GIẢI PHÁP PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO

TS. NGUYỄN VIỆT HÙNG - *Phó Cục trưởng Cục Tin học và Thống kê tài chính (Bộ Tài chính)*

Theo báo cáo của Tổ chức Cảnh sát Hình sự Quốc tế (Interpol), tội phạm sử dụng công nghệ cao đang trở thành mối nguy hại lớn trên giới với thiệt hại gây ra khoảng 400 tỷ USD/năm, cao hơn số tiền mà tội phạm buôn bán ma túy thu được và cứ 14 giây lại xảy ra 01 vụ phạm tội sử dụng công nghệ cao. Ở Việt Nam, tội phạm sử dụng công nghệ cao gia tăng nhanh chóng, diễn biến phức tạp và gây ra nhiều hậu quả nghiêm trọng. Giải pháp nào để phòng chống tội phạm công nghệ cao trong bối cảnh hiện nay là vấn đề đang đặt ra cần giải quyết.

Từ khóa: Tội phạm công nghệ cao, máy tính, không gian ảo, tin tặc

According to a report of International Criminal Police (Interpol), high-tech criminal is becoming a major threat to the world causing losses of about $ 400 per year, higher than the recorded value of drug-trafficking criminal. It is also recorded that cybercrimes are committed every 14 seconds. In Vietnam, high technology crime has grown rapidly and causing serious consequences. Effective solutions to prevent high-tech criminal for the current context is now considered a focus.

Keywords: high-tech criminal, computer, cyberspace, hackers

Ngày nhận bài: 5/5/2017
Ngày chuyển phản biện: 9/5/2017
Ngày nhận phản biện: 26/5/2017
Ngày chấp nhận đăng: 28/5/2017

Tổng quát về tội phạm công nghệ cao

Tội phạm công nghệ cao còn có một số tên gọi khác: tội phạm máy tính, tội phạm sử dụng công nghệ cao, tội phạm ảo, tội phạm không gian ảo, tin tặc. Trên thế giới, cùng với sự phát triển của máy tính, mạng máy tính và Internet, tội phạm công nghệ cao đã trải qua nhiều hình thái, từ đơn giản đến phức tạp, từ những cá thể đơn lẻ phát triển thành các tổ chức lớn và hoạt động ngày càng trở nên tinh vi.

Vào những năm 1960, các cuộc tấn công làm sập hệ thống điện thoại đường dài thường để giải trí hoặc sử dụng dịch vụ không mất tiền. Những năm 1980, các lập trình viên bắt đầu viết phần mềm mã độc, bao gồm các chương trình tự nhân bản, để can thiệp vào hoạt động của máy tính cá nhân.

Giai đoạn Internet bắt đầu phát triển mạnh, tội phạm thông qua Internet truy cập trái phép vào các hệ thống được bảo vệ kém để phá hoại, trục lợi về tài chính hoặc thực hiện các hành động có mục đích chính trị. Những năm 1990, tội phạm tài chính sử dụng phương thức thâm nhập máy tính tăng mạnh, mã độc thay đổi theo hướng khai thác điểm yếu của hệ điều hành.

Từ giữa những năm 1990, các ứng dụng phi pháp liên quan đến thư điện tử phát triển mạnh, tạo ra cơn thác lũ thư điện tử giả mạo và thư quảng cáo. Thế kỷ XXI xuất hiện loại mã độc mới được gọi tên là tấn công đeo bám hay tấn công có chủ đích. Loại mã độc này được thiết kế để thâm nhập một cách hợp pháp vào hệ thống mạng được nhắm tới, sau đó thiết lập kết nối và nhận lệnh từ máy chủ chỉ huy trên Internet để thực hiện hoạt động phá hoại.

Ở thời kỳ đầu, tội phạm công nghệ cao chủ yếu là những cá nhân bất mãn hay nhân viên không trung thực. Tiếp đó, xuất hiện hình thái tội phạm công nghệ cao có tổ chức, trong đó bao gồm các tổ chức hoạt động có mục đích chính trị. Thế kỷ XXI bắt đầu xuất hiện bằng chứng của việc tồn tại các tổ chức tội phạm công nghệ cao được chính phủ tài trợ để thực hiện các hoạt động thâm nhập trái phép vào những cơ quan đầu não của nhà nước đối lập thông qua mạng Internet.

