WINDOWS VISTA CÓ THẬT SỰ AN TOÀN?

Theo M

Theo Microsoft, Vista là hệ điều hành (HĐH) an toàn nhất từ trước đến nay của hãng. Windows Vista hứa hẹn khóa chặt PC và tạo nên kỷ nguyên "điện toán an toàn" và những phần mềm phá hoại (malware) hung hăng trở thành chuyện của quá khứ.

Tuy nhiên, chỉ 3 tháng sau khi HĐH này chính thức tung ra thị trường, đã nảy sinh nhiều vấn đề. Các hãng phát triển phần mềm chống malware, giới hacker và các chuyên gia bảo mật đã đưa ra những nghi ngờ về tính hiệu quả của các giải pháp bảo mật của Microsoft, thậm chí có người còn cho rằng mô hình bảo mật của Vista chỉ là "trò đùa".

Microsoft luôn là mục tiêu hấp dẫn, đặc biệt khi hãng đưa ra những tuyên bố "quá đà". Sự thật thì những thử nghiệm đầu tiên cho thấy Vista an toàn hơn nhiều so với các phiên bản Windows trước đây. Nhưng điều đó không có nghĩa HĐH mới này đánh dấu sự kết thúc những nỗi lo bảo mật của Windows. Một số phiền phức cho các nhà quản trị IT sẽ giảm đi, nhưng những điểm yếu và cách khắc phục vẫn là mối bận tâm hàng đầu.

Không cần quản trị

Một trong những cải tiến bảo mật được tán dương nhiều nhất của Vista lại bị phê phán nhiều nhất. UAC (User Account Control) nhằm giải quyết một lỗ hổng thâm niên trong cách thức Windows kiểm soát quyền của người dùng, nhưng những người không ưa nói rằng nó không đủ mạnh và không hiệu quả do thiết kế không thích hợp.

Vấn đề ở đây là vai trò của tài khoản quản trị. Giải pháp tốt nhất là người dùng chỉ được cấp quyền quản trị khi thực hiện các tác vụ yêu cầu quyền này, như cài đặt trình điều khiển (driver) thiết bị hay thay đổi các thông số (registry). Nhưng thực tế cho thấy, mặc định người dùng thường đăng nhập với tài khoản quản trị, ngay cả với những tác vụ thông thường. Khi người dùng đăng nhập với quyền quản trị, sâu và Trojan horse được mặc sức tung hoành.

Tệ hơn, sự lơ là của Microsoft về quyền người dùng khuyến khích các hãng phần mềm độc lập sử dụng cẩu thả, dùng những cách thức lập trình không an toàn làm vấn đề càng trầm trọng thêm. Nhiều ứng dụng Windows không chịu làm việc trừ phi chúng được phép chạy với quyền quản trị đầy đủ - nghĩa là chạy với cách thức ít an toàn nhất.

UAC cố gắng sửa chữa thói quen xấu này, mặc định chạy phần mềm với quyền tiết giảm. Khi một ứng dụng cố làm điều gì đó yêu cầu quyền quản trị, UAC sẽ nhắc nhở người dùng với hộp thoại hỏi xem có cho phép "nâng" ứng dụng lên cấp có quyền cao hơn hay không.

Không may, UAC có kẽ hở. Trên blog của mình, Joanna Rutkowska đưa ra chi tiết nhiều lỗ hổng của UAC Vista có nguy cơ bị khai thác. Ví dụ, các trình cài đặt phần mềm luôn được phép chạy với quyền quản trị đầy đủ như trong các phiên bản Windows cũ. Thêm nữa, Ollie Whitehouse, chuyên gia bảo mật của Symantec, còn chỉ ra các tập tin thực thi được cung cấp cùng với Vista có thể dùng để "qua mặt" UAC. Như vậy các vấn đề liên quan đến tài khoản quản trị vẫn còn đó.

Tuy nhiên, không chỉ có kẽ hở lập trình qua mặt cơ chế bảo vệ của UAC, mà các hộp thoại xác nhận của UAC có thể phiền toái và hơi khó hiểu. Người dùng có thể tìm cách cấm UAC để khỏi phiền toái, hay có thể coi thường thông điệp cảnh báo và nhấn OK mà không thèm suy nghĩ. Hơn nữa, họ còn có thể dễ dàng bị lừa bởi những chiêu thức tâm lý hay giả mạo.

