ỦY BAN NHÂN DÂN **THỊ XÃ THÁI HÒA**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 39 /UBND-VH V/v tăng cường công tác bảo đảm ATTT mạng trong thời gian Tết Nguyên Đán Giáp Thìn 2024	*Thái Hòa, ngày 10 tháng 01 năm 2024*

Kính gửi:
- Các cơ quan, đơn vị trên địa bàn thị xã;
- Các phòng, ban, ngành, đoàn thể, tổ chức chính trị xã hội thị xã;
- Các doanh nghiệp hoạt động trong lĩnh vực TT&TT;
- UBND các xã, phường.

Thực hiện Công văn số 07/STTTT-CĐS ngày 02/01/2024 của Sở Thông tin và Truyền thông về việc tăng cường công tác bảo đảm ATTT mạng trong thời gian Tết Nguyên Đán Giáp Thìn 2024.

Theo thông tin từ Sở Thông tin và Truyền thông, sự cố mất an toàn thông tin mạng nghiêm trọng tại Việt Nam thường được ghi nhận tại thời điểm diễn ra dịp nghỉ lễ của đất nước, các đối tượng thường tăng cường tấn công mạng vào các hệ thống thông tin quan trọng hoặc lợi dụng không gian mạng để phát tán thông tin xấu độc, lừa đảo trong các dịp này.

Nhằm 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, UBND thị xã yêu cầu các cơ quan, đơn vị, UBND các xã phường thực hiện một số nhiệm vụ sau:

1. Các cơ quan, đơn vị trên địa bàn; Các phòng, ban, ngành, tổ chức chính trị xã hội thị xã; UBND các xã, phường:

- 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.

- Phân công lực lượng tại chỗ triển khai trực giám sát 24/7; 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.

- 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 Cụ An toàn thông tin, Sở Thông tin và Truyền thông cảnh báo hàng tháng hoặc đột xuất.

- 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 Cục An toàn thông tin, Sở Thông tin và Truyền thông cảnh báo, đặc biệt như: lỗ hổng ảnh hưởng nghiêm trọng trong F5 BIG-IP (văn bản số 1943/CATTT-NCSC ngày 01/11/2023 của Cục An toàn thông tin), lỗ hổng zeroday trong hệ thống Zimba (văn bản số 2216/CATTT-NCSC ngày 12/12/2023 của Cục An toàn thông tin) 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 (văn bản gửi kèm theo).

- 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, Sở Thông tin và Truyền thông, UBND thị xã Thái Hòa khi phát hiện dấu hiệu tấn công mạng vào hệ thống thông tin.

- 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.

2. Giao Cổng TTĐT thị xã, Trang Thông tin điện tử các xã, phường

- Đăng tải toàn văn nội dung công văn số 6410/BTTTT-CATTT 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 Tế Dương lịch 2024 và tết Nguyên đán Giáp Thìn lên Cổng/Trang TTĐT đơn vị.

- Tổ chức kiểm tra, rà soát, kịp thời có phương án xử lý đối với hệ thống Cổng/Trang TTĐT của đơn vị.

- Bố trí cá bộ kỹ thuật thường xuyên theo dõi hệ thống, hỗ trợ người sử dụng khi cho nhu cầu.

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

- 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.

- 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.

- Tuân thủ các quy định pháp lý hiện hành và các điều khoản thuộc hợp đồng thuê dịch vụ có liên quan đến công tác an toàn thông tin để đảm bảo hoạt động ổn định, an toàn các hệ thống thông tin đang cung cấp dịch vụ cho thị xã.

Khi gặp sự cố hoặc có vấn đề phát sinh, cần hỗ trợ xử lý, đề nghị liên hệ ngay với Bộ Thông tin và Truyền thông (Cục An toàn thông tin), Sở Thông tin và Truyền thông Nghệ An qua các đầu mối sau:

- 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: 02432091616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 0389942878, thư điện tử ais@mic.gov.vn

- Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Nghệ An: điện thoại: 02383.500027.

Yêu cầu các cơ quan, đơn vị, tổ chức và UBND các xã, phường nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Sở Thông tin và Truyền thông; (báo cáo)
- Chủ tịch UBND thị xã; (báo cáo)
- Cổng TTĐT thị xã;
- Lưu: VT, VH.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Đinh Thế Vinh