BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 5368/BTTTT-CATTT V/v tăng cường công tác bảo đảm an toàn thông tin mạng trong thời gian Tết Dương lịch và Tết Nguyên đán Nhâm Dần 2022	*Hà Nội, ngày 30 tháng 12 năm 2021*

Kính gửi:

- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc 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.

Với những diễn biến phức tạp của đại dịch Covid-19 khiến nhu cầu làm việc, hoạt động trên mạng ngày càng gia tăng, dẫn đến nguy cơ tấn công mạng ngày càng lớn, với quy mô phức tạp và khó lường. Đặc biệt trong các dịp nghỉ lễ Tết Dương lịch và Tết Nguyên đán Nhâm Dần 2022, các tin tặc, đối tượng xấu lợi dụng sự lơ là để tấn công, phát tán thông tin xấu độc.

Nhằm tăng cường bảo đảm an toàn thông tin mạng, không để bị động, bất ngờ với mọi tình huống và tạo tiền đề thúc đẩy mạnh mẽ chuyển đổi số ở mọi ngành trên phạm vi toàn quốc, toàn dân và toàn diện trong năm 2022, Bộ Thông tin và Truyền thông đề nghị các cơ quan, tổ chức, doanh nghiệp triển khai thực hiện một số nhiệm vụ trọng tâm như sau:

1. Triển khai rà soát, kịp thời xử lý, triển khai các giải pháp để khắc phục triệt để các lỗ hổng an toàn thông tin mạng đã được Bộ Thông tin và Truyền thông và các đơn vị chức năng cảnh báo như lỗ hổng tồn tại trong Apache Log4j (Văn bản số 1734/CATTT-NCSC,…).

2. Tăng cường, nâng cao năng lực bảo đảm an toàn thông tin mạng theo mô hình 4 lớp, đặc biệt bổ sung năng lực cho các hệ thống thông tin quan trọng, nhạy cảm trọng tâm là:

a) Phân công lực lượng tại chỗ triển khai trực giám sát, hỗ trợ, ứng cứu và khắc phục sự cố an toàn thông tin mạng 24/7;

b) Yêu cầu các đơn vị chuyên trách, đơn vị cung cấp dịch vụ an toàn thông

tin mạng (nếu có) cam kết và bố trí nguồn lực, nhân lực cho nhiệm vụ giám sát và bảo vệ các hệ thống;

c) Chủ động kiểm tra, đánh giá các lỗ hổng, điểm yếu trên các hệ thống thông tin thuộc phạm vi quản lý; kịp thời cập nhật các bản vá, cấu hình tăng cường bảo mật cho hệ thống và triển khai các giải pháp phòng ngừa để tránh bị lợi dụng, khai thác để tấn công;

d) Bảo đảm duy trì, kết nối, kịp thời chia sẻ thông tin với Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, internet; Các tổ chức, doanh nghiệp cung cấp nền tảng chuyển đổi số, nền tảng chống dịch Covid-19:

a) Tăng cường năng lực, đảm bảo các hệ thống thông tin, nền tảng hoạt động an toàn ổn định;

b) Triển khai các biện pháp kỹ thuật ở mức cao nhất nhằm phát hiện, lọc, ngăn chặn hoạt động tấn công mạng, phát tán thông tin xấu độc, thông tin vi phạm pháp luật trên hệ thống, 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.

4. Trong trường hợp cần hỗ trợ xử lý, ứng cứu và khắc phục sự cố, đề nghị liên hệ với đầu mối kỹ thuật của Cục An toàn thông tin, Bộ Thông tin và Truyền thông như sau:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), Điện thoại 024.3640.4424/086.9100.317, thư điện tử: thongbaosuco@vncert.vn.

- Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Các Sở TT&TT 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.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Huy Dũng