Ở Việt Nam, loại hình tội phạm công nghệ cao ngày càng gia tăng đặc biệt. Tuy nhiên, từ năm 2010 trở lại đây, khi ứng dụng công nghệ thông tin (CNTT) tại Việt Nam phát triển mạnh, số lượng vụ việc của loại hình tội phạm này tăng lên rất nhanh, tác động lớn đến an toàn, trật tự xã hội và an ninh quốc gia.

Xét về động cơ, về cơ bản có 3 nhóm tội phạm sau: (1) Học sinh, sinh viên hay những người muốn chứng minh năng lực của bản thân mà thực hiện các hoạt động tấn công mạng vào các trang tin trên Internet; (2) Các cá nhân, tổ chức chuyên lừa đảo để trục lợi về kinh tế; (3) Các cá nhân, tổ chức thực hiện hoạt động phá hoại hệ thống thông tin với mục đích chính trị.

Nhóm thứ 3 có mức độ tác động lớn nhất, gây ảnh hưởng đến trật tự, an toàn xã hội và an ninh quốc gia. Đặc biệt, nhóm này chủ yếu có nguồn gốc nước ngoài, không loại trừ có trường hợp được hậu thuẫn từ chính phủ, do đó rất khó xử lý, đối phó.

Việc bảo đảm an toàn cho các hệ thống thông tin nói chung và bảo vệ hệ thống trước các cuộc tấn công của tội phạm công nghệ cao đã trở thành nhiệm vụ quan trọng, một phần không thể thiếu trong công tác ứng dụng CNTT của Bộ Tài chính và các đơn vị thuộc Bộ.

Đối với nhóm 1 và nhóm 2, lực lượng công an có thể thực hiện hoạt động phá án, truy bắt thủ phạm. Riêng đối với nhóm 3, việc cơ bản cần làm là thực hiện các hoạt động tự bảo vệ, phát hiện, hạn chế hành động phá hoại và hậu quả của các hành động này, rất khó có thể truy tìm thủ phạm để tiêu diệt tận gốc vấn đề.

Khung pháp lý phòng, chống tội phạm công nghệ cao

Lường được những hậu quả cũng như để tự bảo vệ, phát hiện các hành động phá hoại của tội phạm công nghệ cao, các nước tiên tiến trên thế giới đã thiết lập hành lang pháp lý chặt chẽ nhằm phòng chống tội phạm công nghệ cao. Cụ thể như: Năm 1986, Mỹ đã ban hành Luật Lừa đảo và lạm dụng máy tính. Luật này đã được điều chỉnh một số lần vào các năm 1989, 1994, 1996, 2001, 2002 và 2008; Nhật Bản ban hành Luật Truy cập máy tính trái phép vào năm 1999; Australia ban hành Luật Tội phạm ảo năm 2001; Philippines ban hành Luật Phòng tránh tội phạm ảo tháng 12/2012, tuy nhiên một số phần của Luật này bị Tòa án Tối cao tuyên bố không hợp hiến. Các nước không có luật riêng về tội phạm công nghệ cao thì đều định danh loại tội phạm này trong Luật hình sự.

Bộ Luật hình sự năm 2015 của Việt Nam định danh một số hành vi sau liên quan đến máy tính là tội phạm, phải chịu các các khung hình phạt của Bộ Luật này: Sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào các mục đích trái pháp luật; Phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; Cản trở hoặc gây rối loại hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; Đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông; Xâm phạm trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác; Sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản; Thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng; Cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông… Các tội phạm này bị xử phạt từ 20 triệu đồng đến 1 tỷ đồng hoặc bị phạt tù từ 01 đến 07 năm, có thể bị cấm hành nghề từ 01 đến 05 năm hoặc tịch thu một phần hoặc toàn bộ tài sản.

