SAO Y Ký bởi: Ủy ban nhân dân tỉnh Đồng Nai
Cơ quan:
Thời gian ký: 05.09.2025 22:39:18 +07:00

ỦY BAN NHÂN DÂN TỈNH ĐỒNG NAI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 79 /KH-UBND	*Đồng Nai, ngày 05 tháng 9 năm 2025*

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Đồng Nai

Thực hiện Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Nghị quyết số 71/NQ-CP ngày 01/4/2025 của Chính phủ sửa đổi, bổ sung cập nhật chương trình hành động của Chính phủ thực hiện Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia.

Chủ tịch Ủy ban nhân dân tỉnh Đồng Nai ban hành Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin (ATTT) mạng trên địa bàn tỉnh như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng trên địa bàn tỉnh; bảo đảm khả năng thích ứng chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất ATTT trên mạng; kịp thời khắc phục các tồn tại, lỗ hổng, điểm yếu nhằm phòng ngừa các sự cố tấn công mạng; đề ra các giải pháp ứng phó khi gặp sự cố mất ATTT mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về ATTT đối với cán bộ, công chức, viên chức trong các cơ quan nhà nước trên địa bàn tỉnh.

- Xây dựng, phát triển Đội ứng cứu sự cố ATTT mạng có đầy đủ kiến thức, kỹ năng xử lý sự cố ATTT mạng đảm bảo linh hoạt, hiệu quả, phù hợp với yêu cầu thực tế.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố ATTT mạng.

2. Yêu cầu

- Các hệ thống thông tin của các cơ quan, đơn vị, địa phương phải được đánh giá hiện trạng và khả năng bảo đảm ATTT mạng, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra để đưa ra phương án ứng phó, ứng cứu sự cố kịp thời, phù hợp.

Địa chỉ: Số 02, đường Nguyễn Văn Trị, phường Trấn Biên, tỉnh Đồng Nai.
SĐT: (0251) 3822500 – FAX: (0251) 3823854 – 3824934

- Hoạt động ứng cứu sự cố ATTT mạng phải chuyển từ bị động sang chủ động, bao gồm: chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý.

- Xác định cụ thể các nguồn lực, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, bảo đảm khả thi, hiệu quả.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác bảo đảm ATTT giữa các cơ quan nhà nước trên địa bàn tỉnh; tận dụng sự phối hợp, hỗ trợ của cơ quan điều phối quốc gia về ứng cứu sự cố (Trung tâm An ninh mạng quốc gia - Bộ Công an).

II. CÁC QUY ĐỊNH CHUNG

1. Phạm vi và đối tượng

Kế hoạch này để ứng phó sự cố, bảo đảm ATTT mạng đối với các hệ thống thông tin của tỉnh, áp dụng cho các sở, ban, ngành, đoàn thể tỉnh; UBND các xã, phường; các cơ quan, đơn vị, doanh nghiệp có liên quan (gọi tắt là cơ quan, đơn vị).

2. Nguyên tắc, phương châm ứng phó sự cố

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố ATTT mạng.

- Chủ động, kịp thời, nhanh chóng, chính xác; phối hợp chặt chẽ, đồng bộ và hiệu quả giữa các cơ quan, đơn vị.

- Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

- Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

- Bảo đảm bí mật thông tin khi tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của cơ quan điều phối quốc gia hoặc cơ quan, tổ chức, cá nhân gặp sự cố.

3. Các lực lượng tham gia ứng phó sự cố

- Các sở, ban, ngành, đoàn thể tỉnh; UBND các xã, phường; các cơ quan, đơn vị, doanh nghiệp có liên quan.

- Đội ứng cứu sự cố ATTT mạng của tỉnh (lực lượng chính ứng phó sự cố, trong đó Công an tỉnh là Cơ quan Thường trực).

- Chủ quản hệ thống thông tin; đơn vị quản lý, vận hành hệ thống thông tin.

- Trung tâm Khoa học và Công nghệ thuộc Sở Khoa học và Công nghệ (đơn vị vận hành Trung tâm tích hợp dữ liệu tỉnh).

- Doanh nghiệp cung cấp dịch vụ viễn thông Internet (VNPT, Viettel, FPT, Mobifone…).

- Doanh nghiệp cung cấp dịch vụ ATTT mạng (trường hợp thuê dịch vụ).

