NÂNG CAO HIỆU QUẢ CÔNG TÁC ĐẢM BẢO AN NINH MẠNG VÀ BẢO VỆ BÍ MẬT NHÀ NƯỚC TRÊN ĐỊA BÀN TỈNH QUẢNG BÌNH

TRẦN ANH TUẤN
Công an tỉnh Quảng Bình

1. Thực trạng công tác đảm bảo an ninh mạng và bảo vệ bí mật nhà nước trên địa bàn tỉnh Quảng Bình

Trong bối cảnh phát triển khoa học và công nghệ (KH&CN) hiện nay, thời gian qua, Tỉnh ủy, Ủy ban nhân dân (UBND) tỉnh Quảng Bình đã ban hành nhiều chính sách, biện pháp nhằm đẩy mạnh ứng dụng công nghệ thông tin (CNTT) trong các cơ quan nhà nước; tranh thủ các thành tựu KH&CN tiên tiến để đẩy nhanh hơn tiến trình công nghiệp hóa, hiện đại hóa. Nghị quyết số 26/2017/NQ-HĐND của Hội đồng nhân dân tỉnh Quảng Bình ngày 18/7/2017 về thông qua quy hoạch phát triển CNTT tỉnh Quảng Bình đến năm 2025 và định hướng đến năm 2035 xác định mục tiêu: "*Hạ tầng thông tin của tỉnh được hiện đại, đồng bộ, liên thông với hạ tầng của quốc gia; đẩy mạnh xây dựng, khai thác có hiệu quả mạng diện rộng, trung tâm dữ liệu điện tử, cơ sở dữ liệu và phần mềm dùng chung; kết nối băng rộng chất lượng cao đến vùng sâu, vùng xa, triển khai và sử dụng có hiệu quả truyền số liệu chuyên dùng của cơ quan Đảng, Nhà nước*" [2].

Thực hiện chủ trương của Tỉnh ủy, UBND tỉnh, các sở, ban, ngành, UBND các huyện, thị xã, thành phố trên địa bàn tỉnh Quảng Bình thời gian qua đã triển khai kế hoạch về ứng dụng CNTT, phát triển chính quyền số, bảo đảm an toàn thông tin mạng và bảo vệ bí mật nhà nước (BMNN); đẩy mạnh thực hiện các chỉ tiêu về dịch vụ công trực tuyến, xử lý hồ sơ công việc trên môi trường mạng. Hạ tầng kỹ thuật, hệ thống nền tảng, ứng dụng cơ bản trên địa bàn tỉnh được đầu tư xây dựng trên cơ sở có trọng tâm, trọng điểm, bảo đảm sự thống nhất, kết nối, tích hợp dữ liệu giữa các ứng dụng, phần mềm. Nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh (LGSP) được xây dựng phần lõi, bước đầu kết nối, chia sẻ dữ liệu giữa các hệ thống thông tin, cơ sở dữ liệu của tỉnh và liên thông với nền tảng tích hợp, chia sẻ dữ liệu quốc gia (NGSP). Hệ thống cổng, trang thông tin điện tử tỉnh được nâng cấp, triển khai đến 100% các sở, ban, ngành, UBND cấp huyện. Hệ thống thư điện tử công vụ cấp phát hơn 7.000 tài khoản với 100% cán bộ, công chức hành chính có hộp thư điện tử công vụ [3].

Tuy nhiên, bên cạnh những kết quả đạt được, việc ứng dụng CNTT trong các cơ quan, đơn vị còn tiềm ẩn nhiều nguy cơ, thách thức trong đảm bảo an ninh, an toàn, trong đó có nguy cơ mất an ninh mạng và lộ, mất BMNN. Qua công tác kiểm tra an ninh mạng, bảo vệ BMNN tại các cơ quan, đơn vị trên địa bàn tỉnh thời gian qua cho thấy vẫn còn tồn tại một số hạn chế, thiếu sót trong công tác bảo vệ an ninh mạng, bảo vệ BMNN, trong đó nổi lên một số vấn đề sau:

Một là, công tác hướng dẫn, đôn đốc, kiểm tra việc thực hiện các quy định về bảo vệ an ninh mạng, bảo vệ BMNN của một số cơ quan, đơn vị còn hạn chế như: chưa xác định được hệ

thống thông tin, tài liệu BMNN thuộc phạm vi trách nhiệm quản lý, bảo vệ của đơn vị, địa phương mình; chưa quản lý chặt chẽ hệ thống máy vi tính, thiết bị liên lạc, thiết bị lưu trữ ngoại vi, hoạt động của các trang web, cổng thông tin điện tử; chưa xây dựng nội quy, quy chế bảo vệ BMNN; chưa lập thống kê danh mục tài liệu thuộc phạm vi BMNN do mình quản lý hoặc có lập nhưng còn chung chung, khó xác định được độ mật của tài liệu, dẫn đến bị động, lúng túng trong quá trình thực hiện; công tác tuyên truyền, phổ biến, quán triệt và thực hiện các quy định của pháp luật về bảo vệ BMNN, bảo vệ an ninh mạng chưa thường xuyên, hình thức tuyên truyền chưa phong phú, thiết thực nên chưa nâng cao nhận thức của cán bộ, công chức về công tác vệ BMNN và bảo vệ an ninh mạng [1].

