BẢO ĐẢM AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN TRONG CƠ QUAN NHÀ NƯỚC

Nguyễn Thị Thúy Hoa *

Tóm tắt: *Trong thời đại cách mạng công nghiệp 4.0, sự phát triển mạnh mẽ của khoa học - công nghệ đã tạo ra thời cơ mới để nước ta đẩy nhanh tiến trình công nghiệp hóa, hiện đại hóa đất nước. Tuy nhiên, việc ứng dụng công nghệ thông tin cũng tiềm ẩn rất nhiều nguy cơ đối với an toàn, an ninh thông tin. Vì thế, nâng cao nhận thức và năng lực bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin trong cơ quan nhà nước là một trong những nhiệm vụ quan trọng, cấp thiết hiện nay.*

Từ khóa: *an ninh mạng; hệ thống thông tin; cơ quan nhà nước*

Abstract: *In the era of the Industrial Revolution 4.0, the strong development of science - technology has created new opportunities for our country to accelerate the process of industrialization and modernization of the country. However, the application of information technology is also a lot of potential risks to the safety and security of information. Therefore, awareness-raising and capacity to ensure the safety, security for information systems in state agencies is one of the important and urgent tasks today.*

Keywords: *network security; information system; State agencies*

Ngày nhận bài: 20/12/2017 Ngày sửa bài: 30/12/2017 Ngày duyệt đăng: 15/01/2018

1. Khái quát về hệ thống thông tin và an ninh mạng

Hệ thống thông tin nói chung hay hệ thống thông tin trong cơ quan nhà nước nói riêng là hệ thống tiếp nhận các nguồn dữ liệu như các yếu tố vào và xử lý chúng thành các sản phẩm thông tin là các yếu tố ra [2]. Hoạt động của các hệ thống thông tin như sau: Nhập dữ liệu vào, tiếp theo xử lý dữ liệu thành thông tin, cuối cùng đưa thông tin ra và lưu trữ các nguồn dữ liệu.

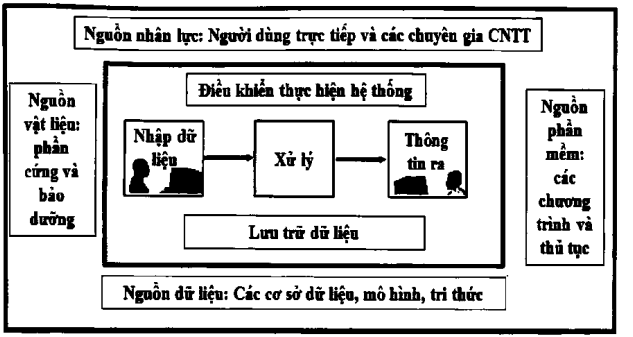
Ngày nay, máy tính đóng vai trò rất quan trọng trong việc xây dựng các hệ thống thông tin, cho nên khi nói đến hệ thống thông tin luôn được hiểu là nói đến hệ thống thông tin có sử dụng máy tính. Dưới đây là mô hình cơ bản về hệ thống thông tin (có sử dụng máy tính):

An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân [1].

Bước sang thế kỷ XXI, thế giới chuyển sang cuộc cách mạng công nghiệp mới - cách mạng công nghiệp 4.0. Đây là cuộc cách mạng gắn liền với sự phát triển của không gian mạng. Sự kết nối và tương tác thông qua Internet đã

* *TS, Trường Đại học Nội vụ Hà Nội.*

Hình 1. Mô hình cơ bản của hệ thống thông tin có ứng dụng công nghệ thông tin



thúc đẩy tiến trình phát triển xã hội. Không gian mạng đã trở thành một bộ phận cấu thành và đóng vai trò quan trọng trong việc xây dựng xã hội thông tin và kinh tế tri thức. Bên cạnh những lợi ích mà công nghệ thông tin đem lại cũng xuất hiện nhiều nguy cơ tiềm ẩn đe dọa an toàn, an ninh mạng đối với hệ thống thông tin trong các cơ quan tổ chức, trong đó có khối cơ quan nhà nước. Hiện nay, xu hướng, tốc độ phát triển, ứng dụng công nghệ thông tin diễn ra nhanh chóng làm cho tình hình an ninh mạng ở nước ta ngày càng diễn biến phức tạp. Nhiều hệ thống thông tin của các cơ quan nhà nước đã trở thành mục tiêu tấn công thường xuyên của tin tặc.

2. Thực trạng an ninh mạng đối với hệ thống thông tin trong các cơ quan nhà nước hiện nay

Mô hình cơ bản về hệ thống thông tin ở Hình 1 cho chúng ta hình dung rõ mối quan hệ giữa các thành phần và các hoạt động của hệ thống thông tin, đó là: tài nguyên, cấu trúc và hoạt động. Khai thác các yếu tố này, những cuộc tấn công gần đây đã lợi dụng lỗ hổng bảo mật để thay đổi giao diện; chèn liên kết giả mạo giao diện nhằm mục đích lừa đảo; dùng phần mềm gián điệp tấn công đánh cắp thông tin, tài liệu và tấn công từ chối dịch vụ,... Hình thức tấn công có chủ đích, nhằm vào các đối tượng cụ thể ngày càng phổ biến, đa dạng và tinh vi thực sự là thách thức đối với công tác đảm bảo an toàn thông tin. Phương thức, thủ đoạn tấn công của tin tặc chủ yếu vẫn tập trung nhằm vào hệ thống mạng thông tin, các website, cổng thông tin điện tử,... Trong đó, xu hướng sử dụng mã độc mã hóa dữ liệu, yêu cầu người sử dụng phải trả tiền mới gỡ bỏ được. Đặc biệt, xuất hiện loại virus gián điệp xâm nhập, tấn công để lại các dấu hiệu trên hệ thống máy tính của một số cơ quan như: Viện nghiên cứu; các công ty làm ăn với nước ngoài,... có dấu hiệu gia tăng và xuất hiện với tần xuất thường xuyên hơn. Một số thủ đoạn tấn công phổ biến là:

Thứ nhất, tấn công vào dữ liệu, chiếm

quyền quản trị website; tấn công chèn các đoạn mã script nguy hiểm có thể gây nguy hại cho người truy cập; tấn công gây treo hệ thống trong thời gian ngắn,... dẫn đến Hacker có thể chiếm quyền kiểm soát máy chủ, lấy toàn bộ thông tin bí mật trong tài khoản sau đó thay đổi nội dung website để thực hiện lừa đảo và tiến hành các hành vi phạm tội. Đó là vụ tấn công hệ thống thông tin của cụm Cảng hàng không Quốc tế Nội Bài, Tân Sân Nhất và hệ thống máy chủ của Vietnam Airlines gây hậu quả nghiêm trọng, làm trễ hàng chục chuyến bay, thông tin của hơn 400.000 khách hàng của Vietnam Airlines bị mất và phát tán lên môi trường mạng,...[3].

Thứ hai, lợi dụng những điểm yếu của các website thuộc các cơ quan nhà nước có tên miền.vn hoặc .gov,... Hacker chiếm quyền điều khiển website, chèn link giả mạo làm cho người sử dụng lầm tưởng đây là các trang website chính thống để khai báo các thông tin, mật khẩu OTP. Điển hình là vụ tấn công của tin tặc giả mạo lệnh chuyển tiền đối với Ngân hàng thương mại Cổ phần Tiên phong [3].

Thứ ba, lợi dụng cơ chế mở của Facebook và Google, các đối tượng lập các trang thông tin điện tử tổng hợp, trang mạng xã hội như Facebook, Zalo,... ẩn các thông tin cá nhân để đăng tải các thông tin không đúng trên các trang mạng nhằm đánh lừa người sử dụng, làm người sử dụng lầm tưởng các trang thông tin chính thống để đăng nhập, chia sẻ, bình luận gây hiệu ứng tâm lý xã hội trước những vấn đề có tính thời sự của đất nước. Năm 2016, Bộ Công an đã phát hiện hơn 120 website, blog của các đối tượng trong và ngoài nước thường xuyên đăng tải các bài viết phản động không đúng sự thật [3].

Thứ tư, triệt để khai thác các lỗ hổng bảo mật của hệ thống, hệ điều hành, hệ quản trị cơ sở dữ liệu, phần mềm ứng dụng, chính sách bảo mật để chiếm quyền điều khiển trang thông tin điện tử, tạo ra sự ngưng trệ của dịch vụ,... Bằng chứng là trong hai ngày ngày 08 - 09/3/2017, sự cố các website của một số Cảng hàng không: Tân Sơn Nhất, Rạch Giá, Tuy Hòa,... bị Hacker tấn công thay đổi giao diện và không truy cập được thông tin [3].

