ویروس‌های کامپیوتری مسئله جدیدی برای حسابرسان

● گردآوری : دکتر محسن شریفی
استادورئیس بخش حسابداری
دانشگاه میشیگان شرقی

اهمیت کامپیوتر برای رشته حسابداری ونقش حسابداران وحسابرسان درکاربرد این وسیله محاسبه بمیزان کافی مورد بحث ومداقه قرار گرفته است . حسابداران ازابتدای کامپیوتریزه شدن سیستم ها نقش عمده ای رادرتجزیه وتحلیل وطراحی این سیستم ها ایفا کرده اند. معذالك نوع این دخالت ها متناسب باتغییراتی که در تکنولوژی صورت گرفته درحال تغییربوده است . دراین زمینه پیشرفت های تکنولوژیك دهه اخیر بترتیبی بوده که نیاز به تخصصی شدن وظایفی که توسط حسابداران وحسابداران انجام میشود رابه میزان بیش از پیش ضروری ساخته است .

این تخصصی شدن درحدخود مسائلی راپیش کشیده که قبلا" مطرح نبوده است . یکی ازاین مسائل درحال حاضر " ویروس های کامپیوتری " است که بصورت کابوس وحشتناکی برای مسئولان سیستم های کامپیوتری سازمان های مختلف اعم از دولتی وخصوصی درآمده است . حسابداران وحسابرسان افرادی هستند که در رابطه بامسائل کنترلهای داخلی درصف اول با این ویروس ها در مبارزه هستند.

پیدایش ویروس ها

اگرچه ویروس ها پدیده جدیدی برای میکروکامپیوترهابحساب آمده واخیرا" درزیر ذره بین قرارگرفته اند ، مفهوم آن ازدهه ۱۹۵۰ درسیستم های بزرگ کامپیوتری مورد استفاده بوده است . این ویروس ها درابتدابمنظور آزمایش عکس العمل واطمینان از امنیت سیستم های کامپیوتری بوجودآمده اند ، برنامه نویس های کامپیوتر نیز ازآن بعنوان وسیله ای برای به رخ کشیدن قدرت خلاقه خود به سایر همکاران استفاده میکنند. درابتدا این ویروس ها بطور کنترل شده ومحدود در یك ناحیه خاصی از کامپیوترتوسط برنامه ریزهای بسیارممبرز بکارمیرفتند . ولی متاسفانه درحال حاضر شماره افرادی که قادر به ایجاداین ویروس ها هستند روبه ازدیاد است . چیزی که این مسئله رابطور خطر ناکتری مطرح میسازد نمونه کاربرداین ویروس ها بصورت آسیب زا واشتیاق افراد به تسری این نوع ویروس ها به سایر سیستم های کامپیوتری میباشد.

دلیل دیگر برترس ازتسری ویروس های کامپیوتری شبکه ارتباطی مدرن امروزه است که موجبات انتقال داده های کامپیوتری راوسیله خطوط تلفن وارتباط ازطریق ماهواره فراهم ساخته است . این خطوط ارتباطی قادر هستند که درهرثانیه میزان بسیارزیادی اطلاعات رابین سازمان های مختلف نقل وانتقال دهند. این نقل و انتقال ها ومشارکت اطلاعات بین دستگاهها خطر تسری ویروس های آسیب زا را بیش از پیش ساخته است .

نگرانی دیگری که این ویروس ها برای مسئولان سازمان هابوجود آورده افزایش بیش از حد میکرو کامپیوترها وافرادی که ازآنها استفاده میکنند میباشد. درحال حاضر میلیون ها نفرازاین میکرو کامپیوترهادرمحل کارخود استفاده میکنند. این افراد قادرهستند که درمحل کارخود ازسیستمی که بطور اختصاصی برای آنها طراحی شده استفاده کرده وازاطلاعات موجود درسازمان بطور اشتراکی استفاده نمایند. درعین حال این افراد قادر هستند که با

