BỘ CÔNG AN
CÔNG AN TỈNH HÀ TĨNH

Số: 1309/CAT-ANM
V/v tăng cường đảm bảo an toàn hệ thống thông tin trong dịp nghỉ lễ 30/4 và 01/5

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

Hà Tĩnh, ngày 22 tháng 4 năm 2025

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành cấp tỉnh;
- UBND các huyện, thành phố, thị xã.

Thực hiện công tác đảm bảo an toàn, an ninh mạng và duy trì các hệ thống thông tin trên địa bàn tỉnh Hà Tĩnh hoạt động ổn định trong và sau dịp kỷ niệm 50 năm Ngày Giải phóng miền Nam thống nhất đất nước (30/04/1975 – 30/04/2025), Công an tỉnh đề nghị các đơn vị thực hiện một số nội dung sau:

1. Phân công cán bộ thường xuyên kiểm tra tình trạng hoạt động của hệ thống thông tin, đảm bảo hệ thống thông tin hoạt động ổn định và ứng cứu sự cố kịp thời. Đối với chủ quản hệ thống thông tin cấp độ 3 và hệ thống thông tin của Văn phòng Tỉnh ủy đề nghị bố trí cán bộ trực, thường xuyên kiểm tra tình trạng hoạt động các hệ thống thông tin, phối hợp với đầu mối ứng cứu sự cố và các đơn vị liên quan khi có yêu cầu.

2. Trong thời gian nghỉ lễ, đề nghị các đơn vị yêu cầu cán bộ, công chức, viên chức tắt các thiết bị máy tính kết nối Internet không cần thiết, tránh để các đối tượng lợi dụng thời gian nghỉ lễ, tấn công xâm nhập vào hệ thống thông tin; cán bộ, công chức, viên chức trong quá trình sử dụng máy tính của cơ quan, đơn vị tuyệt đối không truy cập vào các đường link lạ, các nội dung email bất thường. Nêu cao tinh thần cảnh giác với các loại tấn công mạng, thường xuyên thay đổi mật khẩu các tài khoản trên hệ thống dùng chung của tỉnh, …

3. Đề nghị Sở Khoa học và Công nghệ bố trí cán bộ trực, phối hợp với đầu mối ứng cứu sự cố trong tình huống xảy ra sự cố hoặc có hoạt động tấn công mạng vào hệ thống thông tin sử dụng tên miền hatinh.gov.vn, triển khai phương án bảo đảm hệ thống thông tin khi bị tấn công thay đổi giao diện (*có phương án kèm theo*).

4. Đề nghị Văn phòng UBND tỉnh, chỉ đạo Trung tâm Công báo – Tin học thực hiện thiết lập các tính năng ngăn chặn tấn công DDOS, lọc địa chỉ IP thực hiện truy vấn bất thường; giảm số lượng truy vấn vào hệ thống dịch vụ công trực tuyến trong thời gian nghỉ lễ. Phối hợp Công an tỉnh xử lý sự cố bước đầu, điều tra, truy

vết, xác minh nguồn, nguyên nhân tấn công mạng nhằm vào hệ thống *(nếu xảy ra hoạt động tấn công)*.

Đầu mối ứng cứu sự cố tỉnh: Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh; Số điện thoại cố định: 069.292.6555; Email: anm.cat@hatinh.gov.vn; Địa chỉ: số 04, Nguyễn Thiếp, Phường Tân Giang, Thành phố Hà Tĩnh, Hà Tĩnh; Số điện thoại di động/Zalo/Telegram: 099.338.6777.

Đề nghị các cơ quan, đơn vị triển khai, thực hiện nghiêm túc, trong quá trình thực hiện có khó khăn, vướng mắc liên hệ đ/c Lê Phú Hưng *(Cán bộ Phòng An ninh mạng và phòng chống tội phạm công nghệ cao – Công an tỉnh, số điện thoại: 0866.946.777)* để được phối hợp, hướng dẫn./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc (*để báo cáo*);
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
CÔNG AN TỈNH HÀ TĨNH

Thượng tá Nguyễn Quốc Hùng

PHƯƠNG ÁN

ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG TỈNH HÀ TĨNH

(Kèm theo công văn số 170/CAT-ANM ngày 22/4/2025)

Thực hiện chức năng QLNN về an toàn, an ninh thông tin mạng tỉnh Hà Tĩnh, Công an tỉnh dự kiến một số tình huống và phương án xử lý khi xuất hiện sự cố an toàn, an ninh mạng trên địa bàn tỉnh Hà Tĩnh như sau:

1. Tình huống 1: Trang/cổng thông tin điện tử của đơn vị trên địa bàn tỉnh bị tấn công thay đổi giao diện

a) Công tác phòng ngừa:

- Chủ quản hệ thống thông tin thường xuyên kiểm tra các dấu hiệu bất thường của trang/cổng thông tin điện tử như: phát hiện các tệp tin lạ trong trình quản lý file; tệp tin dạng ảnh nhưng không mở được hoặc không hiển thị khi mở; trang/cổng có nội dung lạ hiển thị.

