CẦN HOÀN THIỆN HÀNH LANG PHÁP LÝ VỚI TỘI PHẠM PHÁT TÁN VIRUS MÁY TÍNH VÀ TẤN CÔNG AN NINH MẠNG

Nguyễn Quang

461 website Việt Nam bị hacker trong và ngoài nước tấn công; 104 website Bkis phát hiện có lỗ hổng nghiêm trọng; 33.137 dòng virus máy tính mới xuất hiện (trong đó 33.101 dòng có xuất xứ từ nước ngoài); 59.450.000 lượt máy tính bị virus tấn công; trong đó virus W32.SecretW.Worm đã lây nhiễm trên 420.000 máy tính, trở thành virus nguy hiểm nhất trong năm – Đó là những nét chính về tình hình an ninh mạng của cộng đồng máy tính, mạng máy tính Việt Nam trong 1 năm (năm 2008). Vậy chế tài nào để điều chỉnh các hành vi vi phạm, tấn công an ninh mạng?

An ninh mạng với nhiều tình huống nguy cấp

Nhiều người sử dụng Internet và nhiều lần bị đặt vào tình huống nguy cấp - Đó là kết luận của những người bảo vệ an ninh mạng. Chưa có năm nào thế giới Internet lại có nhiều tình huống nguy cấp như 2008. Năm qua, ít nhất 3 lần, tất cả người sử dụng Internet trên thế giới đã bị đặt trong tình huống nguy hiểm và người sử dụng Việt Nam cũng nằm trong số đó. Điển hình là sự cố về lỗ hổng DNS Cache Poisoning. Khi lỗi này chưa được vá, kẻ xấu có thể chuyển hướng truy nhập vào nơi nào chúng muốn và lừa đảo bất kỳ ai. Tình hình nguy hiểm tới mức, hầu như tất cả các nhà sản xuất phần cứng hay phần mềm danh tiếng của thế giới như Sun, Cisco, Microsoft, Apple... đều phải tham gia phối hợp khắc phục. Hai lần khác là việc xuất hiện những lỗ hổng liên quan đến hệ điều hành Windows. Trong cả hai sự cố, Microsoft đều phải đưa ra bản vá khẩn cấp, không theo định kỳ như thông lệ.

Ở Việt Nam, tội phạm tin học sau 2 năm im ắng đã có dấu hiệu quay trở lại. Cụ thể là các vụ cướp tên miền của Công ty P.A Vietnam, vụ hack website Techcombank hay vụ tấn công DDoS... Tuy nhiên, sau khi một số vụ việc bị đưa ra ánh sáng và bị cơ quan chức năng xử lý thì làn sóng này đã được ngăn chặn kịp thời. Như Bkis đã nhiều lần phát biểu, những vi phạm trên mạng cũng luôn luôn để lại dấu vết như trong cuộc sống thực. Vì vậy, người có hành vi vi phạm sớm muộn cũng sẽ bị tìm ra.

Việt Nam ghi dấu ấn an ninh mạng với cộng đồng quốc tế. Đó là nhận xét của cộng đồng quốc tế khi nhiều trang tin công nghệ hàng đầu thế giới như CNET, PCWorld, ComputerWorld, InfomationWeek... nhiều lần đăng tải kết quả nghiên cứu, cảnh báo về an ninh mạng của các chuyên gia Việt Nam. Những cảnh báo này liên quan đến các thương hiệu toàn cầu như Google, Microsoft, Asus hay Toshiba... Sự kiện đã chứng tỏ người Việt Nam thực sự có năng lực trong lĩnh vực an ninh mạng.

Ngày 10/9, chỉ vài ngày sau khi ra mắt trình duyệt Chrome, Google Inc phải đưa ra bản vá. nhờ Bkis của Việt Nam cảnh báo về lỗ hổng tràn bộ đệm (Buffer Overflow) trong tính năng SaveAs. Người dùng Chrome khi truy nhập vào các website chứa mã khai thác, sẽ bị hacker chiếm quyền điều khiển máy tính.

Cũng thời điểm này, Microsoft xác nhận lỗ hổng tương tự trên phần mềm Windows Media Encoder được Bkis phát hiện và cảnh báo trước đó 5 tháng. Sau khi phối hợp cùng các chuyên gia Bkis, Microsoft đã phát hành bản vá mã số MS08 – 053.

Tháng 12, Bkis công bố lỗ hổng trong công nghệ nhận dạng khuôn mặt của ba hãng sản xuất Asus, Lenovo, Toshiba. Tính năng giúp ngăn chặn truy cập máy tính xách tay trái phép có thể dễ dàng bị vượt qua, dù được thiết lập ở mức an ninh cao nhất. Sắp tới đây, vào tháng 2/2009, các chuyên gia của Bkis sẽ trình bày nghiên cứu này tại Hội thảo Black Hat tại Mỹ (một hội thảo thường niên có uy tín về an ninh mạng) theo lời mời của Ban tổ chức. Vì vậy, những ghi nhận trên là có cơ sở thực tiễn.