Theo tài liệu về UAC của Microsoft: "Windows Vista cung cấp nhiều tính năng để bảo vệ hệ thống của bạn, nhưng nó yêu cầu việc sử dụng đúng đắn. Việc bảo vệ an toàn hệ thống của bạn tùy thuộc vào hành vi của bạn, vì vậy hãy suy nghĩ trước khi nhấn". Nói cách khác, UAC đặt trách nhiệm về sự an toàn của hệ thống vào tay người dùng - điều khó an toàn tuyệt đối.

Thực sự, Microsoft không khuyến khích khách hàng nghĩ UAC như là màn chắn bảo vệ rõ ràng - và vì vậy, như Rutkowska ghi, hãng không xem các kẽ hở trong việc thực hiện UAC là lỗ hổng bảo mật.

Cần tinh chỉnh

Microsoft còn bổ sung nhiều tính năng khác cho Windows Vista ngoài UAC, nhiều tính năng trong số đó nhằm tăng tính bảo mật toàn diện cho HĐH. Nhưng nếu xem xét kỹ thì những phần bổ sung này chỉ là những cải tiến nhỏ so với các phiên bản Windows trước.

Windows Firewall đã được thiết lập mặc định trên tất cả cài đặt Windows mới kể từ Windows Service Pack 2. Với Vista, Windows Firewall có thêm khả năng chặn các kết nối đi ra cũng như đi vào - một cải tiến đáng kể khi mà các hiểm họa từ phần mềm gián điệp (spyware), giả danh (phishing) và các cuộc tấn công từ chối dịch vụ (DdoS) ngày càng gia tăng. Tuy nhiên, việc lọc các gói tin đi ra mặc định không được kích hoạt. Nếu không có thao tác cấu hình thủ công, firewall của Vista không bảo vệ an toàn hơn bao nhiêu so với firewall của XP SP2.

Một chương trình mới có tên là Windows Defender thêm khả năng phòng chống malware cho Windows, nhưng nó chủ yếu nhắm đến người dùng thông thường và cho đến nay dường như không tốt bằng các phần mềm khác hiện có cho XP. Theo Webroot, hãng cung cấp phần mềm chống malware cạnh tranh, Windows Defender bỏ sót nhiều spyware. Tệ hơn, hồi tháng 2, Windows Defender bị phát hiện chính là kẽ hở để tấn công Vista, do có một điểm yếu có thể khai thác trong cơ chế phát hiện malware. Tương tự, tuy Vista có tính năng mã hoá ổ cứng gọi là BitLocker nhưng nó mặc định không hoạt động, khả năng bảo vệ chống lại các kỹ thuật giám định

máy tính hiện đại vẫn còn đáng ngờ.

Tệ hơn hết, một số tính năng mới thêm vào Vista thực ra lại gây bất lợi cho việc bảo mật tổng thể. Hồi tháng 1, tính năng nhận dạng tiếng nói của Vista bị phát hiện có thể lợi dụng để truy cập (có hạn chế) hệ thống máy tính từ xa, cho phép xóa file bất kỳ.

Kẻ thù bên ngoài

Kẽ hở nhận dạng tiếng nói của Vista nêu lên một điểm yếu trầm trọng. Như với các phiên bản Windows trước đây, hầu hết các cuộc tấn công vào các hệ thống chạy Windows Vista sẽ không khai thác bản thân HĐH, mà là các ứng dụng chạy trên HĐH.

Microsoft thực sự đã tạo nên những cải tiến đáng kể cho Windows Vista, nó được thiết kế để hạn chế một số dạng điểm yếu ứng dụng thông dụng nhất. Một loạt kỹ thuật mới gây khó khăn hơn cho hacker khi khai thác những lỗi quen thuộc bằng cách che khuất không gian địa chỉ bộ nhớ và bảo vệ chống truy cập nhân HĐH. Nghiên cứu ban đầu của Symantec cho thấy Vista vẫn dễ tổn thương trước một số dạng tấn công nhưng kết luận rằng "phương thức bảo vệ này đạt được nhiều mục tiêu bảo mật mà Microsoft đặt ra".

Việc sử dụng .Net như là mô hình phát triển chủ đạo cho Windows Vista cũng giúp tăng cường bảo mật. Mã lệnh được kiểm soát và các tính năng "đóng" an toàn của nền tảng .Net bảo vệ các nhà phát triển khỏi những lỗi lập trình thông thường có thể tạo nên những điểm yếu dễ bị khai thác. Tuy nhiên, điểm yếu cơ bản của các công nghệ này là yêu cầu phải viết lại mã lệnh chương trình. Các ứng dụng truyền thống không tuân theo mô hình bảo mật mới của Vista sẽ vẫn dễ bị tổn thương.

Cho đến khi các ứng dụng cũ được nâng cấp để khai thác các công nghệ bảo mật mới nhất của Microsoft, người dùng sẽ không được lợi gì nhiều khi chạy chúng trên Vista ngoài cái được UAC cung cấp. Mặc dù Microsoft đã thực hiện những cải tiến đáng kể, nhưng Vista không phải liều thuốc thần để tạo nên môi trường điện toán an toàn.

Bảo mật Longhorn đầy hứa hẹn

Những tiến bộ về bảo mật của Vista có thể nhiều tham vọng, nhưng chúng dường như nhỏ nhoi so với bảo mật của Longhorn. Người ta thấy vào cuối năm rồi, Longhorn vẫn còn là phiên bản "tiền thử nghiệm" - prebeta 3, nhưng bảo mật của nó đầy hứa hẹn.

Một điều hấp dẫn là firewall của Longhorn kết hợp quản lý IPSec với firewall. Cơ chế "quy tắc" có thể kiểm soát bảo mật dựa trên chính sách, bao gồm xác thực và mã hóa. Bạn thậm chí có thể gán

quy tắc cho server (như máy chủ Active Directory) hay nhóm người dùng. Tất cả có thể được quản lý với Microsoft Management Console hay trong các ứng dụng thuộc System Center.

Nhân của Longhorn được bảo vệ theo cách thức tương tự Vista, cũng hỗ trợ tính năng mã hóa file BitLocker dùng chip xác thực hay thiết bị bên ngoài như khóa USB. BitLocker cũng được xây dựng đặc biệt để ngăn chặn việc lấy trộm dữ liệu bằng cách cài đặt một HĐH khác hay những cách tương tự. Về bảo mật vật lý, Longhorn hỗ trợ sẵn kiểm soát cài đặt thiết bị có thể tháo rời (dĩ nhiên kiểm soát truy cập USB), và nó có trình quản lý khởi động mới.

Về phần mềm, Microsoft cho biết Windows Services cũng được gia cố. Trên Longhorn, khi một dịch vụ cần cài đặt, trước hết nó cần đăng ký để sử dụng các tác vụ được phép truy cập tài nguyên server và mạng. Dùng kỹ thuật này, Longhorn có thể cảnh giác những dịch vụ yêu cầu truy cập những khu vực nhạy cảm.

Cuối cùng, còn có NAP (Network Access Protection). Tương tự NAC (Network Admission Control) của Cisco, đây là hàng rào kiểm tra được thiết kế để đảm bảo mỗi client đăng nhập mạng xác thực hợp lệ và tuân thủ các quy tắc bảo mật. Người quản trị Longhorn có thể thiết kế những hình thức đáp trả cho nhiều tình huống NAP khác nhau sử dụng tất cả công cụ thông thường: DHCP, VPN, IPSec... Về lý thuyết, NAP có vẻ tuyệt vời, nhưng Mircosoft cần nỗ lực nhiều hơn.

NAP đi sau NAC của Cisco, vì vậy tốc độ phát triển chậm hơn Cisco có thể gây bất lợi cho Longhorn. May là hồi tháng 9/2006 hai công ty đã có thỏa thuận "bắt tay" giữa các giao thức cho phép kết hợp NAC và NAP trên một mạng chung. Miễn là Microsoft có thể lôi kéo được khách hàng, công nghệ này sẽ có chỗ đứng.

