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: 7258 /SGDĐT-VP
V/v thông báo tình hình an toàn, an ninh mạng tháng 8, 9/2025

Hải Phòng, ngày 01 *tháng* 10 *năm 2025*

Kính gửi:
- Trưởng phòng CMNV cơ quan Sở;
- 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;
- Thủ trưởng các đơn vị trực thuộc.

Căn cứ Thông báo của Công an Thành phố Hải Phòng tại các Văn bản: số 1370/CAHP-ANM ngày 25/8/2025 về việc thông báo tình hình an toàn, an ninh mạng tháng 8/2025; số 2839/CAHP - ANM ngày 29/9/2025 về việc thông báo tình hình an toàn an ninh mạng tháng 9/2025;

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 đề nghị các đơn vị giáo dục khẩn trương và chi tiết hóa việc triển khai các biện pháp bảo đảm an toàn thông tin như sau:

I. Phân tích chi tiết các mối đe dọa an ninh mạng (Tháng 8 & 9/2025)

- Ngày 31/7/2025, các chuyên gia an ninh mạng đã phát hiện và cảnh báo về chiến thuật chuyển hướng nhiều lớp (multi layer redirect) được sử dụng để đánh cắp thông tin đăng nhập của người dùng Microsoft 365. Tin tặc lợi dụng dịch vụ đóng gói liên kết từ Proofpoint và Intermedia, thực hiện các bước chuyển hướng liên tiếp qua nhiều trang giả mạo nhằm che giấu đích đến thực sự, khiến các hệ thống bảo mật gặp khó khăn trong việc phát hiện và ngăn chặn.

- Trong tháng 8/2025, các chuyên gia đã phát hiện tình trạng rò rỉ hàng ngàn đoạn hội thoại với ChatGPT lên mạng Internet. Chỉ cần sử dụng một đoạn tìm kiếm đơn giản, người dùng có thể thấy hàng nghìn đoạn hội thoại với ChatGPT xuất hiện trên Google. Đây là một sự cố bảo mật đáng lo ngại, vì nhiều người dùng ChatGPT vẫn đang lầm tưởng rằng các đoạn hội thoại của mình là riêng tư, nhưng trên thực tế chúng đã bị rò rỉ ra ngoài.

- Ngày 06/8/2025, các chuyên gia an ninh mạng đã cảnh báo về việc phần mềm tống tiền Akira đang lợi dụng trình điều khiển điều chỉnh CPU Intel hợp pháp để tắt Microsoft Defender trong các cuộc tấn công mạng. Trình điều khiển bị lạm dụng là "rwdrv.sys". Qua đó, cho thấy việc chỉ sử dụng Microsoft Defender là chưa đủ để bảo vệ Window khỏi các mối đe dọa từ tấn công mã độc.

- Ngày 06/8/2025, các nhà nghiên cứu cảnh báo về việc tin tặc lợi dụng tính năng trên Microsoft 365 để lừa đảo người dùng nội bộ. Cụ thể, tin tặc lợi dụng

tính năng "Gửi trực tiếp" để gửi email lừa đảo từ nội bộ tổ chức, vượt qua các biện pháp kiểm tra bảo mật bằng cách giả mạo nhân sự cấp cao và các bộ phận như nhân sự, tài chính và quản lý.

- Các nhà nghiên cứu bảo mật đến từ Công ty an ninh mạng Profero của Mỹ đã bẻ khóa thành công mã hõa của mã độc tống tiền DarkBitt, cho phép các tổ chức và cá nhân bị ảnh hưởng có thể khôi phục dữ liệu miễn phí mà không cần trả tiền chuộc. Mặc dù công cụ giải mã không được phát hành công khai, người dùng bị nhiễm mã độc mã hóa dữ liệu có thể liên lạc với công ty Profero *(qua đường link https://profero.io)* để nhận được sự trợ giúp khôi phục dữ liệu miễn phí.

- Ngày 11/9/2025, Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT) thông báo có dấu hiệu hoạt động tấn công, xâm nhập của tội phạm để đánh cắp dữ liệu cá nhân tại Trung tâm thông tin tín dụng quốc gia (CIC). VNCERT đã chủ trì phối hợp với các đơn vị nghiệp vụ tiến hành xác minh, triển khai các biện pháp nghiệp vụ, kỹ thuật ứng phó sự cố trên và tăng cường các giải pháp bảo đảm an ninh mạng, thu thập dữ liệu, chứng cứ để xử lý theo quy định của pháp luật.