- Công an tỉnh triển khai hoạt động theo dõi 24/7 hệ thống trang/cổng thông tin điện tử để kiểm tra việc thay đổi bất thường về giao diện hiển thị và tình trạng hoạt động của trang/cổng thông tin điện tử.

- Đối với hệ thống thông tin cấp độ 3 khi được cảnh báo hoặc chủ động phát hiện sự cố an toàn hệ thống thông tin, đề nghị thuê các đơn vị chuyên môn tiến hành pentest hệ thống để đảm bảo các sự cố, lỗ hổng không bị cài cắm mã độc, webshell.

b) Các bước xử lý hoạt động tấn công:

Bước 1: Khi thấy có dấu hiệu của việc tấn công thay đổi giao diện hoặc trang/cổng thông tin không hoạt động, hoạt động không ổn định. Chuyên trách công nghệ thông tin của đơn vị chủ động xác minh sơ bộ nguyên nhân, kiểm tra có phải là nguyên nhân khách quan không, như: sự cố mất điện, mất kết nối mạng, vô tình thay đổi nội dung. Nếu xác định không phải do các lý do khách quan, yêu cầu đơn vị chủ quản liên hệ đầu mối ứng cứu sự cố an toàn thông tin của tỉnh (Phòng An ninh mạng và phòng, chống tội phạm công nghệ cao, Công an tỉnh Hà Tĩnh).

Bước 2: Đầu mối ứng cứu sự cố tiếp nhận thông tin, đánh giá ban đầu mối sự cố được chủ quản đơn vị báo cáo. Khi xác định thấy có hành vi xâm nhập, thay đổi giao diện, thực hiện:

- Phối hợp Sở Khoa học và Công nghệ trỏ tên miền .hatinh.gov.vn của chủ quản đơn vị sang địa chỉ IP máy chủ dự phòng của Đầu mối ứng cứu sự cố, đảm bảo tên miền không bị ảnh hưởng, mất uy tín cơ quan đơn vị.

- Phối hợp đơn vị chủ quản hệ thống thông tin làm việc với nhà cung cấp dịch vụ (hạ tầng kỹ thuật và phần mềm hệ thống) để đánh giá nguyên nhân hệ thống bị tấn công; thu thập thông tin về hành vi tấn công.

2. Tình huống 2: Hệ thống thông tin bị tấn công DDOS

a) Công tác phòng ngừa:

- Đơn vị chủ quản hệ thống cần triển khai các biện pháp kỹ thuật nhằm giới hạn lưu lượng truy cập bất thường, cấu hình tường lửa, thiết lập các chính sách chống DDOS phù hợp trên các thiết bị mạng, máy chủ.

- Thiết lập hệ thống giám sát, phát hiện sớm các dấu hiệu bất thường về lưu lượng truy cập như: tăng đột ngột, xuất hiện từ các địa chỉ IP nghi vấn hoặc đến từ một quốc gia cụ thể trong thời gian ngắn.

- Công an tỉnh phối hợp với Sở Thông tin và Truyền thông hướng dẫn các đơn vị xây dựng kịch bản phòng chống tấn công DDOS, triển khai tập huấn, diễn tập định kỳ.

b) Các bước xử lý hoạt động tấn công:

Bước 1: Khi hệ thống hoạt động chậm, không truy cập được hoặc bị quá tải bất thường, đơn vị chủ quản cần:

- Xác minh có phải do lưu lượng truy cập tăng đột biến hay do sự cố nội bộ (quá tải server, lỗi phần mềm, mạng nội bộ...).

- Nếu loại trừ nguyên nhân kỹ thuật thông thường, liên hệ ngay với đầu mối ứng cứu sự cố an toàn thông tin mạng của tỉnh (Phòng An ninh mạng và phòng, chống tội phạm công nghệ cao, Công an tỉnh Hà Tĩnh).

