UBND TỈNH BÌNH PHƯỚC
TIỂU BAN
AN TOÀN, AN NINH MẠNG

Số: 1552/TBATANM
V/v tăng cường công tác bảo đảm an ninh mạng

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

Bình Phước, ngày 26 tháng 4 năm 2024

Kính gửi:
- Các sở, ban, ngành, đoàn thể tỉnh;
- Các Ban xây dựng Đảng Tỉnh ủy;
- Các Huyện ủy, Thị ủy, Thành ủy;
- UBND các huyện, thị xã, thành phố;
- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh.

Theo Thông báo của Văn phòng Ban Chỉ đạo An toàn, An ninh mạng quốc gia, thời gian qua, tình hình an ninh mạng trong nước diễn ra hết sức phức tạp. Đặc biệt, trong bối cảnh nước ta đẩy mạnh thực hiện Đề án 06/CP của Chính phủ, các Bộ, ngành, địa phương và khối doanh nghiệp đang tập trung xây dựng nhiều hệ thống thông tin quan trọng, phức tạp, mang tính liên kết sâu rộng, lưu trữ khối lượng dữ liệu khổng lồ... dễ bộc lộ các điểm yếu có nguy cơ gây mất an ninh mạng, chỉ một cuộc tấn công nhỏ lẻ có thể lan rộng, xâm nhập toàn bộ hệ thống thông tin trọng yếu quốc gia.

Thực tế đã phát hiện các vụ tấn công mạng nhằm vào cơ quan đầu ngành của Đảng, Nhà nước, các địa phương có vị trí chiến lược về an ninh quốc phòng, doanh nghiệp, tập đoàn kinh tế "mũi nhọn". Nổi lên trong thời gian gần đây là hoạt động của các nhóm tin tặc tấn công vào các doanh nghiệp, tập đoàn nhà nước, khối tư nhân để chiếm đoạt thông tin dữ liệu, mã hóa dữ liệu, đòi tiền chuộc, gây ngưng trệ hoạt động, như một số vụ việc xảy ra tại các đơn vị thuộc ngành tài chính, ngân hàng, điện lực... đã tác động ảnh hưởng đến hoạt động điều hành của các cơ quan nhà nước, gây thiệt hại lớn về kinh tế.

Trên địa bàn tỉnh, qua công tác kiểm tra của Tiểu ban An toàn, An ninh mạng tỉnh nhận thấy công tác đảm bảo an ninh mạng hệ thống thông tin còn nhiều tồn tại, hạn chế như: nhiều hệ thống thông tin của các cơ quan Đảng, chính quyền chưa xây dựng phương án bảo vệ hệ thống thông tin và xác định cấp độ an toàn hệ thống thông tin theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; hệ thống thông tin của một số cơ quan Đảng, chính quyền tồn tại nhiều lỗ hổng bảo mật nghiêm trọng dễ bị tấn công, lây nhiễm mã độc nguy hiểm; việc sử dụng các tài khoản được cấp để khai thác các phần mềm, ứng dụng trong hoạt động công vụ còn chủ quan không thường xuyên thay đổi mật khẩu; còn tình trạng đồng bộ dữ liệu của cơ quan, đơn

vị với tài khoản Google Drive gây nguy cơ mất, lộ dữ liệu của cơ quan, đơn vị.

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 chưa 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; đầu tư về nguồn lực phục vụ công tác bảo đảm an ninh hệ thống mạng còn hạn chế, chưa đáp ứng yêu cầu... hệ thống mạng nội bộ và hệ thống máy tính của các cơ quan Đảng, chính quyền trên địa bàn tỉnh đa số sử dụng hệ điều hành cũ, hệ điều hành không có bản quyền nên tồn tại nhiều lỗ hổng bảo mật nguy hiểm; nhiều máy tính có cấu hình thấp không đáp ứng yêu cầu cài đặt các phần mền phòng, chống mã độc do Sở Thông tin và Truyền thông phối hợp vận hành, quản lý (Cyradar).

Để khắc phục khó khăn, hạn chế, tăng cường công tác phòng, chống tấn công mạng, bảo vệ dữ liệu; Tiểu ban An toàn, An ninh mạng tỉnh đề nghị các sở, ban, ngành, đoàn thể tỉnh; các Ban xây dựng Đảng Tỉnh ủy; các Huyện ủy, Thị ủy, Thành ủy; UBND các huyện, thị xã, thành phố; Văn phòng Tỉnh ủy; Văn phòng UBND tỉnh khẩn trương triển khai một số nội dung sau:

1. Quán triệt, thực hiện nghiêm Luật An ninh mạng năm 2018, 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, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân, Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; cụ thể hóa trách nhiệm của đơn vị, tổ chức, cá nhân trong công tác bảo vệ an ninh mạng hệ thống thông tin trọng yếu, bảo vệ dữ liệu cá nhân; tổ chức tuyên truyền, phổ biến trong toàn cơ quan, đơn vị nâng cao nhận thức, trách nhiệm của cán bộ, đảng viên, công chức, viên chức, người lao động 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; tiến hành rà soát, xây dựng, hoàn thiện các quy định, quy trình, quy chế bảo vệ an ninh mạng; đồng thời, thường xuyên tự kiểm tra, giám sát, đảm bảo việc chấp hành, thực hiện nghiêm túc trong toàn đơn vị; chủ động xây dựng, triển khai phương án, tổ chức diễn tập phòng, chống tấn công mạng và ứng phó, khắc phục sự cố an ninh mạng trên hệ thống thông tin của cơ quan, đơn vị mình. Nếu để xảy ra sai phạm, xem xét trách nhiệm của chủ quản hệ thống thông tin, cán bộ nhân viên chuyên trách và các cá nhân có liên quan theo quy định của pháp luật.

2. Tăng cường đầu tư về công nghệ, hệ thống kỹ thuật đảm bảo các quy chuẩn, tiêu chuẩn theo quy định, tránh tình trạng tập trung chuyển đổi số mà thiếu sự quan tâm tới công tác bảo đảm an toàn, an ninh mạng; ưu tiên sử dụng sản phẩm, thiết bị mạng đã được kiểm tra, đánh giá đảm bảo an ninh mạng; tập trung đầu tư, phân bổ kinh phí, bố trí nhân lực bảo vệ an ninh mạng.

3. Các 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; thực hiện việc đánh giá tác động và chuyển dữ liệu cá nhân ra nước ngoài... 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. Rà soát, đánh giá quy trình thu thập, xử lý dữ liệu cá nhân, đề xuất ban hành các biện pháp quản lý phù hợp với quy mô, mức độ xử lý dữ liệu cá nhân của cơ quan, đơn vị; nghiên cứu chỉ định bộ phận có chức năng bảo vệ dữ liệu cá nhân, nhân sự phụ trách xử lý dữ liệu cá nhân nhạy cảm (nếu có); đối với cơ quan nhà nước, các doanh nghiệp đang xử lý khối lượng lớn dữ liệu cá nhân, đặc biệt là dữ liệu cá nhân nhạy cảm thường xuyên kiểm tra, đánh giá đảm bảo an ninh trong hoạt động xử lý. Trong trường hợp phát hiện xảy ra vi phạm quy định bảo vệ dữ liệu cá nhân thông báo cho Công an tỉnh để phối hợp xử lý.

4. Công an tỉnh - Cơ quan thường trực Tiểu ban An toàn, An ninh mạng tỉnh thường xuyên tổ chức tập huấn, bồi dưỡng, nâng cao kiến thức, kỹ năng cho cán bộ, đảng viên, đội ngũ chuyên trách công nghệ thông tin, an ninh mạng tại các cơ quan, đơn vị đáp ứng năng lực, yêu cầu bảo vệ an ninh mạng và bí mật nhà nước trên không gian mạng; định kỳ, đột xuất kiểm tra, giám sát việc thực hiện các quy định về bảo vệ an ninh mạng, bảo vệ hệ thống thông tin trọng yếu, xử lý nghiêm theo quy định các vụ việc gây mất an ninh mạng, lộ, mất bí mật nhà nước, dữ liệu cá nhân trên không gian mạng.

5. Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh (do đồng chí Giám đốc Sở Thông tin và Truyền thông làm Đội trưởng): thường xuyên tổ chức diễn tập ứng cứu sự cố mạng, phòng, chống tấn công mạng; chủ trì phối hợp với Cơ quan thường trực của Tiểu ban An toàn, An ninh mạng tỉnh rà soát, xác định hệ thống thông tin trọng yếu của tỉnh để khẩn trương kết nối với hệ thống giám sát của Trung tâm An ninh mạng quốc gia đặt tại Bộ Công an để kịp thời phát hiện, cảnh báo, giám sát, khắc phục các sự cố, tình huống nguy cấp mất an ninh mạng; thiết lập các kênh thông tin trao đổi, chia sẻ thông tin, thông báo sự cố an ninh mạng với các lực lượng bảo vệ an ninh mạng tại các sở, ban, ngành, đoàn thể tỉnh.

Tiểu ban An toàn, An ninh mạng tỉnh thông báo để các cơ quan, tổ chức đơn vị, địa phương được biết, thực hiện./.

Nơi nhận:
- CT, các PCT UBND tỉnh;
- Như trên;
- LĐVP, các phòng, ban, trung tâm;
- Lưu: VT, TH49-CV.

TRƯỞNG TIỂU BAN

CHỦ TỊCH UBND TỈNH
Trần Tuệ Hiền