Microsoft đã vẽ nên một bức tranh màu hồng về tính bảo mật của Long horn, cho rằng đây là một bước tiến lớn ở phía server. Khi Longhorn ra mắt chúng ta sẽ có cơ hội kiểm chứng điều này.

Cách thức an toàn

Russ Humphries, giám đốc chương trình bảo mật Windows Vista, nói: "Chúng tôi tự tin cho rằng Windows Vista là phiên bản an toàn nhất của Windows cho đến nay. Tuy nhiên, điều quan trọng cần lưu ý là không có HĐH nào an toàn tuyệt đối".

Tóm lại, Windows Vista không an toàn tuyệt đối nhưng cũng không dễ bị tấn công. Các tiến bộ công nghệ trong HĐH đem lại những lợi ích bảo mật thật sự, nhưng Microsoft cũng nhìn nhận các sản phẩm bảo mật và chống malware khác vẫn có ích cho người dùng Vista như với các phiên bản Windows trước đây.

Như thường lệ với các HĐH Microsoft, có lẽ điểm yếu lớn nhất của Vista nằm ở chỗ mong muốn

tương thích ngược. Hầu hết các điểm yếu được phát hiện trong Vista cho đến nay đều khai thác những ứng dụng truyền thống không áp dụng mô hình bảo mật Windows mới. Ngay cả bản thân UAC cũng là một sự thoả hiệp với các phương thức cũ.

Doanh nghiệp càng áp dụng sớm những công nghệ Windows mới thì họ càng sớm hưởng lợi từ những cải tiến công nghệ của Microsoft trong lĩnh vực bảo mật. Bất kỳ ở đâu có thể, các ứng dụng thông thường nên chuyển sang mã lệnh có kiểm soát và nền .Net, và nên để mắt đến các phương thức và thư viện bảo mật mới của Windows.

Thiết lập bảo mật cụ thể tùy thuộc vào yêu cầu bảo mật của mỗi doanh nghiệp, nhưng nhìn chung để bảo mật hiệu quả trên Windows Vista vẫn phải có sự kết hợp của việc giám sát, tuân thủ các chính sách bảo mật, các công cụ bảo mật và chống malware của hãng thứ ba - nói cách khác, vẫn như cũ. Vista có cải tiến bảo mật đáng kể so với Windows XP, nhưng rốt cuộc, nó vẫn là Windows.

Bảo mật chập chững bước

Windows Vista có nhiều tính năng bảo mật mới, nhưng không tính năng nào loại trừ hẳn mối đe doạ từ hacker và malware.

Tính năng

Tốt

Xấu

UAC (User Account Control)
Hạn chế người dùng chạy với quyền Administrator; yêu cầu xác nhận các hành động có nguy cơ gây hại.
Công cụ chứ không phải rào chắn; một số chương trình có thể qua mặt cơ chế bảo vệ UAC; người dùng có thể cấm nó hoàn toàn.

Windows Firewall
Chặn cả kết nối vào và ra.
Các kết nối ra ngoài không được giám sát mặc định và yêu cầu cấu hình phức tạp.

Windows Defender
Công cụ chống mailware tích hợp có thể chặn các chương trình độc hại trước khi tấn công.
Không hiệu quả bằng công cụ của các hãng khác hiện có.

BitLocker
Dữ liệu được bảo vệ nhờ mã hóa ổ cứng tích hợp, ngăn ngừa trộm cắp.
Mặc định không bật; mức độ bảo mật thật sự không rõ.

Driver Signing, PatchGuard
Chỉ các driver và bản vá được Microsoft xác thực mới có thể cài đặt, giảm nguy cơ bị tấn công kiểu rootkit và Trojan horse.
Chỉ làm việc trên Vista 64-bit; đụng với phần mềm bảo mật của hãng khác.

Các công nghệ hạn chế khai thác
Ngăn không cho hacker khai thác các lỗi cũ trong mã lệnh ứng dụng.
Thường không làm việc trừ phi được các nhà phát triển ứng dụng ủng hộ.

Nguyễn Lê