ỦY BAN NHÂN DÂN TỈNH THANH HOÁ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 805 /UBND-CNTT V/v tăng cường công tác bảo đảm an toàn thông tin mạng trong dịp Tết Nguyên đán Giáp Thìn 2024	*Thanh Hoá, ngày* 16 *tháng* 01 *năm 2024*

Kính gửi:
- Các sở, ban, ngành, đơn vị cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Báo Thanh Hóa, Đài PTTH Thanh Hóa;
- Các doanh nghiệp viễn thông.

Ngày 13/01/2024, UBND tỉnh nhận được Công văn số 6410/BTTTT-CATTT (đề ngày 29/12/2023) của Bộ Thông tin và Truyền thông về việc tăng cường công tác bảo đảm an toàn thông tin mạng trong dịp Tết Dương lịch 2024 và Tết Nguyên đán Giáp Thìn.

Để nâng cao cảnh giác và trách nhiệm bảo đảm an toàn thông tin mạng theo quy định của pháp luật trong thời gian diễn ra dịp nghỉ lễ Tết Nguyên đán Giáp Thìn 2024, Chủ tịch UBND tỉnh yêu cầu các sở, ban, ngành, đơn vị cấp tỉnh; UBND các huyện, thị xã, thành phố; Báo Thanh Hóa, Đài Phát thanh và Truyền hình tỉnh, các doanh nghiệp viễn thông tăng cường triển khai một số biện pháp như sau:

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

a) 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 được phê duyệt.

b) Phân công lực lượng tại chỗ triển khai trực giám sát, bảo đảm an toàn thông tin mạng 24/7 và gửi đầu mối tiếp nhận sự cố về Sở Thông tin và Truyền thông trước ngày **25/01/2024**.

c) 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 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.

d) Chủ động rà soát các lỗ hổng, điểm yếu trên các hệ thống thông tin thuộc phạm vi quản lý và triển khai các giải pháp phòng ngừa và khắc phục triệt để các lỗ hổng, điểm yếu đã được cảnh báo, đặc biệt như: lỗ hổng ảnh hưởng nghiêm trọng trong F5 BIG-IP, lỗ hổng zeroday trong hệ thống Zimba và các lỗ hổng bảo mật ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm Microsoft từ tháng 5 đến tháng 11 năm 2023.

đ) Tổ chức tuyên truyền, nâng cao nhận thức cơ bản kỹ năng về an toàn thông tin mạng, cảnh giác về thông tin xấu độc, tin giả và thông tin lừa đảo trên không gian mạng cho cán bộ thuộc cơ quan.

e) Triển khai công tác bảo đảm an toàn thông tin mạng nêu trên đến các đơn vị trực thuộc, UBND cấp xã để thực hiện đồng bộ, toàn diện trên địa bàn tỉnh.

g) Trong trường hợp cần hỗ trợ giám sát, xử lý, ứng cứu sự cố đề nghị liên hệ với Trung tâm CNTT và Truyền thông tỉnh (cơ quan thường trực Đội ứng cứu sự cố an toàn thông tin mạng tỉnh) thông qua số điện thoại: 02373.718.699, đường dây nóng: 0916.422.583 (đồng chí Trần Ngọc Hưng, Phó Giám đốc Trung tâm) Email: ungcuusuco@thanhhoa.gov.vn.

2. Các doanh nghiệp cung cấp dịch vụ viễn thông, internet; các tổ chức, doanh nghiệp cung cấp nền tảng chuyển đổi số:

a) Bảo đảm bố trí đầy đủ nguồn nhân lực để trực giám sát, hỗ trợ và khắc phục sự cố bảo đảm hạ tầng viễn thông, internet an toàn, thông suốt.

b) Triển khai đầy đủ các biện pháp bảo vệ, bảo đảm phát hiện và ngăn chặn kịp thời 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.

c) Thực hiện nghiêm và kịp thời các biện pháp xử lý theo yêu cầu của Cục An toàn thông tin và cơ quan chức năng có thẩm quyền.

3. Giao Sở Thông tin và Truyền thông:

a) Tăng cường nguồn nhân lực, chủ động theo dõi thường xuyên, liên tục các hệ thống giám sát an toàn thông tin tập trung, hệ thống phòng, chống mã độc tập trung đảm bảo xử lý, khắc phục kịp thời tấn công mạng, cảnh báo mã độc được xác minh.

b) Bảo đảm duy trì kết nối liên tục tới hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia để được hỗ trợ giám sát, phát hiện và cảnh báo sớm, xử lý; kịp thời chia sẻ thông tin với Cục An toàn thông tin khi phát hiện dấu hiệu tấn công mạng vào hệ thống thông tin.

c) Phối hợp với Cục An toàn thông tin và đơn vị liên quan triển khai Sử dụng và khai thác hiệu quả Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRLab) và Nền tảng Hỗ trợ điều tra số (DFLab) trong công tác điều phối và xử lý sự cố tấn công mạng.

d) Trong trường hợp cần hỗ trợ giám sát, xử lý, ứng cứu sự cố đề nghị liên hệ với Cục An toàn thông tin, thông qua các đầu mối theo Công văn số 6410/BTTTT-CATTT của Bộ Thông tin và Truyền thông./.

Nơi nhận:
- Như trên;
- Bộ Thông tin và Truyền thông (để báo cáo);
- Chủ tịch, các PCT UBND tỉnh (để báo cáo);
- CVP, các PCVP UBND tỉnh;
- Trung tâm Phục vụ HCC (để t/h);
- Lưu: VT, CNTT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Mai Xuân Liêm