- Các nhà nghiên cứu về an ninh mạng đã phát hiện ra vụ việc nhóm tội phạm mạng GhostRedirector xâm nhập vào ít nhất 65 máy chủ Windows chủ yếu đặt tại Brazil, Thái Lan và Việt Nam. Nhóm tin tặc này đã khai thác một backdoor C++ thụ động có tên là Rungan và mô-đun IIS đặc biệt (Gamshen) được cài cắm vào phần mềm web server ISS của Microsoft. Mục tiêu của tội phạm là nhằm biến những hệ thống hợp pháp thành công cụ SEO gian lận để "thổi phồng" thứ hạng tìm kiếm cho các website cờ bạc.

- Vừa qua, Cloudflare tiết lộ rằng những kẻ tấn công đã truy cập vào một phiên bản Saleforce mà họ sử dụng để quản lý khách hàng nội bộ và hỗ trợ người dùng, trong đó có 104 mã Token API của Cloudflare. Cloudflare đã thay đổi 104 Token này. Đại diện của Cloudflare cho biết hầu hết dữ liệu bị xâm phạm đều là thông tin liên hệ của khách hàng, nhưng một số thông tin về cấu hình và mã token truy cập của khách hàng cũng có thể bị lộ.

- Cơ quan an ninh mạng và cơ sở hạ tầng Hoa Kỳ (CISA) cảnh báo về việc một số mẫu Router của TP-Link đang đối mặt với lỗ hổng zeroday chưa vá đã được khai thác bởi botnet Quad7, cho thấy nguy cơ tấn công từ xa và rò rỉ dữ liệu và nhấn mạnh tầm quan trọng của cập nhật firmware và các biện pháp phòng ngừa ngay khi có bản vá. Người dùng nên thiết lập các biện pháp phòng thủ bổ sung để tránh bị tin tặc tấn công, đánh cắp dữ liệu.

2. Các lỗ hổng hệ thống và phần mềm nghiêm trọng

- Trong tháng 8/2025, các công ty an ninh mạng đã công bố các lỗ hổng bảo mật sau:

+ Lỗ hổng CVE-2025-6558 bắt nguồn từ việc xác thực không chính xác dữ liệu đầu vào không đáng tin cậy trong các thành phần ANGLE và GPU của trình

duyệt Safari, tương tự như các lỗ hổng Zero-Day trên trình duyệt Google Chrome.

+ Microsoft đã phát hành bản vá Patch Tuesday tháng 8 khắc phục 107 lỗ hổng bảo mật, trong đó nổi bật là một lỗ hổng zero-day liên quan đến Windows Kerberos và nhiều lỗi nghiêm trọng có mức CVSS cao, bao gồm các lỗ hổng tiềm ẩn nguy cơ thực thi mã từ xa (RCE) và leo thang đặc quyền.

+ Lỗ hổng CVE-2025-53786 ảnh hưởng đến các phiên bản phiên bản Exchange Server, có khả năng cho phép tin tặc leo thang đặc quyền trong môi trường đám mây liên kết mà không để lại dấu vết dễ phát hiện.

+ Kỹ thuật tấn công mới TARA (Target Promptware Attacks) cho phép khai thác lỗ hổng trong AI Gemini của Google thông qua các lời mời và email tưởng chừng vô hại. Kỹ thuật này lợi dụng cơ chế xử lý ngữ cảnh của AI để chèn lệnh độc hại dưới dạng prompt injection từ đó kiểm soát hành vi của trợ lý ảo và mở rộng phạm vi xâm nhập sang các ứng dụng và thiết bị khác trong hệ sinh thái của người dùng.

- Trong tháng 9/2025, các tổ chức an ninh mạng đã công bố các lỗ hổng bảo mật sau:

+ Lỗ hổng trong Docker Desktop (CVE-2025-9074) cho phép kiểm soát container, gắn hệ thống tệp của máy chủ và nâng đặc quyền lên thành quản trị viên; lỗ hổng có thể bị khai thác thông qua API HTTP nội bộ mà không yêu cầu xác thực. Lỗ hổng này đã được vá trong phiên bản Docker 4.44.3.

+ Lỗ hổng trong phần mềm camera Dahua (CVE-2025-31700 và CVE-2025-31701) cho phép tấn công từ xa qua ONVIF và trình xử lý tải tệp RPC, dù có cơ chế ASLR giảm thiểu nguy cơ, tin tặc vẫn có thể chiếm quyền điều khiển mà người dùng không tương tác, vượt qua kiểm tra tính toàn vẹn firmware và tải payload ký không hợp lệ.

