NHỮNG "GÓC SÁNG" CỦA AN NINH MẠNG VN 2006

"Góc s

"Góc sáng" trong Bức tranh bảo mật Việt Nam năm 2006 là tiến trình hình thành một nền móng "an ninh mạng tầm cỡ quốc gia".

Một phần "thế giới ngầm" tội phạm mạng bị phá vỡ

"Quyền lực điều khiển thông tin là một ma lực, nếu anh trong sạch ma lực sẽ không phát tán, còn nếu anh nhúng tay vào chàm, chính ma lực này sẽ đưa anh đi hết từ sai lầm này đến sai lầm khác" - Đó là sự tỉnh ngộ muộn mằn của một người trẻ tuổi: Cậu bị bắt vì đã sử dụng các kiến thức về CNTT để tiến hành các hoạt động phi pháp, làm giả thẻ ATM rút tiền trục lợi hàng trăm triệu đồng.

Nhưng người này cũng chỉ là một mắt xích trong những đường dây "bạch tuộc" Cashout tinh vi, lớn cả về số lượng lẫn quy mô ở Việt Nam.

Thậm chí, nhiều người còn cho rằng những đường dây ấy mang dáng dấp những phiên bản của Mafia quốc tế.

Những kẻ kiếm tiền phi pháp qua mạng Internet ở Việt Nam ngày nay đã hình thành những đường dây tinh vi, tự gọi mình là dân "Underground" (thế giới ngầm), chúng hoạt động thực sự có tổ chức.

Các hoạt động phi pháp mang lại nguồn lợi lớn đã khiến những cư dân trong thế giới ấy mờ mắt. Nhưng những kiến thức, thủ thuật, hiểu biết, công nghệ... dù tinh vi đến mấy trên môi trường mạng cũng không thể xoá sạch hay thay đổi bản chất của hành vi phạm pháp.

Năm 2006, một trong những hoạt động hiệu quả nhất của cơ quan an ninh Việt Nam chính là xử lý hàng loạt đường dây Cashout như vậy và những mắt xích quan trọng của nó tại Việt Nam, một phần "Thế giới ngầm" đã bị phá vỡ!

Ngày 4/1/2006, đường dây Cashout lớn do các đối tượng tuổi đời còn rất trẻ người Việt Nam tổ chức đã bị điều tra và phanh phui, sau đó đưa ra khởi tố 7 đối tượng. Đây là sự kiện mở màn cho một năm làm việc thẳng tay của giới chức với đối tượng tội phạm hoàn toàn mới này ở Việt Nam.

"Cảnh sát mạng" hoạt động hiệu quả

"Bức tranh" sự kiện an ninh mạng Việt Nam năm 2006 (Nguồn: VNN)

Hàng chục vụ việc liên quan đến các đường dây ATM - Cashout, "Ship hàng" (trục lợi bằng các thẻ tín dụng ăn trộm của người nước ngoài qua mạng Internet) đã bị cơ quan điều tra đưa ra ánh sáng. Người ta sửng sốt vì tính chất phức tạp và các yếu tố công nghệ vô cùng tinh vi của loại hình tội phạm này, càng chứng tỏ năng lực của cơ quan điều tra chuyên trách tại Việt Nam là đáng tin cậy.

Năm 2006 cũng là năm "loạn" tấn công tên miền và virus nội, năm các doanh nghiệp TMĐT "điêu đứng" vì tội phạm mạng, nhưng tất cả các vụ việc lớn đã nêu cuối cùng đều được điều tra và tìm ra thủ phạm.

Hẳn những người như Casher Tô Phúc Hậu, Nguyễn Đình Cường, Nguyễn Anh Tuấn, Trần Quang Duy, Trần Nguyễn Trung Trực... những hacker như Nguyễn Quang Huy, Nguyễn Thành Công ... còn chưa hết bất ngờ vì những hoạt động sai phạm hết sức tinh vi của họ trên môi trường "ảo" Internet tại sao lại bị cơ quan chức năng phát giác nhanh đến vậy.

Nhiều người nhắc tới phòng Chống tội phạm công nghệ cao thuộc Cục điều tra tội phạm kinh tế và chức vụ - C15 - Bộ Công An. Đây là đơn vị từng tiến hành điều tra và làm rõ hàng loạt vụ việc nổi cộm trong giới tội phạm tin học năm 2006.

Ngoài ra các đơn vị như PC14 hoặc công an kinh tế... hay Trung tâm an ninh mạng ĐH Bách Khoa HN (BKIS) cũng là những đơn vị hoạt động hết sức hiệu quả. Và dần hình thành những quy trình phối hợp nhuần nhuyễn. Đặc biệt BKIS từng nhiều lần tham gia phối hợp cùng C15 phát hiện và xử lý nhiều đối tượng lừa đảo trực tuyến, phát tán virus và tấn công website.

2006 cũng là năm VNCERT - Trung tâm ứng cứu khẩn cấp sự cố máy tính quốc gia (do Bộ BCVT thành lập theo quyết định của Thủ tướng chính phủ tháng12/2005) - bước vào hoạt động và tạo ảnh hưởng lớn trong xây dựng nền móng an ninh mạng quốc gia. Đơn vị này đã có công gắn kết nhiều lực lượng xung yếu trong nước cùng ngồi vào giải quyết bài toán an ninh mạng quốc gia và khu vực.

An ninh mạng tầm quốc gia

Trước hết là hành lang pháp lý: 2006 phải được nhắc đến như một năm xây dựng nền móng hành lang pháp lý tương đối hoàn thiện trong lĩnh vực CNTT - Viễn thông. Tất nhiên có cả các vấn đề cho bảo mật.

Đó là luật CNTT, luật Giao dịch điện tử và hàng loạt văn bản dưới luật được ban hành và đi vào đời sống. Những nỗ lực này của cơ quan chức trách trong điều kiện VN gia nhập WTO, cũng như tình hình an ninh mạng ngày càng có ảnh hưởng lớn, là điều vô cùng đáng mừng cho bức tranh bảo mật của Việt Nam.

Sau đó phải kể đến những dấu ấn rất rõ nét về quá trình phối hợp nhằm đảm bảo an ninh mạng giữa nhiều khối đơn vị trong những sự kiện lớn.

Bảo vệ an toàn thông tin trong tuần lễ APEC 14 tại Hà Nội là một ví dụ điển hình nhất: "Lần đầu tiên những người trong khối doanh nghiệp chúng tôi được yêu cầu đứng chung vào một guồng máy với cơ quan quản lý nhằm đảm bảo an toàn thông tin cho 4 website trọng yếu trong tuần lễ Apec." - Anh Hoàng Trọng Thanh - Giám đốc công ty OTC - đơn vị xây dựng website chính thức của APEC 2006 cho biết.

Để đảm bảo an toàn thông tin cho sự kiện Thủ tướng Nguyễn Tấn Dũng giao lưu trực tuyến với đồng bào, hầu hết các đơn vị trọng yếu về an ninh thông tin và các ISP, OSP, các công ty phần mềm... đều đã được yêu cầu và hình thành quy trình làm việc vô cùng bài bản.

"Kinh nghiệm lớn nhất của chúng tôi trong năm 2006 là chỉ đạo điều phối nhiều đơn vị trong nước cùng thực hiện các yêu cầu và nhiệm vụ cụ thể về an toàn thông tin. Tiếp đó là kinh nghiệm bảo vệ an toàn thông tin các sự kiện nhạy cảm và kinh nghiệm hợp tác quốc tế về an ninh mạng." - Ông Đỗ Ngọc Duy Trác - Trưởng phòng nghiệp vụ của VNCERT nói.

Những ngày đầu năm 2007, giới chức càng tỏ rõ quyết tâm trong quá trình củng cố nền móng an ninh mạng quốc gia khi Bộ BCVT ban hành "Chỉ thị tăng cường đảm bảo an ninh thông tin trên không gian mạng". (Chỉ thị Số 03/2007/CT-BBCVT do Bộ trưởng Đỗ Trung Tá ký).

Người dùng và doanh nghiệp không còn đơn độc?

Thông tin từ trung tâm VNCERT cũng cho hay, sau hai lần diễn tập quy mô lớn với các đơn vị trong nước và các nước khu vực, ngày 20/2/2007 vừa qua, trung tâm này đã phối hợp với JPCERT (Nhật Bản) xử lý hai website do hacker nước ngoài đặt host tại Việt Nam có hành vi phishing các ngân hàng của Nhật.

Đại diện của VNCERT nói rằng trong tương lai, các hoạt động như thế sẽ thường xuyên có sự hợp tác với các trung tâm CERT trong khu vực, "do chúng tôi đã hoàn tất các thủ tục và chỉ còn chờ chính thức trở thành thành viên của APCERT (Hiệp hội các tổ chức ứng cứu sự cố khẩn cấp máy tính khu vực Châu Á Thái Bình Dương). VNCERT tự tin có đủ tư cách và đáp ứng đầy đủ yêu cầu trong phối hợp an ninh tầm cỡ quốc gia với các nước trong khu vực".

Nếu như 2006, khối doanh nghiệp bắt đầu tham gia vào guồng máy an ninh mạng quốc gia, thì năm 2007, người dùng cuối sẽ đóng vai trò quan trọng. Đây là lực lượng mà mọi hoạt động của họ trên môi trường mạng đều có thể tạo ra những tác động về an toàn thông tin.

Năm 2007, ý thức về bảo mật của người dùng Việt Nam sẽ được nâng lên nhiều, sau hàng loạt "bài học đau thương" từ những sự kiện đình đám năm 2006.

VNCERT đưa ra lời hứa: "Năm nay chúng tôi sẽ đưa ra một quy trình tương tác hai chiều với người dùng: Người dùng có thể báo cáo sự cố, thông báo yếu điểm, cho các sở, các ban ngành và trực tiếp cho VNCERT. Ngược lại VNCERT cũng có thể tư vấn, cảnh báo sớm, cung cấp các công cụ miễn phí, nâng cao ý thức... giúp người dùng tự bảo vệ mình trên không gian mạng."

Năm qua, hình ảnh những doanh nghiệp như Vietco, Nhân Hoà, PeaceSoft... một mình trong cuộc chiến với hacker, hay hàng chục ngàn người dùng YM Việt Nam phải "vật lộn" với "đại dịch virus nội"... vẫn là những nét u tối trong bức tranh an ninh mạng. Sang năm 2007, hy vọng những mảng tối ấy sẽ dần được sáng tỏ!.

Thế Phong