BẢO ĐẢM AN TOÀN THÔNG TIN trong chuyển đổi số

■ **Quỳnh Như**
Sở Thông tin và Truyền thông Nghệ An

"Đảm bảo an toàn, an ninh mạng là then chốt để chuyển đổi số thành công và bền vững, đồng thời là phần xuyên suốt, không thể tách rời của chuyển đổi số. Mọi thiết bị, sản phẩm, phần mềm, hệ thống thông tin, dự án đầu tư về công nghệ thông tin đều có cấu phần bắt buộc về an toàn, an ninh mạng ngay từ khi thiết kế" (Chiến lược Chuyển đổi số Quốc gia).

1. Bảo đảm an toàn, an ninh thông tin - vấn đề then chốt trong chuyển đổi số

Trong xu hướng chung của cả nước, Nghệ An xác định chuyển đổi số là nhu cầu tất yếu để phát triển kinh tế - xã hội trên địa bàn tỉnh. Mục tiêu trọng tâm của công cuộc chuyển đổi số trên địa bàn tỉnh trong thời gian tới là phát triển hạ tầng số, cơ sở dữ liệu số, tạo nền tảng phát triển chính quyền số, kinh tế số, hướng đến xã hội số; gắn quá trình chuyển đổi số với cải cách hành chính nhằm nâng cao chất lượng, hiệu lực, hiệu quả quản lý nhà nước và chất lượng cung cấp dịch vụ công của chính quyền các cấp; phấn đấu luôn giữ vị trí thuộc nhóm 30 tỉnh, thành phố có chỉ số cao về Chính phủ số, góp phần thúc đẩy phát triển kinh tế - xã hội, bảo đảm quốc phòng - an ninh.

Để thực hiện thành công chuyển đổi số, bên cạnh việc đảm bảo nguồn lực đầu tư cơ sở vật chất, đào tạo nhân lực… thì một thách thức lớn đó là việc đảm bảo an toàn an ninh thông tin trên môi trường mạng.

Theo thông tin từ Bộ Thông tin và Truyền thông, trên thế giới mới chỉ có khoảng 60% các dự án phát triển phần mềm áp dụng quy trình phát triển đánh giá an toàn thông tin (ATTT) trước khi vận hành. Tại Việt Nam, con số này còn thấp hơn rất nhiều. Vì vậy, vẫn còn tồn tại rất nhiều lỗi lập trình gây mất ATTT nghiêm trọng. Nếu những phần mềm này là các nền tảng số quốc gia thì hậu quả sẽ rất nghiêm trọng.

Tại Việt Nam, theo thống kê từ Bộ Thông tin và Truyền thông, tính đến cuối tháng 10/2022, đã có hơn 10.300 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam, tăng hơn 40% so với cùng kỳ năm 2021 và hơn gấp đôi so với năm 2020. Trung bình mỗi ngày, các hệ thống thông tin trong nước phải hứng chịu hơn 33 sự cố về an ninh thông tin. Nhiều đợt tấn công nhằm vào các hệ thống thông tin quốc gia, phát tán thông tin sai sự thật để lừa đảo, chiếm đoạt tài sản. Các thiết bị dễ bị tấn công nhất thường là điện thoại di động, thiết bị IoT.

Tính đến cuối tháng 10/2022, Bộ Công an đã khởi tố gần 500 vụ án và hơn 1.000 bị can liên quan các loại tội phạm sử dụng công nghệ cao, bằng con số của cả năm 2020, tăng gần 50% so với cùng kỳ năm 2021; số nạn nhân lên đến hàng chục nghìn và thiệt hại kinh tế hàng trăm tỷ.

Thực tế cho thấy, hiện nay ở nước ta đa số các thiết bị cá nhân như điện thoại thông minh, PC, laptop, máy tính bảng… đều chưa được cài phần mềm bảo vệ. Thậm chí các camera chưa được đánh giá an toàn thông tin và cài phần mềm bảo mật cũng gây rò rỉ, lộ lọt hình ảnh riêng tư trên mạng. Trung bình hàng năm, mỗi người dùng trên toàn cầu gặp phải từ 3-4 cuộc tấn công mạng.

