

Số: 1795 /STP-VP

Hà Tĩnh, ngày 13 tháng 7 năm 2026

V/v thông báo lỗ hổng bảo mật
nghiêm trọng

Kính gửi: Các Phòng, Trung tâm thuộc Sở

Ngày 29/6/2026, Công an tỉnh Hà Tĩnh có Văn bản số 2662/CAT-ANM về việc thông báo lỗ hổng bảo mật nghiêm trọng tháng 6/2026, trong đó đã cảnh báo về nhiều chiến dịch tấn công mạng tinh vi, lỗ hổng bảo mật nghiêm trọng trên các phần mềm ứng dụng phổ biến và một số loại mã độc nguy hiểm đang lây nhiễm, có nguy cơ ảnh hưởng trực tiếp đến các cơ quan, đơn vị trên địa bàn tỉnh. Các loại virus, mã độc này có thể bị đối tượng tấn công lợi dụng để chiếm quyền điều khiển hệ thống, đánh cắp và mã hóa dữ liệu đòi tiền chuộc (ransomware). Nhằm bảo đảm an toàn, an ninh thông tin của Sở, chủ động phòng ngừa, ngăn chặn nguy cơ bị tấn công mạng, mất, lộ lọt dữ liệu, Giám đốc Sở yêu cầu Thủ trưởng Phòng, Trung tâm thuộc Sở tổ chức thực hiện các nội dung sau:

1. Về rà soát, xử lý các nguy cơ, lỗ hổng bảo mật

1.1. Rà soát toàn bộ máy tính, thiết bị đang sử dụng tại đơn vị; quán triệt công chức, viên chức, người lao động không sử dụng phần mềm hệ điều hành Windows, Office không có bản quyền (crack, key lậu, activator) dưới bất kỳ hình thức nào; Khẩn trương đề xuất, trang bị phần mềm có bản quyền hợp pháp.

1.2. Đối với các thiết bị (máy tính, ổ cứng, điện thoại) đã hỏng, không còn sử dụng, có nhu cầu thanh lý: không tự ý xóa dữ liệu theo cách thông thường (Delete/Format); thực hiện ghi đè dữ liệu (Zero Fill) hoặc tiêu hủy vật lý chip nhớ, phiên đĩa đối với thiết bị chứa thông tin nhạy cảm trước khi thanh lý, tuyệt đối không rao bán, chuyển giao cho các cơ sở thu mua không rõ nguồn gốc.

1.3. Không cài đặt ứng dụng từ nguồn không rõ ràng (file .APK ngoài kho ứng dụng chính thống Google Play/App Store); không sử dụng điện thoại đã bị can thiệp phần cứng (Root/Jailbreak) hoặc mua điện thoại cũ không rõ nguồn gốc; thận trọng khi cung cấp hình ảnh, video khuôn mặt trên các ứng dụng không uy tín để tránh bị lợi dụng tạo “Camera ảo”, chèn hình ảnh, video Deepfake vào quy trình xác thực sinh trắc học, phục vụ hành vi lừa đảo chiếm đoạt tài sản.

2. Về phòng, chống mã độc qua hệ thống quản trị mã độc tập trung (EDR)

2.1. Tuyệt đối không thực thi (chạy) các file .exe nhận được qua email, ứng dụng nhắn tin (Zalo, Telegram...), thiết bị lưu trữ USB hoặc tải về từ Internet khi chưa xác định rõ nguồn gốc, độ an toàn; không mở file bản vẽ AutoCAD không rõ nguồn gốc; không bấm “Cho phép nội dung hoạt động” (Enable Content) hoặc “Cho phép Macro” (Enable Macros) đối với file Excel, Word nhận từ nguồn không tin cậy để phòng ngừa mã độc lây nhiễm tệp tin đa hình (Virus.Win32.Virut.ce, Virus.Win64.Moiva.a) và mã độc lây nhiễm qua Excel (Virus.MSExcel.Laroux).

2.2. Duy trì bất thường xuyên, cập nhật đầy đủ phần mềm diệt virus Smart IR trên toàn bộ máy tính thuộc đơn vị; khi phát hiện dấu hiệu bất thường (máy chạy chậm bất thường, ứng dụng .exe bị lỗi không mở được...) phải lập tức ngắt kết nối mạng Internet, rút toàn bộ thiết bị lưu trữ ngoài (USB, ổ cứng rời) và báo ngay cho bộ phận công nghệ thông tin của Sở; không tự ý dùng phần mềm diệt virus thông thường chạy trực tiếp trên máy để xử lý, tránh làm mã độc lây lan nhanh hơn hoặc phần mềm diệt virus bị vô hiệu hóa.

2.3. Tiếp tục thực hiện nghiêm chế độ sao lưu dữ liệu theo nguyên tắc 3-2-1 đã triển khai tại Sở; chỉ sao lưu file tài liệu (docx, pdf, xlsx), tuyệt đối không sao lưu file thực thi (.exe) để tránh phát tán mã độc qua bản sao lưu.

(Cụ thể các nguy cơ, cảnh báo và giải pháp khắc phục có tại Văn bản số 2662/CAT-ANM đính kèm Văn bản này)

Đề nghị Trưởng các Phòng, Trung tâm thuộc Sở chỉ đạo, tổ chức thực hiện kịp thời và có hiệu quả. Khi phát hiện dấu hiệu bất thường, mã độc hoặc bị tấn công, kịp thời báo cáo Văn phòng Sở để phối hợp xử lý; trường hợp cần thiết liên hệ Phòng An ninh mạng và Phòng chống tội phạm sử dụng Công nghệ cao - Công an tỉnh (SĐT: 099.338.6777) để được hỗ trợ./.

Nơi nhận:

- Như trên;
- Lãnh đạo Sở;
- Lưu: VT, VP.

**TL. GIÁM ĐỐC
Q. CHÁNH VĂN PHÒNG**



Thiền Thị Chiên