BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số:6410 /BTTTT-CATTT V/v tăng cường công tác bảo đảm an toàn thông tin mạng trong dịp Tết Dương lịch 2024 và Tết Nguyên đán Giáp Thìn	*Hà Nội, ngày 29 tháng 12 năm 2023*

Kính gửi:

- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Các Cơ quan báo chí Trung ương;
- Các Tập đoàn kinh tế, Tổng công ty nhà nước;
- Các Tập đoàn, Tổng Công ty, Công ty cung cấp dịch vụ Internet, viễn thông;
- Các Tổ chức tài chính, Ngân hàng thương mại.

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. Qua công tác theo dõi, giám sát, Bộ Thông tin và Truyền thông thấy rằng 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 Dương lịch 2024 và Tết Nguyên đán Giáp Thìn, Bộ Thông tin và Truyền thông trân trọng đề nghị các cơ quan, tổ chức, doanh nghiệp 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.

b) 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.

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 Cục An toàn thông tin 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 Cục An toàn thông tin, Bộ 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).

đ) 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.

e) 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 bảo sớm, xử lý; kịp thời chia sẻ thông tin với Cục An toàn thông tin, Bộ Thông tin và Truyền thông khi phát hiện dấu hiệu tấn công mạng vào hệ thống thông tin.

g) 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. 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 Bộ Thông tin và Truyền thông (Cục An toàn thông tin) và cơ quan chức năng có thẩm quyền.

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

Trân trọng./.

Nơi nhận:
- Như trên;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Chủ tịch nước;
- Văn phòng Quốc hội và các Ủy ban của Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các đoàn thể;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Các đơn vị chuyên trách về công nghệ thông tin, an toàn thông tin tại các bộ, ngành;
- Các Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc TW;
- Thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Các Trung tâm: VNNIC, Trung tâm Thông tin;
- Lưu: VT, CATTT.PTA.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng