Ký bởi: Ủy ban nhân dân tỉnh

UBND TỈNH ĐIỆN BIÊN
TIỂU BAN AN TOÀN, AN NINH MẠNG

Số: 4269 /CV-TBATANM

V/v tăng cường bảo đảm an ninh mạng, an toàn các hệ thống thông tin trên địa bàn tỉnh

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Điện Biên, ngày 23 tháng 9 năm 2024

Kính gửi:
- Các sở, ban, ngành, đoàn thể tỉnh;
- Các tổ chức, doanh nghiệp Nhà nước trên địa bàn tỉnh;
- UBND các huyện, thị xã, thành phố.

Thời gian qua, tình hình an ninh mạng trên cả nước nói chung và trên địa bàn tỉnh Điện Biên nói riêng diễn biến ngày càng phức tạp, hoạt động tấn công mạng nhằm vào các hệ thống thông tin quan trọng gia tăng về tần suất và mức độ nguy hiểm. Qua công tác rà quét, bảo đảm an ninh, an toàn hệ thống thông tin trên địa bàn tỉnh, từ ngày 10/7/2024 đến ngày 30/8/2024, Công an tỉnh đã phát hiện nhiều hoạt động điều hướng nội dung thông tin xấu độc thông qua trang thông tin điện tử thuộc quyền quản lý của 11 cơ quan, đơn vị, địa phương trên địa bàn tỉnh *(gồm: Sở Văn hóa - Thể thao và Du lịch, Sở Tư pháp, Hội Văn học - Nghệ thuật tỉnh, Trường Cao đẳng Sư phạm Điện Biên, Báo Điện Biên Phủ, Thư viện tỉnh, Công ty TNHH Xổ số kiến thiết Điện Biên, UNBD thị xã Mường Lay, UBND thành phố Điện Biên Phủ, UBND huyện Tuần Giáo, Trường THCS-THPT Quài Tở - huyện Tuần Giáo).* Các website này bị tấn công, khai thác lỗ hổng bảo mật, cài cắm backlink dẫn đến nguy cơ các website và phần mềm ứng dụng bị tấn công bởi mã độc hoặc hiển thị các nội dung không phù hợp trên các trang thông tin điện tử thuộc quyền quản lý của các cơ quan, đơn vị, địa phương.

Nguyên nhân xảy ra các vụ việc trên có thể do: (1) Trang web có thể sử dụng mã JavaScript để tự động chuyển hướng người dùng đến một trang web khác, điều này thường xảy ra một cách nhanh chóng và không hiển thị thông báo hay cảnh báo; (2) Website bị hacker tấn công lợi dụng lỗ hổng bảo mật: Nếu trang web không được bảo vệ đúng cách, hacker có thể tận dụng các lỗ hổng bảo mật để cài cắm, đăng tải, chuyển hướng hoặc liên kết với nội dung không phù hợp. Sự việc này sẽ trở nên rất nguy hiểm và nghiêm trọng nếu bị lợi dụng để đăng tải, phát tán những nội dung xấu độc, xuyên tạc về chủ quyền, chủ trương của Đảng và chính sách, pháp luật của Nhà nước...

Để tăng cường công tác bảo đảm an ninh mạng, an toàn hệ thống thông tin trên địa bàn tỉnh, phòng ngừa nguy cơ bị các đối tượng xấu lợi dụng để phát tán, tấn công vào các hệ thống thông tin do các cơ quan, đơn vị, địa phương đang quản lý, vận hành; chiếm quyền điều khiển, tấn công, phá hoại, truy cập bất hợp pháp các thông tin nhạy cảm, gây mất an toàn, an ninh mạng; Tiểu ban An toàn, An ninh mạng tỉnh yêu cầu các cơ quan, đơn vị, địa phương triển khai thực hiện một số nội dung sau:

1. Tiếp tục phổ biến, quán triệt tới toàn thể cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị, địa phương chấp hành nghiêm các quy định của pháp luật, hướng dẫn về bảo đảm an ninh mạng, nhất là Luật An ninh mạng, Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng.

2. Tăng cường các biện pháp giám sát an ninh, an toàn hệ thống mạng, thông qua các hệ thống giám sát, hệ thống phòng chống mã độc tập trung để chủ động phát hiện sớm các hoạt động bất thường, hành vi tấn công mạng vào hệ thống. Thường xuyên tổ chức rà soát các đường dẫn, khắc phục các điểm yếu, lỗ hổng bảo mật cho các máy chủ, ứng dụng mạng, phần mềm nghiệp vụ, trong đó ưu tiên các hệ thống kết nối mạng internet, hệ thống kết nối với bên thứ 3; thực hiện ngay việc sao lưu hệ thống, dữ liệu trên thiết bị lưu trữ độc lập hoặc giải pháp tương đương; loại bỏ hoặc nâng cấp các máy tính, máy chủ đang sử dụng hệ điều hành không còn được hãng hỗ trợ cập nhật bản vá bảo mật.

3. Quan tâm bố trí kinh phí để kịp thời nâng cấp cơ sở hạ tầng, kỹ thuật bảo đảm an ninh, an toàn thông tin cho Cổng/Trang thông tin điện tử do cơ quan, đơn vị, dịa phương mình đang quản lý, vận hành như tường lửa, thiết bị phòng, chống xâm nhập…Thực hiện tốt quy trình vận hành, bảo trì, bảo dưỡng và phát triển hệ thống, chính sách an toàn thông tin cho Cổng/Trang thông tin điện tử; sử dụng mật khẩu mạnh và định kỳ thay đổi mật khẩu tài khoản quản trị *(sử dụng chữ in thường, in hoa, số và ký tự đặc biệt)*; cập nhật Website lên phiên bản mới nhất, sửa lỗi và cập nhật các mã nguồn; cài đặt phần mềm chống virus và phần mềm chống xâm nhập để bảo vệ dữ liệu được an toàn, ngăn chặn nguy cơ truy cập trái phép từ bên ngoài.

4. Trong trường hợp phát hiện hoạt động tấn công mạng vào các hệ thống thông tin do các cơ quan, đơn vị, địa phương đang quản lý, vận hành thì kịp thời trao đổi với Công an tỉnh - Cơ quan Thường trực Tiểu ban *(qua phòng An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại: 0866.130.113)* để được hướng dẫn, phối hợp xử lý.

5. Giao Công an tỉnh hướng dẫn, kiểm tra, đôn đốc việc triển khai thực hiện Công văn này. Đồng thời, chủ động tham mưu, đề xuất với cấp có thẩm quyền chỉ đạo xử lý các vấn đề phát sinh (nếu có) theo quy định.

Nhận được văn bản này, các cơ quan, đơn vị, địa phương nghiêm túc triển khai thực hiện, đảm bảo nội dung yêu cầu./.

Nơi nhận:
- Như trên;
- Thường trực Tỉnh ủy (b/c);
- Lãnh đạo UBND tỉnh;
- Lưu: VT, NC.

TRƯỞNG TIỂU BAN

ỦY BAN NHÂN DÂN TỈNH ĐIỆN BIÊN

CHỦ TỊCH UBND TỈNH
Lê Thành Đô