BỘ CÔNG AN
CÔNG AN TP HẢI PHÒNG

Số: 12875 /CAHP-ANM
V/v thông báo tình hình an ninh mạng tháng 9/2026

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

Hải Phòng, ngày 01 tháng 10 năm 2026

Kính gửi:
- Các cơ quan Đảng thành phố;
- Các cơ quan Trung ương đóng tại địa phương;
- Các Sở, ban, ngành;
- UBND các xã, phường, đặc khu;
- Các đơn vị sự nghiệp Thành phố;
- Các tổ chức chính trị, xã hội, doanh nghiệp.

Thực hiện nhiệm vụ quản lý nhà nước về an ninh mạng trên địa bàn thành phố; căn cứ kết quả công tác giám sát an ninh mạng tại Trung tâm dữ liệu thành phố, kết quả Hệ thống quản lý mã độc tập trung thành phố và công tác nắm tình hình trong tháng 9/2026, Công an thành phố thông báo một số nội dung sau:

I. TÌNH HÌNH AN NINH MẠNG TRÊN ĐỊA BÀN THÀNH PHỐ

1. Kết quả giám sát an ninh mạng tại Trung tâm dữ liệu thành phố

Hệ thống thông tin tại Trung tâm Dữ liệu thành phố không ghi nhận sự cố an ninh mạng nghiêm trọng; các cảnh báo phát sinh được tiếp nhận, phân tích, xử lý theo quy trình.

2. Kết quả Hệ thống quản lý mã độc tập trung thành phố

Trong tháng 9/2026, Hệ thống quản lý mã độc tập trung của thành phố đã phát hiện và ngăn chặn nguy cơ mất an ninh mạng đối với 219 thiết bị thuộc 74 tổ chức trên địa bàn thành phố, với tổng cộng 143 mối đe dọa từ mã độc, liên kết giả mạo và 2281 tệp tin độc hại.

Công an thành phố đã tiến hành triển khai cài đặt bổ sung **1.500** bản quyền (license) phần mềm Kaspersky thuộc hệ thống quản lý phòng chống mã độc tập trung của thành phố tại 70 sở, ban, ngành và UBND xã, phường, đặc khu.

3. Công tác bảo đảm an ninh mạng

Qua công tác quản lý và nắm tình hình, Công an thành phố đã phát hiện tình trạng mất an ninh mạng liên quan đến việc lộ lọt tài khoản của hệ thống thông tin của Trường Đại học Y Dược Hải Phòng và Công ty cổ phần Cảng Hải Phòng; Công an thành phố đã phối hợp, hướng dẫn triển khai các biện pháp bảo đảm an ninh mạng hệ thống thông tin tại Trường Đại học Hải Phòng.

Trong tháng, Công an thành phố đã chủ trì tiến hành kiểm thử, đánh giá an ninh mạng đối với 05 hệ thống thông tin cấp độ 3 trên địa bàn thành phố.

4. Một số tin tức, phương thức, thủ đoạn tấn công mới cần lưu ý

Hiệp hội an ninh mạng quốc gia (NCA) ghi nhận hoạt động của mã độc Mustang Panda và các biến thể đang được sử dụng khá nhiều để tấn công vào hệ thống thông tin ở Việt Nam. NCA ghi nhận hạ tầng điều khiển của mã độc có sự trùng khớp với hạ tầng của nhóm đã tấn công vào lĩnh vực tài chính ngân hàng tại Việt Nam từ năm 2024. Các đơn vị có nhu cầu rà quét, gỡ bỏ mã độc Mustang Panda có thể chủ động liên hệ với Công an thành phố (qua Phòng An ninh mạng) để được kịp thời hỗ trợ.

II. CẢNH BÁO CÁC LỖ HỔNG BẢO MẬT

Trong tháng 9/2026, các hãng công nghệ và công ty an ninh mạng đã công bố một số lỗ hổng bảo mật đáng chú ý sau:

STT	Lỗ hổng, sản phẩm ảnh hưởng	Mô tả, nguy cơ	Mức độ
1	300 lỗ hổng bảo mật mới được vá trong Chrome 152	Google đã phát hành Chrome 152 với các bản vá cho hơn 300 lỗ hổng bảo mật, trong đó phần lớn (299 lỗ hổng) được phát hiện nhờ sự hỗ trợ của trí tuệ nhân tạo. Trong số này có 10 lỗ hổng được xếp hạng nghiêm trọng (Critical) chủ yếu là các lỗi use-after-free trong các thành phần như Angle, Aura, Chromecast, Views và Safe Browsing, gồm 61 lỗi có mức độ nghiêm trọng cao.	Trung bình đến nghiêm trọng
2	Lỗ hổng CVE-2026-19632 trong Plugin TranslatePress của WordPress	Lỗ hổng trong plugin TranslatePress được sử dụng trên hơn 400.000 trang web WordPress cho phép chiếm đoạt tài khoản quản trị viên. Lỗ hổng xuất phát từ sự kết hợp giữa tính năng tự động lưu chuỗi dịch và việc quản trị viên thiết lập ngôn ngữ phụ, khiến liên kết đặt lại mật khẩu bị lưu trữ trong cơ sở dữ liệu dịch thuật và có thể truy xuất qua API.	Nghiêm trọng
3	Lỗ hổng bảo mật trong phần mềm TeamViewer	Lỗ hổng bảo mật nghiêm trọng trong phần mềm TeamViewer dành cho máy tính để bàn bao gồm: CVE-2026-19042, điểm CVSS 8.8, một lỗi chèn hệ lệnh hệ điều hành cho phép thực thi mã từ xa thông qua việc xử lý liên kết trò chuyện; CVE-2026-16444, một lỗi truy cập đường dẫn trái phép	Nghiêm trọng

