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: 8752 /SGDĐT-VP
V/v thông báo tình hình an toàn, an ninh mạng tháng 10/2025

Hải Phòng, ngày 17 *tháng* 11 *năm 2025*

Kính gửi:
- Trưởng phòng CMNV cơ quan Sở;
- Thủ trưởng các cơ sở giáo dục trên địa bàn thành phố.

Căn cứ Thông báo của Công an Thành phố Hải Phòng tại Văn bản số 4194/CAHP-ANM ngày 24/10/2025 về việc thông báo tình hình an toàn, an ninh mạng tháng 10/2025 *(gửi kèm theo)*;

Sở Giáo dục và Đào tạo (GDĐT) nhận thấy yêu cầu cấp bách trong việc tăng cường bảo mật thông tin trong toàn ngành. Sở GDĐT yêu cầu các đơn vị trực thuộc khẩn trương triển khai các biện pháp nhằm đảm bảo an toàn, an ninh mạng (ATANM) cho các hệ thống thông tin và người dùng, cụ thể như sau:

I. CÁC NGUY CƠ, CẢNH BÁO TRỌNG TÂM TRONG THÁNG 10/2025

1. Nguy cơ nhắm vào nền tảng cộng tác (Microsoft Teams):

- Microsoft đã cảnh báo về việc tội phạm mạng đang lợi dụng nền tảng Teams để thu thập thông tin, lừa người dùng chia sẻ dữ liệu nhạy cảm, mạo danh nguồn tin cậy và phát tán mã độc qua tin nhắn và cuộc gọi đồng thời dùng Teams để duy trì truy cập và thực hiện trộm dữ liệu.

- Teams đang trở thành mục tiêu giá trị trong công tác tấn công, do đó các đơn vị cần tăng cường bảo vệ danh tính, bảo mật điểm cuối và triển khai các biện pháp phòng thủ mạng khác.

2. Cảnh báo về mã độc và tấn công có chủ đích:

- Hiệp hội an ninh mạng Việt Nam (NCA) cảnh báo về hoạt động sử dụng mã độc RUST CHAOSBOT nhắm vào các hệ thống thông tin tại Việt Nam. Chiến dịch này sử dụng mồi nhử liên quan đến các tổ chức tài chính, ngân hàng để phát tán mã độc mới ChaosBot và lợi dụng Discord làm máy chủ C2.

- NCA đã phát hiện và thu thập các mẫu mã độc giả mạo ứng dụng Chính phủ và ngân hàng nhắm vào các người dùng Android tại Việt Nam. Đây là một biến thể của mã độc đã được phát hiện từ năm 2016 có mục đích thu thập và đánh cắp thông tin đăng nhập của người dùng.

3. Tình hình lỗ hổng bảo mật nghiêm trọng và vá lỗi khẩn cấp:

- Trong tháng 10/2025, các công ty an ninh mạng đã công bố các lỗ hổng bảo mật nguy hiểm:

+ Oracle đã phát hành bản vá bảo mật khẩn cấp cho Oracle E-Business Suite phiên bản từ 12.2.3 đến 12.2.14 để khắc phục lồ hổng CVE-2025-61884 có thể bị khai thác từ xa và truy cập dữ liệu nhạy cảm, đồng thời cảnh báo khách hàng áp dụng sớm và tiếp tục duy trì các phiên bản được hỗ trợ.

+ Microsoft phát hành bản vá khắc phục 167 lỗ hổng bảo mật, trong đó có 08 lồ hong zero day, bao gồm các lỗ hổng liên quan đến leo thang đặc quyên, thực thi mã từ xa và bypass bảo mật. Các lỗ hổng được sửa liên quan đên Window Modem driver, Remote Access...

+ Microsoft cảnh báo về việc hai lỗ hổng trên Window là CVE-2025- 49708 và CVE-2025-55315 liên quan đến Secure Boot đang bị khai thác ngoài thực tế, cho phép tin tặc nâng cao đặc quyền, thực thi mã từ xa và vượt qua bảo mật, ảnh hưởng tới mọi phiên bản Window đã phát hành. Hiện chưa có thông tin nào về việc Microsoft đã phát hành bản vá đối với lồ hổng này.

+ Lỗ hổng nghiêm trọng trong bộ định tuyến TP-Link AX1800 có mã định danh CVE-2023-28760 cho phép tin tặc trên cùng một mạng LAN thực hiện thực thi mã độc từ xa dưới quyền root. Mã khai thác đã được công khai, do đó người dùng cần cân nhắc thay đổi thiết bị hoặc chờ bản cập nhật mới nhất của nhà sản xuất.