کامپیوتر اصلی سازمان (Main Frame) تماس برقرار کرده وبه داده پردازی مشغول شوند. گستردگی نقاط ورودی به کامپیوتر اصلی که نتیجه پراکندگی استفاده کنند گان ازآن میباشد خطر بالقوه ای برای گسترش این ویروس هابداخل سازمان هستند. استفاده کننده های این سیستم ها ممکن است که بدون اطلاع خود به این ویروس ها آلوده شوند. این آلودگی ممکن است ازطریق ارتباط باشبکه محلی Local Area Network (LAN) یك دستگاه ، برنامه کامپیوتری که از " تابلوی اعلانات* " یك کامپیوتر اصلی پیاده شده است وبا از اشتراك یك دیسکت بایك دوست یا همکاراداری ایجاد شود.

باتوجه به اینکه تعداد واقعی حمله این ویروس ها که تاکنون گزارش شده بامقایسه باکل عملیات کامپیوتری که درهر لحظه انجام میشود ناچیز میباشد ، تعداد وقایع تائید شده ظرف چند سال اخیر بطرز سرسام آوری روبه افزایش است . این گسترش بیش ازحد وافزایش دررشد این ویروس هاست که اکثر متخصصین این رشته رانگران میکند. پاره ای ازاین متخصصین معتقد هستند که دفعات واقعی حمله ویروس هابمراتب بیش از میزان گزارش شده آن میباشد. ازدلائلی که برای آن ذکرشده بی میلی سازمانها ازایجاد تبلیغات وجو منفی است که دراثر حمله این ویروس ها برای یك دستگاه ایجادخواهد شد. برای مثال اگر ویروس بدستگاهی که شمادرآن کارمیکنید حمله کند باعث رانده شدن مشتریان وبارآمدن زیانهای مالی

---

* تابلوی اعلانات Bulletin Board به گروهی ازبرنامه ها ویا اطلاعات کامپیوتری اطلاق میشود که بصورت رایگان دراختیار عموم قرارداشته وپیاده کردن ویاکپی کردن ازآنها مستلزم تخطی از قانون حفظ حقوق افرادی که آن برنامه هاواطلاعات رابوجودآورده اند نمیباشد.

فراوان خواهدشد. دراین موارد اطمینان افرادی که بـــا آن سازمان درسروکارهستند سلب شده و سعی میکنند کـــه داد و ستد های خودرا باسازمانهای دیگر انجام دهند. ازطرف دیگـــر چون اکثراین ویروس ها بطور اختصاصی برای یك دستگـــاه طرح میشوند ممکن است باعث شوند که این نوع خاص ویروس به نام سازمان شما معروف شود . (مثلا" ویروس بانك صنعت) صرفنظر از کلیه موارد فوق الذکر ، بسیاری از سازمانهـــا بی میل هستند که اقدامات حفاظتی موجوددرسازمان خودرا افشأ سازند. علت آن واضح است . افشأ این نوع اقدامات حفا ظتی باعث کمك بیشتر به افراد خرابکارمیباشد. این به نوبه خود سبب بازداری سازمانهای مختلف ازاشتراك اقدا مـــات احتیاطی بین خود خواهد بود.

انواع ویروس ها

قبل ازذکر انواع ویروس ها لازم به توضیح است که ویروس هـــا دارای مشخصات زیرهستند:

۱ـ مجموعه ای هستند از دستورالعمل های کامپیوتری
۲ـ قابلیت انتشار دارند
۳ـ قابلیت انجام کارهای غیرمجازدارند
۴ـ بوجودآمدن آن بصورت عمدی است

ویروس هامعمولا" برمبنای ویژه گیهای آنها نام گذاری میشو ند . ویروس ها برنامه های (دستورالعمل) کامپیوتری هستند که موجبـات آلودگی برنامه های عادی کامپیوتری راباکپی کردن خود برروی آنها فراهم میسازند. این عمل کپی کردن و " حمله بخود " بطور مداو م ادامه پیداکرده وازیك برنامه قابل اجرای ساده به دستورالعمل های سیستم عملیاتی (Operating System) ، از یك سیستم کامپیوتری به یك سیستم دیگر ازیك شبکه کامپیوتـــری به یك شبکه دیگر سرایت کرده ودرپایان باعث نابود ی کلیه این سیستم ها میشود . درنهایت این ویروس ها منظور اصلی خود رابـــه