Có thể thấy các nguy cơ mất ATTT trước yêu cầu chuyển đổi số là thách thức không nhỏ đối với các cơ quan, tổ chức, doanh nghiệp. Không khó để bắt gặp thông tin về các cuộc tấn công mạng, đánh cắp dữ liệu được đăng tải trên các phương tiện truyền thông với mật độ phủ sóng dày đặc. Những lo ngại về việc bảo mật dữ liệu, bảo đảm ATTT trước yêu cầu chuyển đổi số không chỉ còn là nỗi lo của riêng các nhà chức trách, mà còn của doanh nghiệp, người dân. Vì vậy, càng ý thức cao về sự không an toàn thì người dùng sẽ càng an toàn hơn. Nói cách khác, chỉ khi đảm bảo được an toàn, an ninh thông tin trên môi trường mạng thì công cuộc chuyển đổi số mới có thể được diễn ra toàn diện và bền vững.

2. Việc tăng cường bảo đảm an toàn an ninh thông tin trên địa bàn tỉnh Nghệ An

Nhận thức rõ việc đảm bảo an toàn an ninh thông tin là một trong những vấn đề then chốt

trong chuyển đổi số, trong những năm qua, song song với việc xây dựng phát triển chính quyền, xã hội tỉnh theo hướng số hóa. Trong những năm vừa qua, tỉnh Nghệ An đã quan tâm, chỉ đạo thực hiện nhiều hoạt động từ kiện toàn, xây dựng bộ máy, đào tạo nhân lực đến ứng dụng các giải pháp kỹ thuật nhằm bảo đảm công tác bảo đảm an toàn thông tin trên địa bàn.

Sở Thông tin và Truyền thông là đơn vị chuyên trách về ATTT trên địa bàn tỉnh đã thực hiện tham mưu kiện toàn Ban chỉ đạo xây dựng Chính quyền điện tử tỉnh Nghệ An; xây dựng Trung tâm giám sát, điều hành, an toàn, an ninh mạng (SOC) của tỉnh. Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông đã thực hiện giám sát trực tiếp đối với hệ thống thông tin dùng chung của tỉnh như: phần mềm quản lý văn bản và điều hành; trục liên thông gửi nhận văn bản điện tử 4 cấp; mạng truyền số liệu chuyên dùng; hệ thống cơ sở dữ liệu quốc gia về khiếu nại, tố cáo.

Trong giai đoạn 2016-2022, hoạt động truyền thông về đảm bảo an toàn an ninh mạng đã được triển khai tích cực. Bên cạnh việc phát hành nhiều tài liệu tuyên truyền; chỉ đạo các cơ hệ thống thông tin tăng cường truyền thông, Sở Thông tin và Truyền thông đã tổ chức nhiều lớp đào tạo, tập huấn kiến thức chuyên sâu về ATTT cho cán bộ chuyên trách công nghệ thông tin của các sở, ngành, địa phương; các lớp đào tạo kiến thức cơ bản về ATTT cho cán bộ công chức với số lượng lên đến hàng nghìn lượt đào tạo; thực hiện diễn tập ứng cứu sự cố công nghệ thông tin và ATTT hàng năm. Đây là nguồn nhân lực để sẵn sàng cho hoạt động bảo đảm an toàn an ninh thông tin cho các địa phương, đơn vị.

