BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

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

Số: 2705/CAT-TM(ANM)

Quảng Ngãi, ngày 09 tháng 10 năm 2025

V/v bảo đảm an ninh mạng, an toàn thông tin cho Cổng thông tin điện tử phục vụ Đại hội XIV của Đảng

Kính gửi:
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Văn phòng Tỉnh ủy, Văn phòng UBND tỉnh;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Các sở, ban, ngành, đoàn thể tỉnh;
- Bộ Chỉ huy Quân sự tỉnh; Tòa án nhân dân tỉnh;
- Viện kiểm sát nhân dân tỉnh; Thi hành án dân sự tỉnh;
- Bảo hiểm xã hội tỉnh; Cảng vụ Hàng hải Quảng Ngãi;
- Thống kê tỉnh; Thuế tỉnh Quảng Ngãi;
- Kho bạc Nhà nước khu vực XV;
- Báo và Phát thanh, Truyền hình Quảng Ngãi;
- Các Trường: Đại học Phạm Văn Đồng, Cao đẳng Kon Tum, Cao đẳng Việt Nam - Hàn Quốc - Quảng Ngãi;
- Viettel Quảng Ngãi, VNPT Quảng Ngãi, Mobifone Quảng Ngãi, FPT Quảng Ngãi, SCTV Quảng Ngãi;
- UBND xã, phường, đặc khu Lý Sơn.

Nhằm bảo đảm an ninh mạng, an toàn thông tin cho Cổng thông tin điện tử (TTĐT) phục vụ Đại hội XIV của Đảng, Công an tỉnh Quảng Ngãi đề nghị Thủ trưởng các cơ quan, đơn vị, địa phương trên địa bàn tỉnh chỉ đạo thực hiện các nội dung trọng tâm sau:

1. Tăng cường triển khai hoạt động bảo đảm an ninh mạng, an toàn thông tin

- Rà soát các hệ thống thông tin bảo đảm được triển khai đầy đủ biện pháp bảo vệ theo cấp độ an toàn thông tin, chính sách an ninh đối với hệ thống tường lửa, hệ thống phát hiện xâm nhập, hệ thống phòng chống mã độc; cập nhật đầy đủ bản vá bảo mật cho hệ điều hành, ứng dụng, máy chủ, thiết bị mạng.

- Chủ động kiểm tra, đánh giá, phát hiện và khắc phục lỗ hổng bảo mật; kịp thời phát hiện mối nguy hại và bóc gỡ phần mềm độc hại cho toàn bộ máy chủ, máy trạm trong hệ thống thông tin; cài đặt phần mềm phòng, chống mã độc, bản quyền cho toàn bộ máy chủ, máy trạm người dùng.

- Thiết lập chính sách bảo mật, chính sách kiểm soát truy cập chặt chẽ trong hệ thống; thực hiện phân cấp, phân quyền tài khoản người dùng theo đúng chức năng, nhiệm vụ, đảm bảo quyền tối thiểu và lưu nhật ký sử dụng tài khoản.

- Thiết lập giao thức mạng bảo mật có mã hóa mạnh, xác thực để quản lý, cấu hình máy chủ, ứng dụng từ xa; giới hạn quản trị thiết bị từ một số địa chỉ IP

quản trị trong hệ thống; rà soát, kiểm tra và ngăn chặn các địa chỉ IP nằm trong danh sách IP mạng Botnet được các đơn vị chức năng cảnh báo.

- Lưu nhật ký truy cập và nhật ký thu được từ các thiết bị mạng, bảo mật trong khoảng thời gian tối thiểu bằng thời gian diễn ra Đại hội XIV của Đảng từ khi đưa hệ thống thông tin vào hoạt động.

- Triển khai biện pháp giám sát an ninh mạng, an toàn thông tin và ứng cứu, khắc phục khi có sự cố phát sinh đối với hệ thống thông tin[1].