- Trong trường hợp cần thiết, mời các cơ quan Trung ương có chức năng về ứng cứu sự cố cùng tham gia.

4. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các cơ quan, đơn vị

- Công an tỉnh Đồng Nai là đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh; thực hiện chỉ đạo, tổ chức triển khai hoạt động ứng phó sự cố ATTT mạng và các nhiệm vụ khác khi xảy ra sự cố.

- Đội ứng cứu sự cố ATTT mạng của tỉnh là lực lượng chính tham gia các hoạt động ứng cứu sự cố ATTT mạng; thực hiện nhiệm vụ theo Quy chế hoạt động của Đội; tham gia hoạt động ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia khi có yêu cầu từ Bộ Công an hoặc các bộ, ngành có liên quan.

- Trung tâm Khoa học và Công nghệ (trực thuộc Sở Khoa học và Công nghệ) chịu trách nhiệm xây dựng, thực thi các quy định về an toàn bảo mật thông tin mạng, quản lý, khai thác và vận hành Trung tâm tích hợp Dữ liệu; tham gia Đội ứng cứu sự cố ATTT mạng của tỉnh, xử lý, ứng cứu các sự cố về ATTT, an ninh mạng xảy ra trên địa bàn tỉnh Đồng Nai khi có yêu cầu của đơn vị điều phối.

- Các sở, ban, ngành, cơ quan, đơn vị, UBND các xã, phường: có trách nhiệm cử cán bộ, công chức, viên chức phụ trách ATTT tham gia Đội ứng cứu sự cố ATTT mạng của tỉnh khi xử lý sự cố. Phối hợp với đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh trong công tác ứng phó, xử lý các sự cố.

- Doanh nghiệp cung cấp, xây dựng các hệ thống thông tin: Phối hợp với Công an tỉnh, chủ quản hệ thống thông tin, đơn vị quản lý, vận hành hệ thống thông tin trong công tác ứng phó, xử lý các sự cố ATTT liên quan hệ thống thông tin do mình xây dựng hoặc cung cấp.

- Doanh nghiệp cung cấp dịch vụ viễn thông Internet: Phối hợp với Công an tỉnh, chủ quản hệ thống thông tin, đơn vị quản lý, vận hành hệ thống thông tin trong công tác ứng phó, xử lý các sự cố ATTT liên quan đến hạ tầng viễn thông, dịch vụ Internet do mình cung cấp hoặc quản lý.

III. NỘI DUNG THỰC HIỆN

1. Đánh giá các nguy cơ, sự cố ATTT mạng

a) Đánh giá hiện trạng và khả năng bảo đảm ATTT mạng của hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (bao gồm cả đơn vị cung cấp dịch vụ nếu có).

- Đơn vị chủ trì: Đơn vị quản lý, vận hành hệ thống thông tin.

- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu sự cố ATTT mạng của tỉnh; Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ); các doanh nghiệp cung cấp dịch vụ viễn thông, Internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (trường hợp thuê dịch vụ) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

b) Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý; khắc phục các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng (thực hiện theo quy định tại Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ).

- Đơn vị chủ trì: Đơn vị quản lý, vận hành hệ thống thông tin.

- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu sự cố ATTT mạng của tỉnh; Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ); các doanh nghiệp cung cấp dịch vụ viễn thông, Internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: hàng năm (tối thiểu 01 lần/06 tháng).

2. Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

Đối với mỗi hệ thống thông tin, chương trình ứng dụng, cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố và tuân thủ theo các quy định, hướng dẫn, đảm bảo các nội dung sau:

a) Quy trình triển khai và các bước ưu tiên ứng cứu ban đầu khi hệ thống thông tin gặp sự cố, có phân theo các loại sự cố thực hiện theo mục 3, Phần III Kế hoạch. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố tại Kế hoạch.

b) Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp. Các sự cố thường gặp:

- Sự cố do bị tấn công mạng.

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting...

- Sự cố do lỗi của người quản trị, vận hành hệ thống.

- Sự cố do lỗi từ người dùng cuối trong quá trình khai thác, sử dụng hệ thống.

- Sự cố liên quan đến các thiên tai, thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

c) Phương án đối phó, khắc phục sự cố đối với một hoặc nhiều tình huống.

