ĐẢM BẢO AN TOÀN THÔNG TIN TRONG QUÁ TRÌNH CHUYỂN ĐỔI SỐ NGÀNH TÀI CHÍNH

LÊ LINH CHI

Thực tế triển khai quá trình chuyển đổi số trong ngành Tài chính cho thấy, Bộ Tài chính có số lượng ứng dụng, dịch vụ công trực tuyến hoạt động trên hệ thống mạng khá lớn. Điều này dẫn tới nguy cơ hàng ngày, hàng giờ phải đối diện với vô số các cuộc tấn công mạng và các rủi ro mất an toàn, an ninh mạng… Do đó, việc đảm bảo an toàn thông tin mạng, an ninh mạng là yêu cầu cấp thiết đối với Bộ Tài chính hiện nay, trong khi nguồn nhân lực làm trong lĩnh vực công nghệ thông tin, an ninh mạng còn hạn chế.

Từ khóa: Ngành Tài chính, chuyển đổi số, công nghệ thông tin, Bộ Tài chính, an ninh mạng

INFORMATION SECURITY IN DIGITAL TRANSFORMATION PROCESS OF THE FINANCIAL SECTOR

Le Linh Chi

The actual implementation of the digital transformation process in the financial sector shows that the Ministry of Finance has a large number of online public services and applications operating on the network. This leads to the situation that every day, every hour, we are facing countless cyber-attacks and security risks... This fact requires imperative information security, while human resources for information technology and network security are still limited. To address this limitation, the Ministry of Finance needs to apply appropriate measures.

Keywords: Financial sector, digital transformation, information technology, Ministry of Finance, cyber-security

Ngày nhận bài: 7/10/2022
Ngày hoàn thiện biên tập: 26/10/2022
Ngày duyệt đăng: 31/10/2022

Kết quả đạt được trong bảo đảm an toàn, an ninh thông tin mạng của Bộ Tài chính

Từ năm 2012 đến nay, Bộ Tài chính đã ban hành quy định về an toàn thông tin mạng và liên tục cập nhật quy định này theo yêu cầu thực tiễn, để có căn cứ triển khai việc bảo đảm an toàn thông tin mạng. Văn bản đang có hiệu lực thi hành hiện hành là Quy chế An toàn thông tin mạng Bộ Tài chính ban hành theo Quyết định số 201/QĐ-BTC ngày 12/02/2018, trên cơ sở triển khai các văn bản quy định về an toàn thông tin mạng đã được ban hành. Trên cơ sở Quy chế này, các đơn vị thuộc Bộ Tài chính đã ban hành các quy định cụ thể áp dụng phù hợp với đặc thù của từng đơn vị.

Từ năm 2013, các đơn vị công nghệ thông tin (CNTT) thuộc và trực thuộc Bộ Tài chính gồm: Cục Tin học và Thống kê tài chính, các Cục CNTT trực thuộc Tổng cục Thuế, Tổng cục Hải quan, Kho bạc Nhà nước, Tổng cục Dự trữ Nhà nước đã thành lập phòng/đơn vị quản lý an toàn thông tin mạng, an ninh mạng. Bộ phận chuyên trách này tuy có số lượng nhân sự rất khiêm tốn, nhưng đã được các cơ quản lý nhà nước về lĩnh vực này đánh giá là đầy đủ hơn so với nhiều bộ, ngành, địa phương. Hiện nay, tổng số cán bộ được giao nhiệm vụ về an toàn thông tin mạng, an ninh mạng của khối các đơn vị hành chính thuộc Bộ Tài chính, từ cấp Trung ương đến địa phương, gồm 23 cán bộ chuyên trách và 228 cán bộ kiêm nhiệm.

Hàng năm, Bộ Tài chính bố trí kinh phí đào tạo, bồi dưỡng chuyên sâu về CNTT và an toàn, an ninh mạng cho cán bộ CNTT làm việc tại các đơn vị thuộc Bộ Tài chính. Từ năm 2012 đến nay, đã có 70 khóa đào tạo, bồi dưỡng chuyên sâu được tổ chức, đảm bảo cho cán bộ CNTT của Bộ Tài chính luôn được cập nhật kiến thức mới nhất về an toàn thông tin mạng, an ninh mạng; 19 khóa đào tạo kiến thức cơ bản, nâng cao nhận thức về an toàn thông tin mạng, an ninh mạng cho cán bộ quản lý, cán bộ nghiệp vụ. Đây là số lượng khóa đào tạo do Cục Tin học và Thống kê tài chính và các Tổng cục thuộc Bộ Tài chính triển khai.