Bước 2: Đầu mối ứng cứu sự cố tiếp nhận và phân tích dữ liệu nhật ký truy cập:

- Đánh giá, xác định có dấu hiệu của tấn công DDOS hay không.

- Hướng dẫn đơn vị thực hiện các biện pháp giảm tải, lọc IP, định tuyến truy cập qua các kênh an toàn hơn.

- Phối hợp với nhà cung cấp dịch vụ mạng để chặn lưu lượng độc hại từ upstream, cân bằng tải tạm thời.

- Khi cần thiết, hỗ trợ chuyển hướng tạm thời hệ thống sang máy chủ dự phòng, đảm bảo duy trì dịch vụ thiết yếu.

3. Tình huống 3: Máy tính cá nhân của đơn vị bị nhiễm mã độc mã hóa dữ liệu

a) Công tác phòng ngừa:

- Đơn vị chủ quản hệ thống và cán bộ, công chức, viên chức cần thường xuyên cập nhật hệ điều hành, phần mềm diệt virus, không mở các liên kết, tệp tin đính kèm từ email không rõ nguồn gốc.

- Thực hiện chính sách phân quyền truy cập dữ liệu phù hợp, hạn chế truy cập từ máy trạm tới các thư mục máy chủ khi không cần thiết.

- Định kỳ sao lưu dữ liệu quan trọng vào thiết bị lưu trữ riêng biệt hoặc hệ thống sao lưu tự động, đảm bảo không kết nối trực tiếp với mạng nội bộ.

- Công an tỉnh phối hợp Sở Thông tin và Truyền thông tổ chức tuyên truyền, nâng cao nhận thức về phòng, chống mã độc cho cán bộ trong các cơ quan, đơn vị.

b) Các bước xử lý hoạt động tấn công:

Bước 1: Khi phát hiện máy tính hiển thị thông báo mã hóa dữ liệu, không mở được tệp tin định dạng phổ biến (doc, xlsx, jpg, ...), cần:

- Ngắt kết nối máy tính khỏi mạng nội bộ (rút cáp mạng, tắt Wi-Fi).

- Tuyệt đối không thanh toán tiền chuộc hay cố gắng giải mã khi chưa có hướng dẫn.

- Báo ngay cho đơn vị phụ trách công nghệ thông tin (CNTT) và đầu mối ứng cứu sự cố của tỉnh (Phòng An ninh mạng và phòng, chống tội phạm công nghệ cao, Công an tỉnh Hà Tĩnh).

Bước 2: Đầu mối ứng cứu sự cố tiến hành:

- Hướng dẫn trích xuất dữ liệu nhật ký, xác định loại mã độc và phương thức lây lan.

- Phối hợp với đơn vị phụ trách CNTT cô lập các máy bị nhiễm, kiểm tra mức độ lây lan trong hệ thống.

- Tư vấn phương án phục hồi từ bản sao lưu an toàn, diệt mã độc hoàn toàn trước khi kết nối lại vào mạng nội bộ.

- Tổng hợp nguyên nhân, báo cáo vụ việc cho cấp có thẩm quyền và đề xuất các giải pháp phòng chống.

4. Tình huống 4: Phát hiện trang/cổng thông tin điện tử bị các đối tượng chèn quảng cáo vi phạm pháp luật (backlink)

a) Công tác phòng ngừa:

- Đơn vị chủ quản hệ thống trang/cổng thông tin điện tử cần thường xuyên rà soát mã nguồn, nội dung HTML của website, đặc biệt là các khu vực footer,

header, sidebar hoặc trong các bài viết, thư mục chứa file HTML tĩnh để kịp thời phát hiện các liên kết lạ.

- Thiết lập cảnh báo đối với các trường hợp có thay đổi nội dung trang không qua hệ thống quản trị nội dung (CMS), như chèn mã JavaScript, iframe hoặc link lạ có nội dung quảng cáo, đánh bạc, cá độ, khiêu dâm, lôi kéo người dùng đến các website bất hợp pháp.

- Tăng cường sử dụng phần mềm kiểm tra toàn vẹn hệ thống (file integrity checker), các công cụ quét mã độc, phát hiện webshell, khai thác lỗ hổng phổ biến.