Các tấn công này đã dẫn tới nguy cơ gây rối loạn, mất kiểm soát hệ thống thông tin phục vụ quốc phòng, an ninh; nguy cơ bị tấn công, chiếm đoạt, đánh cắp tài liệu, bí mật nhà nước từ hệ thống cơ sở dữ liệu, hệ thống mạng nội bộ; nguy cơ bị đình trệ, tê liệt hoạt động của hệ thống cổng thông tin điện tử, trang thông tin điện tử của các cơ quan Đảng, Nhà nước; nguy cơ gây rối loạn các giao dịch tài chính, hoạt động vận hành, điều khiển hàng không, điện lưới quốc gia, hệ thống giao thông đường bộ, xử lý hóa chất phục vụ cung cấp nước sinh hoạt, y tế,...; nguy cơ hệ thống thông tin phục vụ phát thanh, truyền hình, báo chí, xuất bản của Nhà nước bị kiểm soát, vô hiệu hóa; nguy cơ bị kiểm soát, chiếm đoạt, phá hủy hệ thống thông tin phục vụ lưu trữ cơ sở dữ liệu quốc gia về thủ tục hành chính, dân cư, xuất nhập cảnh,...

Tình hình an ninh mạng tại một số nơi diễn ra phức tạp, nguyên nhân chủ yếu là do:

Một là, công tác tuyên truyền, giáo dục, phổ biến kiến thức về đảm bảo an ninh, an toàn thông tin trên môi trường mạng cho cán

bộ, đảng viên, công chức, đặc biệt là phát huy vai trò lãnh đạo của các cấp ủy, chính quyền còn hạn chế và chưa tương xứng với tình hình, diễn biến thực tế.

Hai là, công tác quản lý nhà nước về an toàn, an ninh thông tin trên môi trường mạng còn nhiều bất cập, hạn chế, xuất phát từ hành lang pháp lý chưa đầy đủ, chưa chặt chẽ, chậm điều chỉnh trước những vấn đề mới nảy sinh. Việc kịp thời phát hiện, ngăn chặn, xử lý những tổ chức và cá nhân có hành vi làm mất an ninh, an toàn thông tin; lộ, lọt bí mật nhà nước, thông tin nội bộ phương hại đến an ninh quốc gia, lợi ích cơ quan, tổ chức và cá nhân trên môi trường mạng ít được phát hiện và chưa được xử lý nghiêm minh. Mặt khác, còn thiếu các quy định quản lý, phân cấp, phân quyền trong sử dụng, quản lý điều hành hệ thống mạng để quy định rõ trách nhiệm.

Ba là, trước những yêu cầu ngày càng cao về an toàn, bảo mật hệ thống thông tin trong các cơ quan, tổ chức nhà nước, thực trạng đội ngũ cán bộ làm công tác xử lý, ứng cứu sự cố về an ninh thông tin trên môi trường mạng còn thiếu về số lượng; trình độ năng lực chuyên môn nghiệp vụ chuyên ngành còn chưa theo kịp sự phát triển dẫn đến nguy cơ bị tấn công mạng ngày càng lớn. Bên cạnh đó, việc triển khai các biện pháp bảo đảm an toàn, an ninh mạng còn hạn chế. Nhiều cơ quan nhà nước chưa xây dựng giải pháp tổng thể về bảo mật, bảo đảm an ninh thông tin mà chỉ quan tâm đến khắc phục sự cố. Nguy cơ rò rỉ thông tin từ nhân tố bên trong ngày càng tăng.

Bốn là, sự thiếu đồng bộ khi đầu tư, nâng cấp các hệ thống công nghệ thông tin, kinh phí đầu tư, nâng cấp hệ thống và triển khai các giải pháp bảo đảm an ninh mạng còn hạn chế, tính đa dạng của các giải pháp công nghệ gây khó khăn trong công tác quản lý, triển khai các giải pháp bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin trong các cơ quan.

3. Một số giải pháp phòng ngừa, phát hiện và khắc phục sự cố an ninh mạng trong các cơ quan nhà nước

Trong bối cảnh trên, để bảo vệ hệ thống thông tin chống các mối đe dọa tấn công, các cơ quan và tổ chức cần tập trung nâng lực an toàn thông tin ở ba yếu tố cơ bản: con người, quy trình và giải pháp công nghệ. Cụ thể:

Một là, nâng cao nhận thức của người sử dụng về mức độ quan trọng của việc đảm bảo an ninh thông tin. Thường xuyên tổ chức đào tạo, tập huấn, tuyên truyền về công tác đảm bảo an ninh thông tin trong hoạt động của cơ quan nhà nước; tổ chức diễn tập, đào tạo chuyên sâu an ninh thông tin để nâng cao trình độ, chuyên môn nghiệp vụ cán bộ chuyên trách công nghệ thông tin của các cơ quan, đơn vị.