Cùng với việc chú trọng đào tạo cho cán bộ làm công tác CNTT, các đơn vị thuộc Bộ Tài chính đã trang bị các giải pháp kỹ thuật thiết yếu về bảo đảm

an toàn, an ninh mạng như: Hệ thống phòng diệt mã độc, tường lửa mạng, phòng chống tấn công, chống thư rác. Một số đơn vị đã trang bị các giải pháp bảo vệ nâng cao như: Thiết lập tường lửa ứng dụng, tường lửa cơ sở dữ liệu, giám sát an ninh mạng. Một số đơn vị khác đã triển khai các giải pháp nhằm tách biệt giữa hệ thống mạng làm việc và hệ thống mạng internet, giảm thiểu rủi ro mất an toàn, an ninh mạng cho các hệ thống thông tin để cài đặt đầy đủ các bản vá lỗ hổng bảo mật và các rủi ro khác có nguồn gốc từ internet…

Bộ Tài chính đã ban hành Quy chế kiểm tra ứng dụng CNTT tại các cơ quan hành chính, đơn vị sự nghiệp của Bộ Tài chính (Quy chế đang có hiệu lực được ban hành theo Quyết định số 298/QĐ-BTC ngày 21/2/2020). Trên cơ sở đó, hàng năm, Cục Tin học và Thống kê tài chính tổ chức kiểm tra việc triển khai công tác bảo đảm an toàn thông tin mạng tại các đơn vị thuộc Bộ Tài chính.

Bối cảnh an toàn thông tin mạng, an ninh mạng của Việt Nam hiện nay

Sơ bộ về tình hình mất an toàn, an ninh mạng tại Việt Nam

Theo Bản tin Cảnh báo hàng tuần của Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục An toàn thông tin (Bộ Thông tin và Truyền thông), mỗi tuần có khoảng từ hơn 100 đến hơn 200 các cuộc tấn công thành công vào các trang, cổng thông tin điện tử của các cơ quan, tổ chức Việt Nam; bao gồm tấn công thay đổi giao diện, tấn công lừa đảo, tấn công cài cắm mã độc, chiếm quyền điều khiển hệ thống. Số liệu này chưa bao gồm các trường hợp không được báo cáo.

Mỗi tháng, có hàng trăm lỗ hổng bảo mật của các thiết bị công nghệ thông tin, phần mềm, thậm chí là lỗ hổng bảo mật của chính thiết bị, phần mềm hệ thống bảo mật được phát hiện mà có ảnh hưởng tới các hệ thống thông tin tại Việt Nam. Trong đó, nhiều lỗ hổng bảo mật nghiêm trọng được công bố mà chưa có bản vá để ngăn chặn việc khai thác các lỗ hổng này.

Các cơ quan, tổ chức có máy tính làm việc vừa kết nối mạng nội bộ, vừa kết nối internet có rủi ro mất an toàn, an ninh mạng lớn hơn nhiều so với các cơ quan, tổ chức có chính sách tách biệt giữa mạng làm việc và truy cập internet. Nhiều trường hợp máy tính làm việc của cán bộ sử dụng hệ điều hành cũ, không được cài bản vá lỗ hổng bảo mật, thậm chí không được cài phần mềm phòng, diệt mã độc. Các máy này khi truy cập internet dễ dàng bị nhiễm mã độc hoặc bị tin tặc tiếp cận, biến thành bàn đạp để mã độc lan rộng, khoan sâu vào các hệ thống thông tin quan trọng của các cơ quan, tổ chức.

Bộ Tài chính cũng thường xuyên phải đối mặt với các cuộc tấn công mạng, trong đó mục tiêu tấn công là các ứng dụng, trang, cổng thông tin điện tử, máy chủ và máy tính làm việc của cán bộ. Với tổng số hơn 100 hệ thống ứng dụng/trang/cổng thông tin điện tử, hơn 4.000 máy chủ và hơn 60.000 máy tính làm việc của cán bộ thuộc các đơn vị thuộc Bộ Tài chính (từ cấp Trung ương đến cấp huyện), áp lực của việc thực hiện tốt công tác bảo đảm an toàn, an ninh mạng tại Bộ Tài chính là vô cùng lớn.