- Tình huống sự cố do bị tấn công mạng:

+ Tấn công từ chối dịch vụ;

+ Tấn công giả mạo;

+ Tấn công sử dụng mã độc;

+ Tấn công truy cập trái phép, chiếm quyền điều khiển;

+ Tấn công thay đổi giao diện;

+ Tấn công mã hóa phần mềm, dữ liệu, thiết bị;

+ Tấn công phá hoại thông tin, dữ liệu, phần mềm;

+ Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;

+ Tấn công tổng hợp sử dụng kết hợp nhiều hình thức;

+ Các hình thức tấn công mạng khác.

- Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật:

+ Sự cố nguồn điện;

+ Sự cố đường kết nối Internet;

+ Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;

+ Sự cố liên quan đến quá tải hệ thống;

+ Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống:

+ Lỗi trong cập nhật, thay đổi, cấu hình phần cứng;

+ Lỗi trong cập nhật, thay đổi, cấu hình phần mềm;

+ Lỗi liên quan đến chính sách và thủ tục ATTT;

+ Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc;

+ Lỗi khác liên quan đến người quản trị, vận hành hệ thống.

- Tình huống sự cố do lỗi từ người dùng cuối trong quá trình khai thác, sử dụng hệ thống:

+ Chia sẻ thông tin, sử dụng chung tài khoản sai quy định.

+ Lưu mật khẩu mặc định trên trình duyệt, làm lộ, mất thông tin đăng nhập.

+ Không tuân thủ quy trình, quy chế, chính sách ATTT đã ban hành.

- Tình huống sự cố liên quan đến các thiên tai, thảm họa tự nhiên, như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

d) Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, các tổ chức trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.

- Đơn vị chủ trì: Công an tỉnh.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia Trung tâm An ninh mạng quốc gia; các sở, ban, ngành, đoàn thể tỉnh; UBND các xã, phường; Đội ứng cứu sự cố ATTT mạng của tỉnh; Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ); các doanh nghiệp cung cấp dịch vụ viễn thông, Internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên hàng năm.

đ) Phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ, và dự kiến kinh phí để thực hiện, đối phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể.

- Đơn vị chủ trì: Các sở, ban, ngành, đoàn thể tỉnh; UBND các xã, phường.

- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu sự cố ATTT mạng của tỉnh; Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ); các doanh

nghiệp cung cấp dịch vụ viễn thông, Internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên hàng năm.

3. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố

a) Báo cáo sự cố ATTT mạng

- Đơn vị thực hiện:

Đơn vị quản lý, vận hành hệ thống thông tin báo cáo cơ quan chủ quản hệ thống thông tin, Công an tỉnh, Đội ứng cứu sự cố ATTT mạng của tỉnh, đồng gửi Cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia).

- Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

b) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng.

- Đơn vị chủ trì: Công an tỉnh; đơn vị quản lý, vận hành hệ thống thông tin (các cơ quan, đơn vị); Đội ứng cứu sự cố ATTT mạng của tỉnh; Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ).

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia); tổ chức, cá nhân gửi thông báo, báo cáo sự cố; các doanh nghiệp cung cấp dịch vụ viễn thông, Internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có); các cơ quan, đơn vị chức năng liên quan.

- Thời gian thực hiện: Ngay sau khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố của tổ chức, cá nhân.

c) Quy trình ứng cứu sự cố ATTT mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14, Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ và Điều 11, Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) ***(Sơ đồ tại phụ lục kèm theo Kế hoạch)***.

- Đơn vị chủ trì: Công an tỉnh.

- Đơn vị phối hợp: Các sở, ban, ngành, đoàn thể tỉnh; UBND các xã, phường; đơn vị quản lý, vận hành hệ thống thông tin; Đội ứng cứu sự cố ATTT mạng của tỉnh; Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ).

- Thời gian thực hiện: Hàng năm.

4. Triển khai đào tạo, huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố. Đồng thời cần đáp ứng đúng theo quy định tại Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ Thông tin và Truyền thông (nay là

Bộ Khoa học và Công nghệ) về việc tổ chức triển khai diễn tập thực chiến bảo đảm ATTT mạng, bao gồm:

a) Triển khai các lớp đào tạo, nâng cao nhận thức.

Xây dựng kế hoạch đào tạo, tập huấn, nâng cao nhận thức về ATTT cho các đối tượng: cán bộ lãnh đạo quản lý, cán bộ kỹ thuật chuyên sâu và người dùng cuối về kỹ năng điều tra, phân tích mã độc, xử lý sự cố.

