SỰ CẦN THIẾT PHẢI XÂY DỰNG CHÍNH SÁCH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Chu Văn Quang
Bộ KH&CN

Hệ thống giám sát an toàn thông tin (ATTT) cho phép thu thập, chuẩn hóa, lưu trữ và phân tích tương quan toàn bộ các sự kiện ATTT được sinh ra trong hệ thống công nghệ thông tin (CNTT) của tổ chức. Hệ thống này sẽ phát hiện kịp thời các tấn công mạng, các điểm yếu, lỗ hổng bảo mật của các thiết bị, ứng dụng và dịch vụ trong hệ thống; phát hiện kịp thời sự bùng nổ virus trong hệ thống mạng, các máy tính bị nhiễm mã độc, các máy tính bị tình nghi là thành viên của mạng máy tính ma (botnet). Tuy nhiên, việc giám sát về mặt kỹ thuật là chưa đủ. Nó đòi hỏi phải có cơ chế, chính sách nhằm điều chỉnh hành vi ứng xử của mỗi thành tố liên quan trong công tác đảm bảo ATTT.

Vì sao phải có chính sách bảo đảm ATTT mạng?

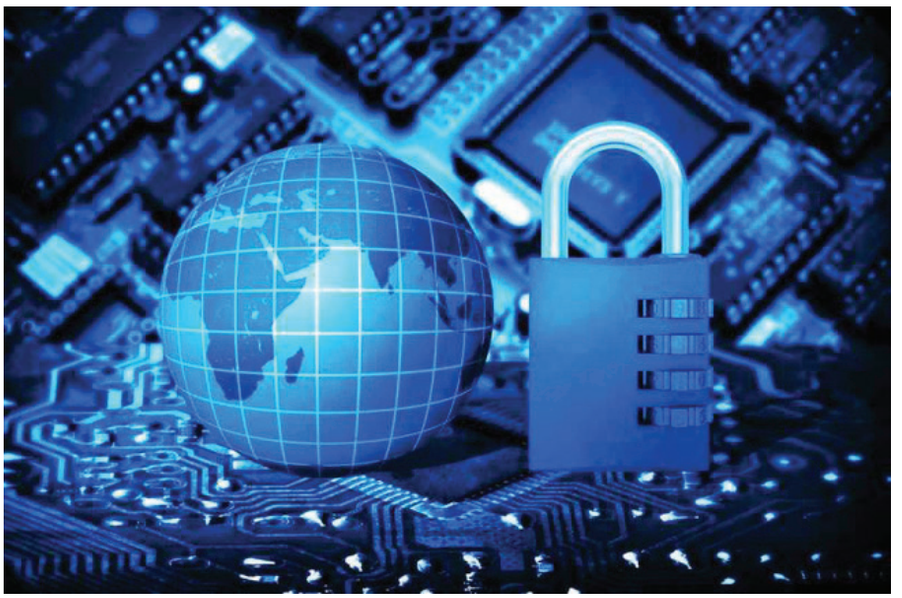
Trong ngành CNTT, ba yếu tố chính: *nhận thức, nhân lực, quy trình* có ảnh hưởng trực tiếp đến công tác bảo đảm ATTT. Các yếu tố này đều gắn chặt với yếu tố con người. Con người không chỉ là chủ nhân của thông tin mà còn có khả năng phân tích, khái quát và rút ra kết luận từ những dữ liệu, do đó con người là một trong những nguồn cung cấp thông tin cơ bản nhất. Nhưng con người còn có những điểm yếu như dễ mất cảnh giác, vụ lợi, một số có thể bị mua chuộc, do đó là đối tượng được tiếp cận để khai thác thông tin. Ngoài yếu tố con người, các phương tiện kỹ thuật là yếu tố tạo nên nhiều nguy cơ đe dọa ATTT. Chính xác hơn, chúng là nguồn gốc làm lộ các nguồn thông tin mật cũng như là nguồn gốc tạo ra các yếu tố mất an toàn của hệ thống.

