بخش دوم

نگاهی به جایگاه امنیت در فناوری اطلاعات و شیوه‌های جدید جاسوسی

خرابکارها اجازه نمی‌گیرند

سعید نوری‌آزاد

برای این‌که حدود خطرپذیری دنیای رایانه را بدانید، چند نمونه را یادآور می‌شویم. با تمام شاخص‌گذاری‌ها و نظارت‌ها بر آثار درونی و بیرونی، محیط دیجیتال در تمام انواع فناوری‌ها و در لایه‌های مختلف دسترسی، می‌تواند مورد استفاده‌های نامطلوبی نیز قرار گیرد.

ریز ابزارهای جاسوسی

امروزه بدافزارها (Spyware) به یکی از مهم‌ترین و جهانی‌ترین تهدیدهای اینترنتی تبدیل شده‌اند. آمار به‌دست آمده توسط شرکت‌های Earthlink و Webroot که در گزارش مشترک آن‌ها در وب سایت مشترک‌شان منتشر شده، نشان می‌دهد که ۹۰درصد کامپیوترهای جهان آلوده به بدافزار هستند (البته این به‌معنای قابل استفاده‌بودن این سیستم‌ها توسط جاسوسان نیست، مانند این‌که همه ما در بدن خود میکروب‌هایی داریم اما آن‌ها همیشه دردسرساز نیستند). هکرها و نفوذگران برای انتشار بدافزارها هر روز از روش‌های جدیدتری استفاده می‌کنند.

علایم وجود بدافزار در یک سیستم را در مجموع این‌گونه می‌توان برشمرد: بیشتر افراد فکر می‌کنند بدافزارها جاسوس‌هایی هستند که تنها اطلاعات مربوط به علایق کاربر در اینترنت را سرقت می‌کنند، در حالی‌که این بدافزارها علاوه بر جاسوسی، بابه‌کارگیری منابع سیستم، باعث کندی آن نیز می‌شوند و حتی می‌توانند باعث ناسازگاری برنامه‌های مختلف با هم شوند. مهم‌ترین مشکلاتی که یک بدافزار برای یک سیستم آلوده ایجاد می‌کند عبارتند از: کندی غیرعادی سیستم، بی‌ثباتی سیستم، کندی ارتباط اینترنتی و دریافت تعداد زیادی هرزنامه.

اما درکل بدافزار یک نام کلی برای برنامه‌هایی است که رفتارهای مشخص انجام می‌دهند؛ مثل نمایش آگهی‌های تبلیغاتی، جمع‌آوری اطلاعات شخصی یا تغییر تنظیمات کامپیوتر شما که معمولا بدون کسب مجوز اجرا می‌شوند. ممکن است نرم‌افزارهای ناخواسته یا بدافزار در کامپیوتر خود داشته باشید که امنیت اطلاعات موجود در کامپیوتر شما را تهدید کند. البته این بدان معنا نیست که هر آگهی تبلیغاتی یا هر نرم‌افزاری مخرب است. به‌عنوان مثال، شما برای دریافت فایل‌های موسیقی در یک سایت، فرم ثبت‌نام را پر می‌کنید، اما برای دریافت سرویس‌های مختلف این سایت مجبور به دریافت آگهی‌های تبلیغاتی نیز هستید. اگر موقع نصب با همه موارد توافق کنید، پس باید قبول کنید که امکان فرستادن آگهی به کامپیوتر شما هم وجود دارد و شما اجازه داده‌اید که آن سایت فعالیت‌های شما را زمانی که در اینترنت هستید، پیگیری کند.

تقلب به‌دلیل ناآگاهی

اسکم (Scam) یا کلک‌های بی‌شماری وجود دارند که به‌تازگی در اینترنت و در تلویزیون‌های ماهواره‌ای کاربران ساده‌دل سراسر دنیا را هدف قرار داده، آن‌ها را فریب می‌دهند و جیب‌شان را خالی می‌کنند و تلفن‌ها و ایمیل‌های اعتراضی فریب‌خوردگان را هم جواب نمی‌دهند. این سایت‌ها که در ظاهر از طرف سایت‌های معتبری مانند گوگل یا توییتر پشتیبانی می‌شوند، در حقیقت به هیچ‌یک از آن‌ها تعلق ندارند و تنها با ایجاد شکلی شبیه آن‌ها از اطلاعات کم افراد استفاده و به‌نوعی کلاه‌برداری اقدام می‌کنند. البته علت این‌که بیشتر شکایت‌ها نیز به‌ثمر نمی‌رسد این است که فرد هنگام ثبت‌نام user agreementها را تایید کرده است. این مرحله همان مرحله‌ای است که تقریبا همه کاربران هنگام ورود به سایت‌ها تنها با زدن کلید تاییدآن‌ها را می‌پذیرند و متنشان را نمی‌خوانند.

