THỦ THUẬT CHỐNG LỖI BẢO MẬT "ZERO-DAY"

Các lỗ

Các lỗi "zero-day" ngày càng phổ biến mà nguy hiểm hơn là chúng lại hiện diện trong các phần mềm được sử dụng khá rộng rãi như Microsoft Excel, Word hay Internet Explorer.

Lỗi "zero-day" là thuật ngữ dùng để chỉ những lỗi bảo mật nguy hiểm có thể bị khai thác bằng các đoạn mã hay chương trình và hoàn toàn chưa được vá lỗi từ nhà sản xuất.

Người dùng sẽ là những nạn nhân chính khi các lỗi "zero-day" được công bố trên các website hacker và bị khai thác. Tuy nhiên, ta cũng có thể bảo vệ hệ thống của mình khi có lỗi "zero-day" trước khi nhà sản xuất phát hành bản vá lỗi chính thức. Sau đây là những đề nghị thay đổi và nâng cấp hệ thống để tránh bị khai thác khi có lỗi "zero-day":

1. Internet Explorer 6 trở về trước là các phiên bản "đầy lỗi" bảo mật, trong đó có các lỗi "zero-day". Không có chương trình, phần mềm nào không có lỗi, tuy nhiên, Internet Explorer 6 vốn đã bị nhiều lỗi nguy hiểm hoặc do số lượng người sử dụng rất lớn nên nó đã trở thành mục tiêu hấp dẫn cho những kẻ tấn công có chủ đích. Nâng cấp lên phiên bản Internet Explorer 7 là lựa chọn thích hợp hoặc sử dụng FireFox, Opera hay Avant Browser là những lựa chọn luôn rộng mở cho người dùng.

2. Cố gắng thay đổi thói quen sử dụng các phần mềm đã bị công bố lỗi "zero-day" mà chưa có bản vá lỗi. Những phần mềm miễn phí đôi khi lại hoạt động tốt không thua gì các phần mềm thương mại. Các chương trình của Foxit Softwares có thể hiển thị và xử lý tốt với các tập tin định dạng PDF hoặc

Quyển sách Zero-Day Exploit của Rob Shein

OpenOffice sẽ là giải pháp tốt đối với việc soạn thảo văn bản (thay thế Word), bảng tính (thay Excel) ... Bạn có thể dễ dàng tìm kiếm thấy những "nhà hảo tâm" cung cấp các phần mềm miễn phí với những từ khóa đơn giản như: "free PDF reader" hay "free editor" trên những công cụ tìm kiếm như Yahoo, Google rồi tìm ra phần mềm thích hợp nhất với mục đích sử dụng của mình.

3. Kích hoạt chức năng tự động cập nhật cho Windows và cho bất kỳ chương trình nào có tính năng cập nhật. Các bản cập nhật vá lỗi chưa hẳn đã chống lại được những lỗi "zero-day" mới nhất, nhưng nó sẽ ngăn chặn những kẻ tấn công khai thác các lỗi cũ hơn vì sẽ có rất nhiều người dùng chủ quan không quan tâm đến việc tải các bản vá lỗi.

Đối với Windows, vào Automatic Updates trong Control Panel rồi thay đổi thành "Download updates for me, but le me choose when to install them" (Tải các bản vá lỗi nhưng để tôi quyết định khi nào cài đặt chúng).

Đối với các phần mềm khác, cũng không khó để tìm ra chức năng cập nhật. Ví dụ với trình duyệt FireFox ta vào Tools - Options - Advanced và chọn thẻ Update. Tương tự như trên, tiếp theo chọn "Ask me what I want to do as the standard course of action when Firefox finds updates". Hoặc đôi khi bạn phải tìm thủ công như trình Adobe Reader, bạn sẽ tìm thấy phần cập nhật trong menu Help sau đó chọn nút Preferences.

4. Lựa chọn những chương trình antivirus hoặc các trình bảo vệ cho PC có chức năng phân tích và ứng phó để bảo vệ hệ thống trước những lỗi chưa biết đến. Tính năng này có trong Panda Antivirus với công nghệ TruPrevent, ngăn chặn và chống virus cũng như các nguy cơ bảo mật khác chưa được định danh.

5. Bảo đảm rằng tường lửa (firewall) luôn luôn ở chế độ thời gian thực (real-time) trên hệ thống của bạn. Tường lửa sẽ bảo vệ hệ thống trước spyware, sâu máy tính ... và quét các yếu điểm trong hệ thống để bảo vệ chúng. Windows XP đã tích hợp sẵn tường lửa ở mức tương đối đối với người dùng trung bình. Để kích hoạt, ta vào Control Panel, mở Security Center và nhấn vào Windows Firewall. Các hệ thống cao cấp có thể lựa chọn những tường lửa mạnh mẽ hơn như BlackICE, ZoneAlarm.

6. Hạn chế quyền hạn người dùng sẽ là cách hay khi hệ thống đã bị khai thác từ lỗi bảo mật. DropMyRights là tiện ích nhỏ và hoàn toàn miễn phí sẽ cung cấp khả năng thiết lập quyền hạn cho hầu hết các chương trình.

7. Luôn luôn cập nhật những thông tin về lỗi bảo mật mới nhất để có thể tự bảo vệ mình hoặc có những giải pháp thích hợp. Tham khảo thêm Zero-day Tracker của hãng bảo mật eEye Digital Security.

Thanh Trực