BAN CHỈ ĐẠO
AN TOÀN, AN NINH MẠNG QUỐC GIA
VĂN PHÒNG

Số: 31 /VP-BCĐ

V/v tăng cường công tác bảo đảm an ninh mạng hệ thống thông tin trọng yếu

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

Hà Nội, ngày 28 tháng 3 năm 2024

BỘ TƯ PHÁP
Đến ngày 01/4
Số 3973

Kính gửi:
- Các bộ, ngành, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Tiểu ban An toàn, An ninh mạng các tỉnh, thành phố trực thuộc Trung ương;
- Các tổ chức chính trị, xã hội ở Trung ương;
- Các tổ chức, doanh nghiệp nhà nước thuộc Trung ương.

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 của Chính phủ, các ban, 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.

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 khắc phục khó khăn, hạn chế, tăng cường công tác phòng, chống tấn công mạng, bảo vệ dữ liệu, Văn phòng Ban Chỉ đạo An toàn, An ninh mạng quốc gia đề nghị các bộ, ngành, cơ quan ngang bộ, cơ quan thuộc Chính phủ;

Tiểu ban An toàn, an ninh mạng các tỉnh, thành phố trực thuộc Trung ương; các tổ chức chính trị, xã hội ở Trung ương; các tổ chức, doanh nghiệp nhà nước thuộc Trung ương khẩn trương triển khai một số nội dung sau đây:

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... 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; 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.

2. Tổ chức tuyên truyền, phổ biến trong toàn hệ thống chính trị, các cơ quan, đơn vị 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.

3. Tiến hành rà soát, xây dựng, hoàn thiện các quy định, quy trình, quy chế, hướng dẫn về bảo vệ an ninh mạng, đồng thời thường xuyên kiểm tra, giám sát, đảm bảo việc chấp hành, thực hiện nghiêm túc trong toàn đơn vị. Chủ quản các hệ thống thông tin 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 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.

4. 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 được kiểm tra, đánh giá đảm bảo an ninh mạng. Chủ quản hệ thống thông tin trọng yếu 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.

5. Tập trung đầu tư, phân bổ kinh phí, bố trí nhân lực bảo vệ an ninh mạng; 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.

6. 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. Xử lý nghiêm các hành vi chuyển giao, mua bán dữ liệu cá nhân trái phép. Trong trường hợp phát hiện xảy ra vi phạm quy định bảo vệ dữ liệu cá nhân thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân - Bộ Công an để phối hợp xử lý.

7. 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.

Các vấn đề vướng mắc trong quá trình triển khai, đề nghị các đồng chí liên hệ, trao đổi về Trung tâm An ninh mạng quốc gia thuộc Bộ Công an *(cử đầu mối đồng chí Trung tá Lê Xuân Thủy - Giám đốc Trung tâm; SĐT: 0939.973.355)* để phối hợp, hướng dẫn kịp thời.

Văn phòng Ban Chỉ đạo An toàn, an ninh mạng quốc gia xin thông báo để các cơ quan, tổ chức được biết, thực hiện./.

Nơi nhận:
- Như trên;
- Đ/c Thủ tướng Chính phủ, Trưởng ban Chỉ đạo An toàn, an ninh mạng quốc gia
- Đ/c Bộ trưởng Tô Lâm, Phó Trưởng ban thường trực Ban Chỉ đạo An toàn, an ninh mạng quốc gia
- Đ/c Thứ trưởng Lương Tam Quang

(để báo cáo);

- Lưu: VPBCĐ(A05-P1).PQV.(280b).

CHÁNH VĂN PHÒNG

VĂN PHÒNG BAN CHỈ ĐẠO AN TOÀN, AN NINH MẠNG QUỐC GIA

Trung tướng Nguyễn Minh Chính
CỤC TRƯỞNG CỤC AN NINH MẠNG VÀ PCTP SỬ DỤNG CÔNG NGHỆ CAO