UBND THÀNH PHỐ HẢI PHÒNG
SỞ GIÁO DỤC VÀ ĐÀO TẠO

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 2509 /SGDĐT-VP
V/v thông báo tình hình an toàn, an ninh mạng tháng 4/2025

Hải Phòng, ngày 25 *tháng* 4 *năm 2025*

Kính gửi:
- Trưởng phòng CMNV cơ quan Sở;
- Trưởng phòng GDĐT quận, huyện, thành phố Thủy Nguyên;
- Hiệu trưởng trường trung cấp, cao đẳng trên địa bàn thành phố;
- Hiệu trưởng trường THPT, PT nhiều cấp;
- Giám đốc trung tâm GDNN-GDTX quận, huyện, thành phố Thủy Nguyên;
- Thủ trưởng các đơn vị trực thuộc.

Ngày 23/4/2025, Sở Giáo dục và Đào tạo (GDĐT) nhận được Văn bản số 1011/CAHP-ANM của Công an thành phố Hải Phòng về việc thông báo tình hình an toàn, an ninh mạng tháng 4/2025 *(gửi kèm theo)*.

Căn cứ tình hình an ninh mạng tháng 4/2025 qua Thông báo của Phòng An ninh mạng - Công an thành phố Hải Phòng, Sở GDĐT đề nghị Thủ trưởng các đơn vị thực hiện nghiêm các quy định về bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin thuộc phạm vi quản lý, cụ thể:

a) Tổ chức các hoạt động tuyên truyền, nâng cao nhận thức kỹ năng cơ bản về an toàn thông tin mạng; Nhận biết, cảnh giác trước thông tin xấu độc, tin giả, thông tin xuyên tạc, chống phá, chính sách của Đảng và Nhà nước; Phòng, chống lừa đảo trên không gian mạng cho toàn thể cán bộ, giáo viên, nhân viên, học sinh và người lao động của đơn vị quản lý.

b) Rà soát các hệ thống thông tin, bảo đảm các hệ thống thông tin được triển khai đầy đủ các biện pháp bảo vệ theo cấp độ an toàn. Chủ động rà soát, xử lý, triển khai các giải pháp nhằm khắc phục triệt để việc cập nhật, bảo mật đối với các trang website; cập nhật các phiên bản mới nhất của các trình duyệt web (Google Chrome, Cốc Cốc, Microsoft Edge, FireFox…) và các phiên bản mới nhất của Window nhằm khắc phục những lỗ hổng bảo mật của trình duyệt web (*Lỗ hổng zero-day CVE-2025-1234 ảnh hưởng đến công cụ JavaScript V8 của trình duyệt Google Chrome, cho phép tin tặc thực thi mã từ xa trên các thiết bị mục tiêu*), Microsoft Office (*Lỗ hổng bảo mật CVE-2025-27745 cho phép kẻ xấu thực hiện nhiều phương thức tấn công, lợi dụng lỗi trong phân bổ và giải phóng bộ nhớ của phần mềm Microsoft Office*) và các lỗ hổng bảo mật của hệ điều hành Window (*Lỗ hổng CVE-2025-26663 cho phép thực thi mã từ xa khai thác cơ chế "use-after-free" của Windows Lightweight Directory Access Protocol (LDAP); Lỗ hổng CVE-2025-26686 cho phép thực thi mã từ xa lợi dụng quá trình khóa bộ nhớ trong ngăn xếp TCP/IP của Window khiến dữ liệu bị phơi bày trong bộ nhớ, tạo cơ hội tấn công từ xa; Lỗ hổng bảo mật CVE-2025-27480 cho phép thực thi*

mã từ xa, lợi dụng lỗ hổng trong tính năng Remote Desktop của Windows; Lỗ hổng bảo mật CVE-2025-27491 cho phép thực thi mã từ xa tận dụng lỗi của Window Hyper-V) để bảo đảm an toàn cho máy tính và các hệ thống thông tin.

c) Đối với các hệ thống thông tin có sử dụng nền tảng xác thực tập trung WSO2 nhanh chóng kiểm tra mức độ ảnh hưởng và cập nhật bản vá mới nhất của WSO2 để phòng, chống các cuộc tấn công khai thác lỗ hổng bảo mật nghiêm trọng đã được Hiệp hội An ninh mạng Việt Nam (NCA) công bố ngày 24/3/2025 (04 lỗ hổng bảo mật nghiêm trọng trên nền tảng xác thực tập trung WOS2 cho phép tin tặc dễ dàng sử dụng thành chuỗi khai thác để chiếm đoạt tài khoản quản trị ứng dụng và chiếm quyền máy chủ, xâm nhập hạ tầng nội bộ, truy cập thông tin nhạy cảm).

d) Thực hiện tắt các cổng và dịch vụ không sử dụng trên các hệ thống thông tin để giảm thiểu bề mặt tấn công và hạn chế điểm yếu nhằm ngăn chặn các cuộc tấn công mã độc tống tiền (ransomware - mã độc mã hóa dữ kiệu với mục đích đòi tiền chuộc để giải mã dữ liệu); thực hiện sao lưu dữ liệu và kiểm tra khả năng khôi phục cần thực hiện thường xuyên để giảm thiểu thiệt hại từ tấn công ransomware.

Sở GDĐT đề nghị Thủ trưởng các đơn vị chỉ đạo thực hiện./.

Nơi nhận:
- Như trên;
- Công an TP (để p/h);
- Lưu: VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
THÀNH PHỐ HẢI PHÒNG

Uông Minh Long