TƯ VẤN IT: BẢO VỆ PC AN TOÀN VỚI TƯỜNG LỬA CÁ NHÂN

Cái kh

Cái khó nhất là làm sao lựa chọn đúng phương pháp để kết hợp hiệu quả các sản phẩm bảo vệ dành cho máy để bàn và cân bằng được giữa các yếu tố: thuận tiện, bảo mật và đơn giản.

Tường lửa cá nhân bây giờ không còn là thứ "xa xỉ" chỉ dành cho các đại gia nữa. Khi ngày càng nhiều người dùng lang thang với chiếc laptop trong tay, làm việc bên ngoài bốn bức tường chật hẹp của văn phòng, thì nguy cơ bị hứng đòn tấn công từ những kẻ suốt ngày rình mò trên mạng ngày càng cao. Nhiều sự kiện cũng như dấu hiệu đã xuất hiện, nhắc nhở các công ty tìm kiếm cách thức và con đường bảo vệ người dùng hiệu quả trước các cuộc tấn công liên tục qua Internet.

Phải, các cuộc tấn công diễn ra liên tục. Một nghiên cứu gần đây do Trung tâm nghiên cứu về nguy hiểm và độ tin cậy của Đại học Maryland Clark School kết hợp với Viện nghiên cứu hệ thống tìm ra rằng, cứ khoảng 39 phút lại có một cuộc tấn công do hacker tiến hành nhắm vào máy tính có kết nối Internet. "Dữ liệu của chúng tôi cung cấp bằng chứng đáng tin cậy cho thấy hoạt động tấn công diễn ra không ngừng nghỉ với tất cả máy tính nối mạng Internet", Michel Cukier - tác giả cuộc nghiên cứu và đồng thời là giáo sư công trình đang giảng dạy trong trường đại học nói. Các máy tính trong nghiên cứu của Cukier đều bị tấn công, trung bình 2.244 lần/ngày.

Thời kỳ tấn công của virus qua e-mail ngày xưa dường như quá ôn hoà và dịu nhẹ khi so sánh với các đe doạ nguy hiểm bảo mật ngày nay. "Các nguy cơ không hề giảm", Richard Weiss - giám đốc marketing sản phẩm bảo mật ở CheckPoint Software khẳng định. "Chúng tôi đã từng chứng kiến thay đổi rất rõ ràng trong kiểu tấn công. Bây giờ không còn kiểu trẻ con ham danh tập phá hoại mà hết sức tinh vi và chuyên nghiệp. Bởi chúng đang chuyển hướng mục tiêu từ ham hố nổi trội, chứng tỏ bản lĩnh sang lợi nhuận, kiếm tiền từ thế giới ngầm thông qua lấy cắp và mua bán dữ liệu doanh nghiệp, thông tin mật". Trojan bây giờ phổ biến gấp 4 lần virus và worm, theo báo cáo của hãng sản xuất phần mềm diệt virus Shophos. Tỷ lệ này tăng gấp hai lần so với nửa đầu năm 2005.

Máy tính xách tay du lịch thường kết nối tới nhiều mạng cục bộ khác nhau, cả có dây và không dây. "Chúng là những mạng mà các doanh nghiệp không thể kiểm soát được", Monte Robertson - chuyên gia tư vấn ở Software Security Solutions và cũng là nhà phân phối sản phẩm bảo mật tự do lưu ý. Đã đến lúc các công ty nên bắt đầu kế hoạch bảo vệ thiết bị di động, như laptop và PDA, với cùng phương thức phân lớp đã từng dùng cho mạng doanh nghiệp của mình.

Hai phương thức cơ bản

Cái khó nhất là làm sao lựa chọn đúng phương pháp kết hợp hiệu quả các sản phẩm bảo vệ dành cho máy để bàn và cân bằng được giữa thuận tiện, bảo mật và đơn giản. Có hai phương thức cơ bản do các hãng bảo mật cung cấp mà cho đến nay vẫn được dùng phổ biến.

Phương thức thứ nhất là sử dụng thiết bị phần cứng để bảo vệ vành đai, hay biên giới mạng và làm việc chung với phần mềm trên từng máy để bàn. Các thiết bị này hoàn toàn có thể sử dụng trong phạm vi rộng của các hãng lớn như CheckPoint, Cisco, Juniper và Symantec. Ưu điểm của phương thức này là một hãng đơn lẻ cũng có thể kiểm soát được cả bảo mật vành đai và bảo mật desktop. Nhưng mặc dù vậy, xét trên khía cạnh khác, có thể nhiều công ty sẽ không tìm ra được cho mình thành phần phù hợp nhất mà họ cần.