صورت محو کردن کلیه اطلاعات از روی دیسک ثابت (Hard Disk) ، قفل کردن کلیدهای کامپیوتر و یا ارسال پیام های ناخوشایند برآورده میکنند. خطرناک ترین نقطه مشخصه این ویروس ها کپی کردن از روی خودشان است که معمولا" هنگامی شروع میشود که ویروس مطمئن شود وارد سیستم شده وقابلیت زیستن در سیستم راخواهد داشت . ویروس ها معمولا" وجودخود را با ارسال پیامی به اطلاع افرادی که باسیستم سروکاردارند میرساند. نکته قابل تذکر اینست که کلیه ویروس ها جنبه تخریبی نداشته وپاره ای ازآنها جهت محافظت سیستم کامپیوتری (بصورت واکسن) طراحی شده است . برای مثال ممکن است که شمابرای صرفه جوئی درکار برد میزان حافظه موجوددرکامپیوترویروسی راطرح نمائید که باعث شناسائی ونابودکردن ویروس های مضر بشود. پاره ای ازویروس های شناسائی شده عبارتند از :

" کرم " ـ کد (Code) هائی است که به جستجوی ناحیه های خالی (استفاده نشده) حافظه پرداخته وباکپی کردن خودآن ناحیه راپر میکند . هدف اصلی این کرم ها پرکردن کلیه ناحیه های استفاده نشده حافظه کامپیوتری بترتیبی است که ادامه فعالیتهای کامپیوتری راکلا" قطع کرده ودرنهایت باعث نابودی سیستم بشود . وظیفه اصلی کرم فقط کپی کردن مداوم خود میباشد که تفاوت اصلی کرم باسایر ویروس هااست . فرق دیگر کرم باسایر ویروس ها اینست که کرم خط ارتباطی خودرابابرنامه اصلی که درحافظه کامپیوتر قرارگرفته حفظ مینماید.

* " اسب تروپا " ـ برنامه هائی هستند که ظاهرا" عملیات مجاز رااجرامیکنند درحالیکه کد غیرمجازی رادرداخل خود مخفی کرده

---

* این اسم ازداستان قدیمی غربی گرفته شده که سربازان خودرادر داخل شکم اسبی بزرگ مخفی کرده وپس ازاینکه اسب بداخل شهر تروپا انتقال پیداکرد ازتاریکی شب استفاده کرده وشهر راتسخیر کردند.

ودرموقع مناسب بطور غیرمنتظره ضربه کاری خودرا وارد میکنند.
این ضربه بصورت پاك کردن یك پرونده کلی (مانند پرونده لیست حقوق) میباشد . این برنامه ها معمولا" بطرزی نوشته شده اند که تامدت مدیدی بصورت طبیعی دستورالعمل های مورد نظررا اجرا کرده وسپس بمحض یافتن فرصت سیستم تخریبی خودرابه کار می اندازند. ازمشخصات اصلی این نوع ویروس اینست که هیچگاه کپی خودرا ایجاد نمیکنند.

" بمب منطقی " ـ قسمتی از کد تخریبی کامپیوتراست که منطبق بریك واقعه ازقبل پیش بینی شده (مثلا" شب یلداویاچهارشنبه سوری) منفجر میشود. پاره ای ازاین نوع برنامه ها بترتیبی نوشته شده اندکه انفجارآنهامبتنی بر وقوع شرایط غیرمعقول (مثلا" ماه ۳۲ روزه) اتفاق خواهد افتاد.

" دریچه " ـ دریچه ها کد کامپیوتری نبوده وجزگروه ویروسهای اصلی طبقه بندی نمیشوند . درواقعیت " دریچه " ورود غیرمترقبه به داخل سیستم وپرش ازروی اقدامات امنیتی عادی میباشد. این نوع برنامه ها باعث میشود افرادخاطی درشرایطی قرارگیرند که بتوانند بطور نامحدودی ازبرنامه هاوپرونده های موجوددرسیستم استفاده نمایند.درحقیقت این روشی است که توسط آن اشخاص مغرض وارد سیستم شده وپس از داخل کردن ویروس کلیه سیستمها راآلوده مینمایند.

