یک حفاظ امنیتی کامل برای کامپیوتر

ساخت یک دیوار آهنین برای مقابله با انواع تهدیدها

یک کامپیوتر جدید برای صاحبش، دنیایی جدید از امکانات حرفه‌ای، سرگرمی، و ارتباطات است. اما اگر دروازه‌های این کامپیوتر باز باشد همین کامپیوتر می‌تواند مورد سوءاستفادهٔ **نفوذیها** (**هکرها**) قرار بگیرد و تهدیدهای فراوانی را به وجود بیاورد.

تهدیدها چنان گسترده هستند که حفظ امنیت کامپیوتر به انواعی از اقدامات و برنامه‌های حفاظتی نیاز دارد.

سه خاکریز حفاظتی

برای امنیت کافی کامپیوتر، دست‌کم سه خاکریز حفاظتی باید ایجاد کرد. سد اول را روزآمدسازیهای ویندوز، یک **نرم‌افزار ضدویروس**، و یک **نرم‌افزار دیوارهٔ آتش** (firewall) به وجود می‌آورند. این سه خط دفاعی در مجموع می‌توانند **حفره‌های** ویندوز را ببندند، و از ورود ویروس، کرم، **اسب تروا**، و سایر کدهای زیان‌آور جلوگیری کنند. اینها یک هستهٔ امنیتی برای کامپیوتر به وجود می‌آورند و اکثر حملات خطرناک شناخته شده را دفع می‌کنند.

خاکریز دوم باید شامل برنامه‌های **ضدجاسوسی** (antispyware) و بررسی‌کننده‌های ویژهٔ **تروا** (Trojan) باشد که کامپیوتر را در برابر برنامه‌های جاسوسی، تبلیغاتی، **شماره‌گیر** (dialer)، و اسبهای ترویایی محافظت می‌کنند که ممکن است از دید برنامهٔ ضدویروس پنهان شوند.

خاکریز سوم می‌تواند شامل برنامه‌های محافظ **کلمهٔ عبور** (password)، **مسدودسازی پاپ-آپ** (pop-up blocker)، نرم‌افزار **رمزنگاری** فایل، نرم‌افزار حذف‌کنندهٔ فایل (file eraser)، و سایر برنامه‌هایی باشد که امنیت کامپیوتر را کامل می‌کنند.

برای کسانی که به تازگی یک کامپیوتر خریده‌اند، توجه فوری باید روی خاکریز اول معطوف باشد چون حضور چنین سدی نگرانیهای فوری در مورد تهدیدهای جدی را برطرف می‌سازد و به شما فرصت می‌دهد که سدهای تکمیلی را برپا کنید. بدین معنی که پیش از آن که حتی فکر ارسال یک ایمیل به دوستان خود یا فکر گشت‌زنی در اینترنت را بکنید، لازم است که یک برنامهٔ دیوارهٔ آتش و یک ضدویروس در کامپیوتر خود نصب کنید و ویندوز خود را **روزآمد** (update) کنید.

اقدامات اساسی دیگر

پیش از روزآمدسازیهای امنیتی و نصب نرم‌افزار جدید، بهتر است ابتدا یک **نقطهٔ بازگردانی** (restore point) بسازید تا در صورت برخورد با یک مسئله در مسیر ساخت سدهای امنیتی، بتوانید سیستم خود را به سرعت به حالت سالم اولیه بازگردانی کنید. در منوی Start، روی Help And Support کلیک کنید، روی گزینهٔ زیر کلیک کنید:

Undo Changes To Your Computer With System Restore

گزینهٔ Create A Restore Point را انتخاب کنید، روی Next کلیک کنید، و دستورالعملهای ساخت یک نقطهٔ بازگردانی را به اجرا درآورید.

همچنین، اطمینان یابید که **کلمهٔ عبور** Administrator _که در زمان برپاسازی کامپیوتر جدید خود ساخته‌اید_ یک کلمهٔ عبور قدرتمند است. برای تغییر دادن کلمهٔ عبور Administrator یا کلمه‌های عبور مربوط به حسابهای کاربری دیگر، به Control Panel بروید، روی User Accounts کلیک کنید، روی حساب موردنظر کلیک کنید، و روی Change My Password کلیک کنید.

