MỘT SỐ BIỆN PHÁP KỸ THUẬT ĐỂ HẠN CHẾ RỦI RO AN TOÀN THÔNG TIN KHI SỬ DỤNG HỆ ĐIỀU HÀNH WINDOWS XP SAU THỜI ĐIỂM MICROSOFT NGỪNG HỖ TRỢ

(Kèm theo công văn số 79/VNCERT-KTHT ngày 03/4/2014)

1. Thông tin chung

1.1. Hệ điều hành Window XP

Hệ điều hành Windows XP (Windows XP) của hãng Microsoft được ra mắt vào ngày 25/10/2001 là một dòng hệ điều hành (HĐH) dành cho các máy tính cá nhân, hỗ trợ bộ vi xử lý 32 bít và 64 bít. Đây được coi là hệ điều hành được sử dụng rất phổ biến của hãng Microsoft và cũng là thế hệ hệ điều hành kế tục của cả các phiên bản hệ điều hành Windows 2000 Professional và Windows Me. Windows XP bản 32 bít được cung cấp kèm theo gói cập nhật mới nhất là Service Pack 3(SP3) và Windows XP bản 64 bít được cung cấp kèm theo gói cập nhật mới nhất là Service Pack 2 (SP2), các gói cập nhật này cung cấp nhiều tính năng bảo mật bổ sung so với phiên bản Windows XP ban đầu.

Hãng Microsoft đã công bố chính thức sẽ ngừng hỗ trợ Windows XP vào ngày 8/4/2014. Sau thời điểm này, các máy tính đang cài đặt Windows XP vẫn có thể tiếp tục sử dụng, cập nhật bản vá đã có. Tuy nhiên hãng Microsoft sẽ ngừng các dịch vụ sau:

- Hỗ trợ kỹ thuật cho người sử dụng,

- Dịch vụ tự động cập nhật (bao gồm các bản vá an toàn thông tin) cho Windows XP,

- Dừng cung cấp phần mềm bảo vệ an toàn thông tin Microsoft Security Essential dành cho Windows XP (các máy tính đã cài phần mềm này sẽ có thể tiếp tục sử dụng và cập nhật dữ liệu từ Microsoft thêm một thời gian nữa).

1.2. Ảnh hưởng đến người sử dụng khi không được tiếp tục hỗ trợ

Do còn một số lượng lớn máy tính tại Việt Nam vẫn đang sử dụng Windows XP nên việc Microsoft chấm dứt hỗ trợ hệ điều hành này sẽ gây những ảnh hướng lớn tới người sử dụng, đặc biệt trong khía cạnh an toàn thông tin. Đây là vấn đề rất nghiêm trọng vì từ năm 2008 đến nay, Microsoft cũng đã

từng phải cung cấp trên 600 hướng dẫn, bản vá khác nhau để khắc phục các lỗi an toàn thông tin cho Windows XP.

Từ thực tế đó, sau thời điểm trên khả năng tiếp tục phát hiện ra các điểm yếu an toàn thông tin mới của Windows XP là không thể loại trừ và điều đó thể tạo ra các lỗ hổng an toàn thông tin cho phép tin tặc tấn công gây hại, ăn cắp hoặc làm hư hỏng dữ liệu, lây nhiễm phần mềm mã độc hoặc thậm chí cướp quyền điều khiển máy tính trái phép. Và Microsoft cũng đã cảnh báo, các phần mềm anti-virus thông thường không đủ khả năng để bảo đảm an toàn khi Windows XP bộc lộ điểm yếu.

Như vậy người sử dụng Windows XP đứng trước hai sự lựa chọn:

a) Nâng cấp hệ điều hành: thay thế Windows XP bằng các hệ điều hành mới được hỗ trợ tốt hơn (của hãng Microsoft hoặc các hãng khác kể cả hệ điều hành nguồn mở đã được Bộ Thông tin và Truyền thông khuyến cáo). Đây là phương án cơ bản trong dài hạn nhưng đòi hỏi phải bảo đảm các điều kiện: chi phí đầu tư để mua sắm và cài đặt hệ điều hành, phần mềm hệ thống, các ứng dụng, thiết bị phần cứng cho tương thích; đào tạo và hướng dẫn sử dụng cho môi trường mới, thời gian để thực hiện chuyển đổi môi trường.

b) Tiếp tục sử dụng Windows XP: phương án này có thể áp dụng trong một thời gian hợp lý (tùy theo mục đích, hiệu quả sử dụng) khi chưa có đủ các điều kiện thực hiện phương án trên. Người sử dụng phải tăng cường áp dụng các biện pháp bảo đảm an toàn thông tin và phòng chống rủi ro. Không khuyến cáo sử dụng biện pháp này trong các trường hợp có yêu cầu bảo mật an toàn thông tin cao.

