ỦY BAN NHÂN DÂN TỈNH LAI CHÂU	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 2268 /UBND-TH V/v tăng cường công tác bảo đảm an toàn, an ninh mạng hệ thống thông tin trọng yếu	*Lai Châu, ngày 17 tháng 6 năm 2024*

Kính gửi:

- Các sở, ban, ngành, đoàn thể tỉnh;
- UBND các huyện, thành phố.

Thời gian qua, trong quá trình đẩy mạnh và triển khai thực hiện Đề án 06 của Chính phủ, nhiều hệ thống thông tin quan trọng, phức tạp, mang tính liên kết sâu rộng, lưu trữ khối lượng dữ liệu lớn được đầu tư, xây dựng nhưng cũng dễ bộc lộ các điểm yếu có nguy cơ gây mất an ninh mạng.

Thực tế đã phát hiện các cuộc tấn công mạng nhằm vào các cơ quan đầu ngành của Đảng, Nhà nước, các tập đoàn kinh tế "mũi nhọn", các hệ thống thông tin quan trọng tại nhiều địa phương[1]. Nguyên nhân của tình trạng trên xuất phát từ nhận thức về vai trò, tầm quan trọng của công tác bảo đảm an toàn, an ninh mạng còn hạn chế; khả năng ứng cứu, xử lý, khắc phục sự cố trước các cuộc tấn công mạng còn thấp, nhiều hệ thống công nghệ thông tin quan trọng đầu tư không đồng bộ, không được giám sát, kiểm tra, đánh giá định kỳ, thường xuyên, tồn tại điểm yếu kỹ thuật, lỗ hổng bảo mật; việc chấp hành quy trình, quy định về bảo đảm an ninh mạng, bảo vệ dữ liệu cá nhân chưa nghiêm, không đầy đủ; việc quan tâm đầu tư về nguồn lực phục vụ công tác bảo đảm an ninh hệ thống mạng còn hạn chế, chưa đáp ứng yêu cầu…

Để tăng cường công tác phòng, chống tấn công mạng, bảo vệ dữ liệu; UBND tỉnh yêu cầu Thủ trưởng các sở, ban, ngành, đoàn thể tỉnh, UBND các huyện, thành phố tổ chức thực hiện một số nội dung công tác trọng tâm sau đây:

1. Quán triệt, triển khai thực hiện quyết liệt, có hiệu quả các quy định của pháp luật về an toàn thông tin mạng, an ninh mạng, nhất là các quy định của Luật An toàn thông tin mạng, Luật An ninh mạng và các Nghị định hướng dẫn thi hành; các chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 09/CT-TTg ngày 23/2/2024 về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ và Công điện số 33/CĐ-TTg ngày 07/4/2024 về tăng cường bảo đảm an toàn thông tin mạng… Cụ thể hóa trách nhiệm của đơn vị, tổ

[1] Vừa qua, tin tặc cũng đã tấn công vào hệ thống thông tin của một số đơn vị trên địa bàn tỉnh bằng mã độc mã hóa dữ liệu đòi tiền chuộc, gây ngưng trệ hoạt động tại đơn vị bị tấn công.

chức, cá nhân trong công tác bảo vệ an toàn, an ninh mạng hệ thống thông tin quan trọng, bảo vệ dữ liệu cá nhân.

2. Xây dựng kế hoạch và triển khai bảo vệ an toàn thông tin mạng, an ninh mạng cho hệ thống thông tin thuộc phạm vi quản lý ở mức độ cao nhất; không để xảy ra các sự cố mất an toàn thông tin mạng, an ninh mạng nghiêm trọng, đặc biệt là trước, trong và sau các ngày lễ lớn, sự kiện quan trọng của tỉnh, của đất nước; áp dụng tài liệu *"Hướng dẫn các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia"*[2] do Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an ban hành để thực hiện thống nhất, đồng bộ cho các hệ thống thông tin.

3. Tổ chức rà soát, đánh giá an ninh, an toàn thông tin tổng thế đối với hệ thống mạng, dịch vụ mạng như: Rà soát, siết chặt các chính sách truy cập trên các thiết bị bảo mật, bảo vệ mạng; rà soát virus, mã độc trên máy chủ, máy tính quản trị, máy tính người dùng; rà soát, khắc phục lỗ hổng bảo mật trên ứng dụng mạng, phần mềm nghiệp vụ; thực hiện ngay việc sao lưu hệ thống, dữ liệu trên các thiết bị lưu trữ độc lập; tạm ngừng chính sách truy cập từ xa; rà soát loại bỏ các thiết bị, máy chủ, dịch vụ mạng và tài khoản trên hệ thống thử nghiệm, hệ thống cũ hoặc không còn sử dụng; kiểm soát, giám sát chặt chẽ nhà thầu, bên thứ 3 trong quá trình hỗ trợ kỹ thuật, cài đặt hệ thống…

4. Tổ chức tuyên truyền, phổ biến đến toàn thể cán bộ, công chức, viên chức nhằm nâng cao nhận thức, trách nhiệm đối với công tác đảm bảo an ninh, an toàn hệ thống mạng, bảo vệ bí mật nhà nước, thông tin dữ liệu cá nhân trên không gian mạng; thường xuyên cập nhật, thực hiện nghiêm các thông báo, cảnh báo của cơ quan chuyên trách về các loại hình tấn công mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao, nguy cơ mất an ninh mạng, thông tin dữ liệu cá nhân.

5. Tiến hành rà soát, xây dựng, hoàn thiện các quy định, quy trình, quy chế, hướng dẫn về bảo vệ an ninh mạng; chủ động xây dựng, triển khai phương án phòng, chống tấn công mạng và ứng phó, khắc phục sự cố an ninh mạng theo quy định, thiết lập các kênh thông tin trao đổi, chia sẻ thông tin, thông báo sự cố an ninh mạng với các lực lượng chuyên trách bảo vệ an ninh mạng.

6. Quan tâm đầu tư, phân bổ kinh phí, bố trí nhân lực bảo vệ an ninh mạng; tăng cường quan tâm tới công tác bảo đảm an toàn, an ninh mạng trong hoạt động chuyển đổi số; ưu tiên sử dụng sản phẩm, thiết bị mạng được kiểm tra, đánh giá đảm bảo an ninh mạng.

---

[2] Tải về tại địa chỉ: https://bocongan.gov.vn/KND/TT/Lists/TinTuc/Attachments/38803/Hướng dẫn ANM các HTTT QTANQG scan (1).pdf

7. Các cơ quan, đơn vị có hoạt động thu thập, xử lý dữ liệu cá nhân tiến hành rà soát tổng thể, phân loại dữ liệu cá nhân đã thu thập, đang xử lý; xác định trách nhiệm bảo vệ tương ứng với từng loại dữ liệu cá nhân theo đúng quy định tại Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân.

8. Trong trường hợp phát hiện hoạt động tấn công mạng vào hệ thống thông tin, các cơ quan đơn vị trao đổi với Công an tỉnh, Sở Thông tin và Truyền thông để phối hợp, xử lý.

9. Giao Công an tỉnh, Sở Thông tin và Truyền thông theo chức năng nhiệm vụ hướng dẫn các cơ quan, đơn vị, địa phương triển khai thực hiện; báo cáo UBND tỉnh về kết quả thực hiện và đề xuất những vấn đề phát sinh vượt thẩm quyền.

Căn cứ nội dung Công văn, yêu cầu Thủ trưởng các cơ quan, đơn vị, địa phương nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Văn phòng Chính phủ;
- Bộ Công an; (b/c)
- TT. Tỉnh ủy;
- TT. HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Công an tỉnh;
- Văn phòng UBND tỉnh: V, C, CB;
- Lưu: VT, Th4.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

ỦY BAN NHÂN DÂN TỈNH AN GIANG CHÂU

Lê Văn Lương