Hai là, bố trí cán bộ, bộ phận chuyên trách công nghệ thông tin của cơ quan hoặc đơn vị tư vấn thường xuyên kiểm tra, rà soát, đánh giá mức độ đảm bảo an toàn, an ninh thông tin cho hệ thống mạng nội bộ (LAN) gồm: máy chủ, máy trạm, thiết bị mạng, phần cứng, phần mềm hệ thống và các hệ thống thông tin, phần mềm ứng dụng nhằm đánh giá tổng thể mức độ an toàn, an ninh thông tin mạng, kịp thời phát hiện và xử lý sự cố, lỗ hổng, ngăn chặn, bóc gỡ mã độc tấn công vào hệ thống mạng.

Ba là, phòng chống mã độc, virus, phần

mềm gián điệp: Cách hiệu quả nhất để có thể ngăn chặn, phòng ngừa các phần mềm độc hại chuyên lây nhiễm trên hệ thống mạng máy tính của cơ quan, đơn vị đó là phải triển khai cài đặt phần mềm chống virus cho tất cả các máy chủ, máy trạm và thiết bị di động trong hệ thống mạng. Sử dụng cơ chế phòng chống tấn công, truy nhập trái phép vào hệ thống mạng, tự động phát hiện và loại trừ mã độc được truyền tải từ thư điện tử, tệp (file) đính kèm, từ các trang web độc hại trên mạng Internet. Thường xuyên cập nhật phiên bản mới, bản vá lỗi của hệ điều hành, phần mềm chống virus. Kiểm soát chặt chẽ cài đặt phần mềm trên máy chủ, máy trạm, không cài đặt phần mềm không rõ nguồn gốc hoặc không có bản quyền; cử cán bộ thường xuyên theo dõi hoạt động của cổng/trang thông tin điện tử của đơn vị nhằm tránh các cuộc tấn công gây ảnh hưởng đến việc cung cấp thông tin phục vụ người dân và doanh nghiệp. Thiết lập cơ chế bảo mật cho mạng không dây như thay đổi các tham số mặc định của thiết bị, mã hóa dữ liệu, đặt mật khẩu truy cập ở mức an toàn cao nhất.

Bốn là, xây dựng và ban hành quy chế về đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động nội bộ của cơ quan, đơn vị. Bố trí kinh phí thường xuyên cho việc triển khai các biện pháp đảm bảo an toàn, an ninh thông tin trong nội bộ cơ quan, mua sắm trang thiết bị công nghệ thông tin chuyên dụng như thiết bị tường lửa (Firewall), thiết bị lưu trữ dữ liệu, phần mềm phòng chống virus, xây dựng được hệ thống mạng an toàn, đầu tư các công cụ kỹ thuật cần thiết như công cụ kiểm tra, đánh giá, giám sát an toàn thông tin mạng; rà soát lỗ hổng website, lỗ hổng hệ điều hành, lỗ hổng cơ sở dữ liệu (database); sao lưu và khôi phục dữ liệu, hệ thống phòng chống tấn công mạng DDOS, hệ thống giám sát an toàn thông tin SIEM,...

Năm là, khi hệ thống bị tấn công, xảy ra sự cố hoặc nguy cơ mất an toàn, an ninh thông tin cần nhanh chóng cách ly hệ thống với môi trường mạng, áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại ở mức thấp nhất.

Sáu là, triển khai Quyết định số 898 của Thủ tướng Chính phủ về bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020 với 3 nhóm nhiệm vụ: bảo đảm an toàn, an ninh thông tin mạng quy mô quốc gia, bảo đảm an toàn, an ninh thông tin mạng trong hoạt động của cơ quan, tổ chức, trọng tâm là đảm bảo an ninh mạng cho 5 hệ thống thông tin quan trọng về an ninh quốc gia (hệ thống máy chủ tên miền quốc gia Việt Nam ".vn"; hệ thống quản lý, điều khiển, khai thác, vận hành mạng đường trục băng rộng; Hệ thống quản lý chuyển mạch quốc tế; hệ thống truyền dẫn và cáp quang biển quốc tế, cáp quang đất liền quốc tế). Hai hệ thống thông tin quan trọng về an ninh quốc gia thuộc lĩnh vực chỉ đạo, điều hành của Chính phủ là Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước và Hệ thống quản lý văn bản 4 cấp chính quyền.

TÀI LIỆU THAM KHẢO

1. Dự thảo Luật An ninh mạng trình xin ý kiến tại phiên họp thứ 20 của Ủy ban Thường vụ Quốc hội khóa XIV.

2. Bộ Nội vụ, *Tài liệu bồi dưỡng ngạch chuyên viên*, năm 2013.

3. Kỷ yếu Hội thảo "*Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia*" của Bộ Công an, tháng 8 năm 2017.