+ Oracle đã công bố bản vá cho ba lỗ hổng bảo mật (CVE-2025-9230, CVE-2025-9231, CVE-2025-9232), trên nhiều phiên bản thư viện, trong đó CVE-2025-2031 có thể cho phép khôi phục khóa riêng tư và từ đó thực thi mã hoặc tấn công DoS, hai lỗ hổng còn lại được đánh giá là mức độ trung bình và thấp, có khả năng gây DoS.

+ Lỗ hổng bảo mật CVE-2025-20333 và CVE-2025-20362 cho phép tin tặc thực thi mã tùy ý trên gần 50.000 thiết bị tường lửa Cisco ASA và FTD mà không cần xác thực. Cisco khuyến cáo người dùng hạn chế tiếp xúc Web VPN và tăng cường ghi nhật ký, giám sát. Quản trị viên cần nhanh chóng cập nhật và cài đặt bản vá nhằm giảm thiểu thiệt hại.

4. Tình hình lây nhiễm tại địa phương:

- Trong tháng 10/2025, Hệ thống quản lý mã độc tập trung của thành phố đã phát hiện 35 thiết bị thuộc 16 tổ chức trên địa bàn thành phố Hải Phòng bị nhiễm mã độc, với tổng cộng 31 loại mã độc đính kèm trong 168 file; hệ thống **SOC** của thành phố đã phát hiện và ngăn chặn 03 trường hợp các IP lạ không rõ nguồn gốc thực hiện hành vi rà quét lỗ hổng và thực thi mã bất thường trên các trang website của thành phố; Qua công tác quản lý và nắm tình hình, Công an thành phố chưa phát hiện vụ việc mất an ninh, an toàn nào trên các cổng thông tin điện tử của thành phố.

II. BIỆN PHÁP TRIỂN KHAI TOÀN NGÀNH

Sở GDĐT đề nghị các đồng chí Thủ trưởng các đơn vị cần nghiêm túc thực hiện các biện pháp sau:

1. Cập nhật và vá lỗi hệ thống định kỳ và khẩn cấp:

- Chủ động rà soát, kiểm tra và khẩn cấp cập nhật, vá lỗi cho tất cả các hệ thống máy tính, máy chủ, và thiết bị mạng, đặc biệt là các bản vá của Microsoft, Oracle và Cisco, nhằm giảm thiểu thiệt hại từ các lỗ hổng đã được công bố.

- Đối với các thiết bị mạng có lỗ hổng (như TP-Link AX1800), cần cân nhắc thay đổi thiết bị hoặc chờ bản cập nhật mới nhất từ nhà sản xuất.

2. Tăng cường bảo mật điểm cuối và nền tảng cộng tác:

- Thực hiện các biện pháp bảo mật điểm cuối (endpoint security) và tăng cường bảo vệ danh tính, đặc biệt khi sử dụng các nền tảng học tập và làm việc trực tuyến như Microsoft Teams để ngăn chặn việc bị đánh cắp thông tin, tài khoản.

- Cảnh báo cán bộ, giáo viên, nhân viên và học sinh/sinh viên về nguy cơ mã độc lợi dụng ứng dụng và giao dịch ngân hàng trên các thiết bị di động Android.

3. Rà soát và Giám sát hệ thống nội bộ:

- Yêu cầu các cán bộ phụ trách CNTT tại các đơn vị khẩn trương rà soát nội bộ các thiết bị máy tính, máy chủ và hệ thống mạng.

- Kiểm tra các hoạt động bất thường, đặc biệt là các dấu hiệu liên quan đến mã độc RUST CHAOSBOT và các địa chỉ IP không rõ ràng (đã phát hiện tại thành phố).

Sở GDĐT đề nghị Thủ trưởng các đơn vị chỉ chủ động cập nhật và nâng cấp giải pháp về bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin. Quá trình thực hiện nếu có khó khăn, vướng mắc hoặc phát hiện dấu hiệu tội phạm sử dụng công nghệ cao các đơn vị cần chủ động liên hệ ngay với Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (PA05) thuộc Công an thành phố Hải Phòng để được hướng dẫn, hỗ trợ kịp thời. Thông tin liên hệ Công an thành phố *(Qua Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; địa chỉ: số 55 Bến Bính, Hồng Bàng, Hải Phòng; SĐT: 069.278.5415)* để được hướng dẫn, hỗ trợ, phối hợp với các đơn vị có liên quan kịp thời khắc phục và nâng cấp hệ thống để đảm bảo an ninh, an toàn.

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

Nơi nhận:
- Như trên;
- Công an TP (để p/h);
- GĐ, PGĐ Sở;
- PCVP N.V. Nhậm;
- Lưu: VT, VP.

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