ỦY BAN NHÂN DÂN **TỈNH KHÁNH HÒA**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 3898/UBND-NC V/v tăng cường thực hiện các biện pháp bảo đảm an toàn thông tin mạng trên địa bàn tỉnh	*Khánh Hòa, ngày 12 tháng 4 năm 2024*

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 Báo cáo số 2135/BC-CAT(ANM) ngày 09/4/2024 của Công an tỉnh về nguy cơ, thực trạng mất an toàn thông tin mạng trên địa bàn tỉnh kèm Tờ trình số 2136/TTr-CAT(ANM) về việc tham mưu UBND tỉnh chỉ đạo các sở, ban, ngành, địa phương và doanh nghiệp trên địa bàn tỉnh tăng cường thực hiện các biện pháp bảo đảm an ninh an toàn đối với hệ thống thông tin đang quản lý, vận hành. Chủ tịch UBND tỉnh – Trưởng Tiểu ban An toàn, An ninh mạng tỉnh Khánh Hòa chỉ đạo như sau:

1. Nghiêm túc quán triệt tinh thần chỉ đạo của Thủ tướng Chính phủ tại Công điện số 33/CĐ-TTg ngày 07/4/2024 yêu cầu các bộ, ngành, địa phương tăng cường bảo đảm an toàn thông tin mạng; thực hiện Chương trình hành động số 12678/CTHĐ-UBND ngày 21/12/2022 của UBND tỉnh Khánh Hòa triển khai thi hành Quyết định 964/QĐ-TTg ngày 10/8/2022 về việc phê duyệt Chiến lược An toàn An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030; trong đó chú trọng một số nội dung sau:

- Bảo vệ cơ sở hạ tầng trên không gian mạng của tỉnh, trọng tâm là các hệ thống thông tin quan trọng về an ninh quốc gia (nếu có) theo quy định của pháp luật về an ninh mạng. Bảo vệ hệ thống thông tin của 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (theo Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ).

- Các sở, ban, ngành, địa phương chủ động phối hợp với Công an tỉnh và Sở Thông tin và Truyền thông thực hiện các biện pháp bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước; rà soát, hướng dẫn các tổ chức, doanh nghiệp cung cấp dịch vụ trực tuyến và doanh nghiệp thuộc phạm vi quản lý nhà nước chú trọng việc bảo vệ an ninh, an toàn hệ thống mạng, tuân thủ đầy đủ quy định pháp luật về an toàn thông tin mạng, đặc biệt là quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Công an tỉnh chủ trì phối hợp với Sở Thông tin và Truyền thông xây dựng Kế hoạch kiểm tra, đánh giá an ninh, an toàn đối với các Hệ thống thông tin

đã được phê duyệt cấp độ trên địa bàn tỉnh trong Quý II năm 2024, tổng hợp kết quả báo cáo UBND tỉnh trong Quý III năm 2024; đồng thời triển khai các biện pháp nghiệp vụ tổ chức nắm tình hình liên quan đến các hoạt động tấn công mạng vào các hệ thống thông tin trên địa bàn phụ trách, đặc biệt là các hệ thống thông tin phục vụ Đề án 06/CP của Chính phủ.

2. Thủ trưởng các sở, ban, ngành, địa phương và doanh nghiệp chủ động rà soát toàn diện an ninh, an toàn hệ thống mạng, cụ thể:

- Chủ động tiếp nhận, nghiên cứu, quản lý tốt tài khoản quản trị hệ thống từ nhà cung cấp dịch vụ; thực hiện phân quyền đúng chức năng nhiệm vụ đối với các tài khoản người dùng được phép truy cập, khai thác, sử dụng dịch vụ đối với hệ thống, đặc biệt là đối với các hệ thống thông tin dùng chung của tỉnh (E-Office, Dịch vụ hành chính công trực tuyến). Tạm ngừng chính sách truy cập từ xa (VPN), thực hiện các thao tác quản trị hệ thống, truy cập các hệ thống nội bộ; trong trường hợp cần triển khai, phải tập trung rà soát, siết chặt chính sách kết nối truy cập; kích hoạt xác thực 2 lớp đối với kết nối VPN và đăng nhập tài khoản quản trị. Thực thi chính sách khóa tài khoản đăng nhập vào hệ thống sau một số lần đăng nhập thất bại.

- Kiểm tra dung lượng cho phép lưu trữ tối thiểu của thiết bị sao lưu dữ liệu (NAS, SAN); thường xuyên thực hiện việc sao lưu dữ liệu quan trọng (tối thiểu 01 tuần/lần). Chủ động đầu tư trang bị bản quyền phần mềm sao lưu dữ liệu và triển khai phương án dự phòng sự cố đối với dữ liệu sao lưu (thiết bị chứa dữ liệu lưu trữ phải tách biệt về vật lý đối với hệ thống mạng).