Trong số các phương tiện kỹ thuật, mạng máy tính (cục bộ hay diện rộng) có vai trò đặc biệt. Từ hạ tầng (vật lý, hệ điều hành, BIOS…) đến thượng tầng của mạng máy tính đều có nhiều lỗ hổng, tạo ra các kênh tiếp cận trái phép cho những kẻ khai thác thông tin bất hợp pháp. Nếu một mạng máy tính không áp dụng các biện pháp bảo vệ thì với một laptop, những kẻ khai thác bất hợp pháp dễ dàng đột nhập vào cơ sở dữ liệu của máy tính để lấy đi hoặc sửa đổi, bóp méo các tệp thông tin mà chúng quan tâm.

Đối với các mạng máy tính diện rộng của các bộ/ngành, khu vực hay quốc gia, người ta thống kê có các loại nguy cơ mất an toàn sau: xâm nhập từ xa tới máy tính và tới cơ sở dữ liệu; thu, chặn thông tin, dữ liệu được truyền trên khoảng cách lớn; phát tán virus điện tử; hủy hoại hoặc làm sai lệch nội dung thông tin. Theo thống kê của Hãng bảo mật Kaspersky, Việt Nam là một trong số các quốc gia đứng đầu thế giới về tỷ lệ lây nhiễm mã độc qua thiết bị lưu trữ ngoài (USB, thẻ nhớ, ổ cứng di động), với tỷ lệ 70,83% máy tính bị lây nhiễm, gần 40% người dùng phải đối mặt với mã độc bắt nguồn từ không gian mạng.

Có thể thấy, công tác bảo đảm ATTT gắn liền với công tác tuyên truyền, nâng cao nhận thức; đào tạo, phát triển nguồn nhân lực ATTT; các biện pháp quản lý, quy trình nghiệp vụ. Để có được điều này nhất thiết phải thông qua việc xây dựng, ban hành, hoàn thiện hệ thống các văn bản, cơ chế chính sách mang tính pháp quy, chỉ đạo điều hành trong lĩnh vực ATTT; vì cơ chế, chính sách ATTT đưa ra các phương pháp, hệ thống các nguyên tắc đòi hỏi các hệ thống thông tin, nhân lực quản lý, vận hành phải tuân thủ, đảm bảo công tác ATTT được thực thi.

Trên phương diện quản lý nhà nước, kết quả giám sát an toàn



mạng giúp tạo ra các báo cáo tổng hợp, thống kê về tình hình tấn công mạng. Đây được coi là cơ sở để xác định xu hướng, xây dựng chính sách về an toàn mạng, ATTT. Việc giám sát an toàn mạng quốc gia là hết sức cấp bách, nhằm tạo ra môi trường để các cơ quan, tổ chức, doanh nghiệp có thể phối hợp, chia sẻ thông tin giám sát, cảnh báo nguy cơ mất ATTT.

Như vậy, cơ chế, chính sách ATTT mạng đóng vai trò quan trọng trong công tác đảm bảo ATTT mà hiện nay Đảng, Nhà nước đã và đang chú trọng thực hiện.

Thực trạng xây dựng, ban hành chính sách bảo đảm ATTT mạng

Trong những năm gần đây, Đảng và Nhà nước đã có nhiều chủ trương, chính sách và các biện pháp đẩy mạnh phát triển ứng dụng CNTT, viễn thông, gắn liền với công tác bảo đảm an toàn, an ninh thông tin, sẵn sàng đối phó với các cuộc chiến tranh trên không gian mạng.

Nghị quyết số 36-NQ/TW ngày 1/7/2014 của Bộ Chính trị về đẩy mạnh ứng dụng, phát triển CNTT đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế đã chỉ rõ: "Gắn kết chặt chẽ việc ứng dụng, phát triển CNTT phải đi đôi với bảo đảm an toàn, an ninh và bảo mật hệ thống thông tin và cơ sở dữ liệu quốc gia", đặc biệt cần "phát huy vai trò các lực lượng chuyên trách bảo vệ an toàn, an ninh thông tin và bí mật Nhà nước. Thực hiện cơ chế phối hợp chặt chẽ giữa các lực lượng công an, quân đội, ngoại giao, cơ yếu, thông tin và truyền thông" để có các biện pháp về tổ chức và kỹ thuật, sẵn sàng đối phó với các cuộc chiến tranh thông tin, chiến tranh mạng, bảo đảm chủ quyền quốc gia, trật tự an toàn xã hội.