این شکل از سرقت و کلاه‌برداری می‌تواند شیوه‌های زیادی را در آستین داشته باشد، پس بدون ذکر انواع آن‌ها توصیه می‌کنیم به شرکت‌هایی که در کشور شما نام و دفتر ثبت شده ندارند، چیزی پرداخت نکنید و هنگام پرداخت نیز رسید رسمی دریافت کنید و علاوه بر این‌ها، از یکی دو نفر از دوستان خود نیز برای پرداخت‌های زیاد مشورت بگیرید. روش دیگری هم که بسیاری از سایت‌های معتبر و غیرمعتبر به‌کار می‌برند، درخواست از شما برای واردکردن پسورد و شناسه ایمیل خود در سایت است. این روش که بیشتر در سایت‌های دوستیابی و شبکه‌های اجتماعی دیده می‌شود، می‌تواند به تمام محتوای نامه‌های ارسالی و دریافتی شما دسترسی پیدا کند. سایت‌هایی مانند فیس‌بوک، اعلام می‌کنند اطلاعات شما را ذخیره نمی‌کنند، اما باید مراقب باشید، چون به‌این گفته‌ها نمی‌شود اعتماد کرد.

عکس: tzimg.com

به این چند توصیه کوتاه که می‌تواند کمک خوبی برای شما باشد، توجه کنید: از یک نرم‌افزار ضدویروس و ضدجاسوسی معتبر استفاده کنید (از نسخه کرک‌شده آن‌ها استفاده نکنید) ضدویروس‌هایی مانند Kaspersky و Nod32 هم‌اکنون در کشور ما به‌صورت رسمی فروخته می‌شوند. پسورد خود را هیچ‌جا غیر از صفحه اصلی سایت اصلی خود وارد نکنید. از یک مرورگر امن مانند فایرفاکس استفاده کنید. سیستم‌عامل و نرم‌افزارهای خود را به‌روز نگه دارید. اطلاعات خصوصی خود را با احتیاط بیشتری انتقال دهید. با لینوکس امنیت شبکه‌های خود را به‌دست بگیرید. یکی از بزرگ‌ترین دغدغه‌های مدیران شرکت‌ها نداشتن دانش کافی برای اطلاع از چگونگی وضعیت امنیتی شبکه داخلی اداره و سازمان است. در بیشتر مواقع، مدیران شرکت‌ها مجبور هستند اطلاعات حساس خود را در اختیار مدیران شبکه قرار دهند که این می‌تواند باعث اشکالاتی برای امنیت شبکه شود. از طرفی متخصصان شبکه باید در سطح کارشناس باشند که به‌نوعی به تافته جدابافته ادارات تبدیل می‌شوند. از جمله مشکلات این کار نیز ترک کار پرسنل امنیتی شبکه‌هاست که می‌تواند خسارت‌های جبران‌ناپذیری به امنیت اطلاعات شرکت‌ها بزند. در حقیقت اداره‌کردن امنیت شبکه به داشتن اطلاعات بسیار زیاد فنی و توانایی اجرای آن با استفاده از خط فرمان‌های پیچیده نیاز دارد که مشکل اصلی مدیران است.

اما یک شرکت آلمانی که به‌طور انحصاری حفاظت از بیشتر شبکه‌های دولتی کشورهای آلمان و ایتالیا را در اختیار دارد، دست به ابداع روش جالبی زده تا براساس آن مدیران اصلی شرکت‌ها بی‌نیاز از متخصصان شبکه، بتوانند امنیت اصلی‌ترین بخش از شبکه، یعنی دیواره‌های آتش را نیز خود برعهده بگیرند.

این شرکت با استفاده از هسته سیستم‌عامل لینوکس در داخل UTMهای خود توانسته یک رابط گرافیکی بسیار ساده را طراحی کند که تنها با چند ساعت آموزش، امکان مدیریت آن برای یک فرد با اطلاعات اولیه رایانه ممکن می‌شود. در این سیستم که توانایی کشف بیشترین مقدار حملات را دارد، جزییات فنی حذف شده و تنظیمات به‌دلخواه تغییرپذیر است. این شرکت در سایت رسمی خود اعلام کرده است که به مشتریان خود به‌طور کتبی گواهی می‌دهد که سیستم‌های تحت لیسانس آن درهای مخفی ندارد که این امکان برای محصولات شرکت‌هایی مانند سیسکو موجود نیست.

