BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 6269 /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 Quý Mão 2023	*Hà Nội, ngày 31 tháng 12 năm 2022*

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 ở 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.

Trước nguy cơ tấn công mạng ngày càng phức tạp, nhằm tăng cường, chủ động bảo đảm an toàn thông tin mạng, không để bị động, bất ngờ với mọi tình huống, nhất là trong dịp nghỉ lễ Tết Dương lịch và Tết Nguyên đán Quý Mão 2023, Bộ Thông tin và Truyền thông đề nghị các cơ quan, tổ chức, doanh nghiệp triển khai một số biện pháp sau:

1. Chủ động rà soát, xử lý, triển khai các giải pháp nhằm khắc phục triệt để các lỗ hổng an toàn thông tin mạng, đặc biệt là các lỗ hổng đã được Bộ Thông tin và Truyền thông cảnh báo (như lỗ hổng bảo mật trong FortiOS và FortiProxy tại văn bản số 1547/CATTT-NCSC ngày 10/10/2022, lỗ hổng bảo mật zero-day Microsoft Exchange tại văn bản số 1485/CATTT-NCSC ngày 30/9/2022, lỗ hổng bảo mật trong các sản phẩm Microsoft tại văn bản 2035/CATTT-NCSC ngày 14/12/2022,...) và chủ động thực hiện săn lùng mối nguy hại tiềm ẩn trong hệ thống.

2. Tổ chức lực lượng tại chỗ trực giám sát, hỗ trợ, ứng cứu và khắc phục sự cố an toàn thông tin mạng 24/7; triển khai các biện pháp kỹ thuật ở mức cao nhất nhằm phát hiện, ngăn chặn tấn công mạng, phát tán thông tin xấu độc; yêu cầu đơn vị, doanh nghiệp đang cung cấp dịch vụ an toàn thông tin mạng (nếu có) cam kết và bố trí lực lượng giám sát và bảo vệ các hệ thống; 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 và các tổ chức, doanh nghiệp cung cấp nền tảng chuyển đổi số tăng cường năng lực hệ thống, nền tảng và đảm bảo các hệ thống thông tin, nền tảng hoạt động an toàn, ổn định để phục vụ người dân, doanh nghiệp.

4. Chủ động tổ chức hoạt động ứng cứu sự cố an toàn thông tin mạng cho các hệ thống thuộc phạm vi quản lý nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn thông tin mạng; thực hiện nghiêm túc và kịp thời các giải pháp theo yêu cầu của Bộ Thông tin và Truyền thông và cơ quan chức năng có thẩm quyền.

5. 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) qua các đầu mối sau đây:

- 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: (024) 3209.1616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 033.6666.905, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- 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 TT&TT các tỉnh, thành phố trực thuộc TW;
- Thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng