BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 4448/BTTTT-CATTT V/v tăng cường công tác bảo đảm an toàn thông tin mạng trong thời gian nghỉ lễ Quốc khánh 02/9	*Hà Nội, ngày 28 tháng 8 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.

Thời gian diễn ra lễ Kỷ niệm 78 năm Quốc khánh nước Cộng hòa xã hội chủ nghĩa Việt Nam (02/9/1945-02/9/2023) là thời điểm các thế lực thù địch, phản động, tin tặc lợi dụng để gia tăng các cuộc tấn công mạng nhằm phá hoại, chống phá Đảng và Nhà nước. Mục tiêu chủ yếu được nhắm đến là các hệ thống thông tin, hệ thống thông tin quan trọng của các cơ quan, tổ chức nhà nước. Để không bất ngờ với mọi tình huống, Bộ Thông tin và Truyền thông 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 đối với các hệ thống thông tin quan trọng, hệ thống thông tin chứa thông tin cá nhân, dữ liệu cá nhân và các nền tảng phục vụ chuyển đổi số quốc gia trọng tâm là:

a) Phân công lực lượng tại chỗ triển khai trực giám sát, bảo đảm an toàn thông tin mạng 24/7.

b) Yêu cầu các đơn vị chuyên trách, đơn vị cung cấp dịch vụ an toàn, an ninh mạng (nếu có) củng cố và ưu tiên nguồn lực, nhân lực cho nhiệm vụ giám sát và bảo vệ các hệ thống thông tin.

c) Thực hiện rà soát tổng thể các hệ thống thông tin đang vận hành, thực hiện kiểm tra, đánh giá rà soát các lỗ hổng, điểm yếu, cấu hình tăng cường bảo mật cho hệ thống thông tin thuộc quyền quản lý và khắc phục triệt để các lỗ

mật cho hệ thống thông tin thuộc quyền quản lý 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 tới các cơ quan như: các lỗ hổng bảo mật ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm Microsoft từ tháng 5 đến tháng 7 năm 2023 (Văn bản gửi kèm theo).

d) Chủ động xây dựng các phương án Ứng cứu khẩn cấp, hỗ trợ và khắc phục sự cố trong trường hợp xảy ra tấn công mạng.

đ) Luôn luôn sẵn sàng cập nhật thông tin cảnh báo, khuyến nghị về an toàn thông tin mạng được Cục An toàn thông tin, Bộ Thông tin và Truyền thông chia sẻ.

e) Bảo đảm duy trì, kết nối liên tục, kịp thời chia sẻ thông tin với Cục An toàn thông tin; trong đó, lưu ý kết nối tới hệ thống giám sát an toàn không gian mạng quốc gia (Trung tâm Giám sát an toàn không gian mạng quốc gia), nhất là các cơ quan hiện có kết nối, chia sẻ dữ liệu bị ngắt quãng hoặc không ổn định.

g) Đẩy mạnh tuyên truyền, nâng cao nhận thức cơ bản kỹ năng về an toàn thông tin mạng, cách nhận diện thư điện tử, liên kết đáng ngờ, cảnh giác về thông tin xấu độc của các thế lực thù địch tuyên truyền nhằm bôi xấu hình ảnh đất nước.

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

a) Tăng cường nguồn nhân lực thực hiện trực giám sát, hỗ trợ và khắc phục sự cố bảo đảm hạ tầng viễn thông, internet an toàn, thông suốt.

b) 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.

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

3. Cử đầu mối tiếp nhận thông tin với Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

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, email: 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 an 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 Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc TW;
- Các đơn vị chuyên trách về công nghệ thông tin, an toàn thông tin tại các bộ, ngành;
- Thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia;
- Lưu: VT, CATTT.PTA.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Huy Dũng