- Tổ chức tuyên truyền, nâng cao nhận thức cơ bản kỹ năng về an ninh mạng, an toàn thông tin, cảnh giác về thông tin xấu độc, tin giả và thông tin lừa đảo trên không gian mạng cho cán bộ, công chức, viên chức, người lao động và quần chúng nhân dân[2].

2. Đơn vị chủ quản, vận hành Cổng/Trang TTĐT: Khảo sát, đánh giá thực trạng Cổng/Trang TTĐT thuộc phạm vi quản lý, triển khai đầy đủ giải pháp bảo đảm an ninh mạng, an toàn thông tin[3]; kiện toàn đội ngũ ban biên tập, quy chế hoạt động của Cổng/Trang TTĐT; bảo đảm nội dung thông tin, bài viết, video… được kiểm duyệt trước khi đăng tải đúng quy định. Tổ chức rà soát, thống kê và cung cấp thông tin đầu mối quản trị viên các Cổng/Trang TTĐT (kể cả trang mạng xã hội)[4] cho Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)* ***trước ngày 30/10/2025*** để kịp thời phối hợp, xử lý khi xảy ra sự cố mất an ninh mạng, an toàn thông tin.

3. Viettel Quảng Ngãi, VNPT Quảng Ngãi - đơn vị cung cấp dịch vụ Giám sát an toàn, an ninh mạng tập trung (SOC) tỉnh Quảng Ngãi: Tiếp tục củng cố và ưu tiên nguồn lực cho nhiệm vụ giám sát và bảo vệ các Hệ thống thông

---

[1] Như: (1) Giám sát tình trạng hoạt động các thiết bị trong hệ thống; (2) Giám sát phát hiện tấn công từ chối dịch vụ (DoS/DDoS); (3) Giám sát các kết nối bất thường trong hệ thống, kịp thời phát hiện mã độc trong hệ thống mạng (nếu có); (4) Giám sát phát hiện tấn công rà quét dịch vụ được sử dụng ngay bên trong hệ thống; (5) Giám sát phát hiện tấn công khai thác lỗ hổng bảo mật có liên quan đến thiết bị, ứng dụng mà hệ thống đang được sử dụng ngoài Internet.

[2] Như: (1) Nâng cao nhận thức về công tác bảo đảm an ninh mạng, an toàn thông tin mạng; (2) Nêu cao tinh thần đấu tranh, phản bác, lên án quan điểm sai trái, thông tin xấu độc, lan tỏa, phủ xanh thông tin tích cực; (3) Thường xuyên cập nhật, bổ sung kiến thức về an ninh mạng, an toàn thông tin: Thay đổi mật khẩu tài khoản thư điện tử công vụ, đảm bảo mật khẩu đủ mạnh (có ít nhất 8 ký tự và bao gồm: chữ hoa, chữ thường, ký tự đặc biệt và chữ số), không lưu giữ mật khẩu trên trình duyệt web; tuyệt đối không sử dụng Thư điện tử công vụ của tỉnh để đăng ký vào các mạng xã hội, diễn đàn và các trang thông tin công cộng khác; không chia sẻ, phát tán thông tin xấu độc, chưa được kiểm chứng, không nhấn vào đường dẫn liên kết lạ, không rõ nguồn gốc qua các ứng dụng trò chuyện trên mạng xã hội, thư điện tử, tin nhắn SMS...

[3] Trọng tâm:

- Bảo đảm mô hình mạng được thiết kế phân chia thành các phân vùng mạng (Vùng mạng trung lập, Vùng mạng ứng dụng, Vùng mạng cơ sở dữ liệu, Vùng mạng quản trị...) riêng biệt, tách biệt về mặt logic hoặc vật lý theo đúng chức năng;

- Việc truy cập giữa các vùng mạng phải được kiểm soát bởi thiết bị tường lửa có tính năng phát hiện, phòng chống tấn công xâm nhập giữa các vùng mạng (IPS/IDS), tính năng phòng chống mã độc lớp mạng;