Bên cạnh đó, các cơ quan quản lý tài chính thuộc chính quyền địa phương các cấp (Sở Tài chính, Phòng Tài chính – Kế hoạch) thiếu nhân lực CNTT và không có cán bộ chuyên trách về an toàn, an ninh mạng. Điều này vừa tạo áp lực cho các cơ quan trong việc bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin quản lý ngân sách và quản lý tài chính của địa phương; vừa tạo áp lực cho Bộ Tài chính trong quản lý nhà nước đối với lĩnh vực tài chính - ngân sách.

Quy định của pháp luật về an toàn thông tin mạng, an ninh mạng

Trong những năm qua, Bộ Tài chính đã quan tâm triển khai việc bảo đảm an toàn thông tin, an ninh mạng với việc trang bị phần mềm phòng diệt mã độc và tường lửa mạng. Trong một thời gian dài, Bộ Tài chính và các đơn vị trực thuộc đã chủ động tìm tư vấn và tự nghiên cứu, tìm kiếm các giải pháp cần thiết để bảo vệ hệ thống thông tin, dữ liệu. Từ năm 2017 và 2018, Luật An toàn thông tin mạng, Luật An ninh mạng và các văn bản quy định chi tiết, hướng dẫn các Luật này là cơ sở pháp lý quan trọng cho việc bảo đảm an toàn, an ninh mạng của Bộ Tài chính.

Hệ thống băn bản quy phạm pháp luật về an toàn thông tin mạng, an ninh mạng đang có hiệu lực bao gồm: Luật An toàn thông tin mạng năm 2015; Luật An ninh mạng năm 2018; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Nghị định số 142/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng; Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ về việc quy định chi tiết một số điều của Luật An ninh mạng 2018; 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 an toàn thông tin mạng quốc gia; Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Căn cứ đề xuất, kiến nghị của Bộ Thông tin và Truyền thông, Bộ Công an, Thủ tướng Chính phủ thường xuyên có văn bản chỉ đạo các bộ, ngành, địa phương về công tác an toàn, an ninh mạng. Các văn bản chỉ đạo quan trọng cần tiếp tục triển khai, thực hiện trong thời gian tới có thể kể tới như: Chị thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại; Chỉ thị số 14/CT-TTg ngày 7/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam; Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ về phát triển Chính phủ điện tử hướng tới Chính phủ số, thúc đẩy chuyển đổi số quốc gia; Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ về việc phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030…

Những văn bản trên cho thấy, hiện nay có rất nhiều quy định về an toàn thông tin mạng và an ninh mạng phải tuân thủ, trong đó bao gồm các thủ tục hành chính cần thực hiện trong công tác này. Điều này cũng gây ra áp lực nhất định đối với lực lượng chuyên trách về an toàn thông tin mạng, an ninh mạng của Bộ Tài chính.

Yêu cầu đặt ra đối với công tác bảo đảm an toàn, an ninh mạng của Bộ Tài chính

Thứ nhất, việc triển khai công tác bảo đảm an toàn, an ninh mạng của Bộ Tài chính phải thực hiện theo quy định của pháp luật và sự chỉ đạo, điều hành của các cấp có thẩm quyền. Để thực hiện tốt nội dung này, Bộ Tài chính cần chuyển hóa các yêu cầu của hệ thống văn bản quy phạm pháp luật và các văn bản chỉ đạo, điều hành của các cấp có thẩm quyền thành các quy định cụ thể về triển khai công tác bảo đảm an toàn, an ninh mạng tại Bộ Tài chính, đưa vào Quy chế An toàn thông tin mạng, an ninh mạng Bộ Tài chính để áp dụng cho giai đoạn mới.

Theo quy định của pháp luật hiện hành, "an toàn thông tin mạng" và "an ninh mạng" là hai lĩnh vực khác nhau. Thực tế, hai lĩnh vực này có nhiều điểm chung và có nhiều nội dung đan xen. Do đó, việc thể hiện một cách rõ ràng yêu cầu của từng lĩnh vực trong cùng một văn bản quy định, quy chế sẽ có khó khăn nhất định.

Thứ hai, phân cấp, ủy quyền triển khai công tác bảo đảm an toàn, an ninh mạng cho các đơn vị thuộc Bộ Tài chính một cách phù hợp, vừa thực hiện đúng quy định của Nhà nước về phân định các vai trò chịu trách nhiệm về công tác bảo đảm an toàn, an ninh mạng, vừa phù hợp với tổ chức bộ máy và phương thức làm việc của Bộ Tài chính; đồng thời, tối ưu hóa các mối quan hệ trong trao đổi công việc, thủ tục hành chính cần thực hiện giữa các đơn vị liên quan đến công tác này.

