

Số: 1752/UBND-THCB

Tuyên Quang, ngày 28 tháng 4 năm 2023

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

Kính gửi:

- Các Sở, ban, ngành thuộc tỉnh;
- Công an tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet;
- Các Ngân hàng thương mại trên địa bàn tỉnh;
- Ủy ban nhân dân huyện, thành phố.

Căn cứ Văn bản số 1520/BTTTT-CATTT ngày 26/4/2023 của Bộ Thông tin và Truyền thông về việc tăng cường đảm bảo an toàn thông tin mạng trong dịp Lễ 30/4 và 01/5.

Ủy ban nhân dân tỉnh yêu cầu:

- Các cơ quan, đơn vị, địa phương (mục kính gửi)
 - 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.
 - Chủ động rà soát các lỗ hổng, điểm yếu trên các hệ thống thông tin thuộc phạm vi quản lý; 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 2023 (có văn bản gửi kèm).
 - 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.
 - Sẵn sàng cập nhật thông tin cảnh báo, khuyến nghị về an toàn thông tin mạng được cơ quan chức năng chia sẻ, nhất là trên các nền tảng cảnh báo, hỗ trợ điều phối, ứng cứu sự cố đã được cung cấp cho các cơ quan, tổ chức sử dụng.
 - Bảo đảm duy trì, kết nối, kịp thời chia sẻ thông tin với Cục An toàn thông tin, Bộ Thông tin và Truyền thông; Đội ứng cứu sự cố mạng máy tính tỉnh.
 - Đẩy mạnh tuyên truyền, nâng cao nhận thức cơ bản kỹ năng về an toàn thông tin mạng, cảnh giác về thông tin xấu độc của các thế lực thù địch tuyên truyền nhằm hạ cấp uy tín, hình ảnh của Đảng, Nhà nước và Lãnh đạo Đảng, Nhà nước qua các thời kỳ.

2. Sở Thông tin và Truyền thông

- Chủ trì, phối hợp với các cơ quan, đơn vị chủ động rà soát, triển khai các giải pháp đảm bảo an toàn thông tin cho các hệ thống thông tin; đặc biệt là Cổng

thông tin điện tử, hệ thống thư điện tử, Cổng dịch vụ công, hệ thống Quản lý văn bản và điều hành, ...

- Củng cố và ưu tiên nguồn lực, nhân lực cho nhiệm vụ giám sát và bảo vệ các hệ thống thông tin của tỉnh.

- Cử đầu mối tiếp nhận 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

- 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.

- 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.

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

- Có phương án, kế hoạch để bảo đảm an toàn thông tin, đặc biệt là tổ chức dự phòng để duy trì tính sẵn sàng cho các dịch vụ viễn thông và Internet mà đơn vị cung cấp.

Trong trường hợp cần hỗ trợ giám sát, xử lý, ứng cứu sự cố đề nghị liên hệ: Sở Thông tin và Truyền thông (điện thoại: 0207.6251.788); Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), điện thoại: 024.3640.4421, đường dây nóng: 0869.100.317; thư điện tử: ir@vncert.vn; Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 024.3209.1616, đường dây nóng: 0389.942.878, thư điện tử: ais@mic.gov.vn để có phương án xử lý kịp thời, hiệu quả.

Ủy ban nhân dân tỉnh yêu cầu các cơ quan, đơn vị nghiêm túc triển khai, thực hiện./.

Nơi nhận:

- Như trên (thực hiện);
- Chủ tịch UBND tỉnh (báo cáo);
- Các PCT UBND tỉnh;
- Chánh VP UBND tỉnh;
- Phó CVP UBND tỉnh;
- Lưu VT, TG CNTT 02.

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**

Hoàng Việt Phương