Chỉ thị 28-CT/TW ngày 16/9/2013 của Ban Bí thư về tăng cường công tác đảm bảo ATTT mạng được quán triệt, triển khai, giúp tăng cường lãnh đạo, chỉ đạo, quản lý; kịp thời phát hiện, ngăn chặn, xử lý những thông tin có nội dung xấu, độc hại gây tổn hại đến uy tín của Đảng, Nhà nước, chế độ, ảnh hưởng xấu đến tiến trình phát triển kinh tế - xã hội, an ninh, quốc phòng. Chủ động phòng ngừa, hạn chế những sơ hở, thiếu sót, không để các thế lực thù địch và các loại đối tượng lợi dụng xâm nhập hệ thống thông tin, thu thập, chiếm đoạt bí mật nhà nước, thông tin nội bộ gây phương hại đến an ninh quốc gia, lợi ích của cơ quan, tổ chức và công dân.

Luật ATTT mạng được ban hành năm 2015 đã thể chế hóa các chủ trương, đường lối, chính sách của Đảng và Nhà nước về ATTT, đáp ứng yêu cầu phát triển bền vững kinh tế - xã hội, bảo vệ thông tin và hệ thống thông tin, góp phần bảo đảm quốc phòng, an ninh, chủ quyền và lợi ích quốc gia trên không gian mạng.

Các Nghị quyết, Chỉ thị của Đảng, cũng như các văn bản quy phạm pháp luật của Nhà nước đều thống nhất quan điểm chỉ đạo về bảo đảm an toàn, an ninh thông tin và bảo vệ chủ quyền quốc gia trên không gian mạng, cụ thể là:

- Chủ quyền trên không gian mạng là bộ phận quan trọng của chủ quyền quốc gia. Bảo vệ chủ quyền quốc gia trên không gian mạng là nhiệm vụ cấp bách, lâu dài của cả hệ thống chính trị, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý của Nhà nước; là yếu tố then chốt hình thành không gian mạng quốc gia an toàn và ổn định, tạo bước đột phá trong xây dựng, bảo vệ Tổ quốc.

- Huy động sức mạnh mọi nguồn lực của hệ thống chính trị và toàn xã hội bảo vệ chủ quyền quốc gia trên không gian mạng, tạo thế trận quốc phòng toàn dân gắn với thế trận an ninh nhân dân

trong việc bảo vệ chủ quyền quốc gia trên không gian mạng. Đầu tư cho bảo vệ chủ quyền quốc gia trên không gian mạng là đầu tư cho bảo vệ Tổ quốc, cần được ưu tiên.

- Chủ động phòng vệ, sẵn sàng đáp trả hợp pháp các mối đe dọa, bảo vệ vững chắc chủ quyền, an ninh quốc gia trên không gian mạng. Xây dựng lực lượng bảo vệ chủ quyền quốc gia trên không gian mạng chính quy, tinh nhuệ, hiện đại.

- Ứng dụng CNTT trong tất cả các lĩnh vực phải gắn với đảm bảo an toàn, an ninh thông tin, bảo vệ chủ quyền quốc gia trên không gian mạng.

Nhận thức được tầm quan trọng của ATTT nên Đảng, Nhà nước đã chỉ đạo các bộ/ngành, địa phương triển khai xây dựng nhiều chủ trương, chính sách về ATTT. Bộ Thông tin và Truyền thông (TT&TT) với trách nhiệm quản lý nhà nước trong lĩnh vực ATTT đã phối hợp với các bộ/ngành xây dựng, hoàn thiện hệ thống nhiều văn bản quy phạm pháp luật về ATTT.

Tuy nhiên có một thực tế là, về vận hành duy trì hệ thống, đại đa số các cơ quan chưa xây dựng và áp dụng các chính sách bảo mật thông tin; cán bộ nhân viên chưa tuân thủ nghiêm túc các quy định ATTT (trong sử dụng email, sử dụng hệ thống quản lý văn bản điều hành…), tạo lỗ hổng để tin tặc có thể tấn công hệ thống thông tin một cách dễ dàng. Theo Sách trắng CNTT năm 2013, tỷ lệ đơn vị có ban hành quy trình thao tác chuẩn phản ứng, xử lý sự cố máy tính chỉ chiếm 27%. Hiệp hội ATTT Việt Nam (VNISA) đã công bố nhiều dẫn chứng cho thấy 56% số tổ chức, doanh nghiệp chưa có quy chế về ATTT.