Năm 2015, Quốc hội Việt Nam thông qua Luật An toàn thông tin mạng, tạo nền tảng pháp lý và nâng cao chất lượng hoạt động bảo vệ các hệ thống CNTT và mạng máy tính của Việt Nam trước các cuộc tấn công của tội phạm công nghệ cao. Trên cơ sở đó, Chính phủ đã ban hành nhiều văn bản triển khai thực hiện Luật An toàn thông tin mạng vào cuộc sống như: Nghị định 58/2016/NĐ-CP quy định chi tiết về kinh doanh sản phẩm, dịch vụ mật mã dân sự và xuất khẩu, nhập khẩu sản phẩm mật mã dân sự; Nghị định 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ; Nghị định 108/2016/NĐ-CP quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; Quyết định 05/2017/QĐ-TTg ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.. Dự kiến trong năm 2017 Chính phủ sẽ tiếp tục ban hành một số văn bản thực thi Luật này.

Về lực lượng tham gia phòng chống tội phạm công nghệ cao của Việt Nam hiện có Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông và các Bộ chủ quản hệ thống thông tin. Một số bộ chủ quản, trong đó có Bộ Tài chính, đã thành lập phòng chuyên trách về an toàn an ninh thông tin.

Cục Cảnh sát phòng, chống tội phạm sử dụng công nghệ cao, trực thuộc Tổng cục Cảnh sát, bộ Công an, được thành lập năm 2010. Cho đến nay, đơn vị đã phát hiện, xác minh, điều tra và chỉ đạo lực lượng tại địa phương điều tra trên hàng nghìn đầu mối vụ việc liên quan đến công nghệ cao. Trong đó, đã điều tra, làm rõ và chuyển cơ quan điều tra các cấp hàng trăm vụ việc, hơn 1000 bị can; chuyển cơ quan thanh tra chuyên ngành các cấp xử phạt hành chính hàng trăm vụ, thu hồi tiền và hàng nghìn máy

tính xách tay, điện thoại di động, linh kiện điện tử, hàng hóa, máy móc… trị giá hàng trăm tỷ đồng.

Phòng chống tội phạm công nghệ cao tại các cơ quan tài chính

Trong những năm qua, Bộ Tài chính được đánh giá là đơn vị đi đầu trong khối các cơ quan nhà nước về ứng dụng CNTT. CNTT được áp dụng mạnh trong giao dịch nội bộ, các hoạt động nghiệp vụ và đặc biệt trong các dịch vụ hành chính công phục vụ người dân, doanh nghiệp. Đối với một số đơn vị thuộc và trực thuộc Bộ như Kho bạc Nhà nước, Tổng cục Hải Quan, Tổng cục Thuế, các Sở Giao dịch chứng khoán, Trung tâm Lưu ký chứng khoán, nghiệp vụ của đơn vị sẽ không thể vận hành/vận hành hiệu quả nếu không có hệ thống thông tin. Việc bảo đảm an toàn cho các hệ thống thông tin nói chung và bảo vệ hệ thống trước các cuộc tấn công của tội phạm công nghệ cao đã trở thành nhiệm vụ quan trọng, một phần không thể thiếu trong công tác ứng dụng CNTT của Bộ Tài chính và các đơn vị thuộc Bộ.

Các hoạt động về an toàn thông tin của ngành Tài chính được thực hiện theo "Khung an toàn thông tin ngành Tài chính" và chỉ đạo của Lãnh dạo Bộ, bao gồm 8 khía cạnh cần quan tâm về an toàn thông tin để đảm bảo tính tổng thể, toàn diện và hiệu quả của các hoạt động này, cụ thể như sau:

Thứ nhất, tuân thủ các quy định, tiêu chuẩn về an toàn thông tin: Xây dựng và tổ chức triển khai các quy định, quy trình, tiêu chuẩn về an toàn thông tin của ngành Tài chính trên cơ sở các quy định, tiêu chuẩn an toàn thông tin của quốc tế và Việt Nam (bộ tiêu chuẩn ISO/IEC 27000 và các tiêu chuẩn liên quan).

