سپرهای امنیتی سیستم‌های عامل

● علیرضا قاضی سعیدی
کارشناس ارشد فناوری اطلاعات و ارتباطات

در این شماره به بررسی روشهای مقابله با بدافزارها می‌پردازیم.

به روزرسانی[1] سیستم عامل

با توجه به این که پرمخاطب‌ترین سیستم‌های عامل در ایران ویندوزهای XP و ۷ متعلق به شرکت «مایکروسافت» و هم‌چنین «اوبونتو»[2] (پرکاربردترین توزیع لینوکس[3]) هستند، به بررسی امنیت این سیستم‌ها می‌پردازیم. در مورد سیستم‌های عامل ویندوز، چنان‌چه اطمینان دارید سیستم عامل شما اصل است و به عبارت دیگر «کرک» شده نیست، حتماً سیستم خود را به روز کنید تا حفره‌های امنیتی توسط «Patch»[4]ها از بین بروند. اما اگر سیستم عامل ویندوز شما اصل نیست، به روز رسانی آن حتی ممکن است موجب از کار افتادن سیستم عامل شود. در مورد سیستم عامل اوبونتو، از آن‌جا که این سیستم عامل کاملاً رایگان است، بدون هیچ مشکلی می‌توانید آن را به روز کنید.

کاربران ویندوز XP، با مراجعه به سایت «www.microsoft.com» می‌توانند نرم‌افزار «Windows Malicious Software Removal tool» را دانلود و سیستم خود را برای بررسی وجود بدافزارها چک کنند. توجه شود که این نرم‌افزار به هیچ وجه نقش یک بستهٔ امنیتی یا حتی آنتی ویروس را ایفا نمی‌کند. در مورد ویندوز ۷ کافی است با مراجعه به «Control Panel» و سپس «Windows Defender»، به بررسی وضعیت سیستم خود بپردازید.

۲.دیوارهٔ آتش[5]

در سیستم عامل ویندوز بخشی به نام دیوارهٔ آتش وجود دارد که تا حد امکان مانع از دسترسی هکرها و بدافزارها به سیستم شما می‌شود. برای اطمینان از روشن (On) بودن دیوارهٔ آتش ویندوز ابتدا وارد «Control Panel» و سپس وارد «Windows Firewall» شوید تا از عملکرد آن اطمینان حاصل کنید. سیستم عامل لینوکس اوبونتو، اگر چه ذاتاً از امنیت بسیاری برخوردار است، با این حال می‌توانید انواع آنتی ویروس‌ها و دیواره‌های آتش را به صورت رایگان برای آن دانلود و نصب کنید.

آشنایی با برخی از نرم‌افزارهای امنیتی

نرم‌افزارهای امنیتی موجود را می‌توان به سه دستهٔ عمدهٔ تقسیم کرد:

- **آنتی ویروس**[6]
- **اینترنت سکیوریتی**[7]
- **وتوتال سکیوریتی**[8]

چنان‌چه قصد تهیهٔ یکی از این نرم‌افزارها را دارید، به این نکته توجه کنید که اینترنت سکیوریتی‌ها علاوه بر داشتن تمامی بخشهای یک آنتی ویروس، دارای یک فایروال یا دیوارهٔ آتش نیز هستند که به کاربرانی که سر و کار زیادی با شبکهٔ اینترنت دارند، توصیه می‌شود از این نسخه از نرم‌افزارها استفاده کنند. چرا که این دیوارهٔ آتش ترافیک ورودی و خروجی شما را کنترل می‌کند و اگر خطری متوجه سیستم شما باشد، به شما اخطار خواهد داد. به مدد دیوارهٔ آتش شما می‌توانید متوجه شوید که کدام برنامه‌ها در سیستم شما در حال ارتباط از طریق اینترنت هستند.

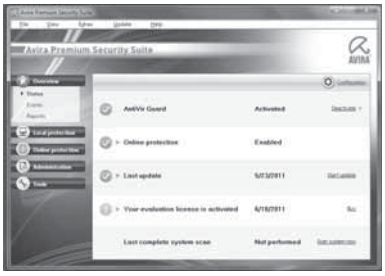
توتال سکیوریتی نیز کامل‌ترین بسته، نرم‌افزاری شرکتها به حساب می‌آیند که توسط کاربران حرفه‌ای مورد استفاده قرار می‌گیرند. ضمن این که معمولا منابع بیشتری از سیستم را درگیر می‌کنند و نسبت به دو بستهٔ امنیتی دیگر سنگین‌تر هستند. از میان آنتی‌ویروس‌های رایگان و قدرتمند می‌توان به «Avira»، «AVG» و «Avast» اشاره کرد و از میان اینترنت سکیوریتی‌های رایگان نیز می‌توان از «Comodo Internet Security» نام برد.