پیش از آن که به اینترنت وصل شوید، باید برنامهٔ دیوارهٔ آتش همراه شده با ویندوز را فعال کنید؛ هرچند، اگر ویندوز اکس‌پی شما شامل SP2 (سرویس‌پک۲) باشد دیوارهٔ آتش از قبل فعال شده است. اگر SP2 را ندارید، گزینه‌ای را برای فعال کردن Internet Connection Firewall به هنگام پیکربندی ارتباط اینترنت خود خواهید دید. برای اطلاعات بیشتر به پایگاه وب زیر سربزنید:

www.microsoft.com/windowsxp/using/networking/learnmore/icf.mspx

در بعضی از کامپیوترهای جدید، سازنده یک نرم‌افزار اضافی دیوارهٔ آتش نصب می‌کند. اگر با کار با این نرم‌افزار دیوارهٔ آتش آشنا باشید و بتوانید بفهمید که فعال است و به درستی پیکربندی شده است، دیوارهٔ آتش توکار ویندوز را غیرفعال کنید؛ در غیر این صورت، دیوارهٔ آتش ویندوز را فعال کنید. همچنین، اگردستگاه **مسیریاب** (router) یا **مودم باند عریض** شما حاوی یک دیوارهٔ آتش سخت‌افزاری باشد، بازهم به دیوارهٔ آتش ویندوز یا دیوارهٔ آتش نرم‌افزاری دیگر نیاز خواهید داشت؛ بعداً در این باره بیشتر توضیح خواهیم داد.

پیش از وصل شدن به اینترنت، بهتر است نوعی نرم‌افزار ضدویروس را در کامپیوتر خود نصب کرده باشید. اگر کامپیوتر جدید شما حاوی نرم‌افزار ضدویروس باشد، از آن استفاده کنید؛ اگر نداشته باشد، و از طریق یک کامپیوتر دیگر به اینترنت دسترسی دارید، یک برنامهٔ ضدویروس رایگان را از اینترنت دریافت کنید، آن را در یک سی‌دی ضبط کنید، و آن را بر روی کامپیوتر جدید خود نصب کنید. اگر کامپیوتر جدید شما حاوی نرم‌افزار ضدویروس نباشد و از طریق یک کامپیوتر دیگر به وب دسترسی ندارید، بلافاصله بعد از نصب نرم‌افزار روزآمدکنندهٔ ویندوز، یک برنامهٔ ضدویروس رایگان از اینترنت دریافت و نصب کنید.

حال که دیوارهٔ آتش و برنامهٔ ضدویروس خود را برپا کرده‌اید، موقع رفتن به پایگاه Windows Update برای دریافت و نصب روزآمدکننده‌های با ارجحیت بالا است. اکثر کامپیوترهایی که امروزه به فروش می‌رسند حاوی ویندوز اکس‌پی با SP2 هستند. SP2 یک مجموعه از وصله‌هایی است که بسیاری از **حفره‌های** خطرناک ویندوز اکس‌پی را پرمی‌کند –اما نه همهٔ آنها را؛ در نتیجه، بازهم لازم است که آخرین روزآمدکننده‌های با ارجحیت بالا را از پایگاه وب مایکروسافت دریافت و نصب کنید. اگر کامپیوتر شما SP2 را ندارد، لازم است یک سی‌دی ویندوز SP2 بخرید و آن را نصب کنید، و بعد به پایگاه Windows Update بروید و آخرین وصله‌های مهم را دریافت و نصب کنید.

روی Start کلیک کنید، روی Help And Support کلیک کنید، و روی گزینهٔ زیر تحت Pick A Task کلیک کنید:

Keep Your Computer Up-To-Date With Windows Update

(اگر از یک دیوارهٔ آتش به جز دیوارهٔ آتش ویندوز بهره می‌گیرید، لازم است به این برنامه دستور بدهید که به Windows Update اجازهٔ دسترسی اینترنت را بدهد.) تحت عنوان Keep Your Computer Up-To-Date، روی Express کلیک کنید تا روزآمدکننده‌های با ارجحیت بالا را دریافت کنید، و سپس دستورالعملها را برای نصب آنها دنبال کنید. اگر SP2 را نصب نکرده باشید، ابتدا SP2 را نصب کنید و بعد به پایگاه Windows Update بروید.