Theo Báo cáo số 58/BC-BTTTT của Bộ Thông tin và Truyền thông ngày 29/7/2015 về việc sơ kết 5 năm triển khai thực hiện Quyết định số 63/QĐ-TTg của Thủ tướng Chính phủ phê duyệt Quy hoạch phát triển ATTT số quốc gia đến năm 2020, hiện có 11 bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và 37 tỉnh/thành phố trực thuộc Trung ương ban hành Quy chế bảo đảm ATTT, điển hình như các Bộ: Giáo dục và Đào tạo, Quốc phòng, Công an, Nội vụ, Tư pháp, Tài chính, Xây dựng, Nông nghiệp và Phát triển nông thôn…; một số địa phương như: Hà Nội, An Giang, Bắc Ninh, Đà Nẵng, Đồng Nai, Cần Thơ, Hòa Bình, Hải Dương, Tuyên Quang, Vĩnh Phúc… Mỗi bộ/ngành, địa phương đều xây dựng và ban hành các chính sách bảo đảm ATTT phù hợp với cơ cấu tổ chức và điều kiện thực tế của mình. Việc triển khai và thực thi các chính sách theo đó cũng khác nhau. Tuy nhiên, các chính sách bảo đảm ATTT cần đáp ứng yêu cầu quản lý, giám sát sự tuân thủ và thực hiện các biện pháp bảo đảm ATTT ở mức độ cơ bản và trong các tình huống khẩn cấp.

Số liệu trên cho thấy, việc ban hành các cơ chế chính sách tại một số bộ/ngành, địa phương còn chậm trễ. Nguyên nhân chính có thể kể đến sau đây:

- ATTT là lĩnh vực mới, các văn bản hướng dẫn thực hiện còn chưa đầy đủ, dẫn đến công tác xây dựng chính sách gặp nhiều khó khăn.

- Cán bộ chuyên trách công tác ATTT chủ yếu là kiêm nhiệm, không được đào tạo bài bản, thiếu chuyên môn chuyên sâu và kinh nghiệm triển khai thực tế.

- Công tác quản lý chưa được chuẩn hóa làm cho việc xây dựng chính sách bảo mật thông tin khó khăn.

Đề xuất xây dựng Quy chế bảo đảm ATTT mạng của Bộ KH&CN

Vài nét về thực trạng đảm bảo ATTT tại Bộ KH&CN

Tại Bộ KH&CN, hệ thống CNTT được xây dựng và hình thành từ thập niên 90 của thế kỷ trước. Trải qua nhiều giai đoạn nâng cấp, đầu tư và phát triển, hiện nay hệ thống CNTT tại Bộ KH&CN tương đối hiện đại và đồng bộ. Hệ thống này đang cung cấp các dịch vụ CNTT của Bộ như: xác thực AD, thư điện tử, quản lý văn bản và điều hành công việc.

Các đơn vị trực thuộc Bộ như: Tổng cục Tiêu chuẩn Đo lường Chất lượng, Cục Sở hữu trí tuệ, Cục Thông tin KH&CN Quốc gia, Viện Năng lượng Nguyên tử Việt Nam, Khu Công nghệ cao Hòa Lạc... đều có hạ tầng kỹ thuật riêng với quy mô và dịch vụ CNTT khác nhau. Các hệ thống này hoạt động độc lập và chưa có sự liên kết dữ liệu. Các đơn vị có bộ phận kỹ thuật quản trị, vận hành hệ thống riêng và chưa có các chính sách bảo đảm ATTT cũng như các quy chế quản lý hoạt động thống nhất. Việc phối hợp thực hiện nhiệm vụ dựa trên sự vụ cụ thể là chính.

