UBND TỈNH HÀ TĨNH
SỞ TƯ PHÁP

Số: 3815 /STP-VP

V/v tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu và cảnh báo, khắc phục lỗ hổng bảo mật nghiêm trọng tháng 11

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

Hà Tĩnh, ngày 18 tháng 12 năm 2025

Kính gửi: Các Phòng, Trung tâm thuộc Sở

Thực hiện Văn bản số 9453/UBND-NC ngày 27/11/2025 của UBND tỉnh Hà Tĩnh về việc triển khai công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu và Văn bản số 4454/CAT-ANM ngày 11/12/2025 của Công an tỉnh về việc thông báo lỗ hổng bảo mật nghiêm trọng tháng 11, Giám đốc Sở Tư pháp yêu cầu các Phòng, Trung tâm thuộc Sở nghiêm túc triển khai các nội dung sau:

1. Về an ninh mạng và an toàn dữ liệu

- Tập trung chỉ đạo, quán triệt, triển khai quyết liệt, đồng bộ các biện pháp tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu, đáp ứng yêu cầu chuyển đổi số liên thông, đồng bộ, nhanh chóng, hiệu quả.

- Đẩy mạnh công tác tuyên truyền, phổ biến nâng cao nhận thức, kiến thức pháp luật, nghiệp vụ về đảm bảo an ninh mạng, bảo mật và an toàn thông tin, an toàn dữ liệu.

- Rà soát và khắc phục ngay những lỗ hổng bảo mật, không chấp nhận tình trạng "nợ tuân thủ" các điều kiện về an toàn, an ninh mạng.

- Bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu là thành phần bắt buộc trong mọi dự án công nghệ thông tin.

- Đảm bảo tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, dữ liệu đạt tối thiểu 15% tổng kinh phí triển khai các đề án, dự án công nghệ thông tin.

- Chịu trách nhiệm trực tiếp về tính chính xác, đầy đủ, kịp thời của dữ liệu do mình quản lý và đảm bảo kết nối, chia sẻ, liên thông dữ liệu với Cơ sở dữ liệu quốc gia và Trung tâm dữ liệu quốc gia.

- Các đơn vị sự nghiệp thuộc Sở xây dựng, duy trì cơ chế bảo đảm an toàn, an ninh mạng, phương án ứng phó sự cố, phương án khôi phục dữ liệu; Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet và hoàn thành trong tháng 12 năm 2025.

2. Cảnh báo và giải pháp khắc phục mã độc, lỗ hổng bảo mật

Thủ trưởng các đơn vị sự nghiệp thuộc Sở cần đặc biệt lưu ý các cảnh báo nghiêm trọng từ Công an tỉnh tại Văn bản số 4454/CAT-ANM và triển khai ngay các giải pháp sau:

- Đối với mã độc gián điệp tinh vi (AMDHealth CheckerV12) - Mức độ rất nghiêm trọng, cần lắp đặt, cấu hình tường lửa (Firewall) chặn kết nối đến các tên miền độc hại như: "s1336z.grpc-test.me", "ltwyq.experimental-tech.com", "gaylorr.icu", "baumbahh.run", "bnrgnaum.live". Kiểm tra sự tồn tại của tác vụ Scheduled Task "AMDHealthCheckerV12" trên các máy tính để xử lý.

Công chức, viên chức, người lao động không tải và cài đặt các phần mềm từ các nguồn không chính thống.

- Đối với mã độc Worm.Win32.FakeDoc (lây lan qua USB, Zalo, Email) - Mức độ nghiêm trọng: Rà soát, cách ly các máy tính có dấu hiệu nhiễm. Sử dụng Group Policy để vô hiệu hóa tính năng AutoRun đối với các thiết bị USB.

Công chức, viên chức, người lao động quét virus tất cả các thiết bị USB trước khi sử dụng. Bật chế độ hiển thị file ẩn để phát hiện các tệp tin đáng ngờ. Đặc biệt phải cẩn trọng với các tệp tin gửi qua Zalo, Email có biểu tượng tài liệu nhưng có đuôi là ".exe" hoặc là dạng "Shortcut" và luôn bật phần mềm diệt virus Smart IR.

- Đối với mã độc lây nhiễm qua file Excel (macro-virus) - Mức độ nghiêm trọng: Cấu hình Group Policy để vô hiệu hóa hoặc cảnh báo nghiêm ngặt việc thực thi macro trong các văn bản Office.

Công chức, viên chức, người lao động tuyệt đối không bấm "cho phép nội dung hoạt động (Enable Content) hoặc "cho phép Macros" (Enable Macros) đối với các tệp tin nhận được từ nguồn không tin cậy và luôn bật phần mềm diệt virus Smart IR.

- Đối với lỗ hổng bảo mật trên các phần mềm phổ biến (Google Chrome, 7-Zip) - Mức độ nghiêm trọng: Cập nhật lại các phần mềm lên phiên bản mới nhất: Google Chrome: 142.0.7444.176 trở lên; 7-Zip: 25.00 trở lên (Winrar cũng cần nâng lên phiên bản mới nhất).

Yêu cầu các Phòng, Trung tâm nghiêm túc, triển khai thực hiện có hiệu quả các nội dung trên. Khi phát hiện dấu hiệu tấn công mạng các Phòng, Trung tâm thuộc Sở khẩn trương báo cáo về Văn phòng Sở (là đầu mối tiếp nhận ứng cứu sự cố của Sở) để phối hợp với Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh kịp thời xử lý./.

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

GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ TƯ PHÁP
TỈNH HÀ TĨNH

Nguyễn Quốc Tuấn