NGÂN HÀNG NHÀ NƯỚC TĂNG CƯỜNG CÁC BIỆN PHÁP BẢO ĐẢM AN NINH, AN TOÀN CHO CÁC HỆ THỐNG THÔNG TIN

NGUYỄN HUY HÙNG
Ngân hàng Nhà nước

Trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư (CMCN 4.0), ngành Ngân hàng Việt Nam đã chủ động bước vào giai đoạn chuyển đổi số, cung cấp các dịch vụ thanh toán số cũng như nhiều dịch vụ khác trên nền tảng số và mang lại những kết quả đáng ghi nhận. Tuy nhiên, bên cạnh những kết quả đạt được là tình trạng gia tăng các sự cố mất an toàn, an ninh thông tin. Thời gian qua, công tác đảm bảo an ninh, an toàn trong các hoạt động ngân hàng luôn được ngành Ngân hàng coi là nhiệm vụ trọng tâm, có ý nghĩa then chốt.

Giai đoạn 2016 - 2020, các giải pháp đảm bảo an ninh, an toàn thông tin (ATTT) trong các hoạt động ngân hàng đã được Ngân hàng Nhà nước (NHNN) triển khai đồng bộ, từ ban hành chính sách, xây dựng nguồn lực cho đến việc thực hiện các giải pháp kỹ thuật. Vừa qua, NHNN đã ban hành Kế hoạch ứng dụng công nghệ thông tin (CNTT), phát triển Chính phủ số và bảo đảm ATTT mạng trong hoạt động của NHNN giai đoạn 2021 - 2025, mục tiêu tổng quát của Kế hoạch này là nhằm xây dựng cơ sở pháp lý tạo môi trường thuận lợi cho việc ứng dụng toàn diện CNTT, các công nghệ mới của CMCN 4.0 vào các hoạt động nghiệp vụ ngân hàng và từng bước chuẩn hóa hạ tầng CNTT của ngành Ngân hàng.

Tình hình tấn công vào lĩnh vực ngân hàng - tài chính

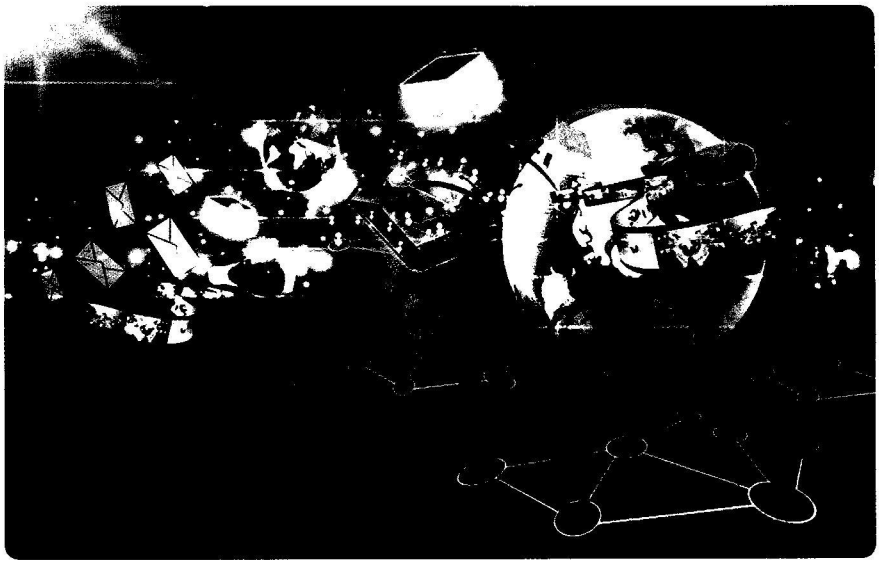
Ngày 19/01/2021, Tập đoàn công nghệ Bkav công bố chương trình đánh giá an ninh mạng thực hiện vào tháng 12/2020. Theo đó, năm 2020, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã đạt kỷ lục mới, vượt mốc 1 tỷ USD (23,9 nghìn tỷ đồng).

Trong các lĩnh vực bị tấn công, lĩnh vực tài chính - ngân hàng vẫn là "đích ngắm" của tội phạm mạng. Chỉ tính riêng năm 2020, hàng trăm tỷ đồng đã bị hacker chiếm đoạt qua tấn công an ninh mạng liên quan đến ngân hàng, trong đó, chủ yếu là các vụ đánh cắp mã OTP giao dịch của người dùng. Cách thức chính của các hacker là lừa người dùng cài đặt phần mềm gián điệp trên điện thoại để lấy trộm tin nhắn OTP, thực hiện giao dịch bất hợp pháp. Trung bình mỗi tháng, hệ thống giám sát virus của Bkav đã phát hiện hơn 15.000 phần mềm gián điệp trên điện thoại di động. Điển hình là vụ việc VN84App, phần mềm thu thập tin nhắn OTP giao dịch ngân hàng đã gây ra thiệt hại lên đến hàng tỷ đồng, lây nhiễm hàng nghìn Smartphone tại Việt Nam.

Theo đánh giá của các chuyên gia, ngành Ngân hàng đang đối mặt với một số thách thức về an ninh mạng, cụ thể như sau: Hacker tấn công vào hệ thống dữ liệu ngân hàng qua các đối tác của ngân hàng; tấn công trực tiếp vào website, thay đổi giao diện để tống tiền, lấy dữ liệu; thâm nhập hệ thống để thực hiện lệnh chuyển tiền nhằm chiếm đoạt thông tin, tài sản của ngân hàng và cả khách hàng; lập các website mạo danh ngân hàng để lừa đảo khách hàng... Cả ba chủ thể tham gia không gian ngân hàng số là các ngân hàng, khách hàng và các đối tác liên kết của ngân hàng đều có thể trở thành mục tiêu để tội phạm mạng tấn công.

Tăng cường các biện pháp bảo đảm an ninh, an toàn hệ thống thông tin

Thời gian qua, NHNN tăng cường xây dựng các giải pháp số nhằm đáp ứng yêu cầu xử lý thủ tục hành chính, dịch vụ công và kết nối chia sẻ dữ liệu phù hợp với lộ trình của Chính phủ. Đồng thời, ứng dụng hiệu quả CNTT theo chiều sâu cho toàn bộ các hoạt động nghiệp vụ của NHNN, trước mắt ưu tiên cho công tác thanh tra, giám sát và thanh toán. Tự động hóa, giám sát liên tục hạ tầng và các hệ thống thông tin đảm bảo hoạt động ổn định, liên tục, an toàn trên cơ sở ứng dụng các thành tựu công nghệ của CMCN 4.0.



Bên cạnh việc phát triển các ứng dụng CNTT, NHNN luôn chú trọng công tác đảm bảo an toàn, an ninh thông tin, cụ thể: Ngày 26/10/2020, Thống đốc NHNN Việt Nam ban hành Quyết định số 1820/QĐ-NHNN về Quy chế an toàn bảo mật hệ thống thông tin của NHNN Việt Nam. Quy chế có hiệu lực từ ngày 01/11/2020. Theo đó, việc bảo đảm an toàn hệ thống thông tin theo các cấp độ trong hoạt động của NHNN được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ hệ thống thông tin.

Ngày 4/3/2021, Thống đốc NHNN ra Quyết định số 260/QĐ-NHNN ban hành Kế hoạch ứng dụng CNTT, phát triển Chính phủ số và bảo đảm ATTT mạng trong hoạt động của NHNN giai đoạn 2021 - 2025. Theo Quyết định, mục tiêu tổng quát của Kế hoạch này là nhằm xây dựng cơ sở pháp lý, tạo môi trường thuận lợi cho việc ứng dụng toàn diện CNTT, các công nghệ mới của CMCN 4.0 vào các hoạt động nghiệp vụ ngân hàng và từng bước chuẩn hóa hạ tầng CNTT của ngành Ngân hàng. Kế hoạch này đã đề ra các nhiệm vụ, giải pháp và phân công các đơn vị triển khai thực hiện các mục tiêu cụ thể: Hoàn thiện môi trường pháp lý; phát triển Chính phủ điện tử tại NHNN; ứng dụng CNTT cho các hoạt động nghiệp vụ; phát triển hạ tầng CNTT; công tác an ninh bảo mật nhằm bảo đảm ATTT mạng trong hoạt động của NHNN...