STT	Lỗ hổng, sản phẩm ảnh hưởng	Mô tả, nguy cơ	Mức độ
		cho phép ghi tệp tùy ý vào các vị trí không mong muốn.	
4	Lỗ hổng bảo mật trên điện thoại iPhone và hệ điều hành iOS	Lỗ hổng zero-click trên iMessage có dấu hiệu lây nhiễm từ tháng 12/2025 đến tháng 1/2026 và đã được Apple vá lỗi trong bản cập nhật iOS 18.4.1. Mục đích là để cài đặt phần mềm gián điệp Pegasus.	Nghiêm trọng
5	Lỗ hổng CVE-2026-62911 trong Microsoft Exchange Server	Lỗ hổng cho phép thực thi mã tùy ý và chiếm quyền kiểm soát toàn bộ hộp thư của người dùng trên gần 22.000 máy chủ chưa được vá lỗi. Việc mã tấn công khai thác (POC) bị công khai làm gia tăng nguy cơ bị tấn công, đặc biệt vì Exchange 2016 và 2019 đã hết thời gian hỗ trợ. Bản vá chỉ có qua chương trình Extended Security Updates.	Nghiêm trọng
6	Lỗ hổng CVE-2026-0768	Lỗ hổng thực thi mã từ xa trong LangFlow, một công cụ mã nguồn mở cho phép bạn tự động hóa các quy trình làm việc AI đang bị khai thác tích cực để đánh cắp khóa API OpenAI, AWS và thông tin đăng nhập bằng cách truy vấn biến môi trường và đọc tệp nhạy cảm trên hệ thống. Khóa API và thông tin đăng nhập bị đánh cắp qua lỗ hổng bảo mật này chính là "chìa khóa vạn năng" cho phép kẻ tấn công vượt qua các lớp xác thực, trực tiếp chiếm đoạt tài nguyên đám mây và dịch vụ của nạn nhân mà không cần phải tấn công vào mạng nội bộ.	Nghiêm trọng

Đề nghị các cơ quan, đơn vị, địa phương rà soát các sản phẩm, dịch vụ nêu trên trong phạm vi quản lý; cập nhật ngay bản vá của nhà sản xuất (nâng cấp trình duyệt Chrome lên phiên bản 152 trở lên, cập nhật bản vá bảo mật cho thiết bị di động, nâng cấp plugin và mã nguồn website, cập nhật kernel đối với hệ điều hành); trường hợp chưa thể cập nhật ngay phải áp dụng biện pháp giảm thiểu rủi ro (giới hạn truy cập, tăng cường giám sát, sao lưu dữ liệu).

III. CÔNG TÁC BẢO ĐẢM AN NINH MẠNG TRONG THỜI GIAN TỚI

Trong thời gian tới, Công an thành phố đề nghị các cơ quan, đơn vị, địa phương phối hợp, triển khai các nội dung sau:

- Cử cán bộ, công chức, viên chức tham gia Chương trình tập huấn, diễn tập an ninh mạng thành phố năm 2026 theo Kế hoạch 105-KH/TBANM ngày 27/8/2026 của Tiểu ban an ninh mạng thành phố *(Dự kiến từ ngày 06/10/2026 đến 09/10/2026)*.

- Phối hợp với Công an thành phố triển khai dịch vụ Giám sát an ninh mạng (SOC) đối với các hệ thống thông tin của các cơ quan, đơn vị trên địa bàn thành phố.

- Tổ chức rà soát tổng thể các hệ thống thông tin thuộc phạm vi quản lý; huy động mọi nguồn lực khắc phục ngay các lỗ hổng bảo mật, ưu tiên xử lý trước các lỗ hổng ở mức nghiêm trọng, mức cao và các lỗ hổng đang bị hoặc có nguy cơ cao bị khai thác; cài đặt đầy đủ, kịp thời bản vá bảo mật mới nhất cho hệ điều hành, phần mềm máy chủ, ứng dụng web, cơ sở dữ liệu, thiết bị mạng và thiết bị bảo mật; đổi mật khẩu mặc định, mật khẩu yếu; gỡ bỏ dịch vụ, tài khoản không cần thiết; sao lưu dữ liệu quan trọng.

Công an thành phố đề nghị các cơ quan, đơn vị, địa phương quan tâm, phối hợp triển khai thực hiện. Quá trình thực hiện nếu có khó khăn, vướng mắc, đề nghị liên hệ Công an thành phố (*qua Phòng An ninh mạng; địa chỉ: số 55 Bến Bính, phường Hồng Bàng, thành phố Hải Phòng; số điện thoại: 069.278.5415*) để được hướng dẫn, hỗ trợ./.

Nơi nhận:
- Như trên;
- Cục A05-BCA
- Đ/c Giám đốc CATP
- Lưu: VT, ANM(Đ4).

(*để báo cáo*);

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Lê Đức Thành