Máy tính bị virus ồ ạt tấn công

Người sử dụng Yahoo Messenger khốn đốn vì virus Kavo. Hàng triệu người sử dụng Yahoo!Messenger tại Việt Nam đã lao đao, mất liên lạc với bạn bè, đối tác do Yahoo!Messenger không dùng được khi máy tính bị nhiễm virus Kavo, từ Trung Quốc. Chỉ tính riêng trong tháng 6, đã có 1,2 triệu máy tính tại Việt Nam bị nhiễm Kavo, với hàng loạt biến thể mới. Bình quân hơn 40.000 máy tính bị nhiễm trong một ngày, một kỷ lục về tốc độ lây lan. Đây cũng là loại virus có tốc độ xuất hiện biến thể nhiều nhất từ trước tới nay, trung bình mỗi ngày có tới 20 biến thể mới của Kavo được tung lên mạng.

Điều trớ trêu ở chỗ, việc nạn nhân cứ đăng nhập vào Yahoo!Messenger là bị thoát ra, không thể chat được lại không phải là chủ đích của kẻ phát tán virus. Mục tiêu của hacker là nhằm tấn công các game online để lấy cắp tài khoản của người chơi. Nhưng do mắc lỗi trong lập trình, khi virus can thiệp vào bộ nhớ của Yahoo!Messenger đã tự sinh ra lỗi truy xuất bộ nhớ (memory exception), khiến người sử dụng không thể đăng nhập vào ứng dụng này.

Ghi đè file chuẩn của Microsoft Windows – Xu hướng mới của virus: Không chỉ xuất hiện với số lượng lớn, xu hướng của các dòng virus mới còn là "lùng xục" những "ngóc ngách" của hệ điều hành Windows để ẩn náu, cũng như để tấn công trở lại những phần mềm diệt virus không có khả năng khôi phục mã gốc. Đây sẽ là xu hướng chính của virus trong năm 2009.

Cách thức của những virus này là ghi đè mã độc lên các file chuẩn của hệ điều hành. Việc ngụy trang lập lờ như vậy đánh lừa được hầu hết các phần mềm diệt virus không có cơ chế khôi phục file gốc đã bị virus ghi đè. Vì thế khi diệt virus, các phần mềm này đồng thời xóa luôn cả file chuẩn của hệ điều hành

(file gốc). Hậu quả là làm hỏng hệ điều hành. Chỉ trong tháng 10/2008, Bkis đã thống kê được tới 92 dòng virus mới xuất hiện sử dụng cơ chế ghi đè file chuẩn và lây nhiễm trên 41.600 máy tính tại Việt Nam. Cũng theo một khảo sát mới nhất mà Bkis vừa thực hiện, có tới 91% người sử dụng đã phải cài lại hệ điều hành khi máy tính bị nhiễm virus.

Đối phó với loại virus nguy hiểm này, các chuyên gia Bkis đã phải giải mã (debug) virus, tìm những đoạn mã gốc của file chuẩn bị virus mã hóa, sau đó cập nhật thuật toán diệt virus vào Bkav. Như vậy, có thể diệt virus này triệt để mà không gây hỏng hệ điều hành.

Virus giả gateway "quậy phá" tại hầu hết các cơ quan, doanh nghiệp: Mạng sập, website bị chèn banner, popup chữ Trung Quốc là những hiện tượng phổ biến nhất trong năm 2008 tại các cơ quan, doanh nghiệp, trong đó có cả các công ty Hosting (cho thuê máy chủ) cũng như các ISP (Nhà cung cấp dịch vụ Internet). Hầu hết các quản trị đã rất lúng túng khi gặp những sự cố virus giả gateway do chưa trang bị một giải pháp tổng thể phòng chống virus.

Hiện tượng này do các dòng virus giả gateway có xuất xứ từ Trung Quốc gây ra. Từ một máy tính bị nhiễm, virus gửi quảng bá (broadcast) gói tin theo giao thức ARP (giao thức phân giải địa chỉ) tới tất cả các máy tính khác trong cùng mạng để mạo danh là Gateway của hệ thống. Các kết nối ra Internet của tất cả các máy tính trong mạng lúc này sẽ bị lừa đi qua gateway giả mạo trước, rồi sau đó mới tới gateway thật. Không phải máy tính nào có hiện tượng bị chèn banner cũng là máy nhiễm virus và trong mạng hàng trăm máy tính, chỉ một máy tính bị nhiễm cũng có thể làm sập toàn bộ hệ thống mạng.

Năm 2009, hacker sẽ bị sờ gáy

Đúng như các dự báo mà Bkis đưa ra hồi cuối năm 2007, tình hình phức tạp của các mạng xã hội, blog đã trở thành vấn đề nổi cộm và các nhà cung cấp dịch vụ nước ngoài như Yahoo đã hợp tác với cơ quan quản lý nhà nước xử lý một số blog vi phạm. Google cũng cho biết, họ sẵn sàng hợp tác và tuân thủ luật pháp của từng nước, không ngoại trừ Việt Nam, để giải quyết những vấn đề bất trắc nảy sinh từ Internet. Virus là một trong những điểm nóng trong toàn cảnh an ninh mạng 2008. So với năm ngoái, số dòng virus mới tăng gấp 5 lần và số lượt máy tính bị nhiễm tăng gần gấp đôi năm ngoái, từ 33 triệu lên gần 60 triệu.