Hai là, việc chấp hành các quy định về bảo vệ an ninh mạng, bảo vệ BMNN tại một số cơ quan, đơn vị vẫn còn tồn tại những bất cập, thiếu sót. Tình trạng cán bộ, nhân viên sử dụng máy tính kết nối mạng internet để soạn thảo, lưu trữ, trao đổi thông tin, dữ liệu thuộc phạm vi BMNN còn xảy ra; việc chấp hành các quy định về bảo vệ BMNN trong soạn thảo, in ấn, xác định và đóng dấu độ mật, phát hành, giao nhận, tiêu hủy tài liệu thuộc phạm vi BMNN chưa thực sự nghiêm túc; tình trạng sử dụng thiết bị lưu trữ ngoài như USB, thẻ nhớ để lưu trữ, trao đổi tài liệu BMNN còn tồn tại. Hệ thống lưu trữ bảo quản tài liệu mật ở cơ quan còn đơn giản, sơ sài, chưa bảo đảm an toàn về cháy nổ, chống ẩm ướt, mối mọt. Nhiều cán bộ làm công tác bảo mật chưa được đào tạo bài bản về công tác lưu trữ, bảo vệ tài liệu BMNN, chưa làm cam kết bảo mật theo quy định [1].

Ba là, việc đầu tư trang, thiết bị phục vụ công tác đảm bảo an ninh mạng, bảo vệ BMNN của một số cơ quan, đơn vị còn nhiều hạn chế. Nhiều hệ thống máy chủ của cổng thông tin, trang thông tin điện tử của các cơ quan, đơn vị không có thiết bị bảo vệ như tường lửa (Firewall), thiết bị phát hiện và ngăn chặn phòng chống tấn công mạng (IPS/IDS), hệ thống giám sát an ninh mạng để phát hiện, cảnh báo tự động ngăn chặn tấn công mạng (SIEM); hoặc nếu có thì không tương xứng với quy mô hệ thống, không được bổ sung, nâng cấp thường xuyên. Với tình trạng trang, thiết bị kỹ thuật phục vụ đảm bảo an ninh, an toàn thông tin như vậy, rất khó để các cơ quan, đơn vị phát hiện, ngăn chặn kịp thời các cuộc tấn công mạng, nhất là khi thủ đoạn của các đối tượng ngày càng trở nên tinh vi, khó phát hiện như hiện nay [3].

Bốn là, cổng, trang thông tin điện tử của nhiều cơ quan, đơn vị còn tồn tại nhiều lỗ hổng bảo mật, điểm yếu kỹ thuật khác. Thực tế cho thấy, các cơ quan, đơn vị thường tự xây dựng cổng, trang thông tin điện tử theo tư vấn của đơn vị thiết kế, theo nhu cầu ứng dụng, khả năng kinh phí và năng lực điều hành của mình mà ít chú ý tập trung vào các tiêu chuẩn kỹ thuật, tiêu chuẩn an ninh, an toàn cho hệ thống. Điều này đưa đến tình trạng cổng, trang thông tin điện tử của các cơ quan, đơn vị được xây dựng trên nhiều nền tảng công nghệ khác nhau, không có một tiêu chuẩn thống nhất về an ninh, an toàn thông tin; trong đó, nhiều cổng, trang thông tin điện tử tồn tại nhiều lỗ hổng bảo mật, điểm yếu kỹ thuật. Qua rà soát của các cơ quan chức năng, nhiều các cổng thông tin, trang tin điện tử của cơ quan Đảng, Nhà nước trên địa bàn tỉnh hiện nay tồn tại lỗ hổng bảo mật, trong đó, có những lỗ hổng bảo mật nghiêm trọng, có thể bị tin tặc lợi dụng để tấn công, chiếm quyền kiểm soát cổng, trang thông tin điện tử [3].