Lựa chọn thứ hai là sử dụng bộ phần mềm bảo mật hoạt động cùng với cổng vào doanh nghiệp hoặc giải pháp diệt virus trung tâm hoá. Ví dụ, bộ phần mềm có thể là:

Symantec Client Security v3.1

McAfee Host IPS for desktops v6.0.1

Windows Live OneCare

Cái hay của phương thức này là người dùng không cần cài đặt hay cấu hình bất kỳ thành phần nào trên hệ thống của riêng họ. Các bộ phần mềm doanh nghiệp (hoặc trong trường hợp của Windows Live, một dịch vụ nền tảng Web) sẽ quản lý chương trình update riêng. Như thế có nghĩa là cơ sở dữ liệu dấu hiệu tấn công được update tự động một cách tập trung để chương trình bảo vệ luôn thực hiện được công việc như hiện tại. Điểm hạn chế trong phương thức này là các giải pháp thường bị tổn thương do không có chương trình bảo vệ tốt nhất và cơ hội khai thác có thể bị tuột qua. Thêm vào đó, chúng không hỗ trợ tất cả phiên bản cũ hơn của Windows.

Các nhà quản lý IT đang tìm kiếm phương thức kiểm soát PC không chịu sự quản lý nào như máy tính của những người làm việc tại nhà hay người làm việc tạm thời chứ không phải nhân viên chính thức. “Một vài năm trước, sau cuộc tấn công của sâu Blaster họ phát hiện ra rằng, hệ thống dò tìm xâm phạm và diệt virus truyền thống giờ trở nên quá đơn giản và không có tác dung”, Weiss khẳng định.

Các điểm yếu của Windows Firewall

Nhược điểm lớn nhất của Windows Firewall là dựa trên tường lửa cá nhân tích hợp sẵn của

Windows (hoặc Mac OS). Nhãn "cá nhân" khiến Windows Firewall được phân biệt với tường lửa doanh nghiệp, có nhiệm vụ bảo vệ toàn bộ mạng công ty trước các cuộc tấn công. Phiên bản cá nhân chỉ chạy được trên máy tính để bàn.

Dựa trên tường lửa cá nhân dựng sẵn do hệ điều hành cung cấp không phải là giải pháp bảo mật hay, vì người dùng có thể dễ dàng tắt tường lửa (do tình cờ hoặc có chủ đích) mà quên bật lại chúng khi cần. Với nhiều phiên bản hệ điều hành cũ, cụ thể như Windows XP và một số phiên bản trước nữa, tường lửa dựng sẵn thường cung cấp chương trình bảo vệ không làm hài lòng người dùng, thậm chí đem lại cảm giác an toàn sai.

Ví dụ, Windows XP chỉ bắt đầu tích hợp sẵn tường lửa với hệ điều hành từ Service Pack 2 trở lên. Tuy nhiên, tường lửa XP chỉ bảo vệ được các kết nối bên trong chứ không ngăn chặn được nguy hiểm đến từ bên ngoài đường biên mạng. Tức là, bất kỳ nguy hiểm tiềm ẩn nào, vì một lý do nào đó tìm ra được cách thâm nhập vào ổ cứng của người dùng đều có thể tiến đến chiếm quyền kiểm soát máy tính và sử dụng chính máy tính này để gửi đi các cuộc tấn công hay tham gia botnet. "Yếu tố quan trọng then chốt trong bảo mật máy tính là bảo vệ được mạng trước các cuộc tấn công từ bên ngoài đường biên, nơi thông tin nhạy cảm đi ra ngoài" (Robertson).

"SP2 đã vá rất nhiều lỗi, giúp XP mạnh hơn và Internet Explorer an toàn hơn nhiều", Igor Pankov - quản lý tiếp thị sản phẩm của Agnitum nhận xét. "Nhưng SP2 không làm gì nhiều để nâng cao tổng thể tính bảo mật hợp nhất, vì malware, dù ít hay nhiều vẫn luôn gửi dữ liệu cá nhân ra ngoài biên giới mạng".

