

Số: /BTTTT-CATTT
V/v tăng cường đảm bảo an toàn thông tin mạng trong dịp Lễ 30/4 và 01/5

Hà Nội, ngày tháng 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 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.

Nhằm phòng, chống nguy cơ mất an toàn thông tin mạng xảy ra trong thời gian diễn ra Lễ Giải phóng miền Nam, thống nhất đất nước 30/4 và Quốc tế lao động 01/5, Bộ Thông tin và Truyền thông đề nghị các cơ quan, tổ chức, doanh nghiệp tăng cường triển khai công tác bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý, cụ thể:

1. Tăng cường triển khai hoạt động bảo đảm an toàn thông tin mạng đối với 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, 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) 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 như: các lỗ hổng bảo mật ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm Microsoft từ tháng 01 đến tháng 4 năm 2022; lỗ hổng bảo mật Spring4Shell,...

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.

2. 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) 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.

b) 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 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;
- 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, CATT.

**KT. BỘ TRƯỞNG
THỨ TRƯỞNG**

Nguyễn Huy Dũng