Những hoạt động ứng dụng công nghệ để bảo đảm ANTT trên địa bàn tỉnh đã được triển khai và thu được hiệu quả tốt phải kể đến là: Địa chỉ IP và tên miền của các cơ quan, đơn vị trong tỉnh (bao gồm 42 địa chỉ IP, 148 tên miền (Domain) đã được kết nối Trung tâm Giám sát an toàn không gian mạng Quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông thực hiện giám sát, cảnh báo kịp thời khi có sự cố về an toàn, an ninh thông tin. Cổng Thông tin điện tử của tỉnh cũng được phối hợp

Giám sát hệ thống thông tin tỉnh Nghệ An tại VNPT

với Cục Tin học nghiệp vụ (H49), Bộ Công An và Trung tâm Ứng cứu khẩn cấp sự cố máy tính Việt Nam VNCERT (nay là VNCERT/CC) để luôn đảm bảo hệ thống luôn được vận hành an toàn. Ngoài ra, Nghệ An cũng đã thực hiện đẩy mạnh đầu tư thuê các thiết bị, công cụ bảo đảm an toàn an ninh thông tin cho hệ thống số hóa của các địa phương trên địa bàn tỉnh như: hệ thống phòng chống virus tập trung của tỉnh từ năm 2019 tiếp tục được duy trì; thường xuyên kết nối với các doanh nghiệp nhiều kinh nghiệm (VNPT, Viettel, BKAV, CyRada…) để thực hiện kiểm tra, đánh giá định kỳ các hệ thống thông tin tỉnh Nghệ An.

Bên cạnh đó, các cơ quan chức năng cũng đã có sự phối hợp chặt chẽ trong hoạt động kiểm tra, xử lý đối với các hành vi vi phạm trên môi trường mạng nhằm phòng ngừa tối đa các hiện tượng đăng tải thông tin giả mạo, giả mạo trang thông tin điện tử của cơ quan nhà nước, tổ chức, doanh nghiệp khác… hoặc các hành vi lợi dụng môi trường mạng để thực hiện các tội phạm khác như lừa đảo chiếm đoạt tài sản, xúc phạm danh dự cá nhân, uy tín của tổ chức…

Do được triển khai khá đồng bộ những giải pháp bảo đảm ATTT trên địa bàn tỉnh trong thời gian qua cơ bản được đảm bảo. Tuy nhiên, theo các chuyên gia, vấn đề ATTT trên không gian mạng vẫn tiềm ẩn nhiều rủi ro. Vì vậy, tỉnh Nghệ An đã xây dựng kế hoạch sẽ tiếp tục tăng cường thực hiện các giải pháp đảm bảo an toàn an ninh thông tin trong thời gian tới. Theo đó các biện pháp được chú trọng gồm: Rà soát, kiện toàn các quy chế, quy trình về quản lý, bảo đảm ATTT mạng tại các cơ quan, đơn vị; Bảo đảm an toàn, an ninh mạng theo mô hình 4 lớp thống nhất trên phạm vi toàn tỉnh; Triển khai, phát triển Trung tâm Điều hành an toàn, an ninh mạng (SOC) tỉnh Nghệ An; Tăng cường xây dựng đội ngũ chuyên gia an toàn, an ninh mạng để kịp thời theo dõi, phòng ngừa, ngăn chặn, phối hợp xử lý, khắc phục các sự cố về an toàn, an ninh mạng và tội phạm sử dụng công nghệ cao. Nâng cao năng lực Đội ứng cứu sự cố mạng, máy tính tỉnh Nghệ An, cơ quan thường trực Đội ứng cứu cả về năng lực chuyên môn và hệ thống trang thiết bị chuyên dùng; Quan tâm đầu tư trang thiết bị, phương tiện khoa học kỹ thuật để chủ động phòng ngừa, ứng phó với các nguy cơ, tác động tiêu cực của quá trình chuyển đổi số; Bảo đảm an toàn, an ninh mạng, bảo vệ dữ liệu cá nhân trong chuyển đổi số, góp phần thúc đẩy hoạt động trên môi trường số; Tăng cường quản lý an ninh mạng, bảo mật thông tin và an toàn dữ liệu; Phòng chống hiệu quả các hoạt động phá hoại, thâm nhập hệ thống quản lý, điều hành chính quyền điện tử; Tham gia chia sẻ dữ liệu quản lý công dân trong một số lĩnh vực công trực tuyến như: định danh điện tử, lưu trữ và truy xuất thông tin người dân.

