

Số: 5969 /UBND-NC

Khánh Hòa, ngày 04 tháng 6 năm 2024

Về việc tăng cường công tác bảo
đảm an ninh, an toàn các hệ
thống thông tin trọng yếu

Kính gửi:

- Công an tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Bộ Chỉ huy Bộ đội Biên phòng tỉnh;
- Các sở, ban, ngành;
- UBND các huyện, thị xã, thành phố;
- Các doanh nghiệp trên địa bàn tỉnh.

UBND tỉnh nhận Văn bản số 31/VP-BCĐ ngày 28/3/2024 của Văn phòng Ban Chỉ đạo An toàn, An ninh mạng quốc gia về việc tăng cường công tác bảo đảm an ninh mạng hệ thống thông tin trọng yếu và Thông báo số 2009/TB-A05-TTANMQG của Cục An ninh mạng và phòng chống tội phạm (PCTP) sử dụng công nghệ cao về việc hướng dẫn các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia; xét Tờ trình số 3189/TTr-CAT(ANM) ngày 22/5/2024 của Công an tỉnh, Chủ tịch UBND tỉnh – Trưởng Tiểu ban An toàn An ninh mạng tỉnh Khánh Hòa yêu cầu các cơ quan, đơn vị, địa phương trên địa bàn tỉnh tập trung chỉ đạo và thực hiện một số nội dung sau:

1. Quán triệt tinh thần chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 09/CT-TTg ngày 23/02/2024 về Tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ; trong đó xác định một số nội dung quan trọng:

- Việc bảo đảm an toàn hệ thống thông tin theo cấp độ là biện pháp trọng tâm, cốt lõi để bảo vệ hệ thống thông tin theo quy định tại Luật An toàn thông tin mạng;

- Nguyên nhân dẫn đến thực trạng tồn tại gần 40% các hệ thống thông tin quan trọng chưa hoàn thành việc phê duyệt cấp độ an toàn thông tin hệ thống mạng và chưa triển khai đầy đủ phương án bảo đảm an toàn theo hồ sơ đề xuất cấp độ đã được phê duyệt là do: ⁽¹⁾ Các cơ quan chủ quản hệ thống thông tin chưa thấy hết trách nhiệm, vai trò, tầm quan trọng của việc phê duyệt cấp độ an toàn thông tin và triển khai đầy đủ các biện pháp bảo đảm an toàn thông tin cho các hệ thống thông tin thuộc phạm vi quản lý; ⁽²⁾ Nhiều đơn vị, tổ chức được giao quản lý, vận hành hệ thống thông tin chưa nhận thức được tầm quan trọng của công tác này, dẫn đến chưa chú trọng thực hiện các nhiệm vụ một cách hiệu quả, chất lượng theo quy định của pháp luật; ⁽³⁾ Hoạt động thanh tra, kiểm tra, đánh giá tuân thủ



các quy định, giám sát việc thực hiện công tác bảo đảm an toàn thông tin theo cấp độ trong phạm vi quản lý tại các cơ quan, đơn vị, địa phương hầu như chưa được tổ chức để kịp thời nắm bắt tình hình, hướng dẫn triển khai và xử lý vi phạm; ⁽⁴⁾ Nguồn lực dành cho công tác bảo đảm an toàn thông tin nói chung, trong đó có công tác bảo đảm an toàn hệ thống thông tin theo cấp độ còn thiếu, chưa đáp ứng yêu cầu thực tiễn.

- Thời gian tới, phải bảo đảm việc tất cả các hệ thống thông tin quan trọng đang trong quá trình thiết kế, xây dựng, nâng cấp, mở rộng trước khi đưa vào vận hành, khai thác phải được phê duyệt cấp độ an toàn hệ thống thông tin và triển khai đầy đủ phương án bảo đảm an toàn thông tin theo hồ sơ đề xuất cấp độ được phê duyệt.

2. Nghiêm túc thực hiện Công điện số 33/CD-TTg ngày 07/4/2024 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn thông tin mạng, Văn bản số 31/VP-BCĐ ngày 28/3/2024 của Ban Chỉ đạo An toàn, An ninh mạng quốc gia, chỉ đạo của UBND tỉnh tại Văn bản số 3898/UBND-NC ngày 12/4/2024 và Văn bản số 3681/UBND-NC ngày 09/4/2024 về việc tăng cường thực hiện các biện pháp bảo đảm an toàn thông tin mạng trên địa bàn tỉnh, chú trọng thực hiện một số nội dung:

- 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 bí mật nhà nước, dữ liệu cá nhân trên không gian mạng; 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 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; rà soát, đánh giá quy trình thu thập, xử lý dữ liệu cá nhân; 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⁽¹⁾ phải thường xuyên kiểm tra, đánh giá việc đảm bảo an ninh, an toàn 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 – Công an tỉnh để phối hợp xử lý.

¹ Dữ liệu cá nhân nhạy cảm chia thành 4 mức: (1) Công khai; (2) Nội bộ: yêu cầu chỉ những người trong tổ chức mới có quyền truy cập; (3) Hạn chế: yêu cầu quyền truy cập, chỉ những người dùng được cấp quyền mới có thể truy cập vào dữ liệu. Việc tiết lộ tài sản thông tin bị hạn chế sẽ ảnh hưởng đến hoạt động của các đơn vị; (4) Bí mật nhà nước: thông tin có nội dung quan trọng, do cơ quan, tổ chức có thẩm quyền xác định; chưa công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc (thực hiện theo quy định của Luật Bảo vệ bí mật nhà nước).

