ỦY BAN NHÂN DÂN **XÃ KIẾN THỤY**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 1300/UBND-CA V/v đảm bảo an toàn, an ninh mạng	*Kiến Thụy, ngày* 23 *tháng* 10 *năm 2025*

Kính gửi:
- Các cơ quan thuộc Đảng ủy xã;
- Các cơ quan, đơn vị trên địa bàn xã.

Theo thông báo của Công an thành phố Hải Phòng về tình hình an ninh mạng và kết quả hoạt động của công tác giám sát an ninh mạng tháng 9/2025:

- 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 chuyên gia khuyến cáo người dùng nên 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.

- 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 IIS 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. Các chuyên gia khuyến cáo doanh nghiệp cần 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.

- 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. 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.

- 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.

- 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 WebAssembly 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 lỗ hổng này trong các bản cập nhật mới nhất của hệ điều hành Android.

- 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. Công an thành phố đã thông báo tới các đơn vị trên, 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.

Để đảm bảo tốt an ninh, an toàn mạng, không để tin tặc tấn công gây ra các rủi ro cho an ninh hệ thống, chiếm đoạt quyền kiểm soát; Ủy ban nhân dân xã có ý kiến như sau:

1. Đề nghị các cơ quan thuộc Đảng ủy xã, các cơ quan, đơn vị trên địa bàn xã chủ động cập nhật và nâng cấp giải pháp về bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin.

2. Giao Công an xã

- Tham mưu, đề xuất việc đảm bảo an toàn, an ninh mạng, ứng cứu sự cố an toàn thông tin mạng trên địa bàn xã.

- Cử cán bộ đầu mối phụ trách công tác đảm bảo an toàn, an ninh mạng, ứng cứu sự cố an toàn thông tin mạng; thông tin gửi về Ủy ban nhân dân xã *(Qua phòng Văn hóa – Xã hội, Văn phòng HĐND và UBND xã)* **trước ngày 29/10/2025.**

- Hướng dẫn các đơn vị triển khai nghiêm túc, hiệu quả công tác bảo đảm an toàn, an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng trong quá trình sáp nhập, sắp xếp các đơn vị; đẩy mạnh công tác đấu tranh phòng, chống các loại tội phạm mạng, tội phạm sử dụng công nghệ cao lợi dụng việc sắp xếp đơn vị hành chính để thực hiện hành vi vi phạm pháp luật.

3. Yêu cầu các cơ quan, đơn vị trên địa bàn xã

- Tổ chức rà soát toàn bộ hệ thống thông tin trọng yếu, bố trí nhân sự vận hành, thực hiện kết nối, tích hợp, liên thông hệ thống dữ liệu; chủ động xây dựng, triển khai phương án bảo vệ các hệ thống thông tin, cơ sở dữ liệu, tài liệu số và tổ chức bàn giao đúng yêu cầu đối với các đơn vị thuộc diện sắp xếp; tổ chức rà soát, thu hồi các loại USB Token, USB cơ yếu, USB an toàn đối với cán bộ có thay đổi vị trí công tác, hết nhiệm vụ tiếp cận hệ thống dữ liệu, mã hoá; kiểm soát việc phân quyền truy cập, bảo vệ tài khoản quản trị, tài khoản vận hành hệ thống; chủ động kiểm tra, đánh giá an ninh, an toàn hệ thống mạng, rà quét khắc phục các điểm yếu, lỗ hổng bảo mật; hạ tầng máy chủ, dung lượng truyền tải, các điều kiện cần thiết khác... đảm bảo trước khi kết nối, liên thông hệ thống.

- Đối với các hệ thống thông tin trọng yếu phục vụ trực tiếp công tác lãnh đạo, chỉ đạo của chính quyền địa phương: Hệ thống Quản lý văn bản điện tử, Hệ thống Thư điện tử công vụ, Hệ thống Cổng thông tin điện tử, Hệ thống Tiếp nhận, xử lý dịch vụ công, hệ thống cơ quan phát thanh... yêu cầu các đơn vị thực hiện giám sát 24/7, tăng cường kiểm tra an ninh, an toàn hệ thống, kịp thời phát hiện, khắc phục, ứng cứu sự cố gây mất an ninh, an toàn hệ thống mạng.

Đối với các hệ thống lưu trữ, xử lý thông tin quan trọng, tài liệu bí mật nhà nước chủ động phương án dự phòng hệ thống, sao lưu dữ liệu để bảo đảm khả

năng khôi phục khi sự cố xảy ra. Đặc biệt trong giai đoạn chuyển giao công nghệ, đồng bộ dữ liệu trong quá trình sáp nhập, sắp xếp các đơn vị.

- Tăng cường công tác tuyên truyền, phổ biến, hướng dẫn cho người dân trên địa bàn về những thay đổi, điều chỉnh trong thực hiện các dịch vụ công, thủ tục hành chính; cảnh giác trước các phương thức, thủ đoạn hoạt động của các loại tội phạm mạng, tội phạm sử dụng công nghệ cao.

Ủy ban nhân dân xã thông báo để các cơ quan, đơn vị triển khai thực hiện. Trong quá trình thực hiện nếu có khó khăn, vướng mắc, các cơ quan, đơn vị báo cáo Ủy ban nhân dân xã *(Qua Công an xã – Tổ An ninh)* để chỉ đạo, hướng dẫn./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Lưu Văn Thụy

Nơi nhận:
- Như trên;
- TT ĐU, HĐND xã *(Báo cáo);*
- CT, các PCT UBND xã;
- Lưu: VT.