Vista và dịch vụ quản lý Windows Live OneCare luôn được tích hợp sẵn tường lửa riêng với khả năng nâng cao hơn một chút. Nhưng Vista firewall mặc định cũng chỉ có thể bảo vệ được kết nối trong đường biên. Có thể cấu hình chương trình bảo vệ ngoài đường biên nhưng không hề đơn giản và phần nào đấy vượt ra ngoài tầm của người dùng mức trung bình. "Vista kế thừa nhiều tính năng và an toàn hơn các phiên bản Windows trước, nhưng chưa phải là hoàn hảo", Shane Coursen - chuyên gia tư vấn kỹ thuật nhiều kinh nghiệm của Kaspersky Labs cho hay.

Cân bằng giữa vấn đề an toàn hơn và dễ sử dụng đã tạo ra một thị trường thay thế tường lửa tích hợp sẵn trên Windows. Các chương trình này cũng có thể sử dụng cho người dùng từ xa hay những người hay lưu động, làm việc bên ngoài mạng nội bộ của tổ chức họ.

Tường lửa cá nhân nhóm thứ ba

Hai phương thức cơ bản không đáp ứng được yêu cầu và thay vào đó, phương thức thứ ba mới được sử dụng thường xuyên: kết hợp tường lửa mạnh hơn trên từng desktop với thiết bị bảo mật trung tâm hoá hoặc một bộ phần mềm bảo mật. Đây chính là vấn đề cốt lõi của các sản phẩm bảo mậthiện đang có trên thị trường, như sản phẩm của Cisco, Consentry, Juniper, Lockdown Networks và Mirage Networks. Tất cả đều triển khai công cụ giám sát trạng thái của từng thiết bị mạng và đảm bảo cho chúng an toàn.

Nhưng các giải pháp này thường rất tốn kém và tốn lượng lớn thời gian để triển khai. Một lựa

chọn tốt hơn là sử dụng tường lửa cá nhân của nhóm thứ ba như Zone Labs của CheckPoint Software, Panda Software, Prevx và một số hãng khác như trong bảng tóm tắt dưới đây:

Sản phẩm
Địa chỉ (URL)
Thành phần chính

Panda Software Client Shield 2006

Pandasoftware.com

Hỗ trợ Windows 98/2000, phiên bản doanh nghiệp.

Zone Alarm Internet Security Suite v7.0, CheckPoint Integrity

Zonelabs.com

Có phiên bản miễn phí (chỉ tường lửa) và thu tiền; bộ sản phẩm bao gồm chương trình bảo vệ IM và antivirus/spyware

Prevx v1.0

Prevx.com

Ngăn chặn miễn phí, nhưng mất 25 USD một năm nếu thay đổi hay dàn xếp lại.

Jetico Personal Firewall v1.01

Jetico.com

Miễn phí, dùng cho Win98/2000

Agnitum Outpost Pro v4.0

Agnitum.com

Dùng cho Windows 64-bit và Win98/2000; Chức năng: anti-malware/spyware

Kaspersky Internet Suite v6.0

Kaspersky.com

Dành cho Windows 64-bit và hỗ trợ Vista; thành phần: anti-malware/spyware

Sản phẩm tường lửa cá nhân nhóm thứ ba

Lợi ích từ việc sử dụng các sản phẩm này đã được thể hiện trong thực tế. Chúng giúp bảo vệ hiệu quả các máy để bàn và ngăn chặn tốt hơn việc khai thác lỗ hổng ze-ro day trước khả năng tấn công của nhiều người qua mạng doanh nghiệp.

Một ví dụ điển hình là công ty viễn thông VAR Tele-Verse đã dùng phần mềm diệt virus Norton của Symantec để bảo vệ hàng loạt máy Windows 2000 20-plus khoảng 9 tháng trước đây, khi một

máy tính được phát hiện bị tấn công bởi virus và phát tán ra toàn bộ máy trong công ty. "Chúng tôi đã phải bỏ ra mất gần một ngày trời để tìm kiếm chương trình có thể diệt được virus này, kể cả update phiên bản mới nhất của Norton trên tất cả cá máy", Scott Rendell - quản lý hoạt động của Tele-Verse kể lại. "Cuối cùng chúng tôi tìm ra Prevx và nó đã cứu cả công ty. Nó làm việc rất dễ dàng và nhanh chóng phát hiện ra vấn đề, rồi cách ly ngay lập tức virus. Chúng tôi không gặp phải phiền phức gì từ sau lần đó".

Prevx kiểm tra thường xuyên các bản update có dấu hiệu mới và cũng phát hiện được hoạt động tựa virus của ứng dụng. Một số sản phẩm tường lửa cá nhân nhóm thứ ba khác cũng đã bắt đầu kết hợp chặt chẽ với các kỹ thuật tương tự. Và các nhà nghiên cứu bảo mật đang bỏ ra nhiều thời gian để kiểm tra và tìm kiếm cách loại bỏ malware mà không cần đòi hỏi dấu hiệu cụ thể.

Tìm ra được tường lửa cá nhân tốt nhất không hề đơn giản. Các nhà quản lý IT sẽ cần kiểm tra một lượng lớn cấu hình desktop và ứng dụng trước khi có được bất kỳ quyết định nào. Chúng phải đảm bảo được hai yếu tố: có thể bảo vệ được những gì và có dễ sử dụng trong các hoạt động tin học thường ngày không. "Thách thức nằm ở chỗ, làm sao tối thiểu hoá được gánh nặng quản lý phần mềm bổ sung cho chương trình bảo vệ desktop bổ sung", Weiss của CheckPoint phân tích. "Các doanh nghiệp luôn có giới hạn nhất định về số lượng khác nhau của phần mềm họ muốn hỗ trợ".

Người ta đã tiến hành một số kiểm tra thử nghiệm độc lập để xác định tính hiệu quả của tường lửa cá nhân. Một trong số đó là Firewall Leak Tester. Một loạt sản phẩm khác nhau được đưa và chương trình kiểm tra nhằm xác định liệu các tường lửa có thể ngăn chặn một số kiểu tấn công cụ thể từ bất kỳ đe doạ nào. Các nhà quản lý IT có thể đánh giá chương trình kiểm tra và xác định độ mạnh tương ứng trên từng sản phẩm.

Một trong những điểm đáng ngạc nhiên phát hiện được từ các chương trình kiểm tra này là sự khác nhau nhiều giữa bản miễn phí và bản trả tiền của Zone Alarm. Bản miễn phí chỉ có thể loại bỏ được 27 kiểu tấn công khác nhau trong khi bản trả tiền có thể loại bỏ được thêm gần 20 kiểu nữa.

Tường lửa cá nhân được đánh giá ở top đầu là Jetico. Tường lửa này miễn phí hoàn toàn nhưng không hề dễ cấu hình. Nếu sử dụng sản phẩm này, các nhà quản lý IT sẽ cần đến nhiều thời gian để thiết lập và đưa nó vào hoạt động cho từng người dùng. Chương trình kiểm tra cho thấy, Jetico rất khó cấu hình, nhất là với người dùng dùng ứng dụng đa chức năng Internet chứ không phải chỉ e-mail và Web browsing.

Hai tường lửa cũng ở top đầu khác là Outpu Pro firewall của Agnitum và Internet Suite của Kaspersky Labs. Cả hai đều là sản phẩm thương mại, đã được tung ra thị trường vài năm nay. Cả hai đều tích hợp tường lửa cá nhân với chương trình diệt virus và chống spyware. Kaspersky hỗ trợ Vista cũng như các phiên bản Windows cũ hơn.

Một số hãng sản xuất bắt đầu đưa tường lửa cá nhân vào như một phần trong giải pháp bảo mật hợp nhất tổng thể cho các công ty. Thường họ phân phối phần mềm bảo mật điểm cuối tốt hơn

hoặc đơn giản chỉ là kết hợp các dòng sản phẩm doanh nghiệp và cá nhân riêng rẽ lại với nhau. Một ví dụ là trường hợp của Symantec với Client Security, Integrity của CheckPoint Software và Open Space Security của Kaspersky. Cả ba dòng tường lửa cá nhân này đều được kết hợp với các công cụ quản lý doanh nghiệp tổng thể.

Vấn đề không nằm ở chỗ bạn chọn sản phẩm nào, mà quan trọng là hãy nhanh chóng bắt đầu đánh giá các tường lửa cá nhân. "Với laptop, bạn nên lựa chọn giải pháp bảo mật tốt nhất với chức năng anti-virus, anti-spyware và firewall", Robertson của Software Security Solutions khẳng định. "Đã đến lúc bắt đầu suy nghĩ về yêu cầu cần thiết đòi hỏi ở tường lửa cá nhân với vai trò là công cụ cực kỳ quan trọng cho người dùng từ xa".