2. Một số biện pháp kỹ thuật cần chú ý

Trước tình hình thực tế như trên, Trung tâm VNCERT khuyến cáo các tổ chức, cá nhân một số biện pháp kỹ thuật cần lưu ý để bảo đảm an toàn thông tin khi nâng cấp hệ điều hành hoặc tiếp tục sử dụng các máy tính với Windows XP.

2.1 Bảo đảm an toàn khi nâng cấp hệ điều hành

Khi cơ quan, tổ chức tiến hành nâng cấp hoặc cài đặt mới hệ điều hành để thay thế Windows XP cần chú ý các biện pháp kỹ thuật sau:

Bước 1: Kiểm tra kỹ các điều kiện trước khi nâng cấp

- Kiểm tra và bảo đảm tính tương thích của các phần mềm hệ thống và các ứng dụng đối với hệ điều hành dự kiến sẽ nâng cấp.

- Kiểm tra, bảo đảm tính tương thích và yêu cầu tối thiểu của thiết bị phần cứng đối với hệ điều hành dự kiến sẽ nâng cấp.

Tham khảo các thông tin yêu cầu tối thiểu về phần cứng của phiên bản Windows 7, Windows 8 tại địa chỉ Internet:
http://windows.microsoft.com/vi-vn/windows7/products/system-requirements và http://windows.microsoft.com/vi-vn/windows-8/system-requirements.

Tham khảo yêu cầu phần cứng đối với các phiên bản hệ điều hành mã nguồn mở Linux như Ubuntu và Fedora tại địa chỉ Internet:
https://help.ubuntu.com/community/Installation/SystemRequirements và
http://docs.fedoraproject.org/en-US/Fedora/13/html/Virtualization_Guide/chap-Virtualization-System_requirements.html.

Bước 2: Thực hiện sao lưu dự phòng trước khi nâng cấp (để bảo đảm khả năng khôi phục khi nâng cấp thất bại)

- Lưu lại các thông tin liên quan đến bản quyền, giấy phép sử dụng của hệ điều hành và các ứng dụng khác.

- Sao lưu dự phòng bộ cài đặt hệ điều hành, các bản vá, các phần mềm đang sử dụng để sử dụng khi cần thiết.

- Sao lưu ổ cứng trước khi cài đặt, dữ liệu này sẽ được sử dụng để bảo đảm khả năng khôi phục lại khi có sự cố xảy ra.

Bước 3: Thực cài đặt hệ điều hành mới và các phần mềm ứng dụng

- Thực hiện nâng cấp hoặc cài đặt mới hệ điều hành theo đúng hướng dẫn của nhà sản xuất.

- Cài đặt các phần mềm hệ thống và ứng dụng (tương thích) cần thiết.

- Khôi phục lại hệ thống thông qua các dữ liệu đã được sao lưu ở bước 2 khi việc nâng cấp thất bại.

Bước 4: Thực hiện các biện pháp bảo đảm an toàn thông tin cho môi trường mới

- Áp dụng các biện pháp và thiết lập các chính sách bảo vệ an toàn thông tin cho hệ thống mới được cài đặt.

- Tạo lập các bản sao dữ liệu, hệ thống để hỗ trợ việc phục hồi hệ thống.

2.2 Bảo đảm an toàn khi tiếp tục sử dụng Windows XP

Khi chưa có điều kiện nâng cấp hoặc cài đặt hệ điều hành mới thay thế Windows XP, các tổ chức, cá nhân cần chú ý thực hiện các biện pháp sau:

a. Thực hiện sao lưu dự phòng như bước 2 mục 2.1.

b. Thiết lập chế độ bảo đảm an toàn thông tin cho hệ thống máy tính Windows XP trong quá trình sử dụng vận hành:

- Sử dụng tường lửa được tích hợp sẵn trên hệ điều hành, kết hợp với tường lửa của hệ thống mạng để quản lý truy cập từ các máy tính khác tới máy tính của mình và ngược lại. Việc thiết lập tường lửa phải bảo đảm yêu cầu chỉ cho phép các dịch vụ được phép sử dụng mở cổng ra bên ngoài, đóng toàn bộ các cổng dịch vụ không cần thiết.

- Gỡ bỏ hoặc tắt các dịch vụ không dùng đến hoặc ít dùng, trong đó đặc biệt chú ý các dịch vụ cho phép kết nối bên ngoài: Netmeeting Remote Desktop Sharing, Remote Desktop, Remote Registry, Routing & Remote Access, SSDP Discovery Service, Universal Plug and Play Device Host, Telnet v.v…

- Trong trường hợp bắt buộc phải kết nối quản trị từ xa, không kết nối trực tiếp tới các dịch vụ cho phép quản trị hệ điều hành từ xa như dịch vụ Remote Desktop. Trong trường hợp người sử dụng cần phải quản trị máy tính từ xa thì cần sử dụng kết nối gián tiếp sử dụng giao thức hỗ trợ mã hóa, bảo mật như VPN, SSH v.v...

c. Tham khảo áp dụng giải pháp bảo đảm an toàn thông tin cho Windows XP "VKT Total Security" của công ty Việt Kiến Tạo.