+ Lỗ hổng CVE-2025-55177 trên WhatsApp cho phép thực thi xử lý nội dung từ một URL tùy ý và có thể bị khai thác để tấn công người dùng iOS và Mac, nhất là trong các cuộc tấn công zero-click kết hợp với lỗ hổng hệ điều hành trước đó (CVE-2025-43300). Người dùng cần cảnh giác với các tin nhắn có nội dung kỳ lạ, xuất hiện ký tự bất thường, kèm các liên kết được rút gọn... và cập nhật phiên bản mới nhất của ứng dụng WhatsApp.

+ Lỗ hổng CVE-2025-54236 (SessionReaper) trong Adobe Commerce, Magento Open Source và các phiên bản liên quan cho phép tin tặc chiếm đoạt tài khoản khách hàng thông qua REST API nếu khai thác thành công. Adobe đã phát hành bản vá và triển khai WAF để giảm thiểu rủi ro. Người dùng cần cập nhật bản vá mới nhất để tránh bị tin tặc tấn công.

+ Google đã phát hành bản vá tháng 9/2025 để giải quyết 120 lỗ hổng bảo mật trên Android, trong đó có hai lỗ hổng (CVE-2025-38352, CVE-2025- 48543) có thể đã bị khai thác trong thực tế và cho phép leo thang đặc quyền khi không cần tương tác người dùng, đồng thời không tiết lộ chi tiết khai thác thực tế. Các lỗ hổng còn lại tập trung vào khả năng thực thi mã từ xa, tiết lộ thông tin và từ

chối dịch vụ, trong đó có: Lỗ hổng bảo mật nghiêm trọng CVE-2025- 10200 liên quan đến thành phần Serviceworker của Google Chrome có thể được khai thác để gây ra sự cố, hỏng dữ liệu hoặc thực thi mã từ xa nếu khai thác thành công; Lỗ hổng bảo mật nghiêm trọng CVE-2025-10585 trong công cụ Javascript và Web Assembly V8 có thể cho phép thực thi mã tùy ý và gây sập chương trình khi bị khai thác trên thực tế. Google khuyến nghị người dùng cập nhật lên phiên bản mới nhất của trình duyệt Chrome để nhận được bản vá.

+ Lỗ hổng thực thi mã từ xa CVE-2025-21043 trong thư viện phân tích hình ảnh trên các thiết bị Android từ Android 13 trở lên, có thể cho phép tin tặc triển khai mã độc từ xa và nhắm mục tiêu đến các ứng dụng nhắn tin. Samsung đã vá lồ hổng này trong các bản cập nhật mới nhất của hệ điều hành Android.

II. Tình hình Lộ lọt thông tin và Mã độc tại Hải Phòng

- Trong tháng 8/2025, Hệ thống quản lý mã độc tập trung của thành phố đã phát hiện 18 thiết bị thuộc 11 tổ chức trên địa bàn thành phố Hải Phòng bị nhiễm mã độc, với tổng cộng 59 loại mã độc đính kèm trong 291 file. Qua công tác quản lý và nắm tình hình thông qua hệ thống soc của thành phố, Công an thành phố đã phát hiện 06 vụ việc lộ lọt tài khoản đăng nhập khai thác sử dụng các hệ thống thông tin của các đơn vị trên địa bàn (gồm cả tài khoản quản trị hệ thống); 01 vụ việc khai thác lỗ hổng bảo mật để tấn công hệ thống thông tin trên địa bàn thành phố.

- Trong tháng 9/2025, Hệ thống quản lý mã độc tập trung của thành phố đã phát hiện 34 thiết bị thuộc 17 tổ chức trên địa bàn thành phố Hải Phòng (chủ yếu thuộc khối UBND, các Sở) bị nhiễm mã độc, với tổng cộng 52 loại mã độc đính kèm trong 128 file (phần lớn là mã độc trojan, mã độc được đính kèm vào file excel, ngoài ra còn có các mã độc được tải từ website bị nhiễm mã độc về). Hệ thống SOC của thành phố đã phát hiện và ngăn chặn 04 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 đã phát hiện vụ việc cổng thông tin điện tử xã Quốc Tuấn (huyện An Lão cũ) bị tấn công, xâm nhập thay đổi giao diện.