- Đơn vị chủ trì: Công an tỉnh.

- Đơn vị phối hợp: Các sở, ban, ngành, đoàn thể tỉnh; UBND các xã, phường; các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

b) Triển khai các chương trình huấn luyện, diễn tập.

Tổ chức diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; huấn luyện, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố; tham gia huấn luyện, diễn tập vùng, miền, quốc gia, quốc tế.

- Đơn vị chủ trì: Công an tỉnh; Đội ứng cứu sự cố ATTT của tỉnh.

- Đơn vị phối hợp: Đơn vị quản lý, vận hành hệ thống thông tin, Cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia); các doanh nghiệp cung cấp dịch vụ viễn thông, Internet; doanh nghiệp cung cấp dịch vụ ATTT (nếu có); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

c) Triển khai nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố.

Thực hiện nghiêm công tác giám sát, phát hiện sớm nguy cơ, sự cố; kiểm tra, đánh giá ATTT mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc; phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro ATTT mạng, phần mềm độc hại; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn ATTT; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Đơn vị chủ trì: Công an tỉnh; đơn vị quản lý, vận hành hệ thống thông tin; Đội ứng cứu sự cố ATTT mạng của tỉnh; Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ).

- Đơn vị phối hợp: cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Thường xuyên, hàng năm.

d) Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố.

Mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng nhân lực, vật lực, tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của Đội ứng cứu sự cố, bộ phận ứng cứu sự cố;

thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- Đơn vị chủ trì: Công an tỉnh; các sở, ban, ngành, đoàn thể tỉnh; UBND các xã, phường.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

IV. KINH PHÍ THỰC HIỆN

Nguồn kinh phí thực hiện Kế hoạch được bố trí từ nguồn ngân sách nhà nước theo phân cấp ngân sách hiện hành; lồng ghép với kinh phí thực hiện các chương trình, kế hoạch, đề án khác có liên quan và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

V. PHÂN CÔNG NHIỆM VỤ

1. Các sở, ban, ngành, đoàn thể tỉnh, UBND các xã, phường

- Phân công lãnh đạo phụ trách, thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về ATTT mạng tại cơ quan, đơn vị, địa phương theo thẩm quyền quản lý.

- Thực hiện bố trí cán bộ, công chức, viên chức chuyên trách về ATTT mạng tại cơ quan, đơn vị, địa phương; kịp thời thông báo về Công an tỉnh khi có sự thay đổi cán bộ, công chức, viên chức chuyên trách về ATTT mạng tại cơ quan, đơn vị hoặc đang là thành viên tham gia Đội ứng cứu sự cố ATTT mạng của tỉnh.

- Xây dựng nội dung, lập dự toán kinh phí thực hiện các nhiệm vụ về ứng phó sự cố, bảo đảm ATTT mạng của cơ quan, đơn vị, địa phương.

- Thực hiện đánh giá, xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Định kỳ 06 tháng và hàng năm hoặc đột xuất, báo cáo tình hình ứng phó sự cố, bảo đảm ATTT mạng tại cơ quan, đơn vị, địa phương về Công an tỉnh để tổng hợp báo cáo các cơ quan cấp trên theo quy định.

- Cử cán bộ tham gia các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn về ứng cứu sự cố, bảo đảm ATTT mạng để nâng cao kỹ năng và công tác tham mưu, triển khai giám sát, bảo đảm ATTT mạng.

- Triển khai tổ chức tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn, các hoạt động liên quan đến đảm bảo ATTT mạng của tỉnh, của cơ quan đơn vị trên Trang thông tin điện tử, các phương tiện thông tin đại chúng: nội dung của Luật An toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP; Thông tư số 12/2022/TT-BTTTT; các Công điện, Chỉ thị của Thủ tướng Chính phủ và các Chỉ thị, văn bản của Bộ Công an, Bộ Khoa học và Công nghệ.

- Tích cực phối hợp với cơ quan, đơn vị chủ trì thực hiện các nhiệm vụ được giao theo Kế hoạch này.

2. Công an tỉnh

- Là cơ quan đầu mối, chuyên trách về ứng cứu sự cố ATTT mạng trên địa bàn tỉnh, có trách nhiệm xây dựng và triển khai Kế hoạch này; tổ chức theo dõi, đôn đốc, phối hợp với các sở, ban, ngành, UBND các xã, phường trong việc triển khai thực hiện Kế hoạch. Định kỳ 06 tháng, hàng năm hoặc đột xuất tổng hợp báo cáo kết quả thực hiện gửi UBND tỉnh, Trung tâm An ninh mạng quốc gia để theo dõi, chỉ đạo.

