BỘ CÔNG AN
CÔNG AN TỈNH ĐẮK NÔNG

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

Số: 466/CAT-PA05

Đắk Nông, ngày 09 tháng 4 năm 2024

V/v cảnh báo tình trạng tấn công mạng và phát tán mã độc

Kính gửi:
- Các Sở, ban, ngành tỉnh Đắk Nông;
- Ủy ban nhân dân các huyện, thành phố.

Thời gian qua, tình hình an ninh mạng trong nước diễn biến hết sức phức tạp, hoạt động tấn công mạng nhằm vào các hệ thống thông tin quan trọng gia tăng về tần suất và mức độ nguy hiểm, đặc biệt là hoạt động tấn công mạng bằng mã độc mã hóa dữ liệu đòi tiền chuộc *(Ransomware)* đã tấn công mạng, làm ngưng trệ nhiều hệ thống thông tin của các đơn vị, tổ chức, gây thiệt hại về kinh tế, ảnh hưởng đến an ninh quốc gia, trật tự xã hội *(về loại mã độc Ransomware, ngày 24/3/2023 Công an tỉnh đã ban hành Công văn số 493/CAT-PA05 về việc cảnh báo tình trạng lây lan mã độc và kiến nghị một số biện pháp bảo đảm an ninh an toàn thông tin đến các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố)*. Qua công tác giám sát mạng, Bộ Công an phát hiện nhiều hoạt động rà quét lỗ hổng bảo mật, tấn công mạng vào nhiều hệ thống Cơ sở dữ liệu quan trọng của các Bộ, ban, ngành *(trong đó có cả hệ thống Cơ sở dữ liệu quốc gia về dân cư, Hệ thống định danh và xác thực điện tử của Bộ Công an)* gây nguy cơ mất an ninh mạng, an toàn thông tin.

Trước diễn biến phức tạp của tình hình trên, để tăng cường công tác bảo đảm an ninh mạng, an toàn thông tin các hệ thống thông tin, Công an tỉnh thông báo, kiến nghị các Sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố triển khai một số mặt công tác sau:

1. Tăng cường giám sát an ninh, an toàn hệ thống mạng thông qua hệ thống giám sát, hệ thống phòng, chống mã độc tập trung để chủ động phát hiện sớm các hoạt động bất thường, hành vi tấn công mạng vào hệ thống.

2. Tổ chức rà soát đánh giá an ninh, an toàn thông tin tổng thể đối với hệ thống mạng, dịch vụ mạng, như: Rà soát, siết chặt chính sách truy cập trên các thiết bị bảo mật, bảo vệ mạng *(Firewall, IDS, IP...)* chỉ cho phép kết nối đến địa chỉ IP, cổng dịch vụ cần thiết; rà quét virus, mã độc trên các máy chủ, máy tính quản trị, máy tính người dùng; Rà soát, khắc phục lỗ hổng bảo mật cho các máy chủ, ứng dụng mạng, phần mềm nghiệp vụ, trong đó ưu tiên các hệ thống kết nối mạng Internet, hệ thống kết nối bên thứ 3; Thực hiện ngay việc sao lưu hệ thống, dữ liệu trên thiết bị lưu trữ độc lập hoặc giải pháp tương đương; Loại bỏ hoặc nâng cấp

các máy chủ đang sử dụng hệ điều hành không còn được hãng hỗ trợ cập nhật bản vá bảo mật; Thay đổi mật khẩu các tài khoản quản trị, tài khoản cán bộ…

3. Tạm ngừng chính sách truy cập từ xa *(VPN)* thực hiện các thao tác quản trị hệ thống, truy cập các hệ thống nội bộ. Trong trường hợp cần triển khai, cần rà soát, siết chặt chính sách; kích hoạt xác thực 02 lớp đối với kết nối VPN và đăng nhập tài khoản quản trị.

4. Rà soát loại bỏ các thiết bị, máy chủ, dịch vụ mạng và tài khoản trên các hệ thống thử nghiệm, hệ thống cũ hoặc không còn sử dụng.

5. Kiểm tra việc thực hiện các quy trình trong vận hành, quản trị hệ thống; giám sát sự kiện an ninh, an toàn thông tin; ứng cứu, khắc phục sự cố; sao lưu dự phòng hệ thống…

6. Kiểm soát, giám sát chặt chẽ nhà thầu, bên thứ 3 trong quá trình hỗ trợ kỹ thuật, cài đặt hệ thống.

Trong trường hợp phát hiện hoạt động tấn công mạng nghiêm trọng vào các hệ thống của đơn vị cần trao đổi về Công an tỉnh và Đội ứng cứu sự cố Tỉnh để phối hợp, hướng dẫn xử lý.

Đề nghị các đơn vị triển khai Kế hoạch phòng chống mã độc Ransomware và báo cáo kết quả về Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)* **trước ngày 03/5/2024**. Công an tỉnh cử đồng chí Đại úy Nguyễn Xuân Hải, Cán bộ Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, SĐT: 0946.6691213 làm đầu mối phối hợp.

Công an tỉnh thông báo đến các đơn vị biết phối hợp, thực hiện./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc (để báo cáo);
- Tiểu ban an toàn an ninh mạng;
- Phòng PV01 (để theo dõi);
- Lưu: VT, PA05 (Đ3).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Hồ Quang Thắng