پس از آن که همهٔ روزآمدکننده‌های با ارجحیت بالای ویندوز را نصب کردید، باید برنامهٔ ضدویروس و برنامهٔ دیوارهٔ آتش (اگر مستقل از ویندوز باشد) خود را روزآمد کنید.

برنامه‌های دیوارهٔ آتش مستقل از ویندوز هم داده‌های ورودی و هم داده‌های خروجی از کامپیوتر را زیرنظر می‌گیرند، و یک حفاظت کامل را فراهم می‌سازند. پس از نصب و روزآمدسازی دیوارهٔ آتش جدید خود، لازم است که دیوارهٔ آتش ویندوز را در Security Center (واقع در Control Panel) غیرفعال کنید. ویندوز می‌تواند اکثر دیواره‌های آتش را شناسایی کند، اما اگر ویندوز به اشتباه به شما هشدار بدهد که یک برنامهٔ دیوارهٔ آتش نصب نشده است (با آن که نصب شده است)، می‌توانید به ویندوز دستور بدهید که دیوارهٔ آتش شما را زیرنظر نگیرد، و بدین وسیله هشدارهای پیوستهٔ ویندوز را حذف کنید. برای این کار، به پنجرهٔ Windows Security Center بروید، روی Recommendations تحت Firewall کلیک کنید، گزینهٔ زیر را انتخاب کنید:

I Have A Firewall That I'll Monitor Myself

و بعد روی OK کلیک کنید.

پنجرهٔ Windows Security Center همچنین حاوی گزینه‌هایی برای زیرنظر گرفتن حفاظت ویروسی و روزآمدسازیهای خودکار است. تنظیم Automatic Updates باید همیشه فعال باشد، اما می‌توانید یکی از موارد زیر را انتخاب کنید: اجازه به ویندوز برای دریافت و نصب خودکار وصله‌های روزآمدسازی، دریافت وصله‌های روزآمدسازی با امکان نصب آنها به انتخاب خودتان، یا صرفاً اطلاع دادن حضور وصله‌های روزآمدسازی به شما.

جلوی جاسوسها را بگیرید

حال که ویندوز خود را روزآمد کرده‌اید، و نرم‌افزارهای ضدویروس و دیوارهٔ آتش خود را نصب کرده‌اید می‌توانید با آرامش نفسی بکشید،

اما فقط برای چند لحظه. پیش از وصل شدن به اینترنت و گشت‌زنی در وب، باید خودتان را در برابر نوع دیگری از **آزارافزار** (malware)، شامل برنامه‌های جاسوسی، که می‌توانند کامپیوتر شما را در عرض چند دقیقه آلوده کنند، و سایر تهدیدهایی که نرم‌افزار ضدویروس از مقابله با آنها عاجز هستند محافظت کنید.

در حال حاضر تعدادی نرم‌افزار جامع امنیتی پرطرفدار وجود دارد که حاوی برنامهٔ ضدجاسوسی هستند. در نتیجه، اگر روی کامپیوتر جدیدتان از قبل یک برنامهٔ جامع امنیتی نصب شده باشد، لازم است حتماً از به روز بودن بخش ضدجاسوسی آن اطمینان یابید، و به طور منظم این بخش را به اجرا درآورید و از آلوده نبودن کامپیوترتان به برنامه‌های جاسوسی مطمئن شوید. استفاده از چند برنامهٔ ضدجاسوسی در یک کامپیوتر، برخلاف برنامه‌های ضدویروس و دیوارهٔ آتش، که اگر به طور همزمان چند تا از آنها در حال استفاده باشد با هم تداخل پیدا می‌کنند، مفید است. با آن که بعضی از برنامه‌های ضدجاسوسی بهتر از بقیه عمل می‌کنند و تعداد زیادی از برنامه‌های جاسوسی را می‌توانند شناسایی و نابود کنند، هیچ کدام از آنها ضمانت نمی‌کنند که بتوانند **همهٔ تهدیدهای ممکن** را شناسایی کنند.

چند برنامهٔ ضدجاسوسی رایگان و کارآمد وجود دارد که می‌توانید آنها را از اینترنت دریافت و نصب کنید. اما به خاطر بسپارید که این برنامه‌ها نمی‌توانند جلوی آلودگی به برنامه‌های جاسوسی را بگیرند؛ بلکه، آنها پس از آلوده شدن کامپیوتر می‌توانند برنامهٔ جاسوسی را از کامپیوتر حذف کنند. برای جلوگیری از آلودگی به برنامه‌های جاسوسی، استفاده از برنامه‌ای چون SpywareBlaster را درنظر بگیرید که پیش از آن که برنامه‌های جاسوسی بتوانند خودشان را در کامپیوتر شما نصب کنند جلوی ورود آنها را می‌گیرد:

www.javacoolsoftware.com

علاوه بر برنامه‌های ضدجاسوسی، باید یک برنامهٔ بررسی‌کنندهٔ ویژهٔ تروا (Trojan) نیز داشته باشید که می‌تواند آزارافزارهایی را شناسایی و نابود کند که برنامه‌های ضدویروس همیشه نمی‌توانند آنها را شناسایی کنند. در این بخش، برنامهٔ رایگان کمتر پیدا می‌شود، اما نگارش رایگان Ewido Anti Malware عمل حذف تروا‌ها، **ثبت‌کننده‌های کلیدزنی** (keylogger)، کرمها، **شماره‌گیرها** (dialer)، و حتی بعضی از برنامه‌های جاسوسی و گروگان‌گیر را به خوبی انجام می‌دهد:

www.ewido.net

یک دیوار آهنین

حال، کامپیوتر جدید شما باید امکان دفع بدترین حملات را داشته باشد، چون از اکثر نقاط آسیب‌پذیر حفاظت به عمل آورده‌اید. با وجود این، چند نقطهٔ دیگر وجود دارد که آسیب‌پذیرند و باید حفاظت شوند تا حریم خصوصی شما حفظ شود و یک دیوار آهنین در برابر خطرات مختلف به وجود آید.

برنامه‌های **مسدودساز پاپ-آپ** (pop-up blocker)، مانند آنها که در نوارابزارهای گوگل و یاهو یا برنامه‌های مرورگر فایرفاکس و اپرا وجود دارد می‌توانند آگهیهای آزاردهنده را حذف کنند و از این که به طور تصادفی روی یک لینک ریسک‌دار کلیک کنید جلوگیری کنند.

همچنین یک **برنامهٔ مدیریت کلمهٔ عبور** مانند برنامهٔ رایگان Password Safe نیز سودمند است. این برنامه‌ها می‌توانند همهٔ کلمه‌های عبور شما را در یک بانک اطلاعاتی رمزی‌شده نگهداری کنند که آنها را با یک کلید می‌توانید دستیابی کنید. به طور مشابه، یک **برنامهٔ رمزنگاری فایل** مانند برنامهٔ رایگان AxCrypt می‌تواند داده‌های حساس شما را از چشمان نامحرمان حفظ کند. نشانی پایگاه وب دو برنامهٔ فوق به ترتیب به قرار زیر است:

http://passwordsafe.sourceforge.net

http://axcrypt.axantum.com

حذف مطمئن فایل نیز برای کامپیوتر جدید شما مهم است، چون شما فایلها را به Recycle Bin انتقال می‌دهید و آن را تخلیه می‌کنید، اما این فایلها همچنان بر روی دیسک سخت باقی می‌مانند و می‌توانند با استفاده از برنامه‌های خاصی بازیابی شوند. حتی بعضی از برنامه‌های بازیافت داده‌ها رایگان هستند. از همین روی، باید برنامه‌ای چون برنامهٔ رایگان Eraser را درنظر بگیرید، که با استفاده از الگوریتمهای پیچیده، بر روی فایلهای شما داده‌های تصادفی می‌نویسد تا کسی نتواند آنها را بازیابی کند:

www.heidi.ie/eraser

کاملاً مجهز

با آن که اشتیاق فراوانی برای استفادهٔ فوری از کامپیوتر خود برای گشت‌زنی در وب، ایمیل، و سایر کارها دارید، بهتر است ابتدا جلوی انواع آلودگیهایی را بگیرید که می‌توانند به کامپیوتر و داده‌های شما صدمه بزنند و وقت شما را بگیرند.□