Giải pháp của công ty Việt Kiến Tạo cho phép bảo vệ máy tính sử dụng Windows XP khỏi ảnh hưởng của mã độc và các sự cố khác dẫn đến mất an toàn thông tin, giải pháp này cung cấp có ba nhóm tính năng chính sau:

- VKT Internet Security (VIS): Chống mã độc xâm nhập qua đường internet.

- VKT Smart Recovery (VSR): Phục hồi hệ thống thông minh.

- VKT User Security (VUS): Bảo vệ toàn vẹn một tài khoản người dùng.

Một số tính năng của giải pháp trên đã được Trung tâm VNCERT kiểm tra, đánh giá cho thấy hoạt động ổn định, phù hợp để nâng cao tính năng an toàn cho máy tính sử dụng Windows XP. Tham khảo thông tin chi tiết tại địa chỉ Internet: http://vkt.com.vn/

d. Sử dụng các trình duyệt web như Firefox, Mozillar, Chrome hoặc Internet Explorer phiên bản mới (còn được Microsoft hỗ trợ) để thay thế cho trình duyệt Internet Explorer đi kèm theo Windows XP.

e. Sử dụng các ứng dụng khác (còn được nhà sản xuất hỗ trợ) thay thế cho phần mềm duyệt thư điện tử Outlook Express đi kèm theo hệ điều hành Windows XP. Ví dụ như: Thunder Bird, Office Outlook v.v…

g. Không tải (download) và cài đặt các bản vá mà không rõ nguồn gốc, kiểm tra tính toàn vẹn các bản vá trước khi sử dụng.

2.3 Một số chú ý về cách sử dụng an toàn hệ điều hành

a. Thiết lập chính sách đặt mật khẩu an toàn cho các tài khoản có trong hệ thống, có thể tham khảo hướng dẫn "Hướng dẫn đặt và sử dụng mật khẩu an toàn" của Trung tâm VNCERT tại địa chỉ Internet:
http://www.vncert.vn/tainguyen/Huong_dan_su_dung_mat_khau_an_toan.pdf

b. Thiết lập tài khoản người dùng với quyền thấp nhất, chỉ vừa đủ để phục vụ công việc theo đúng chức năng, nhiệm vụ được giao. Quản lý và đặt mật khẩu an toàn cho các tài khoản mặc định Administrator và Guest. Có thể vô hiệu hóa tài khoản Guest khi không sử dụng.

c. Không sử dụng tài khoản có quyền quản trị (Administrator) khi không cần thiết để giảm khả năng lây nhiễm mã độc vào hệ thống. Chỉ sử dụng quyền quản trị khi cài đặt, gỡ bỏ, cấu hình thay đổi thông tin về hệ thống v.v…

d. Bật chức năng ghi nhật ký hoạt động để theo dõi và giám sát hoạt động sau: Account logon events, Account management, Logon events, Object access, Policy change, Privilege use, System events.

e. Vô hiệu hóa chức năng chia sẻ tài nguyên mặc định cho một số phân vùng và dịch vụ bao gồm: C$ D$ E$, ADMIN$, FAX$, IPC$, NetLogon, PRINT$.

g. Tắt bỏ các tính năng tự động chạy ứng dụng khi kết nối với thiết bị lưu trữ ngoài (ví dụ thẻ nhớ ngoài giao tiếp qua cổng USB) để giảm nguy cơ lây lan mã độc thông qua việc sao chép thông tin. Trong trường hợp cần thiết người sử dụng có trình độ kỹ thuật có thể tạo phân vùng (partition) riêng để ghi, lưu dữ liệu nhưng cấm chạy các tệp tin thực thi trên phân vùng này, biện pháp này sẽ cho phép ngăn cản thực thi các tệp tin có chứa mã độc.

h. Cài đặt và định kỳ cập nhật dữ liệu cho phần mềm Antivirus và thường xuyên sử dụng phần mềm này để kiểm tra và phát hiện mã độc.

i. Sử dụng công cụ "Tcpview.exe" để kiểm tra và phát hiện các kết nối mạng bất thường từ máy tính của mình ra các địa chỉ lạ bên ngoài mạng và sử dụng công cụ "procexp.exe" để kiểm tra các tiến trình lạ sinh ra trong khi máy

tính khởi động hoặc không sử dụng. Hai công cụ này được tích hợp trong bộ công cụ "Sysinternals Suite" do hãng Microsoft cung cấp tại địa chỉ Internet: http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx.

k. Tắt máy tính, đăng xuất khỏi hệ thống hoặc khóa màn hình (có mật khẩu) khi không sử dụng.

l. Tham khảo thêm các biện pháp bảo mật do hãng Microsoft hướng dẫn tại địa chỉ Internet "http://www.microsoft.com/vietnam/support/".