لینک‌های آنتی ویروس‌های رایگان و رابطهای گرافیکی

برخی از آنها از این قرارند:

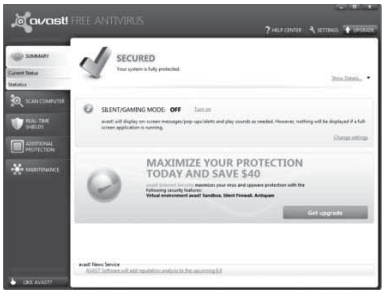
Avira

http://www.avira.com/en/avira-free-antiviruirus



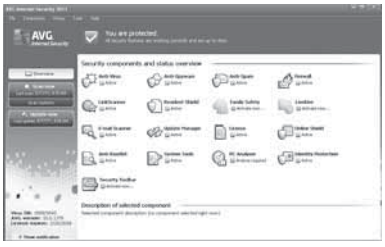
Avast

http://www.avast.com/free-antivirus-download



AVG

http://free.avg.com/us-en/download-free-antivirus



Comodo

http://www.comodo.com/home/internet-security/free-internet-security.php

در مورد تمامی بسته‌های امنیتی توجه به این نکته بسیار ضروری است که سعی کنید همیشه بستهٔ امنیتی شما به روز باشد، چرا که بهترین بستهٔ امنیتی چنان‌چه به روز نباشد، نمی‌تواند از سیستم شما به صورت کارا محافظت کند.

چند نکتهٔ مهم

۱. نرم‌افزارهای امنیتی جانبی

گاه بهترین آنتی‌ویروس‌ها و اینترنت سکیوریتی‌ها هم از پس معدودی از بدافزارها (به خصوص تروجان‌ها) برنمی‌آیند. در این موارد می‌توان از نرم‌افزارهای کوچکی که به همین منظور ساخته شده‌اند، استفاده کرد. این نرم‌افزارها با نامهایی مثل «Anti-Malware»، «Anti-Spyware»، «Anti-Trojan» قابل دانلود هستند و برای نابودی این دسته از بدافزارها و یا به کار می‌روند.

۲. حافظه‌های قابل حمل

حافظهٔ قابل حمل به سخت‌افزارهایی هم‌چون «فلش مموری» و دیسک‌های سخت خارجی اطلاق می‌شود. اگر نرم‌افزار امنیتی شما قابلیت بلوکه کردن (جلوگیری از اجرای Auto run) حافظه‌های قابل حمل را دارد، ابتدا حافظهٔ قابل حمل را بلوکه کنید و پس از اطمینان از عدم وجود بدافزار، (چک کردن توسط بستهٔ امنیتی) می‌توانید به وضع عادی برگردید و حافظهٔ جانبی را از حالت بلوکه خارج کنید.

توجه: نرم‌افزارهایی برای اسکن‌پورت‌های USP وجود دارند که همین کار را انجام می‌دهند. یعنی به محض این‌که حافظهٔ قابل حمل را به پورت USP وارد می‌کنید، ابتدا حافظهٔ خارجی را اسکن می‌کند و سپس اجازهٔ دسترسی به محتویات آن را می‌دهد. در مجموع به خاطر داشته باشید، همواره حافظه‌های خارجی را ابتدا توسط نرم‌افزار امنیتی خود چک کنید و سپس به انتقال اطلاعات بپردازید.

۳. نامه‌های الکترونیکی

- چنان چه ایمیل مشکوکی به شما رسید، از باز کردن آن خودداری کنید و ترجیحاً فرستندهٔ این ایمیل را در فهرست فیلترینگ ایمیل خود قرار دهید.
- «پیوست»[9]های دریافتی را (با وجود اینکه توسط سرویس‌دهنده‌های ایمیل از لحاظ وجود بدافزار چک می‌شوند) مجدداً قبل از باز کردن، توسط نرم‌افزار امنیتی چک کنید.

۴. پرداختهای الکترونیکی

اگر می‌خواهید کارهای بانکی و مالی خود را از طریق شبکهٔ اینترنت انجام دهید، برای وارد کردن اعداد و حروف در سیستم‌های بانکی حتماً از کیبورد مجازی صفحه استفاده کنید تا پسورد شما توسط «Keylogger»ها به سرقت نرود.

در شماره‌های بعدی به بررسی برخی از نرم‌افزارهای امنیتی می‌پردازیم.

پی نوشت

1. Update
2. Ubuntu
3. Linux
4. Patch
5. Fire Wall
6. Anti Virus
7. Internet Security
8. Total Security
9. Attachment