ترکیب کردن روشهای فوق بصورت ایجاد ویروسی واحد باعث میشود که ضربه وارد کردن به سیستم کامپیوتری بطرز موثرتری انجام پذیرد. برای مثال ویروس معمولا" درداخل برنامه ای مخفی شده وبصورت " اسب ترویا" به داخل سیستم راه داده میشود. در غیراینصورت امکان نشراین آلودگیها ازیك استفاده کننده به استفاده کننده دیگر ویاازیك تابلو اعلانات به سایر استفاده کنندگان امکان پذیرنخواهدبود.
ویروس ها اغلب دارای " چاشنی" ای هستند که معمولا" جلب نظر

نکرده وقادرهستند مدت زیادی درسیستم کامپیوتری باقی بمانند .
این چاشنی ها دقیقا" همان بمب های منطقی هستند که منتظرند در صورت یافتن فرصت مناسب کشیده شده و سبب انفجارسیستم را فراهم نمایند. طبقه بندی فوق مانع الجمع نیست و ممکن است که یك ویروس ازیك یاچند خاصیت فوق برخورداراباشد. معذالك شناخت آنها برمبنای خاصیت غالبی است که درآن نوع ویروس به خصوص مشاهده شده است .

چگونگی همه گیرشدن ویروس ها

یکی از منابع بروز ویروس ها دردستکاههای دولتی ویاخصوصی کارمندان ناراضی هستند. این قبیل کارمندان معمولا" چند روز یاچند ساعت پس از دریافت اخطاربه حاکی ازاخراجشان ویاتذکر برای کارهائی که انجام داده اند شروع به عملیات تخریبی مینمایند درپاره ای از موارد مشاهده شده که این قبیل کارمندان باقرارداد یك " بمب منطقی " باعث ازبین بردن هزاران پرونده اطلاعاتی مربوط به فروش ویالیست حقوق شده اند.

سازمانهاباید بمنظور جلوگیری از عواقب ناشی ازاخراج این قبیل کارمندان چند قاعده کلی رامراعات کنند. برای مثال هرگز نباید به کارمندانی که اخراج شده اند امکان دسترسی به مدارك واسنادسازمان داده شود . عملی کردن این سیاست بصورت باطل کردن " اسم رمزی* " این نوع کارمندان ومطلع نمودن مسئولین ازاینکه این کارمندان حق استفاده از سیستم کامپیوتری راندارند امکان پذیرخواهدبود. مرتب گوش بزنگ باشید که آیااین کارمندان ازاسم رمز کارمندان دیگر استفاده میکنند یاخیر ؟ درصورت یافتن

---

* اسم رمز معمولا" کلمه ویاشماره هائی‌است که بطور اختصاصی به افراد واگذارشده وآنهاراقادرمیسازد که بتوانند به آزادی واردسیستم کامپیوتری شوند. درعمل معادل داشتن کلید برای وارد شدن به محل کاریامنزل میباشد.

پاسخ مثبت به این سئوال فورا" اسم رمز این نوع کارمندان راعوض کرده وبه آنها گوشزد نمائید که ازاسم رمزخود مراقبت کافی بعمل آورند.

کارمندان صادق خطرناك ترین نوع تهدید برای یك سازمان هستند ! این خطر معمولا" بصورت آوردن یك برنامه کامپیوتری شخصی به محل کار بروز میکند. این نوع برنامه ها معمولا"ازنوع پیچیده وتخصصی نبوده ودرنتیجه اگرویروسی درآنهاوجودداشته باشد بمجرد تماس باکامپیوترهاویاترمینال های سازمان منجر به سرایت به سایر کامپیوترهامیشود. واضح است که این نوع کارمندان بیگناه ازاین خطر اطلاع نداشته وبدون توجه بانسخه گرفتن یك برنامه از روی یك تابلوی اعلانات سبب تسری ویروس بداخل سازمان میشوند. دربسیاری ازموارد ممکن است که این همکارمدت مدیدی ازاین برنامه استفاده میکرده وتصادفا" نسخه جدیدی ازاین برنامه را(که تصادفا" آلوده نیز میباشد) دریك تابلوی اعلانات پیدا کرده که بمجرد نسخه گرفتن با عث پاك شدن نسخه قبلی خودشده وپس ازاین عمل باعث عفونت زدگی برنامه خود میشود.