- Hàng năm tham mưu UBND tỉnh ban hành quyết định kiện toàn Đội ứng cứu sự cố ATTT mạng cho phù hợp với tình hình đảm bảo ATTT trên địa bàn tỉnh Đồng Nai.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát, hướng dẫn công tác bảo đảm ATTT định kỳ hàng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước, doanh nghiệp trên địa bàn tỉnh. Tiến hành xử lý theo quy định của pháp luật các cá nhân, cơ quan vi phạm trong công tác bảo đảm ATTT mạng.

- Thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ ATTT thông tin theo thẩm quyền quy định tại Nghị định số 85/2016/NĐ-CP và theo hướng dẫn tại Thông tư số 12/2022/TT-BTTTT *(Công an tỉnh đã có hướng dẫn gửi các đơn vị, địa phương)*.

- Xây dựng nội dung, lập dự toán kinh phí bảo đảm cho hoạt động của Đơn vị chuyên trách ứng cứu sự cố và Đội ứng cứu sự cố ATTT mạng của tỉnh.

3. Sở Khoa học và Công nghệ

- Tổ chức triển khai, xây dựng, quản lý, vận hành hạ tầng mạng, trung tâm dữ liệu, hạ tầng, nền tảng, cơ sở dữ liệu dùng chung, phục vụ chuyển đổi số, ứng dụng công nghệ thông tin; phối hợp Công an tỉnh trong thực hiện công tác đảm bảo ATTT đối với hệ thống thông tin tập trung, dùng chung của tỉnh Đồng Nai.

- Cử cán bộ có trình độ, kinh nghiệm tham gia xử lý, ứng cứu các sự cố về ATTT, an ninh mạng xảy ra trên địa bàn tỉnh Đồng Nai khi có yêu cầu của đơn vị điều phối.

- Tiếp tục giám sát ATTT đối với hệ thống thông tin tại Trung tâm tích hợp dữ liệu. Trao đổi kịp thời cho Công an tỉnh mọi thông tin liên quan đến các sự cố gây mất an ninh mạng, ATTT đối với hệ thống thông tin tập trung, dùng chung của tỉnh.

- Phối hợp Công an tỉnh Đồng Nai phát huy thế mạnh về truyền thông cũng như các hệ thống thông tin sẵn có (Fanpage, Email, Trang/Cổng thông tin điện tử...) phục vụ triển khai hiệu quả công tác tuyên truyền, phổ biến pháp luật về ATTT, an ninh mạng.

4. Sở Tài chính

- Căn cứ khả năng cân đối ngân sách tỉnh, chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tham mưu UBND tỉnh bố trí kinh phí chi thường xuyên để thực hiện Kế hoạch theo quy định của Luật Ngân sách nhà nước và các văn bản hướng dẫn có liên quan.

- Thực hiện việc rà soát, kiểm tra, hướng dẫn thực hiện nhiệm vụ, dự án hoặc các chương trình, kế hoạch hàng năm của tỉnh về công tác ứng phó sự cố, bảo đảm ATTT mạng có sử dụng nguồn đầu tư công theo đúng quy định pháp luật.

VI. TỔ CHỨC THỰC HIỆN

1. Căn cứ nội dung Kế hoạch này và tình hình thực tế, các cơ quan, đơn vị, địa phương xây dựng kế hoạch Ứng phó sự cố, bảo đảm ATTT mạng theo thẩm quyền quản lý và tổ chức triển khai các nhiệm vụ về ứng phó sự cố, bảo đảm ATTT mạng theo đúng tiến độ, chất lượng, hiệu quả.

2. Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương kịp thời trao đổi, phối hợp Công an tỉnh (qua Phòng an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để tổng hợp, hướng dẫn xử lý theo thẩm quyền hoặc báo cáo, đề xuất UBND tỉnh chỉ đạo, giải quyết theo quy định./.