Trong những năm gần đây, tình hình ATTT trong và ngoài nước có những diễn biến phức tạp. Các hành vi tấn công mạng cũng trở lên tinh vi và nguy hiểm hơn. Tại Bộ KH&CN cũng đã ghi nhận một số cuộc dò quét và tấn công mạng điển hình như: các thư mạo danh tên miền most.gov.vn nhằm phát tán mã độc

chiếm quyền kiểm soát máy tính (8/2015); các hành vi tấn công lợi dụng lỗ hổng bảo mật của các ứng dụng Microsoft Ofice, Adobe Flash Player (10/2015); các hoạt động dò quét địa chỉ IP và tấn công tràn bộ nhớ hệ thống (11/2016)… Gần đây nhất là việc tấn công Deface lên trang điện tử của Cục Ứng dụng và Phát triển công nghệ (7/2017). Rất may sự cố đã được Trung tâm CNTT phát hiện kịp thời và phối hợp ngăn chặn. Với vai trò chuyên trách CNTT của Bộ, Trung tâm CNTT hiện đang là đầu mối trong mạng lưới ứng cứu sự cố mạng máy tính quốc gia do VNCert điều phối.

Đề xuất xây dựng Quy chế bảo đảm ATTT của Bộ KH&CN

Ngay từ năm 2009, Bộ KH&CN đã xây dựng và ban hành Quy chế quản lý và khai thác tài nguyên mạng máy tính (theo Quyết định số 1331/QĐ-BKHCN ngày 23/7/2009 của Bộ trưởng Bộ KH&CN), trong đó quy định về trách nhiệm của các đơn vị, cá nhân trong việc khai thác tài nguyên mạng máy tính của Bộ và dành riêng 1 Chương quy định về hệ thống thư điện tử. Đối với tình hình ứng dụng CNTT hiện tại thì Quy chế trên chưa đủ để đáp ứng nhu cầu tại Bộ, và tính đến thời điểm hiện tại Bộ cũng chưa ban hành được văn bản cụ thể nào liên quan trực tiếp đến ATTT. Đây là một hạn chế lớn trong bối cảnh tình hình ATTT trong nước và quốc tế có diễn biến phức tạp. Vì vậy, việc khẩn trương xây dựng và ban hành Quy chế đảm bảo an toàn an ninh thông tin mạng của Bộ KH&CN là hết sức cấp thiết nhằm đẩy mạnh ứng dụng, phát triển CNTT đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế theo định hướng chung của Đảng và Nhà nước.

Trước tình hình trên, năm 2017 Trung tâm CNTT đã được giao chủ trì xây dựng Quy chế bảo đảm an toàn, an ninh thông tin mạng Bộ KH&CN. Quy chế gồm 4 chương 24 điều, trong đó quy định cụ thể đối tượng, phạm vi, cách thức, yêu cầu cần thiết để đảm bảo an toàn, an ninh thông tin tại Bộ KH&CN. Nội dung của Quy chế đảm bảo thực hiện theo yêu cầu của Nghị định 85/2016/NĐ-CP ngày 1/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia và các văn bản khác của Bộ Thông tin và Truyền thông…

Các quy định về đảm bảo an toàn, an ninh thông tin của Bộ KH&CN được quy định chi tiết tại Chương II, gồm các nội dung chính: i) Quản lý trang thiết bị CNTT; ii) Bảo dảm an toàn hệ thống CNTT (bảo đảm ATTT đối với trung tâm dữ liệu máy chủ, bảo đảm ATTT khi sử dụng máy tính, hệ thống mạng máy tính, quản lý tài khoản truy cập…); iii) Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin; iv) Giám sát an toàn thông tin mạng; v) Kiểm tra, đánh giá ATTT, vi) Ứng cứu sự cố ATTT mạng…

Dự kiến, Quy chế sẽ được triển khai thực hiện từ năm 2019. Việc tuân thủ Quy chế sẽ giúp đảm bảo ATTT cho các hệ thống thông tin của Bộ đúng theo yêu cầu của Đảng và Nhà nước trong lĩnh CNTT. Bên cạnh đó, Quy chế được ban hành sẽ góp phần hoàn thiện hệ thống văn bản quản lý hành chính, văn bản chỉ đạo điều hành của Bộ KH&CN trong lĩnh vực ATTT, phục vụ công tác quản lý nhà nước trong thời gian tới, tránh được những sự cố về CNTT đã từng xảy ra trong những năm vừa qua ✍