مسئله مهم اینست که آیاکارکنان میتوانند نرم افزارهای خودرابه محل کاربیاورند ویاباید طبق دستورالعملی ازورودآنهابمحل کار جلوگیری بعمل آید. دلیل بروقوع این امر اینست که بسیاری از کارکنان کارآئی بمراتب بیشتری ازخود نشان میدهند درصورتیکه قادرباشند درمحیط قابل انعطافی فعالیت نمایند. دراینجا مشکل مدیریت اینست که باید بین دوعامل مختلف یعنی کارآئی کارکنان وخطر آلودگی سیستم های کامپیوتری یکی راانتخاب نماید. بسیاری ازسازمان ها بهیچوجه به کارمندان خود اجازه نمیدهند که نرم افزارهای کامپیوتری خودرابه محل کاربیاورند. درحالیکه پارهٔ از شرکتها راه عملی تررابرگزیده وازکارکنان خود میخواهند که اولا" نرم افزارهای خودراقبل ازاستفاده حتما" ازقرنطینه ای که به این منظورایجاد شده بگذرانند ثانیا" فقط ازنرم افزارهای به ثبت رسیده استفاده کرده وثالثا" ازآوردن نرم افزارهائیکه ازروی تابلو

اعلانات کپی شده به محل کارخودداری نمایند. دربسیاری ازموارد مشاهده شده که کارکنان مجاز هستند که فقط اطلاعات (داده های) کامپیوتری خودرابه محل کارآورده ومجاز نیستند که برنامه های کامپیوتری به محل کاربیاورند. درپاره ای ازسازمانهامشاهده میشود که پرونده های مربوط به " داده ها " وبرنامه های کامپیوتری بصورت مجزا از یکدیگر نگهداری میشود. درحالتهای دیگر مشاهده شده که ویروس ها بطور تصادفی وارد برنامه هائی شده اند که بصورت مجازدربازاربفروش میرسند. برای جلوگیری ازاین خطرات لازم است که نرم افزارهای خودراازفروشندگان معتبر خریداری کرده وپس از ابتیاع مطمئن شوید که لاك ومهربسته آن قبلا " دست نخورده باشد.

●

چگونه سلامت سیستم کامپیوتری خود راتامین کنید ؟

جهت جلوگیری ازبروز وقایع ناگوارناشی ازویروس ها راه های مختلفی وجوددارد ولی متاسفانه هیچکدام محفوظ از خطا نمیباشد. اگر چه امکان دفع کامل حمله ویروس هاوجودندارد معذالك اقدامات احتیاطی که توسط یك سازمان میشود سبب کاهش بروز این حمله ها میگردد.

یکی از مهمترین اقداماتی که باید انجام گیرد ایجادسیاستی واحد برای یك دستگاه ویاگروه صنعتی واشاعه این سیاست بین کارکنان میباشد. این اقدامات باید ازحمایت کامل مدیریت برخورداربوده وعواقب تخطی ازآن تعیین وبه اطلاع کارمندان برسد. موارد زیر بصورت پیشنهادی ارائه شده است :

۱- مجاز نبودن ارتهیه نسخه ازبرنامه هائی که درروی تابلوی اعلانات قراردارد. اگربرنامه مفیدی درروی این تابلوی اعلانات پیداشد باید مطمئن شد که از قرنطینه گذشته وبدون ویروس وارد سازمان بشود. قسمت قرنطینه باید مطمئن شود که این برنامه بطور دقیق مورد آزمایش قرارگرفته وارکپی کردن آن بروی دیسك های ثابت خودداری شود. ضمنا" قراردادن این نوع برنامه ها بر روی شبکه

محلی غیرمجاز اعلان شود.

۲ـ ایجاد سیاست روشن در رابطه باهمراه آوردن نرم افزارهاو پرونده اطلاعات (" داده ها) به محل کار. همانطور که قبلا ذکر شدتدوین این سیاست باید باتوجه به کارآئی کارکنان واثر منفی آن بر روی روحیه کارمندان انجام پذیرد.

۳ـ ایجاد رویه خاص جهت جلوگیری ازنوشتن بر روی برنامه های اجرائی موجود. دراین حالت کلیه برنامه ها درپرونده هائی ضبط میشود که فقط " قابل خواندن * " هستند وامکان نوشتن روی آن پرونده هاوجودندارد.

۴ـ درهنگامی که ازمنابع کامپیوتری دیگران استفاده میشود کارمندان باید مطمئن شوند که ازبرنامه های " اجرائی " استفاده نکرده وفقط مجاز به استفاده ازپرونده های اطلاعاتی (داده ها) باشند.تجربیات گذشته نشان داده که امکان فساد داده ها بمراتب کمتر از فساد برنامه های قابل اجرامیباشد.

۵ـ درهنگام استفاده ازیك میکروکامپیوتر حتما" قبل از استفاده آن راخاموش نمایند. عمل خاموش کردن باعث تمیز شدن حافظه میشود که درنتیجه ویروس هائی که بطور احتمالی درسیستم حافظه مرکزی کامپیوتر ازبرنامه های قبلی باقیمانده باشند ازبین خواهند رفت.

۶ـ میکروکامپیوترها فقط بادیسکت هائی روشن شوند که بطور اختصاصی برای کارمندان تهیه شده است. این رویه باعث خواهد شد که فقط سیستم عملیاتی (Operating System)مجاز وارد کامپیوتر شود.

---

* نرم افزارهادراثر خواندن ازبین نرفته وآلوده نمیشوند. عمل نوشتن بر روی این برنامه هاویانرم افزارهاست که سبب تخریب وآلودگی ویا ازبین بردن کلی آنها میشود.

۷ـ سیستم های کامپیوتری چه بصورت " فیزیکی " وچه بصورت " منطقی " مورد محافظت قرارگیرند. قفل کردن میکروکامپیوترها ازاستفاده غیرمجاز آنها جلوگیری خواهد نمود. همچنین ایجاد اسم رمز برای بکاربردن برنامه های موجود باعث خواهدشدکه افرادغیر مجاز قادربه دسترسی به آنها نباشند.

۸ـ نصب برنامه های ضد ویروس برروی کامپیوترها. این نوع برنامه ها معمولا" قادرهستند وقایع ناگوار را(مثلا" پاک کردن کامل دیسک ثابت) اعلان نمایند.

۹ـ تهیه نسخ متعدد ازپرونده های اطلاعاتی وبرنامه های موجود دریک سازمان . این نسخه ها معمولا" درمکان امن مثل گاوصندوق نگهداری میشوند. این رویه سبب بازسازی کلیه پرونده های ازبین رفته میشود.

خلاصه

ویروس های کامپیوتری مجموعه دستورالعمل های کامپیوتری هستند که بسادگی ازیک کامپیوتریادیسک به یک کامپیوتر یادیسک دیگر انتقال پیداکرده وباانجام کارهای غیرمجاز باعث تخریب وآلودگی سیستم میگردند. حسابداران وحسابرسان بخصوص آندسته ازحسابرسان که باکامپیوترسروکاردارند باید بااین نوع ویروس ها آشنائی کامل داشته باشند. فقط دراین صورت حسابرسان قادر خواهندبود توصیه های خودرادرخصوص سیستم کنترلهای داخلی وحفظ تمامیت این نوع سیستم ها به مشتریان خود بنمایند. البته باکامپیوتری شدن کلیه سیستم های مالی واطلاعاتی کلیه حسابداران ناگزیر خواهند بود که خودرابااین بلای تکنولوژی آشناساخته ودرصورت لزوم باآن مبارزه نمایند●