Có thể thấy, chuyển đổi số không chỉ là hoạt động của cơ quan nhà nước mà nó đang diễn ra trong từng doanh nghiệp, cá nhân. Điều đó cũng đồng nghĩa với việc nguy cơ mất an toàn, an ninh thông tin trên môi trường mạng cũng tồn tại và diễn ra sâu rộng nếu không được cảnh báo và phòng ngừa sớm. Vì vậy, bên cạnh những nỗ lực của chính quyền để xây dựng nguồn nhân lực, vật lực thì việc tăng cường công tác thông tin tuyên truyền, hướng dẫn người dân nâng cao nhận thức tự bảo vệ trên môi trường số, tuân thủ các quy định pháp luật về ATTT cũng là một giải pháp được cơ quan chuyên môn đề xuất đẩy mạnh thực hiện trên địa bàn tỉnh trong thời gian tới./.

CẢNH BÁO 8 THỦ ĐOẠN CÁC ĐỐI TƯỢNG THƯỜNG LỪA ĐẢO QUA MẠNG

1. Giả mạo các trang thông tin điện tử cơ quan, doanh nghiệp (bảo hiểm xã hội, ngân hàng...) đánh cắp, chiếm đoạt thông tin dữ liệu cá nhân của người đăng nhập; hoặc thiết lập các trạm BTS viễn thông giả mạo để phát tán tin nhắn thương hiệu (SMS Branname) của các ngân hàng để đánh cắp thông tin, tài khoản người dùng sau đó thực hiện hành vi chiếm đoạt tài sản.

2. Thông qua hoạt động của các sàn đầu tư chứng khoán quốc tế, giao dịch vàng, ngoại hối, quyền chọn nhị phân (BO), giao dịch tiền ảo, dự án bất động sản… hoặc hoạt động kinh doanh đa cấp trái phép qua mạng để quảng cáo, lôi kéo số lượng lớn người tham gia đầu tư, kinh doanh nhằm mục đích lừa đảo chiếm đoạt số tiền của người tham gia.

3. Đăng tin tuyển cộng tác viên bán hàng online trên các trang mạng xã hội để chiếm đoạt số tiền tạm ứng hoặc thanh toán đơn hàng.

4. Sử dụng nhiều thủ đoạn khác nhau để chiếm quyền điều khiển tài khoản mạng xã hội, sau đó, nhắn tin lừa đảo đến danh sách bạn bè của người bị hại; hoặc chiếm đoạt quyền sử dụng SIM điện thoại bằng cách gọi điện tư vấn chuyển đổi hoặc nâng cấp SIM điện thoại sang mạng 4G miễn phí, từ đó chiếm đoạt mật khẩu tài khoản ngân hàng, ví điện tử, tài khoản mạng xã hội để thực hiện hành vi chiếm đoạt tài sản.

5. Giả danh cơ quan công an, viện kiểm sát, tòa án gọi điện qua giao thức VoIP để hăm dọa bị hại có liên quan đến các vụ án đang điều tra, yêu cầu bị hại chuyển tiền đến các tài khoản do các đối tượng chỉ định hoặc yêu cầu cung cấp mã OTP để xác thực chuyển tiền để kiểm tra, xác minh sau đó chiếm đoạt.

6. Thông qua hoạt động thương mại điện tử để rao bán hàng giả, hàng nhái.

7. Sử dụng thông tin trên CCCD để đăng ký mã số thuế ảo hoặc để vay tiền các tổ chức tín dụng trên mạng xã hội với lãi suất "cắt cổ" hoặc sử dụng thông tin để thực hiện hành vi lừa đảo chiếm đoạt tài sản.

8. Thủ đoạn cố ý chuyển nhầm tiền vào tài khoản ngân hàng để lừa đảo: các đối tượng cố ý chuyển nhầm một khoản tiền vào tài khoản của bị hại, rồi giả danh là người thu hồi nợ, yêu cầu người nhận trả lại số tiền kia như một khoản vay với lãi suất "cắt cổ"./.

(Nguồn: Báo điện tử Đảng cộng sản VN https://dangcongsan.vn/)