منابع

IT Security: Risking the Corporation, by Linda McCarthy,(Prentice Hall PTR: NJ, 2003).
http://digitalrevolution.bbc.com|
http://www.gateprotect.com/

ادامه از صفحه ۱۰

کمبود چارچوب قانونی مناسب در حوزه اطلاعات و امنیت زیرساختار و جرم‌های فضای الکترونیکی، کشورهای در حال توسعه را تهدید می‌کند و باعث عدم استفاده از فرصت‌های تجارت الکترونیکی می‌شود. اگر پشتیبانی مناسب قانونی برای تولیدکنندگان و مصرف کنندگان وجود نداشته باشد؛ آن‌ها با ریسک‌های تجارت الکترونیکی انطباق نمی‌یابند. طبق گزارش UNCTAD، موارد قانونی در ۸۵درصد کشورهای توسعه یافته و ۴۱درصد کشورهای روبه‌توسعه، از جمله استراتژی‌های اصلی است.

مانع مهم تجارت الکترونیکی در ایران، سرعت کم و هزینه زیاد دسترسی به اینترنت است. برای کشورهای روبه‌توسعه، توجه اصلی به فراهم‌سازی روش دسترسی آسان به اینترنت با سرعت بالا، امن و ارزان است. دسترسی به اینترنت در کشورها، دسترسی به اطلاعات قیمت کالاها و خدمات، ایجاد فرصت‌های جدید، دسترسی به‌آموزش، دانش و سلامت برای عموم را باعث می‌شود. برای فهم نتایج و روش‌شناسی پیاده‌سازی تجارت الکترونیکی، وزارت بازرگانی، مطالعه امکان‌سنجی تجارت الکترونیکی را انجام داده است. این پروژه با هدف مشخص کردن حالت موجود و مطلوب، تحلیل و تعیین نقشه‌راه برای تحقق حالت مطلوب در تجارت الکترونیکی ایران، تعریف شده است.

تامین خدمات مالی به‌مفهوم فراهم‌سازی خدمات مالی و بازار با استفاده از ابزارهای الکترونیکی است. اعتماد و اطمینان مصرف کنندگان به اینترنت و امنیت خدمات مالی الکترونیکی بسیار پایین است. شرکت‌هایی که هویت‌شناسی مناسبی ندارند، آسیب‌پذیر هستند. کشورهای صنعتی توسعه یافته، در پرداخت الکترونیکی، بانکداری الکترونیکی، بیمه الکترونیکی و تبادل الکترونیکی سهام، سرمایه‌گذاری زیادی کرده‌اند. بدون توجه به تامین مالی الکترونیکی، توسعه تجارت الکترونیکی محقق نخواهد شد. بانک‌های ایران، عضو شتاب هستند. بانک‌ها در ایران، دستگاه‌های خودپرداز و کارت‌خوان را در شعبه‌هایشان فراهم کرده‌اند. آن‌ها اقدام به الکترونیکی کردن بسیاری از خدمات کرده‌اند؛ هرچند که بانکداری در ایران با حالت مطلوب مورد انتظار فاصله بسیار دارد.

دولت الکترونیکی به‌معنای استفاده از نهادهای دولت از فناوری اطلاعات و ارتباط با شهروندان، کسب‌وکارها و سایر نهادهای دولت، به‌صورت الکترونیکی است که شامل مواردی مانند تحویل بهتر خدمات دولت به شهروندان، بهبود تعامل با کسب و کارها و صنعت، تقویت شهروندان از طریق دسترسی به اطلاعات و مدیریت کاراتر دولت می‌شود.

وزارت بازرگانی برای توسعه و نفوذ تجارت الکترونیکی، فعالیت‌هایی را شبیه‌سازی کرده‌است. فعالیت‌های اصلی شامل مواردی مانند ارائه جوایز به‌سازمان‌ها، پروژه‌ها، مقالات و کتاب‌های برتر است.

منابع

[1] Abbasi, A. (2008), "A strategic plan for e-commerce development in Iran", IEEE Computer Society. P. 32 41.
[2] "The national report on e-commerce in Iran 2004", E-Commerce Development Office, Document No 84/581, 2005.
[3] "Overview of e-commerce in Iran", 2006, Available in: http://www.ebusinessforum.com

پی‌نوشت‌ها

1. McConnel
2. United Nations Conference on Trade and Development
3. Forrester
4. Business to Business
5. International Telecommunications Union