III. Khuyến nghị và Hướng dẫn Bảo đảm An toàn, An ninh mạng

Để đảm bảo an toàn cho hệ thống thông tin, dữ liệu và thiết bị phục vụ công tác giảng dạy, quản lý, Sở GDĐT đề nghị các đơn vị giáo dục triển khai khẩn trương các biện pháp sau:

1. Nâng cấp và vá lỗ hổng Bảo mật

- Cập nhật Phần mềm và Hệ điều hành: Chủ động cập nhật và nâng cấp các giải pháp về bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin. Đặc biệt:

+ Vá lỗ hổng: Cập nhật ngay các bản vá mới nhất cho Windows (Patch Tuesday tháng 8), Exchange Server, Adobe Commerce/Magento.

+ Trình duyệt và Ứng dụng: Cập nhật lên phiên bản mới nhất của Google Chrome , WhatsApp và các trình duyệt, ứng dụng khác để khắc phục lỗ hổng.

+ Thiết bị: Cập nhật firmware cho các mẫu Router TP-Link và các thiết bị camera Dahua.

+ Docker: Cập nhật lên phiên bản Docker 4.44.3 để vá lỗ hổng CVE-2025-9074.

- Bảo mật Máy chủ Web (IIS): Liên hệ với các đơn vị cung cấp giải pháp, phần mềm thực hiện vá kịp thời các lỗ hổng web, đặc biệt là SQL injection, theo dõi log PowerShell và hoạt động bất thường trên IIS, kiểm tra định kỳ các mô-đun IIS để phát hiện cài cắm trái phép và sử dụng giải pháp giám sát an ninh nâng cao, phát hiện cả hành vi bất thường chứ không chỉ dựa vào chữ ký malware.

2. Tăng cường Bảo mật Tài khoản và Hệ thống

- Xác thực Đa yếu tố (MFA): Bắt buộc bật và sử dụng xác thực đa yếu tố (Multi-Factor Authentication - MFA) cho tất cả các tài khoản quan trọng, đặc biệt là tài khoản quản trị hệ thống, email Microsoft 365, và các dịch vụ liên quan đến tài chính, ngân hàng.

- Siết chặt cơ chế quản lý nội bộ và tránh phụ thuộc hoàn toàn vào các tính năng của bộ phần mềm Microsoft 365 để xác thực nội bộ và gửi, nhận file.

- Cảnh giác với các email lừa đảo nội bộ lợi dụng tính năng "Gửi trực tiếp"; - Cần siết chặt cơ chế quản lý nội bộ, triển khai các biện pháp xác thực bổ sung và tránh phụ thuộc hoàn toàn vào các tính năng của bộ phần mềm Microsoft 365 để xác thực nội bộ và gửi, nhận file.

- Không chỉ dựa vào Microsoft Defender, cần sử dụng các giải pháp bảo mật bổ sung để đảm bảo an toàn cho thiết bị Windows trước các mối đe dọa từ mã độc, đặc biệt là ransomware Akira.

- Sử dụng giải pháp giám sát an ninh nâng cao, phát hiện cả hành vi bất thường chứ không chỉ dựa vào chữ ký malware.

3. Nâng cao Cảnh giác Người dùng và Quản lý Dữ liệu Cá nhân

- Cảnh giác với liên kết lạ và Chuyển hướng: Cảnh giác khi truy cập các liên kết lạ. Ngừng truy cập đường link nếu phát hiện nhiều hành vi chuyển hướng web khả nghi, dẫn đến các đường link phi chuẩn (chứa các chuỗi ký tự vô nghĩa, mạo danh các Website phổ biến).

- Bảo mật Dữ liệu Tài chính: Thay đổi mật khẩu tài khoản ngân hàng trực tuyến và dữ liệu liên quan đến tài chính, bật xác thực đa yếu tố, cảnh giác với các email hoặc cuộc gọi lừa đảo giả danh các tổ chức tài chính, nâng cao tinh thần cảnh giác trước hoạt động của tội phạm mạng.

- Người sử dụng các dịch vụ của Cloudflare nên thay đổi thông tin đăng nhập và liên hệ với hỗ trợ của Cloudflare để yêu cầu thay đổi token truy cập, sử dụng dịch vụ.

- Quản lý Hội thoại ChatGPT: Người dùng ChatGPT nên chủ động kiểm tra lại các đoạn hội thoại đã được chia sẻ, đặc biệt nếu có chứa thông tin cá nhân.

- Phòng chống Tấn công AI (Gemini): Cảnh giác với các lời mời và email tưởng chừng vô hại, vì chúng có thể là một phần của kỹ thuật TARA nhằm khai thác lỗ hổng trong AI.

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 đề nghị liên hệ về 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, Hông 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);
- 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