- Có các phương án: (1) Quản lý truy cập, quản trị hệ thống từ xa an toàn; (2) Cân bằng tải, dự phòng nóng cho các thiết bị mạng chính; (3) Phòng chống tấn công từ chối dịch vụ; (4) Giải pháp tường lửa ứng dụng web (WAF); (5) Giám sát hệ thống thông tin tập trung; phương án giám sát an toàn thông tin tập trung; (6) Quản lý sao lưu dự phòng tập trung sử dụng; (7) Quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính quản trị viên, biên tập viên, sử dụng giải pháp có chức năng quản lý tập trung; (8) Giải pháp đảm bảo an toàn thông tin cho hệ thống thư điện tử (nếu có); (9) Phòng, chống thất thoát dữ liệu; (10) Dự phòng kết nối mạng Internet cho các máy chủ dịch vụ.

[4] Nội dung danh sách thống kê gồm: Tên Cổng/Trang TTĐT (kể cả trang mạng xã hội); đường dẫn truy cập; quản trị viên (Họ và tên; chức vụ/đơn vị công tác; số điện thoại).

tin cấp độ 3 trên địa bàn tỉnh; triển khai giải pháp kỹ thuật rà quét, cảnh báo, xử lý mã độc đối với các dữ liệu và ưu tiên nguồn lực đảm bảo an toàn thông tin đối với hệ thống thông tin dùng chung của tỉnh.

4. Thành viên Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi: Chủ động rà soát, theo dõi hệ thống mạng của cơ quan, đơn vị; kịp thời hỗ trợ công tác đảm bảo an toàn thông tin, an ninh mạng cho các cơ quan Đảng, Nhà nước trên địa bàn tỉnh khi cần thiết và khi có yêu cầu của Cơ quan thường trực Đội ứng cứu (Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao - Công an tỉnh).

5. Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao - Công an tỉnh: Phối hợp với Trung tâm chuyển đổi số và đổi mới sáng tạo, Sở Khoa học và Công nghệ; Trung tâm Công báo - Tin học; Văn phòng UBND tỉnh quản trị, vận hành các Trung tâm dữ liệu của tỉnh, tăng cường công tác bảo đảm an ninh mạng, an toàn thông tin hệ thống thông tin dùng chung của tỉnh và phân công cán bộ kỹ thuật trực, quản trị hệ thống đảm bảo 24/7 để kịp thời phối hợp và xử lý sự cố liên quan; thực hiện kế hoạch ứng phó sự cố an toàn thông tin mạng, phương án ứng cứu khi có sự cố xảy ra trên địa bàn tỉnh.

6. Công an các đơn vị, địa phương - Công an tỉnh: Triển khai biện pháp nghiệp vụ nắm tình hình trên không gian mạng liên quan hoạt động của Cổng TTĐT phục vụ Đại hội XIV của Đảng trên địa bàn, lĩnh vực phụ trách.

7. Khi xảy ra sự cố về an toàn thông tin, an ninh mạng, các đơn vị, địa phương khẩn trương thông báo về Công an tỉnh *(qua Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao)* để hỗ trợ, phối hợp xử lý và tổng hợp, báo cáo UBND tỉnh, Bộ Công an. Trường hợp cần hỗ trợ xử lý, ứng cứu và khắc phục sự cố đề nghị liên hệ đầu mối kỹ thuật sau:

- Đồng chí Thượng tá Võ Văn Hoan - Phó Trưởng Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; Điện thoại: 0980.331.268.

- Đồng chí Đại úy Phạm Nhật Trí - Cán bộ, Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; Điện thoại: 0966.833.937.

- Đồng chí Thượng úy Hoàng Gia Bảo - Cán bộ, Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; Điện thoại: 0964.634.357.

Đề nghị các cơ quan, đơn vị, địa phương quan tâm triển khai thực hiện./.

Nơi nhận:
- Như trên (t/hiện);
- Cục ANM & PCTP sử dụng CNC (b/cáo) - BCA;
- Lãnh đạo Công an tỉnh;
- Công an các đơn vị, địa phương (t/hiện);
- Lưu: VT, TM(AN), ANM.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH QUẢNG NGÃI

Đại tá Hồ Song Ân