3. Giao Sở Thông tin và Truyền thông chủ trì, phối hợp với Công an tỉnh rà soát, tổng hợp danh sách các cơ quan, đơn vị, sở, ban, ngành, địa phương thuộc diện chủ quản hệ thống thông tin quan trọng nhưng chưa tiến hành thực hiện quá trình đề xuất phê duyệt cấp độ; yêu cầu các đơn vị chủ quản hệ thống thông tin quan trọng tự nghiên cứu, đánh giá mức độ quan trọng của dữ liệu điện tử⁽²⁾ thuộc hệ thống thông tin đang quản lý vận hành; xây dựng hồ sơ đề xuất cấp độ trình UBND tỉnh thẩm định, phê duyệt đúng cấp độ (Tiêu chí xác định cấp độ an toàn hệ thống thông tin quy định tại Điều 7, 8, 9, 10, 11 Nghị định số 85/2016/NĐ-CP); có báo cáo giải trình nguyên nhân chưa thực hiện đúng quy định của Luật An toàn thông tin mạng và 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 (căn cứ Kế hoạch số 3386/KH-UBND-NC ngày 02/4/2024 về kiểm tra công tác chuyển đổi số năm 2024 của UBND tỉnh).

4. Thủ trưởng các sở, ban, ngành, địa phương và doanh nghiệp nhà nước nghiêm túc thực hiện chỉ đạo của UBND tỉnh tại Công văn số 4828/UBND-NC ngày 08/5/2024: chủ động phối hợp với Công an tỉnh nghiên cứu, thực hiện các biện pháp, yêu cầu về quản lý, quản trị, bảo vệ, phòng chống, sao lưu cần thiết để tăng cường bảo đảm an ninh mạng, nâng cao nhận thức, khả năng phòng thủ, ngăn chặn tấn công mạng cho hệ thống thông tin quan trọng trên địa bàn tỉnh; xây dựng kế hoạch và thực hiện việc tự kiểm tra, đánh giá về an ninh, an toàn thông tin đối với hệ thống thông tin đang quản lý vận hành, kịp thời có phương án, biện pháp khắc phục các điểm yếu, lỗ hổng bảo mật, phòng chống và ngăn chặn tấn công mạng. Đồng thời tạo thuận lợi cho công tác của lực lượng chuyên trách bảo vệ an ninh mạng như: giám sát bảo vệ, điều phối ứng phó sự cố, thẩm định, kiểm tra, đánh giá điều kiện bảo đảm an ninh mạng, nâng cao hiệu quả hoạt động bảo vệ hệ thống thông tin của cơ quan chủ quản. Kết quả thực hiện các nội dung trên, đề nghị Thủ trưởng các cơ quan, đơn vị báo cáo về UBND tỉnh (qua Công an tỉnh, địa chỉ: Số 80 Trần Phú, phường Lộc Thọ, thành phố Nha Trang, tỉnh Khánh Hòa) trước ngày 20/6/2024 để tổng hợp, báo cáo UBND tỉnh (Đầu mối liên hệ: Đ/c Trung tá Đinh Quang Hưng, Phó trưởng phòng Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao. Số điện thoại: 0905369669).

5. Giao Công an tỉnh – Cơ quan Thường trực Tiểu ban An toàn, An ninh mạng tỉnh nghiên cứu Thông báo số 2009/TB-A05-TTANMQG ngày 11/4/2024 của Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, vận dụng vào thực tế địa phương, ban hành hướng dẫn cụ thể các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng trên địa bàn tỉnh Khánh Hòa; đồng thời chủ trì theo dõi, đôn đốc các cơ quan, đơn vị, địa phương triển

² Dữ liệu trong hệ thống, được cơ quan, tổ chức xác định là quan trọng, cần được ưu tiên bảo vệ. Dữ liệu quan trọng bao gồm, nhưng không giới hạn các loại dữ liệu chứa các thông tin sau: thông tin nghiệp vụ, thông tin bí mật nhà nước, thông tin riêng và các loại thông tin quan trọng khác (nếu có); kể cả dữ liệu cá nhân nhạy cảm.

khai thực hiện các nội dung nêu trên. Trong quá trình thực hiện, phát sinh khó khăn, vướng mắc (nếu có), các sở, ban, ngành, cơ quan, đơn vị, doanh nghiệp trên địa bàn tỉnh, UBND dân các huyện, thị xã, thành phố chủ động phối hợp, báo cáo Công an tỉnh để được hướng dẫn triển khai thực hiện./.

Nơi nhận:

- Thủ tướng Chính phủ (báo cáo);
- Bộ Công an (báo cáo);
- Bộ Thông tin và Truyền thông (báo cáo);
- Văn phòng Chính phủ (báo cáo);
- Thường trực Tỉnh ủy (báo cáo);
- Thường trực HĐND tỉnh (báo cáo);
- Chủ tịch và các PCT UBND tỉnh;
- Lãnh đạo VP.UBND tỉnh;
- Lưu VT, NL, NgM. 10

CHỦ TỊCH



Nguyễn Tấn Tuân