

Số: /UBND-VHXH Bạch Sam ngày tháng 8 năm 2024

V/v tăng cường công tác bảo đảm
an toàn thông tin mạng trong
thời gian nghỉ lễ Quốc khánh 02/9

Kính gửi: Các đ/c Trưởng các ngành, đoàn thể, CBCC phường

Thực hiện Công văn số 1202/STTTT-BCVTCNTT ngày 29/8/2024 của Sở Thông tin và Truyền thông tỉnh Hưng Yên về việc tăng cường công tác bảo đảm an toàn thông tin mạng trong thời gian nghỉ lễ Quốc khánh 02/9. Nhằm phòng, chống nguy cơ mất an toàn thông tin mạng xảy ra trong thời gian diễn ra lễ Kỷ niệm 79 năm Quốc khánh nước Cộng hòa xã hội chủ nghĩa Việt Nam (02/9/1945-02/9/2024) và tăng cường bảo đảm an toàn thông tin mạng, không để bị động, bất ngờ với mọi tình huống trong năm 2024,

UBND phường đề nghị các ngành, đoàn thể, CBCC phường triển khai thực hiện một số nhiệm vụ trọng tâm 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, hỗ trợ, ứng cứu và khắc phục sự cố an toàn thông tin mạng 24/7.

b) Chủ động Rà soát, cập nhật đầy đủ các bản vá lỗ hổng bảo mật cho hệ thống thông tin, thực hiện theo dõi, xử lý các văn bản cảnh báo an toàn thông tin mạng (văn bản cảnh báo các lỗ hổng nghiêm trọng gửi kèm theo) hàng tuần, hàng tháng do Cục An toàn thông tin công bố tại địa chỉ <https://khonggianmang.vn/canhbaoattt/>, Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRlab.vn) và từ các cơ quan, tổ chức liên quan cung cấp.

c) Bảo đảm duy trì, kết nối, kịp thời chia sẻ thông tin với Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh. Khi phát hiện dấu hiệu của các cuộc tấn công mạng, kịp thời thông báo về Sở Thông tin và Truyền thông, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) để có biện pháp xử lý kịp thời, giảm thiểu thiệt hại.

d) Xây dựng kế hoạch, phương án Ứng cứu khẩn cấp để sẵn sàng triển khai các giải pháp ứng phó, xử lý sự cố tấn công mạng.

đ) Thực hiện sao lưu dữ liệu theo nguyên tắc 3-2-1: có ít nhất 03 bản sao dữ liệu, lưu trữ bản sao trên 02 phương tiện lưu trữ khác nhau, với 01 bản sao lưu ngoại tuyến “offline” (sử dụng tape/USB/ổ cứng di động,...); Triển khai giải pháp để sẵn sàng phục hồi nhanh hoạt động của hệ thống thông tin khi gặp sự cố, đưa hoạt động

của hệ thống thông tin trở lại bình thường trong vòng 24 tiếng hoặc theo yêu cầu nghiệp vụ.

2. Khi triển khai các nội dung trên, trong trường hợp cần thiết để hỗ trợ, đề nghị Quý cơ quan có thể liên hệ:

- Đầu mối Sở Thông tin và Truyền thông: Ông Đặng Xuân Dương, Điện thoại: 0988283898, thư điện tử: dxduong@hungyen.gov.vn;

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

- Cục An toàn thông tin; điện thoại 024.3640.4421/086.9100.317; thư điện tử: ir@vncert.vn;

- Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) – Cục An toàn thông tin; điện thoại: 02432091616/0389942878; thư điện tử: ais@mic.gov.vn.

- Phòng An toàn hệ thống thông tin, số điện thoại trực đường dây nóng hỗ trợ tổng thể các giải pháp an toàn thông tin 0888.133.359, thư điện tử: athttt@mic.gov.vn.

Nơi nhận:

- Như kính gửi;
- Chủ tịch, PCT UBND phường;
- Các ngành, đoàn thể, CBCC phường;
- Lưu: VP. VHXXH;

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Phạm Ngọc Chiến