- Thường xuyên rà soát, kiểm tra, đóng lại các cổng dịch vụ (port) quan trọng kết nối internet (Well Known Port: 20-FTP data, 21-FTP control, 22-TPC/UDP-SSH Remote Login Protocol, 25-TPC/SMTP-Email, 66-TPC/Oracle SQLNET, 80-Website/ASP, 143-IMAP…); siết chặt chính sách truy cập trên các thiết bị bảo mật, bảo vệ mạng, chỉ cho phép kết nối đến các địa chỉ IP, cổng dịch vụ cần thiết. Chỉ mở tính năng SSH, Telnet (đăng nhập vào máy chủ từ xa) khi cần sử dụng.

- Kiểm tra lại thời hạn hiệu lực bản quyền đối với các tính năng bảo mật của thiết bị tường lửa, ứng dụng, hệ điều hành của máy chủ; kịp thời có kế hoạch gia hạn hoặc phương án bảo đảm an toàn có hiệu quả tương đương. Các tính năng bảo mật trên thiết bị tường lửa phải tương thích với kiến trúc mạng diện rộng, có chức năng định tuyến, kiểm soát, giám sát truy cập; căn cứ cấp độ hệ thống thông tin được phê duyệt để chủ động lựa chọn tính năng thiết bị, ứng dụng bảo mật phù hợp: phòng chống tấn công DDoS, IDS/IPS, Web/App Control, Web Threat Protection, Advanced Threat Protection. Máy chủ yêu cầu hệ điều hành bản quyền có phiên bản từ 2018 về sau.

- Thường xuyên theo dõi, 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 nguy cơ từ các hoạt động bất thường, kịp thời ngăn chặn hành vi tấn công mạng vào hệ thống. Tổ chức rà soát, xử lý thiết bị hệ thống mạng, dịch vụ mạng: Loại bỏ hoặc nâng cấp các máy vi tính, máy chủ đang sử dụng hệ điều

hành không còn được hãng hỗ trợ cập nhật bản vá bảo mật; ngắt kết nối, xử lý thanh loại các thiết bị, máy chủ, dịch vụ mạng và tài khoản trên các hệ thống thử nghiệm, hệ thống cũ hoặc không còn sử dụng.

- Xây dựng quy trình quản trị vận hành hệ thống và định kỳ kiểm tra việc thực hiện các quy trình; giám sát sự kiện an toàn thông tin mạng; ứng cứu, khắc phục sự cố; kiểm soát, giám sát chặt chẽ nhà thầu, bên thứ 3 trong quá trình hỗ trợ kỹ thuật, cài đặt hệ thống. Ban hành cơ chế, quy định cụ thể về số lượng, thời gian mở cổng dịch vụ internet, phân quyền truy cập, mật khẩu đăng nhập, người giám sát, ghi nhận kết quả trong quá trình thực hiện mở các cổng kết nối hệ thống ra internet để thực hiện các nhiệm vụ liên quan đến hoạt động của hệ thống.

- Có kế hoạch chủ động định kỳ tự rà quét lỗ hổng bảo mật đối với toàn hệ thống hoặc thuê dịch vụ rà quét độc lập nhằm phát hiện điểm yếu, chủ động nâng cấp, khắc phục, cập nhật phiên bản mới cho các ứng dụng bảo mật, đáp ứng các yêu cầu về bảo đảm an ninh, an toàn thông tin hệ thống. Chủ động nghiên cứu nắm vững hệ thống và xây dựng kịch bản ứng phó sự cố, không để bị động bất ngờ, giảm thiểu thời gian hệ thống bị gián đoạn, ngưng trệ.

3. Chủ động phối hợp với Công an tỉnh xây dựng kế hoạch và thực hiện 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.

** Kết quả thực hiện các nội dung trên, yêu cầu các cơ quan, đơn vị báo cáo về Công an tỉnh, địa chỉ: Số 80 Trần Phú, phường Lộc Thọ, thành phố Nha Trang, tỉnh Khánh Hòa) trước ngày **20/4/2024** để tổng hợp, báo cáo UBND tỉnh. (Đầu mối liên hệ: Đồng chí 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: 0905.369.669).*

4. Giao Công an tỉnh – Cơ quan Thường trực Tiểu ban An toàn, An ninh mạng tỉnh chủ trì theo dõi, đôn đốc các cơ quan, đơn vị, địa phương triển 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 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

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lê Hữu Hoàng