Thứ hai, hoàn chỉnh cơ cấu quản lý an toàn thông tin: Hoàn thiện tổ chức bộ phận chuyên trách về quản lý an toàn thông tin; Quy định đầy đủ và rõ ràng các vai trò, trách nhiệm và mối quan hệ giữa các đơn vị, bộ phận và từng vị trí công tác trong công tác đảm bảo an toàn thông tin.

Thứ ba, nâng cao năng lực đội ngũ cán bộ làm công tác đảm bảo an toàn thông tin: Xây dựng các tiêu chuẩn về năng lực, đào tạo nâng cao năng lực cán bộ quản lý và kỹ thuật làm công tác đảm bảo an toàn thông tin; hình thành đội ngũ chuyên gia về an toàn thông tin.

Thứ tư, duy trì và nâng cấp hệ thống kỹ thuật đảm bảo an toàn thông tin: Duy trì hệ thống đã trang bị và nâng cấp thường xuyên, đảm bảo tính tuân thủ của các hệ thống này đối với các chính sách, quy định về an toàn thông tin của ngành Tài chính và khả năng bảo vệ hiệu quả thông tin và các hệ thống thông tin của ngành Tài chính.

Thứ năm, ứng cứu khẩn cấp: Xây dựng liên minh ứng cứu sự cố an toàn thông tin. Thiết lập cơ chế ứng phó hiệu quả và kịp thời với các sự cố, vi phạm và tấn công về an toàn thông tin.

Thứ sáu, nghiên cứu, hợp tác: Nghiên cứu tình hình, xu hướng tấn công và giải pháp đảm bảo an toàn thông tin của Việt Nam và thế giới và khả năng ứng dụng vào công tác đảm bảo an toàn thông tin của ngành Tài chính; Đẩy mạnh các hoạt động hợp tác, phối hợp về an toàn thông tin với các cơ quan chức năng, các tổ chức, chuyên gia có uy tín về an toàn thông tin.

Thứ bảy, giám sát đảm bảo thực thi: Triển khai công tác kiểm tra, kiểm toán về CNTT (bao gồm kiểm tra, kiểm toán về an toàn thông tin).

Bộ Tài chính được đánh giá là đơn vị đi đầu trong khối các cơ quan nhà nước về ứng dụng công nghệ thông tin. Công nghệ thông tin được áp dụng mạnh trong giao dịch nội bộ, các hoạt động nghiệp vụ và đặc biệt trong các dịch vụ hành chính công phục vụ người dân, doanh nghiệp.

Thứ tám, đào tạo, nâng cao nhận thức cho cán bộ toàn ngành về an toàn thông tin: Thực hiện đào tạo, nâng cao nhận thức thường xuyên cho toàn thể cán bộ, công chức, viên chức ngành tài chính, thúc đẩy hình thành văn hóa có nhận thức cao về an toàn thông tin trong ngành Tài chính.

Cho đến nay, công tác đảm bảo an toàn thông tin, phòng chống tội phạm công nghệ cao tại Bộ Tài chính vẫn đang tiếp tục được đẩy mạnh và triển khai một cách toàn diện trên tất cả các khía cạnh từ chính sách, con người cho đến giải pháp kỹ thuật. Tình trạng thiếu nhân lực cấp độ chuyên gia về an toàn thông tin đang được nghiên cứu bù đắp bằng việc sử dụng các dịch vụ an ninh mạng chuyên nghiệp. Bên cạnh đó, các quy định và chính sách mới của Nhà nước về an toàn thông tin mạng cũng giúp làm thành một điểm tựa vững chắc cho công tác đảm bảo an toàn thông tin của Bộ Tài chính, vượt qua giai đoạn tự mày mò và tìm hiểu, áp dụng các tiêu chuẩn, kinh nghiệm của nước ngoài có nhiều điểm không phù hợp với điều kiện của Việt Nam.

Tài liệu tham khảo:

1. Các báo cáo của Tổng cục Cảnh sát phòng, chống tội phạm - Bộ Công an;

2. Luật An toàn thông tin mạng (2015);

3. Tài liệu Brief History of Computer Crime của M.E.KaBay.