Một số đơn vị sự nghiệp công lập thuộc Bộ Tài chính chưa có bộ phận chuyên trách về CNTT và bảo đảm an toàn, an ninh mạng. Do đó, việc phân cấp, ủy quyền về trách nhiệm bảo đảm an toàn, an ninh mạng đối với các đơn vị này cũng có khó khăn.

Thứ ba, có giải pháp để vượt qua khó khăn lớn nhất là vấn đề thiếu hụt nhân sự làm công tác triển khai ứng dụng CNTT và bảo đảm an toàn, an ninh mạng. Đây sẽ là khó khăn lâu dài, do thị trường trong nước hiện nay đang rất "khát" nhân lực chuyên sâu về lĩnh vực này, đặc biệt trong giai đoạn mà cả khối cơ quan Nhà nước và doanh nghiệp đều triển khai chuyển đổi số một cách mạnh mẽ. Hiện tượng "chảy máu chất xám" từ khối cơ quan nhà nước sang khối doanh nghiệp đã diễn ra nhiều năm thì nay càng trở nên phổ biến hơn.

Bên cạnh đó, phương thức tuyển dụng tại cơ quan nhà nước đối với nhân sự làm việc trong lĩnh vực CNTT chưa thực sự phù hợp. Các bài thi kiến thức hành chính nhà nước có tính thách thức lớn đối với sinh viên CNTT/an toàn, an ninh mạng, vô hình trở thành một rào cản cho việc bổ sung lực lượng nhân sự đang bị thiếu hụt trầm trọng. Nhân sự CNTT và đặc biệt nhân sự chịu trách nhiệm về bảo đảm an toàn thông tin mạng, an ninh mạng của Bộ Tài chính đang trở nên "già hóa", tương lai sẽ khó theo kịp tốc độ thay đổi của kỹ thuật, công nghệ.

Thứ tư, lựa chọn giải pháp kỹ thuật, công nghệ phù hợp, vừa đáp ứng yêu cầu đặt ra về bảo đảm an toàn, an ninh mạng; đáp ứng định hướng của Nhà nước về hướng tới sử dụng các giải pháp do doanh nghiệp nội địa sản xuất; đáp ứng xu hướng mới về công nghệ; nhưng phải phù hợp với trình độ, năng lực của nhân sự trực tiếp quản lý, vận hành các giải pháp này.

Việc lựa chọn giải pháp kỹ thuật phù hợp còn nhằm xử lý tình huống: Các ứng dụng, hệ thống tin, máy chủ và máy tính làm việc của cán bộ không có đủ điều kiện để xử lý các lỗ hổng bảo mật ngay khi được phát hiện vẫn có thể hoạt động an toàn. Ví dụ: Sử dụng tường lửa ứng dụng để che chắn lỗ hổng bảo mật lớp ứng dụng trong thời gian chưa được xử lý; không cho phép kết nối internet trực tiếp đối với các máy tính sử dụng hệ điều hành cũ, không còn được hỗ trợ bản vá lỗ hổng bảo mật… Bộ Tài chính có nhiều hệ thống ứng dụng có số lượng người sử dụng truy cập hàng ngày rất lớn, cần đảm bảo truy cập sử dụng 24/7. Các hoạt động can thiệp vào hệ thống để vá lỗi bảo mật có thể gây lỗi hoặc làm hệ thống dừng hoạt động. Do đó, cần áp dụng các biện pháp bảo vệ các hệ thống này trong trường hợp không thể vá lỗi bảo mật kịp thời.

Thứ năm, biến công tác bảo đảm an toàn thông tin mạng và an ninh mạng thành công việc thường xuyên, lồng ghép vào các hoạt động ứng dụng CNTT, triển khai chuyển đổi số. Để giải quyết vấn đề này cần biến các quy định chung về an toàn thông tin mạng, an ninh mạng của Bộ Tài chính thành các quy trình làm việc cụ thể, áp dụng cho từng công đoạn triển khai, ứng dụng, sử dụng CNTT; đồng thời, tăng cường đào tạo, nâng cao nhận thức về an toàn thông tin mạng, an ninh mạng cho tất cả cán bộ, công chức, viên chức, người lao động của Bộ Tài chính có sử dụng máy tính, hệ thống thông tin.

