ارتباط خود را با اینترنت قطع کنیم؛ فایل‌های موجود در کامپیوتر و سیستم‌های اطلاعاتی حسابداری را از دسترس افراد ناشناس حفظ کنیم؛ از حافظه‌های جانبی به صورت مناسب استفاده کنیم و در آخر این‌که از نظرات کارشناسان حوزه امنیت نیز بهره بگیریم.

پی نوشت ها

[1] Abu-musa
[2] Williams
[3] Qureshi
[4] Davis
[5] Flame
[6] Stuxnet
[7] Usb
[8] Hard Disk
[9] Boot Sector
[10] Macro Viruses
[11] File Infecting Viruses
[12] Polymorphic Viruses
[13] Hidden Viruses

[14] Trojan
[15] Worms
[16] Logical bombs
[17] Cyber
[18] Antivirus
[19] Firewall
[20] Backup
[21] Update

منابع و مآخذ

۱. سجادی، سید حسین؛ طباطبایی‌نژاد، سید محسن.(۱۳۸۵).سیستمهای اطلاعات حسابداری، انتشارات دانشگاه شهید چمران، چاپ اول.

۲. صفار، محمد جواد.(۱۳۸۵)." بیانیه شش شبکه جهانی حسابرسی"، *حسابرس*، شماره ۳۵.

۳. میرمجربیان، حمید، شهشهانی، سید محمد حسن.(۱۳۸۵)." کارایی تصمیم گیری در گزارشگری مالی در محیط شبکه گسترده جهانی"، *حسابرس*، شماره ۳۵.

۴. ودیعی، محمد حسین، موسوی‌نژاد، سید روحا...(۱۳۸۷)."حسابرسی در عصر تجارت الکترونیک"، *حسابرس*، شماره ۴۱.

۵. ودیعی، محمد حسین، محمدی، جمال.(۱۳۸۹). "امنیت در سیستمهای اطلاعاتی حسابداری"، *حسابرس*، شماره ۵۱.

6. Abu-Musa, Ahmad A.(2002), "Computer Crimes: How Can You Protect Your Computerized Accounting Information Systems", *The Journal of American Academy of Business*, Cambridge, USA, Vol. 2. No.1 September 2002, pp. 91-111 .
7. Davis, C. E.(1997)," An Assessment of Accounting Information Security", *CPA Journal*, March,:28 35
8. Qureshi, Anique A and Joel G Siegel(1997), "The accountant and computer security", *The National Public Accountant*; Washington, May.
9. Williams, Paul(1995), "Safe, Secure and up to Standard", *Journal of Accountancy*,(Apr. 1990) p. 60.
10. http://fa.wikipedia.org/wiki/