Năm là, số lượng, chất lượng của đội ngũ chuyên trách về an ninh, an toàn thông tin còn

hạn chế. Sự thiếu hụt nguồn nhân lực CNTT chất lượng cao, nhất là về nguồn nhân lực về an ninh, an toàn thông tin tại các cơ quan, đơn vị trên địa bàn tỉnh là một vấn đề đáng lo ngại dẫn đến việc không thể làm chủ cũng như tự chủ được về hạ tầng và dịch vụ mạng, không kiểm soát được các vấn đề về an ninh, an toàn thông tin đối với hệ thống thông tin của cơ quan, đơn vị mình. Bên cạnh đó, trình độ cán bộ làm nhiệm vụ quản trị, vận hành hệ thống thông tin của các cơ quan, đơn vị còn nhiều hạn chế như: Đội ngũ chuyên viên kỹ thuật không có khả năng tự phát hiện, khắc phục các lỗ hổng bảo mật, các lỗi kỹ thuật, nhất là các lỗi liên quan đến mã nguồn lập trình mà phụ thuộc vào các công ty thiết kế, xây dựng hệ thống hoặc cảnh báo của cơ quan an ninh; Ý thức bảo mật của các cán bộ tham gia quản trị, điều hành và sử dụng hệ thống thông tin chưa cao, việc chấp hành các quy định về bảo vệ dữ liệu quan trọng, tài khoản đăng nhập hệ thống, quy trình xử lý các sự cố kỹ thuật, ngăn chặn các cuộc tấn công mạng,… còn nhiều hạn chế, thiếu sót [1].

2. Giải pháp nâng cao hiệu quả công tác đảm bảo an ninh mạng và bảo vệ bí mật nhà nước trên địa bàn tỉnh Quảng Bình thời gian tới

Trong bối cảnh cuộc cách mạng KH&CN 4.0 tác động ngày càng sâu vào các ngành, các lĩnh vực của đời sống, thời gian tới, hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh sẽ được phát triển, mở rộng kết nối, chia sẻ dữ liệu với Cổng dịch vụ công quốc gia; tích hợp với nhiều hệ thống cơ sở dữ liệu lớn như: Cơ sở dữ liệu quốc gia về dân cư, Cơ sở dữ liệu quốc gia về đăng ký doanh nghiệp, Cơ sở dữ liệu quốc gia về trẻ em,... hướng tới một Chính phủ điện tử thông suốt, có tính liên thông, liên kết ở các ngành, các cấp. Cùng với đó, các cơ quan Đảng, Nhà nước sẽ tiếp tục tập trung xây dựng và hoàn thiện hệ thống thông tin, cơ sở dữ liệu chuyên ngành để từ đó tạo nền tảng phát triển chính quyền điện tử của tỉnh; xây dựng triển khai các hệ thống thông tin, cơ sở dữ liệu dùng chung một cách đồng bộ theo kiến trúc chính quyền điện tử đã được phê duyệt.

Trong bối cảnh đó, việc đảm bảo an ninh mạng và bảo vệ BMNN các hệ thống thông tin trên địa bàn tỉnh là yêu cầu cấp bách, quan trọng hàng đầu. Trong đó, cần tập trung vào một số giải pháp trọng tâm sau:

Một là, các cơ quan, đơn vị cần đẩy mạnh công tác tuyên truyền, phổ biến, giáo dục pháp luật về bảo vệ BMNN, bảo vệ an ninh mạng cho cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị trên địa bàn tỉnh. Nội dung tuyên truyền bên cạnh phổ biến, quán triệt các quy định của pháp luật và mục tiêu, nhiệm vụ công tác bảo vệ BMNN, bảo vệ an ninh mạng; cần đưa ra những chỉ dẫn cụ thể trong việc bảo vệ an ninh, an toàn hệ thống thông tin; quản lý, bảo vệ tin, tài liệu, vật mang BMNN; các chỉ dẫn phải phải có tính khái quát cao, dễ nhớ, dễ thuộc và dễ thực hiện, bám sát vào tình hình thực tiễn trên địa bàn.

Hai là, nâng cao hiệu lực, hiệu quả quản lý nhà nước về an ninh mạng, quản lý nhà nước về bảo vệ BMNN. Cần tăng cường hướng dẫn, đôn đốc các cơ quan, đơn vị trên địa bàn tỉnh nghiên cứu sửa đổi, bổ sung danh mục BMNN và quy chế bảo vệ BMNN, tạo hành lang pháp lý đầy đủ, vững chắc giúp các cơ quan, tổ chức, đơn vị thực hiện có hiệu quả công tác bảo vệ BMNN trong lĩnh vực này. Hướng dẫn các cơ quan, đơn vị căn cứ vào danh mục BMNN đã được Thủ tướng Chính phủ ban hành xác định độ mật của từng tin, tài liệu cụ thể để tổ chức quản lý. Thường xuyên rà soát danh mục BMNN hiện hành để kịp thời đề xuất sửa đổi

những danh mục không còn phù hợp, bổ sung, đưa vào danh mục BMNN những loại tin, tài liệu mới phát sinh trình cấp có thẩm quyền quyết định, ban hành.