Năm 2009, virus vẫn sẽ tiếp tục xuất hiện hàng ngày với số lượng ngày càng tăng, đặc biệt là các dòng virus ghi đè file chuẩn. Tuy nhiên, những điều này có thể sẽ thay đổi nếu dự thảo sửa đổi luật hình sự mới đây của Trung Quốc sớm được thông qua. Theo đó, những hành vi phát tán virus để đánh cắp dữ liệu hoặc thâm nhập máy tính tại quốc gia này sẽ phải đối mặt với các hình phạt rất nặng. Khi đó số lượng virus trên toàn cầu có thể sẽ giảm bớt, bởi phần lớn số lượng mã độc hiện nay là có xuất xứ từ Trung Quốc.

Các cuộc tấn công và hack sẽ có chiều hướng giảm bớt vì nhiều vụ vi phạm trên mạng đã được xử lý. Những vụ việc phạm tội liên quan tới an ninh mạng trong những năm qua ở Việt Nam phần lớn là do thiếu hiểu biết về luật pháp. Trong năm tới, Luật Hình sự sửa đổi và bổ sung sẽ được Quốc hội chính thức thông qua và ban hành vào đầu năm 2010. Trong đó, các điều khoản liên quan đến tội phạm công nghệ cao đã được Bộ Tư pháp phối hợp cùng Bộ Công an (cụ thể là Cơ quan phòng chống tội phạm công nghệ cao C15), chỉnh sửa và bổ sung. Theo đó, các hành vi phạm tội như tấn công từ chối dịch vụ, phát tán virus, lừa đảo, tấn công trực tuyến... đã được định nghĩa rất chi tiết. Và hình phạt cao nhất cho các hành vi này có thể lên đến 12 năm tù giam. Đây chính là hành lang pháp lý để áp dụng xử lý nghiêm việc phạm tội của tin tặc ■

Express Advantage - Gói Giải Pháp dành cho các DNN&V

Hồ Điệp

IBM Việt Nam đã ra mắt gói giải pháp Express Advantage mới với các sản phẩm, dịch vụ bổ sung và tăng cường dành cho các doanh nghiệp nhỏ và vừa (DNN&V), giúp các DNN&V tối đa hóa hiệu quả kinh doanh trong nền kinh tế hội nhập.

Express Advantage tích hợp các sản phẩm công nghệ, các giải pháp kinh doanh toàn diện được hỗ trợ bởi một mạng lưới tại chỗ bao gồm các đối tác kinh doanh của IBM và các loại hình dịch vụ khách hàng sẽ hỗ trợ khách hàng tích cực hơn và toàn diện hơn thúc đẩy sáng tạo và tăng trưởng.

Ông Võ Tấn Long, Tổng Giám Đốc Công ty IBM Việt Nam cho biết: "Các DNN&V cũng gặp nhiều thách thức về công nghệ và kinh doanh tương tự như các công ty lớn và cần phải giải quyết những thách thức đó với nguồn lực và thời gian có hạn. Express Advantage của IBM được thiết kế để đáp ứng những nhu cầu này với các giải pháp đã được tích hợp trọn gói, dễ chọn lựa, dễ mua và dễ quản lý."

Các danh mục sản phẩm Express Advantage gồm: dịch vụ lưu trữ và phục hồi an ninh mạng, dòng sản phẩm máy chủ, phần mềm doanh nghiệp, hệ thống tích hợp toàn phần cho các giải pháp bán lẻ, các giải pháp lưu trữ hệ thống cũng như các gói dịch vụ và dòng máy chủ hoạt động trên bộ xử lý POWER6Ă. Express Advantage cũng bao gồm các gói giải pháp trọn gói như: giải pháp bán lẻ, giải pháp chứng khoán, giải pháp quản lý nguồn lực hiệu quả dành cho các doanh nghiệp sản xuất kinh doanh tạo ra nhiều lựa chọn ứng dụng và giảm chi phí năng lượng và quản trị cho khách hàng.

Ông Hoàng Thanh Tùng, Giám đốc điều hành công ty cổ phần Giải Pháp Truyền Thông APZON cho biết: "Các sản phẩm có trong gói Express Advantage giúp công ty chúng tôi tự tin hơn khi đưa ra các giải pháp quản trị kinh doanh được tích hợp và thiết kế đặc biệt cho các nhu cầu quản lý, vận hành toàn diện của doanh nghiệp là các khách hàng của chúng tôi. Sử dụng các sản phẩm trong gói Express Advantage chúng tôi có thể tối ưu hóa tính năng cập nhật và tích hợp để giúp các khách hàng ứng dụng phần mềm duy nhất để tự động hóa quy trình hoạt động, có tầm nhìn toàn cảnh về mua bán hàng, tình hình tài chính..., qua đó doanh nghiệp có thể đưa ra các quyết định đúng đắn, kịp thời và hiệu quả trong hoạt động kinh doanh.