Xây dựng nền tảng an ninh mạng chuyên nghiệp, hiện đại, chủ động phát hiện và xử lý kịp thời các sự cố an ninh mạng, đảm bảo an toàn, an ninh thông tin phục vụ tốt cho các hoạt động nghiệp vụ của NHNN và hỗ trợ công tác giám sát, ứng cứu sự cố ATTT ngành Ngân hàng là mục tiêu tổng quát về đảm bảo ATTT mà NHNN hướng tới trong giai đoạn 2021 - 2025.

Trong Chiến lược phát triển ngành Ngân hàng Việt Nam đến năm 2025, định hướng đến năm 2030, NHNN đã nêu quan điểm, mục tiêu: Kịp thời nắm bắt cơ hội và thách thức từ tác động của CMCN 4.0 để định hướng hoạt động của ngành Ngân hàng. Nhận thức sâu sắc ứng dụng khoa học, công nghệ hiện đại và đổi mới sáng tạo đi đôi với phát triển nguồn nhân lực có chất lượng cao là những thành tố chính, then chốt cho sự phát triển nhanh và bền vững, nâng cao sức cạnh tranh, rút ngắn khoảng cách về trình độ phát triển của ngành Ngân hàng Việt Nam so với khu vực và thế giới.

Chiến lược đã đưa ra nhiệm vụ: "Chú trọng phát triển, ứng dụng khoa học công nghệ và phát triển nguồn nhân lực của ngành Ngân hàng". Để cụ thể hóa nhiệm vụ này, Thống đốc NHNN đã ban hành Quyết định số 1537/QĐ-NHNN ngày 17/7/2019 phê duyệt Kế hoạch triển khai Chương trình hành động của ngành Ngân hàng thực hiện Chiến lược phát triển ngành Ngân hàng Việt Nam trong lĩnh vực phát triển nguồn nhân lực, cụ thể là: Nâng cao năng lực, trình độ chuyên môn của các cán bộ làm công tác ATTT của NHNN để có thể chủ động giám sát, phát hiện và xử lý các sự cố về ATTT xảy ra, trong đó đạt tối thiểu 20% cán bộ chuyên trách về ATTT có chứng chỉ quốc tế về an toàn bảo mật. Nâng cao nhận thức ATTT cho toàn bộ cán bộ, công chức, viên chức tại NHNN nhằm giảm thiểu các nguy cơ tấn công xâm nhập, lây lan mã độc từ hạ tầng máy trạm đầu cuối. Phấn đấu đến năm 2025, 100% cán bộ, công chức, viên chức NHNN sử dụng máy tính được tuyên truyền, tập huấn nâng cao nhận thức về ATTT.

NHNN đề ra những nhiệm vụ, giải pháp đảm an ninh, an toàn hệ thống thông tin trong thời gian tới

Với mục tiêu xây dựng nền tảng an ninh mạng chuyên nghiệp, hiện đại, chủ động phát hiện và xử lý kịp thời các sự cố an ninh mạng, đảm bảo an toàn, an ninh thông tin phục vụ tốt cho các hoạt động nghiệp vụ của NHNN và hỗ trợ công tác giám sát, ứng cứu sự cố ATTT ngành Ngân hàng, trong giai đoạn từ nay đến năm 2025, có 3 nhóm nhiệm vụ bảo đảm ATTT sẽ

được NHNN tập trung thực hiện, đó là:

Một là, triển khai hạ tầng an ninh thông tin thiết yếu thay thế các công nghệ cũ để chủ động trong công tác theo dõi, giám sát và ứng cứu sự cố an ninh thông tin.

Hai là, tăng cường hiệu quả hoạt động Mạng lưới ứng cứu sự cố an ninh thông tin ngành Ngân hàng và hợp tác với các tổ chức an ninh thông tin trong và ngoài nước; tăng cường công tác kiểm tra, kiểm soát về ATTT. Theo đó, về triển khai hạ tầng an ninh thông tin thiết yếu, NHNN xác định tiếp tục duy trì, nâng cấp, hoàn thiện mô hình bảo đảm ATTT 4 lớp.