Ba là, đẩy mạnh hoạt động kiểm tra, xử lý vi phạm pháp luật về an ninh mạng, bảo vệ BMNN. Trong đó tập trung kiểm tra việc chấp hành quy định về bảo vệ an ninh mạng, bảo vệ BMNN được quy định trong Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước, Nghị định 53/2022-NĐ-CP ngày 15/8/2022 về việc quy định chi tiết một số điều của Luật An ninh mạng.

Bốn là, chú trọng nghiên cứu, ứng dụng các giải pháp về KH&CN và đảm bảo điều kiện cần thiết tổ chức phòng, chống hoạt động tấn công mạng, lộ mất BMNN qua thiết bị thông tin, liên lạc. Lực lượng Công an cần tham mưu với các cơ quan, đơn vị đầu tư kinh phí để trang bị, nâng cao hiệu quả của "bức tường lửa" (Firewall), hệ thống phát hiện tấn công mạng nhằm ngăn chặn các thông tin độc hại, virus gián điệp xâm nhập lấy cắp, chiếm đoạt BMNN. Nghiên cứu đa dạng hóa, nâng cao hiệu quả bảo vệ hệ thống dữ liệu bằng mật khẩu (password). Tập trung nghiên cứu, đầu tư xây dựng các hệ thống có khả năng phát hiện, cảnh báo sớm các nguy cơ gây mất an ninh, an toàn hệ thống thông tin của các cơ quan Đảng, Nhà nước. Trong đó, ưu tiên đầu tư, xây dựng một số hệ thống như: hệ thống thu thập, xử lý, giám sát tập trung, đồng bộ, liên tục và cảnh báo sớm hoạt động tấn công mạng đối với cổng thông tin điện tử của các cơ quan Đảng, Nhà nước; hệ thống thu thập thông tin và cảnh báo sớm hoạt động tấn công mạng; hệ thống phòng, chống các cuộc tấn công từ chối dịch vụ quy mô lớn thông qua triển khai các hệ thống tiếp nhận, phân luồng, điều hướng các lưu lượng tấn công từ chối dịch vụ phân tán nhắm vào cổng, trang thông tin điện tử các cơ quan, đơn vị trên địa bàn tỉnh.

Năm là, củng cố, kiện toàn tổ chức, xây dựng cơ chế phối hợp chặt chẽ, đồng bộ và hiệu quả trong công tác bảo vệ an ninh mạng, bảo vệ BMNN. Triển khai cơ chế phối hợp chặt chẽ giữa Công an tỉnh với các cơ quan, đơn vị trong tỉnh về đảm bảo an ninh mạng, bảo vệ BMNN. Trong đó, xác định rõ trách nhiệm của các bên, cơ chế phối hợp trong hoạt động tuyên truyền, nâng cao ý thức của cán bộ, nhân viên trong đảm bảo an ninh mạng, bảo vệ BMNN; thu thập thông tin, nắm tình hình về hoạt động của hệ thống thông tin; phối hợp trong xây dựng, triển khai phương án đảm bảo an ninh mạng đối với hệ thống thông tin; hướng dẫn trang bị các phần mềm bảo mật, phòng chống hoạt động tấn công mạng, phòng chống lộ mất BMNN trên hệ thống thông tin của các cơ quan Đảng, Nhà nước; phối hợp trong quá trình diễn tập phòng chống tấn công mạng hoặc các hành vi xâm hại an ninh, an toàn thông tin. Xây dựng quy trình ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh ■

Tài liệu tham khảo:

1. Công an tỉnh Quảng Bình (2018-2023), *Báo cáo sơ kết công tác bảo vệ bí mật nhà nước và dự kiến một số công tác trọng tâm năm từ 2018-2023,* Quảng Bình.

2. Hội đồng nhân dân tỉnh Quảng Bình, *Nghị quyết số 26/2017/NQ-HĐND của Hội đồng nhân dân tỉnh Quảng Bình ngày 18/7/2017 về thông qua quy hoạch phát triển công nghệ thông tin tỉnh Quảng Bình đến năm 2025 và định hướng đến năm 2035,* Quảng Bình.

3. Phòng An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao, Công an tỉnh Quảng Bình, *Báo cáo tình hình, kết quả công tác năm 2021, 2022, 2023*, Quảng Bình.