Giải pháp bảo đảm an toàn, an ninh mạng của Bộ Tài chính trong quá trình chuyển đổi số

Thực tế cho thấy, thách thức lớn nhất của Bộ Tài chính hiện nay trong bảo đảm an toàn thông tin mạng, an ninh mạng là thiếu hụt nhân sự. Để ứng phó với tình hình này, Bộ Tài chính cần huy động và sử dụng hợp lý nguồn nhân sự, bao gồm nhân sự nội bộ; nhân sự có trình độ cao từ các hợp đồng thuê dịch vụ CNTT, các cơ quan chuyên môn, chuyên trách về an toàn thông tin mạng, an ninh mạng của Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng.

Nhận diện chính xác năng lực của đội ngũ nhân sự, phân công trách nhiệm hợp lý và phối hợp nhuần nhuyễn giữa các lực lượng nhân sự trong nội bộ và lực lượng nhân sự bên ngoài trong quá trình triển khai bảo đảm an toàn thông tin mạng, an ninh mạng là "chìa khóa" để triển khai thành công việc này.

Bên cạnh các quy trình đã được cụ thể hóa và phân công trách nhiệm rõ ràng cho các bên, bộ phận chuyên trách về an toàn thông tin mạng, an ninh mạng của các đơn vị CNTT của Bộ Tài chính cần hoạt động vừa như một "nhạc trưởng" để tạo sự phối hợp hài hòa giữa các lực lượng để thực hiện hiệu quả nhiệm vụ được giao.

Bộ Tài chính là cơ quan có nhiều đơn vị chuyên trách về CNTT và bảo đảm an toàn thông tin mạng, an ninh mạng (Cục Tin học và Thống kê tài chính, 05 Cục CNTT trực thuộc Tổng cục, các phòng CNTT thuộc các doanh nghiệp thuộc Bộ Tài chính). Cán bộ chuyên trách về bảo đảm an toàn thông tin mạng và an ninh mạng của các đơn vị này có thể thường xuyên trao đổi, học hỏi kinh nghiệm lẫn nhau, rút kinh nghiệm trong đơn vị mình từ các giải pháp kỹ thuật được áp dụng thành công hoặc không thành công tại đơn vị khác.

Thúc đẩy triển khai hiệu quả công tác bảo đảm an toàn thông tin mạng, an ninh mạng tại các cơ quan đơn vị. Căn cứ kế hoạch kiểm tra CNTT hàng năm được Lãnh đạo Bộ Tài chính phê duyệt, mỗi năm, Cục Tin học và Thống kê tài chính thực hiện kiểm tra tại một số đơn vị được lựa chọn.

Thông qua hoạt động kiểm tra, Cục Tin học và Thống kê tài chính giúp các đơn vị phát hiện các vấn đề còn tồn tại trong bảo đảm an toàn thông tin mạng, an ninh mạng, để các đơn vị có giải pháp giải quyết các tồn tại này. Tương tự, các đợt kiểm tra của Bộ Công an, Bộ Thông tin và Truyền thông thực hiện tại Bộ Tài chính giúp các đơn vị thuộc Bộ rà soát, đánh giá kỹ lưỡng hơn về công tác bảo đảm an toàn thông tin mạng, an ninh mạng; rút kinh nghiệm để thực hiện tốt hơn công tác này.

Tài liệu tham khảo:

1. *Luật An toàn thông tin mạng năm 2015;*
2. *Luật An ninh mạng năm 2018;*
3. *Chính phủ (2016), Nghị định số 15/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;*
4. *Chính phủ (2016), Nghị định số 142/2016/NĐ-CP ngày 01/7/2016 về ngăn chặn xung đột thông tin trên mạng;*
5. *Bộ Tài chính (2018), Quyết định số 201/QĐ-BTC ngày 12/02/2018;*
6. *Bộ Tài chính (2020), Quyết định số 298/QĐ-BTC ngày 21/2/2020;*
7. *Các báo cáo Cảnh báo tuần của Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục An toàn thông tin (Bộ Thông tin và Truyền thông); Báo cáo về công tác bảo đảm an ninh mạng, an toàn thông tin mạng của Bộ Tài chính đến tháng 10/2022.*

Thông tin tác giả:

Lê Linh Chi - Cục Tin học và Thống kê tài chính (Bộ Tài chính)
Email: lelinhchi@mof.gov.vn.vn