SỞ Y TẾ NINH THUẬN

Số: 2931 /SY-SYT

SAO Y

Ninh Thuận, ngày 09 tháng 7 năm 2024

Nơi nhận:
- Lãnh đạo Sở;
- Các phòng chức năng sở;
- Các đơn vị trực thuộc;
- Website Sở;
- Lưu: VT, KHNVTC.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH NINH THUẬN

Bùi Văn Kỳ

UBND TỈNH NINH THUẬN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1914 /STTTT-TTCNTTTT

V/v triển khai các giải pháp tăng cường bảo đảm an toàn hệ thống thông tin

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

Ninh Thuận, ngày 08 tháng 7 năm 2024

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Hội đồng nhân dân;
- Văn phòng Ủy ban nhân dân tỉnh;
- UBMTTQVN và các tổ chức chính trị-xã hội;
- Các Sở, Ban, ngành thuộc tỉnh;
- Ủy ban nhân dân các huyện, thành phố;
- Các Thành ủy, Huyện ủy.

Tiếp nhận Công văn số 2675/VPUB-VXNV ngày 01/07/2024 của Ủy ban nhân dân tỉnh về việc Triển khai một số giải pháp tăng cường bảo đảm an toàn hệ thống thông tin.

Từ đầu năm 2024 đến nay, đã xảy ra một số sự cố an toàn thông tin mạng, đặc biệt là các sự cố tấn công mã độc mã hóa tống tiền (ransomware), gây thiệt hại và làm gián đoạn dịch vụ trực tuyến của các cơ quan, tổ chức, doanh nghiệp. Việc khắc phục và phục hồi sau sự cố an toàn thông tin mạng còn chậm và lúng túng.

Nguyên nhân chủ yếu là do chưa tuân thủ và triển khai đầy đủ các quy định bảo đảm an toàn thông tin mạng, điển hình là: Không có bản sao lưu dữ liệu ngoại tuyến "offline", không có hoặc có kế hoạch khôi phục nhanh sau sự cố nhưng không phù hợp, để xảy ra sự cố do những lỗi cơ bản; chưa triển khai phần mềm chống mã độc trên các máy chủ quan trọng, chưa giám sát an toàn thông tin mạng (SOC) đầy đủ để kịp thời phát hiện bất thường trong hệ thống.

Để tăng cường hiệu quả công tác bảo đảm an toàn thông tin và phục hồi nhanh hoạt động sau sự cố, bên cạnh việc triển khai đầy đủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, Sở Thông tin và Truyền thông hướng dẫn triển khai 06 giải pháp trọng tâm sau:

1. Các cơ quan định kỳ thực hiện sao lưu dữ liệu ngoại tuyến "offline". Với chiến lược sao lưu dữ liệu theo nguyên tắc 3-2-1: Có ít nhất 03 bản sao dữ liệu, lưu trữ bản sao trên 02 phương tiện lưu trữ khác nhau, với 01 bản sao lưu ngoại tuyến "offline" (sử dụng tape/USB/ổ cứng di động...). Dữ liệu sao lưu offline phải được tách biệt hoàn toàn, không kết nối mạng, cô lập để phòng, chống tấn công leo thang vào hệ thống lưu trữ.

2. Triển khai giải pháp để sẵn sàng phục hồi nhanh hoạt động của hệ thống thông tin khi gặp sự cố, đưa hoạt động của hệ thống thông tin trở lại bình thường trong vòng 24 giờ hoặc theo yêu cầu nghiệp vụ.

3. Triển khai các giải pháp, đặc biệt là giải pháp giám sát an toàn thông tin, để ngăn ngừa, kịp thời phát hiện sớm nguy cơ tấn công mạng đối với cả 03 giai đoạn: Xâm nhập vào hệ thống; nằm gián điệp trong hệ thống; khởi tạo quá trình phá hoại hệ thống.

4. Phân tách, kiểm soát truy cập giữa các vùng mạng và chuyển đổi, nâng cấp các ứng dụng, giao thức, kết nối lạc hậu, không còn được hỗ trợ kỹ thuật sang phương án sử dụng các nền tảng, ứng dụng (app) để giảm thiểu nguy cơ tấn công mạng leo thang vào hệ thống thông tin thông qua máy tính, thiết bị đầu cuối của người dùng.

5. Tăng cường giám sát, quản lý các tài khoản quan trọng, tài khoản quản trị hệ thống bằng giải pháp xác thực 02 lớp (OTP...) hoặc giải pháp quản lý tài khoản đặc quyền (PIM/PAM) nhằm phòng ngừa, giảm thiểu thiệt hại trong trường hợp kẻ tấn công chiếm được mật khẩu của tài khoản quản trị.

6. Rà soát, cập nhật thường xuyên các bản vá bảo mật của hệ điều hành được cảnh báo từ các cơ quan chức năng, thay đổi mật khẩu quản trị định kỳ; sử dụng mật khẩu có độ dài từ 8 ký tự trở lên, chữ thường, chữ hoa, số và ký tự đặc biệt.

Trường hợp cần hướng dẫn, hỗ trợ và điều phối xử lý, ứng cứu sự cố an toàn thông tin mạng, các cơ quan, đơn vị có thể liên hệ qua các đầu mối:

Trung tâm Giám sát an toàn, an ninh, thông tin mạng qua tổng đài 1022, thư điện tử ioc@ninhthuan.gov.vn.

Phòng An toàn hệ thống thông tin, Cục An toàn thông tin, Bộ TT-TT, số điện thoại 0869.100.319, thư điện tử athttt@mic.gov.vn để được hướng dẫn.

Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), Cục An toàn thông tin, Bộ TT-TT, điện thoại 024.3640.4421 hoặc số điện thoại trực đường dây nóng ứng cứu sự cố 086.9100.317, thư điện tử: ir@vncert.vn.

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, Bộ TT-TT, điện thoại: 024.3209.1616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 038.9942.878.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Lãnh đạo STTTT;
- Lưu: VT, TTCNTTTT.

GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Đào Xuân Kỳ