- Công an tỉnh phối hợp Sở Thông tin và Truyền thông tổ chức kiểm tra định kỳ hệ thống thông tin của các đơn vị, đồng thời tuyên truyền nhận diện thủ đoạn cài cắm backlink và hậu quả pháp lý liên quan.

b) Các bước xử lý hoạt động tấn công:

Bước 1: Khi cán bộ phụ trách CNTT hoặc người dùng phát hiện trên trang/cổng thông tin điện tử của đơn vị có hiển thị các liên kết quảng cáo bất thường, nội dung vi phạm pháp luật (liên quan đến cờ bạc, mại dâm, mua bán hàng giả, tín dụng đen, ...):

- Lập tức ghi nhận thông tin hiển thị, URL liên kết, mã nguồn liên quan (nếu có), chụp ảnh màn hình.

- Chủ động ngắt kết nối cập nhật nội dung từ máy chủ hoặc tạm thời đưa về trạng thái bảo trì.

- Báo cáo ngay tới đầu mối ứng cứu sự cố an toàn thông tin của tỉnh (Phòng An ninh mạng và phòng, chống tội phạm công nghệ cao, Công an tỉnh Hà Tĩnh).

Bước 2: Đầu mối ứng cứu sự cố thực hiện:

- Phối hợp đơn vị chủ quản hệ thống trích xuất log truy cập, log cập nhật nội dung để xác minh thời điểm chèn backlink, thông tin IP, tài khoản thao tác.

- Phân tích mã nguồn để xác định phương thức chèn: qua lỗ hổng plugin, mã độc webshell, lộ tài khoản quản trị...

- Hướng dẫn đơn vị chủ quản thực hiện khôi phục phiên bản sạch của hệ thống, cập nhật bảo mật và thay đổi toàn bộ thông tin tài khoản quản trị, mật khẩu máy chủ.

- Phối hợp đơn vị chủ quản hệ thống thông tin liên hệ Google để xóa bỏ quảng cáo trên công cụ tìm kiếm.

5. Tình huống 5: Rò rỉ tài khoản nội bộ qua tấn công phishing hoặc bị đánh cắp dữ liệu

a) Công tác phòng ngừa:

- Đơn vị chủ quản cần tổ chức tuyên truyền, nâng cao nhận thức cho cán bộ, công chức, viên chức về các hình thức tấn công lừa đảo qua email (phishing), tin nhắn giả mạo (smishing), hoặc các trang đăng nhập giả mạo (fake login page).

- Thiết lập xác thực đa yếu tố (MFA/2FA) cho các tài khoản truy cập hệ thống thông tin, tài khoản email công vụ, tài khoản quản trị hệ thống, nhằm giảm thiểu rủi ro khi bị lộ thông tin đăng nhập.

- Giới hạn quyền truy cập hệ thống theo nguyên tắc phân quyền tối thiểu, chỉ cấp tài khoản có quyền tương ứng với chức năng, nhiệm vụ.

- Định kỳ thay đổi mật khẩu truy cập, kiểm tra lịch sử đăng nhập từ các địa chỉ IP bất thường hoặc vùng địa lý không phù hợp.

- Công an tỉnh phối hợp Sở Thông tin và Truyền thông tổ chức huấn luyện kỹ năng nhận diện email giả mạo, liên kết độc hại và cách xử lý khi nghi ngờ bị tấn công.

b) Các bước xử lý khi phát hiện sự cố:

Bước 1: Khi cán bộ, nhân viên phát hiện: (1) Có email lạ yêu cầu cung cấp thông tin tài khoản, đổi mật khẩu qua liên kết không rõ nguồn gốc; (2) Có hiện tượng mất quyền truy cập tài khoản, bị thay đổi mật khẩu, hoặc phát hiện truy cập trái phép; (3) Có dữ liệu nội bộ bị tiết lộ, phát tán trái phép.

Cần lập tức ngắt kết nối internet (nếu nghi ngờ bị chiếm quyền điều khiển máy), báo ngay với cán bộ CNTT và đầu mối ứng cứu sự cố an toàn thông tin của tỉnh.

Bước 2: Đầu mối ứng cứu sự cố thực hiện:

- Phối hợp đơn vị chủ quản kiểm tra lịch sử đăng nhập của tài khoản nghi bị lộ, truy vết IP, thiết bị, thời gian truy cập bất thường.

- Hướng dẫn đơn vị chủ động vô hiệu hóa hoặc thay đổi thông tin đăng nhập toàn bộ các tài khoản có nguy cơ bị lộ.

- Phân tích các email nghi vấn, liên kết hoặc phần mềm độc hại đã được mở/cài đặt trong thời gian gần.

- Trong trường hợp có dấu hiệu phát tán dữ liệu nội bộ, phối hợp cơ quan chuyên môn thu thập chứng cứ, xử lý theo quy định của pháp luật.