UBND TỈNH KHÁNH HÒA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 133 /STTTT-CNTTBCVT

V/v tăng cường công tác bảo đảm an toàn thông tin mạng dịp Tết Nguyên đán Ất Tỵ và Lễ kỷ niệm 95 năm thành lập Đảng Cộng sản Việt Nam

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

Khánh Hòa, ngày 15 tháng 01 năm 2025

Kính gửi:
- Các cơ quan Đảng, Mặt trận, Đoàn thể tỉnh;
- Các Sở, ban, ngành;
- UBND các huyện, thị xã, thành phố;
- Các đơn vị sự nghiệp trực thuộc UBND tỉnh;
- Các cơ quan ngành dọc Trung ương;
- Các doanh nghiệp viễn thông – công nghệ thông tin.

Căn cứ Chỉ thị số 45/CT-TTg ngày 18/12/2024 của Thủ tướng Chính phủ về việc tăng cường các biện pháp bảo đảm đón Tết Nguyên đán Ất Tỵ năm 2025 vui tươi, lành mạnh, an toàn, tiết kiệm;

Thực hiện Công văn số 5644/BTTTT-CATTT ngày 29/12/2024 của Bộ Thông tin và Truyền thông về việc tăng cường công tác bảo đảm an toàn thông tin mạng hướng tới dịp Tết Dương lịch 2025, Tết Nguyên đán Ất Tỵ và Lễ kỷ niệm 95 năm thành lập Đảng Cộng sản Việt Nam; Công văn số 14910/UBND-TH ngày 26/12/2024 của UBND tỉnh về việc triển khai các Chỉ thị của Ban Bí thư, Thủ tướng Chính phủ và Ban Thường vụ Tỉnh ủy về việc tổ chức Tết Ất Tỵ năm 2025;

Nhằm đảm bảo an toàn thông tin mạng trong thời gian hướng đến những sự kiện lớn của đất nước như Tết Nguyên đán Ất Tỵ, Lễ kỷ niệm 95 năm ngày thành lập Đảng Cộng sản Việt Nam (03/02/1930 – 03/02/2025), Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương thực hiện các nội dung sau:

1. Tăng cường triển khai hoạt động bảo đảm an toàn thông tin mạng cho hệ thống thông tin thuộc thẩm quyền quản lý

- Rà soát các hệ thống thông tin, bảo đảm các hệ thống thông tin được triển khai đầy đủ các biện pháp bảo vệ theo cấp độ an toàn. Thực hiện cấu hình tăng cường bảo mật cho hệ thống thông tin thuộc quyền quản lý và khắc phục triệt để các lỗ hổng, điểm yếu đã được cảnh báo an toàn thông tin mạng của Cục An toàn thông tin công bố tại địa chỉ: *https://khonggianmang.vn/canhbaoattt*, Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRlab.vn) và từ các cơ quan, tổ chức liên quan cung cấp;

- Tăng cường công tác giám sát an toàn thông tin mạng, rà soát, xử lý mã độc, bảo đảm an toàn thông tin mạng 24/7. Xây dựng các kế hoạch, phương án ứng cứu khẩn cấp, phân công nhân sự theo dõi thường xuyên, liên tục để đảm bảo phát hiện sớm các nguy cơ tấn công mạng *(đặc biệt là tấn công mã hóa dữ liệu, thay đổi giao diện)* để kịp thời xử lý, khắc phục nhanh sự cố tấn công mạng;

- Rà soát, kiểm tra và bóc gỡ các phần mềm độc hại cho toàn bộ máy chủ, máy trạm trong hệ thống mạng. Trong đó, cần ưu tiên các hệ thống thông tin có địa chỉ IP nằm trong Danh sách IP mạng Botnet được các cơ quan chức năng cảnh báo hàng tháng hoặc đột xuất;

- Tăng cường tuyên truyền, nâng cao nhận thức kỹ năng cơ bản về an toàn thông tin mạng; nhận biết, cảnh giác trước thông tin xấu độc, tin giả, thông tin xuyên tạc, chống phá chính sách của Đảng và Nhà nước; phòng, chống lừa đảo trên không gian mạng cho cán bộ, công chức, viên chức, người lao động của cơ quan và người dân trên địa bàn quản lý. Khẩn trương thông báo nội dung văn bản này đến tất cả các cơ quan, đơn vị trực thuộc mình để tổ chức triển khai thực hiện.

2. Đối với các doanh nghiệp cung cấp dịch vụ viễn thông, internet và các tổ chức, doanh nghiệp cung cấp nền tảng chuyển đổi số

- Bố trí nguồn lực thực hiện trực giám sát, hỗ trợ và khắc phục sự cố bảo đảm hạ tầng viễn thông, internet an toàn, thông suốt;

- Triển khai các biện pháp kỹ thuật ở mức cao nhất nhằm phát hiện, chặn lọc, ngăn chặn hoạt động tấn công mạng, phát tán thông tin xấu độc, thông tin vi phạm pháp luật trên hệ thống thông tin, hạ tầng mạng lưới thuộc phạm vi quản lý;

- Tăng cường theo dõi, cập nhật, xử lý các phản ánh, khiếu nại của người dùng về tin nhắn rác, cuộc gọi rác, đặc biệt là tin nhắn lừa đảo, cuộc gọi lừa đảo qua hệ thống tiếp nhận phản ánh tin nhắn rác, cuộc gọi rác do Bộ Thông tin và Truyền thông (Cục An toàn thông tin) chia sẻ; xử lý quyết liệt, triệt để các trường hợp phát tán tin nhắn rác, tin nhắn lừa đảo, cuộc gọi rác, cuộc gọi lừa đảo mà người dùng phản ánh;

- Thực hiện nghiêm và kịp thời các biện pháp xử lý theo yêu cầu của Bộ Thông tin và Truyền thông, Sở Thông tin và Truyền thông và cơ quan chức năng có thẩm quyền.

3. Trường hợp cần hỗ trợ giám sát, xử lý, ứng cứu sự cố đề nghị liên hệ với Cục An toàn thông tin (Bộ Thông tin và Truyền), Sở Thông tin và Truyền thông thông qua đầu mối

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), điện thoại 024.3640.4421 hoặc số điện thoại trực đường dây nóng ứng cứu sự cố 086.9100.317, thư điện tử: ir@vncert.vn;

- Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 024.32091.616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 038.9942.878, thư điện tử: ais@mic.gov.vn;

- Phòng An toàn hệ thống thông tin, số điện thoại trực đường dây nóng hỗ trợ tổng thể các giải pháp an toàn thông tin 0888.133.359, thư điện tử: athttt@mic.gov.vn;

- Đầu mối quản lý, vận hành Trung tâm dữ liệu tỉnh Khánh Hòa: Ông Phan Quang Vinh – Phó Trưởng phòng Hệ thống thông tin, Trung tâm Công nghệ thông tin và Dịch vụ hành chính công trực tuyến tỉnh Khánh Hòa, điện thoại (0258.3899.888 – Di động: 079.4687442);

- Đầu mối tiếp nhận thông báo và phối hợp xử lý sự cố của Sở Thông tin và truyền thông: Bà Võ Thị Chương Nguyệt (0258.3563.533 – Di động: 0935883380).

Sở Thông tin và Truyền thông thông báo và đề nghị Quý cơ quan, đơn vị, địa phương quan tâm thực hiện.

Trân trọng./.

Nơi nhận:
- Như trên(VBĐT);
- Cục ATTT (VBĐT, để b/c);
- UBND tỉnh (VBĐT, để b/c);
- Lưu: VT, CNTTBCVT (BN).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Văn Hiền