

Số: /SGDDĐT-VP

Hải Phòng, ngày tháng năm 2024

V/v nâng cao công tác bảo đảm an toàn
thông tin mạng trên địa bàn thành phố

Kính gửi:

- Trưởng các phòng cơ quan Sở;
- Trưởng phòng GDĐT các quận, huyện;
- Hiệu trưởng trường THPT, PT nhiều cấp học;
- Giám đốc trung tâm GDNN-GDTX các quận, huyện;
- Thủ trưởng các đơn vị trực thuộc.

Ngày 19/6/2024, Sở Giáo dục và Đào tạo nhận được Văn bản số 1327/STTTT-BCVT của Sở Thông tin và Truyền thông về việc nâng cao công tác bảo đảm an toàn thông tin mạng trên địa bàn thành phố (gửi kèm theo);

Sở Giáo dục và Đào tạo đề nghị các đồng chí Trưởng các phòng cơ quan Sở, Thủ trưởng các đơn vị chỉ đạo đơn vị quan tâm, triển khai thực hiện một số nội dung sau:

1. Xây dựng Hồ sơ đề xuất cấp độ theo hướng dẫn tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông trình cấp có thẩm quyền phê duyệt theo quy định.

2. Xây dựng kế hoạch, bố trí nguồn lực, kinh phí để tổ chức tập huấn, kiểm tra, đánh giá an toàn thông tin đối với các hệ thống thông tin chưa thực hiện kiểm tra, đánh giá định kỳ (tối thiểu 01 lần/02 năm đối với hệ thống cấp độ 1, cấp độ 2; tối thiểu 01 lần/01 năm đối với hệ thống cấp độ 3); Kịp thời khắc phục các tồn tại, lỗ hổng, điểm yếu nhằm phòng ngừa các sự cố tấn công mạng, đặc biệt là các hệ thống cung cấp dịch vụ trực tuyến cho người dân và doanh nghiệp.

3. Xây dựng kế hoạch kinh phí, tổ chức diễn tập thực chiến an toàn thông tin đối với các hệ thống thông tin thuộc phạm vi quản lý theo chỉ đạo tại Chỉ thị số 18/CT-TTg ngày 13/8/2022 về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam và Kế hoạch số 200/KH-UBND ngày 17/7/2023 của Ủy ban nhân dân thành phố (ít nhất 01 lần/01 năm).

4. Thực hiện xây dựng kế hoạch Ứng phó sự cố đối với các hệ thống thông tin thuộc phạm vi quản lý. Kịp thời cập nhật phương án xử lý sự cố tương ứng với loại sự cố/hình thức tấn công mạng, đặc biệt là các phương án ứng phó sự cố đối với nguy cơ tấn công mã độc/mã hóa tống tiền (ransomware), tấn công chiếm quyền điều khiển, thay đổi giao diện,...

5. Tăng cường giám sát và sẵn sàng các phương án xử lý khi phát hiện có dấu hiệu bị cài cắm, khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng. Thực hiện đăng ký trên hệ thống

Tín nhiệm mạng của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) tại địa chỉ <https://tinnhiemmang.vn/>.

6. Triển khai mạng truyền số liệu chuyên dùng theo Quyết định số 08/2023/QĐ-TTg ngày 05/4/2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước; Kế hoạch số 72/KH-UBND ngày 23/3/2022 của Ủy ban nhân dân thành phố về việc triển khai Mạng truyền số liệu chuyên dùng trên địa bàn thành phố Hải Phòng. Thực hiện kiểm tra, chuẩn bị các điều kiện, trang thiết bị, nâng cấp mạng nội bộ, thực hiện kết nối hệ thống mạng nội bộ với hệ thống mạng truyền số liệu chuyên dùng thành phố chạy IPv6, trước mắt đưa một số ứng dụng như: Hội nghị truyền hình, mã độc tập trung,..).

Sở Giáo dục và Đào tạo đề nghị Thủ trưởng các đơn vị quan tâm chỉ đạo thực hiện./.

Nơi nhận:

- Như trên;
- UBND TP (để b/c);
- Sở TTTT (để p/h thực hiện);
- Lưu: VT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Phạm Quốc Hiệu