Một mô hình phòng thủ hiệu quả và chắc chắn là thiết lập nhiều tuyến phòng vệ, nào là phòng vệ bên ngoài với tường lửa cứng (tích hợp trong router), tường lửa mềm (phần mềm trong máy tính), phần mềm chống virus, phần mềm chống spyware... rồi phải cập nhật bản sửa lỗi những lỗ hổng bảo mật của hệ điều hành và của những phần mềm cài đặt trên máy tính. Tuy nhiên, nhiều người dùng gia đình không đủ khả năng (tài chính, kiến thức) để thực hiện điều này. Vậy tuyến phòng vệ nào là cần thiết và phù hợp?

1. Tường lửa (firewall) kiểm soát dữ liệu ra vào máy tính của bạn và cảnh báo những hành vi đáng ngờ; là công cụ bảo vệ máy tính chống lại sự xâm nhập bất hợp pháp bằng cách quản lý toàn bộ các cổng của máy tính khi kết nối với môi trường bên ngoài (mạng Lan, Internet...). Tường lửa có sẵn trong Windows XP chỉ giám sát được dòng dữ liệu vào máy tính chứ không kiểm soát được dòng dữ liệu ra khỏi máy tính. Người dùng gia đình thường ít có kinh nghiệm về bảo mật và virus, tường lửa sẽ không phát huy tác dụng vì người dùng không thể xử lý các cảnh báo. Hơn nữa, việc cài đặt tường lửa sẽ làm cho máy tính hoạt động chậm đi.

2. Phần mềm chống virus. Rất nhiều bài viết của chúng tôi đã giới thiệu với bạn đọc những phần mềm chống virus tốt nhất, từ những bộ phần mềm "tất cả trong một" đến những phần mềm độc lập và miễn phí. Chúng đều có những điểm mạnh yếu riêng nhưng đáng buồn là không phần mềm nào có thể bảo vệ máy tính của bạn một cách toàn diện. Một số bạn đọc không cài đặt phần mềm chống virus vì thấy hệ thống trở nên chậm chạp. Họ chấp nhận mạo hiểm (hoặc không biết) những rủi ro khi đánh đổi sự an toàn của máy tính để lấy tốc độ. Một vài bạn đọc lại cho rằng máy tính sẽ an toàn hơn, được bảo vệ tốt hơn nếu cài đặt nhiều phần mềm chống virus. Điều này cũng không tốt vì sẽ xảy ra tranh chấp giữa các phần mềm khi chúng tranh giành quyền kiểm soát hệ thống.

Ghi chú:

- Thường xuyên cập nhật danh sách nhận dạng virus (virus definitions) sẽ giúp phần mềm làm việc hiệu quả hơn.

- "Thủ" sẵn địa chỉ, nơi có thể tải về phần mềm BKVA trong trường hợp những phần mềm phòng chống virus của nước ngoài không phát hiện được virus có xuất xứ từ Việt Nam.

3. Cập nhật bản sửa lỗi. Lỗ hổng bảo mật của phần mềm là "điểm yếu" virus lợi dụng để xâm nhập vào máy tính của bạn. Thật không may là những điểm yếu này lại khá nhiều và người dùng cũng không quan tâm đến việc này. Hãy giữ cho hệ điều hành, trình duyệt web và phần mềm chống virus luôn được cập nhật bằng tính năng tự động cập nhật (auto update); nếu tính năng này không hoạt động (do sử dụng bản quyền bất hợp pháp), hãy cố gắng tải về từ website của nhà sản xuất bằng cách thủ công. Bạn sẽ tăng cường tính năng phòng thủ hiệu quả cho hệ thống và tránh tình trạng virus "tái nhiễm" sau khi diệt.

4. Trình duyệt an toàn hơn. Nếu so sánh, bạn dễ dàng nhận thấy Internet Explorer là trình duyệt web có nhiều lỗ hổng bảo mật nhất dù Microsoft liên tục đưa ra những bản sửa lỗi. Sử dụng những trình duyệt thay thế như Mozilla Firefox, Opera... hoặc cài đặt thêm một trong những trình duyệt này để tận dụng những ưu điểm của mỗi phần mềm và tăng tính bảo mật khi lướt web.

5. Suy nghĩ kỹ trước khi cài đặt. Nhiều bạn đọc thích táy máy, tải về và cài đặt nhiều phần mềm khác nhau để thử nghiệm. Điều này dẫn đến việc chúng ta không kiểm soát được những phần mềm sẽ làm gì trên máy tính. Thực tế cho thấy cài đặt quá nhiều phần mềm sẽ "bổ sung" thêm những lỗ hổng bảo mật mới, tạo điều kiện cho tin tặc dễ dàng xâm nhập vào máy tính của bạn, góp phần làm đổ vỡ hệ thống phòng thủ mà bạn dày công tạo dựng.

6. Sử dụng máy tính với quyền user. Với Windows NT/2000/XP, việc đăng nhập và sử dụng máy tính với tài khoản mặc định thuộc nhóm Administrators là một hành động mạo hiểm vì virus sẽ

được "thừa hưởng" quyền hạn của tài khoản này khi xâm nhập vào hệ thống, máy tính của bạn có thể trở thành zombie và tấn công máy tính khác. Tài khoản thuộc nhóm Users sẽ không được phép thay đổi các thiết lập liên quan đến hệ thống, bạn sẽ tránh được nhiều nguy cơ bị phá hoại và những phiền toái, cả khi virus xâm nhập vào máy tính.

Sử dụng máy tính với quyền User sẽ khiến người dùng gặp nhiều khó khăn trong quá trình cài đặt ứng dụng và thực hiện một số tác vụ liên quan đến hệ thống nhưng chúng tôi vẫn khuyến khích bạn đọc tự giới hạn quyền sử dụng trên máy tính của mình. Tham khảo thêm thông tin trong bài viết "Sử dụng máy tính với tài khoản thuộc nhóm Users" (ID: A0504_139, A0505_139) và thông tin bên trên sẽ giúp bạn vượt qua những khó khăn này. Hơn nữa, bạn không cần cài thêm phần mềm phòng chống spyware. Tài nguyên hệ thống không bị chiếm dụng, máy tính hoạt động nhanh hơn.

7. Sao lưu hệ thống. Bạn có thể bỏ qua bước này nếu tin rằng máy tính của mình luôn chạy tốt. Hãy thực hiện việc sao lưu vào thời điểm máy tính hoạt động ổn định, đã cài đặt những phần mềm cần thiết. Bạn có thể đưa hệ thống trở lại trạng thái đã sao lưu chỉ với vài thao tác đơn giản khi cần thiết. Để tạo tập tin ảnh của phân vùng đĩa cứng, bạn có thể sử dụng một trong những phần mềm như Drive Image của PowerQuest, Norton Ghost của Symantec, DriveWorks của V Communications, Acronis True Image của Acronis...

Việc sao lưu sẽ rất hữu ích với những bạn đọc thích táy máy, thử nghiệm tính năng phần mềm, thường xuyên truy cập vào những website "đen". Bạn sẽ tiết kiệm rất nhiều thời gian thay vì phải đi xử lý những sự cố do virus gây ra hoặc phải cài lại HĐH và những phần mềm cần thiết.

Lời kết

Ý thức người dùng là yếu tố quan trọng nhất để mô hình phòng thủ có hiệu quả chứ không phải từ việc sử dụng những phần mềm phòng chống mạnh nhất, tốt nhất. Không phần mềm nào đủ khả năng ngăn chặn virus nếu người dùng vẫn "vô tư” truy cập vào những những website "đen", website cung cấp serial, keygen (dùng để "bẻ khoá” phần mềm). Trên thực tế, máy tính cá nhân của chúng tôi chỉ cài đặt phần mềm phòng chống virus và sử dụng tài khoản thuộc nhóm Users (cả trong văn phòng) mà vẫn đảm bảo an toàn khi lướt web.

Đông Quân