Ba là, tăng cường các biện pháp bảo đảm an ninh, an toàn bảo mật cho các hệ thống thông tin NHNN đáp ứng các yêu cầu về bảo đảm an toàn hệ thống thông tin theo cấp độ; trong đó chú trọng đến các hệ thống thanh toán, hệ thống ngân hàng lõi và các hệ thống cung cấp dịch vụ công để đảm bảo duy trì hoạt động nghiệp vụ liên tục, an toàn trước các rủi ro về CNTT và tấn công mạng.

Những nhiệm vụ và mục tiêu cụ thể cần đạt được về an ninh bảo mật của giai đoạn tới là:

- NHNN chỉ đạo các đơn vị trực thuộc thường xuyên rà soát, cập nhật, phê duyệt cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ, thực hiện kiểm tra, đánh giá ATTT cho các hệ thống thông tin trong đơn vị theo quy định; phát hiện sớm các điểm yếu, lỗ hổng của hệ thống thông tin để có giải pháp xử lý phù hợp...

- Theo kế hoạch, trong năm 2022, sẽ hoàn thành triển khai quản lý các thiết bị đầu cuối truy cập mạng NHNN. Cùng với đó, hoàn thành xây dựng hệ thống điều hành, giám sát an ninh mạng ứng dụng CMCN 4.0 (Big Data, AI/Machine Learning), tự động hóa công tác giám sát, phân tích, phát hiện sớm các rủi ro an ninh, các hành vi xâm nhập, tấn công mạng vào hệ thống thông tin của NHNN; kết nối và chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia.

- Đối với nhiệm vụ kiểm tra, kiểm soát về an ninh thông tin, NHNN dự kiến năm 2023 sẽ hoàn thành xây dựng hệ thống thu thập, báo cáo và giám sát công tác tuân thủ các văn bản quy phạm pháp luật về CNTT của các đơn vị trong ngành Ngân hàng. Ứng dụng CNTT để thúc đẩy tự động hóa và giám sát liên tục tình hình tuân thủ văn bản quy phạm pháp luật về CNTT của các đơn vị trong Ngành; công tác kiểm tra tại chỗ tập trung vào kiểm tra các rủi ro trọng yếu phát hiện qua công tác giám sát.

- Xây dựng hạ tầng chữ ký số chuyên dùng NHNN tuân thủ tiêu chuẩn quốc gia về cung cấp dịch vụ chữ ký số; sẵn sàng cung cấp dịch vụ chữ ký số trên Mobile, dịch vụ cấp dấu thời gian (TSA) và dịch vụ kiểm tra chứng thư số trực tuyến (OCSP).

- Tiếp tục đổi mới hoạt động của mạng lưới ứng cứu sự cố ATTT ngành Ngân hàng, chuyên nghiệp, hiệu quả, hỗ trợ các đơn vị trong Ngành ứng phó nhanh chóng với các sự cố ATTT.

- Trong giai đoạn từ năm 2021 đến năm 2025, đảm bảo 100% thiết bị đầu cuối được quản lý an toàn theo chính sách tập trung khi truy cập mạng NHNN. Dữ liệu của người dùng khi trao đổi, chia sẻ trong mạng NHNN được quản lý, lưu trữ tập trung, an toàn.

- Hằng năm, tổ chức kiểm tra tuân thủ các tổ chức tín dụng theo định hướng kiểm tra chuyên sâu về việc quản trị, vận hành các hệ thống thông tin và thiết lập chính sách ATTT trên các hệ thống phát hiện qua công tác giám sát từ xa; cung cấp thông tin về các sai phạm phát hiện được qua công tác kiểm tra gửi các đơn vị có thẩm quyền xử phạt, cấp/thu hồi giấy phép để xử lý.■

TÀI LIỆU THAM KHẢO:

1. Quyết định số 260/QĐ-NHNN ngày 4/3/2021 của Thống đốc NHNN ban hành Kế hoạch ứng dụng CNTT, phát triển Chính phủ số và bảo đảm ATTT mạng trong hoạt động của NHNN giai đoạn 2021 - 2025.

2. https://ictnews.vietnamnet.vn/bao-mat/20-can-bo-lam-attt-cua-ngan-hang-nha-nuoc-co-chung-chi-quoc-te-vao-2025-279160.html