Nơi nhận:
- Cục A05 - Bộ Công an;
- Chủ tịch, các PCT UBND tỉnh;
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Các cơ quan ngành dọc trên địa bàn tỉnh;
- Các sở, ban, ngành;
- Chánh, các phó CVP UBND tỉnh;
- UBND các xã, phường;
- Các Doanh nghiệp cung cấp dịch vụ viễn thông, Internet trên địa bàn tỉnh;
- Lưu: VT, KGVX, HCTC, NC.

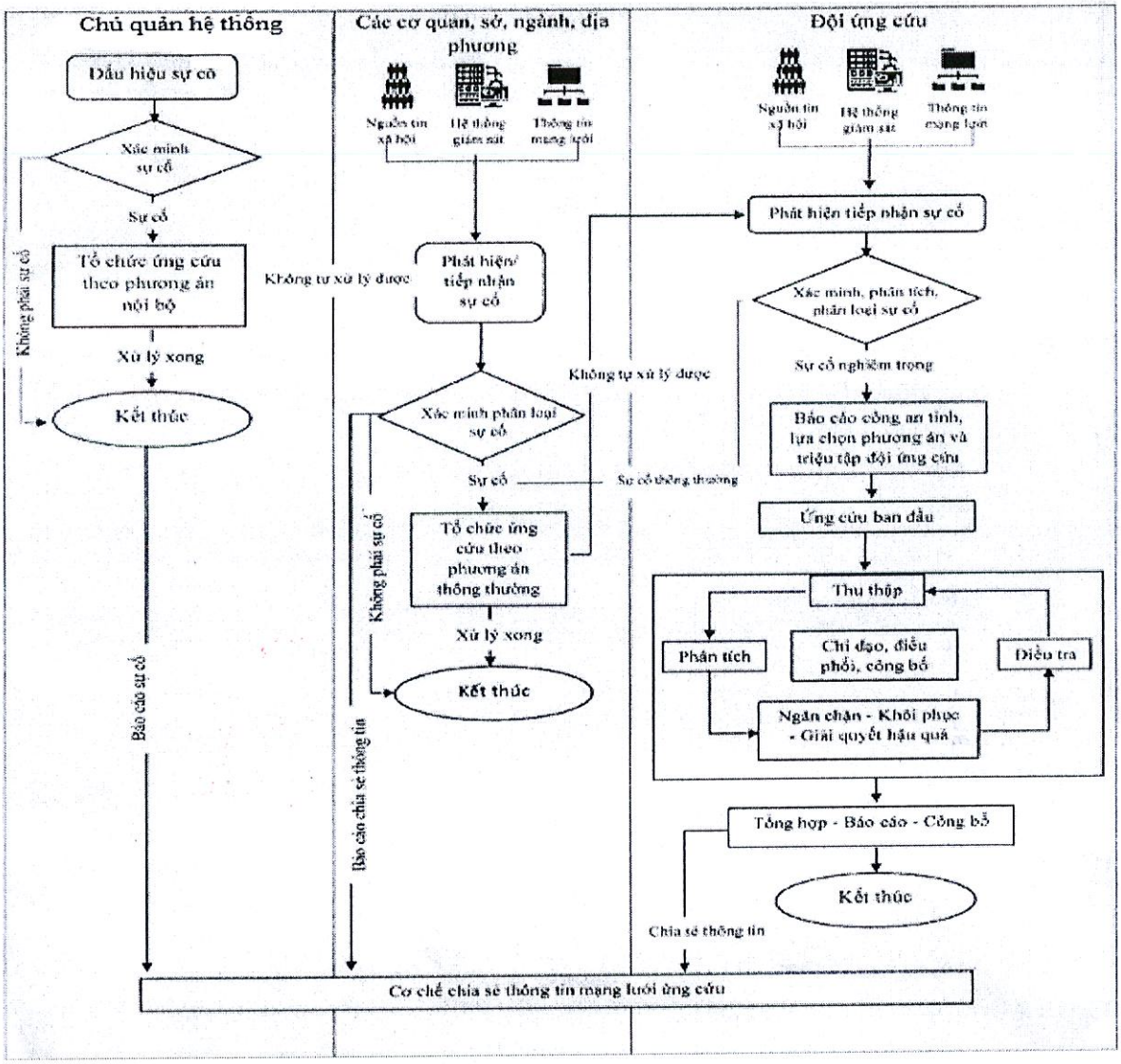
CHỦ TỊCH

Võ Tấn Đức

PHỤ LỤC

Quy trình tổng thể hệ thống phương án ứng cứu sự cố an toàn thông tin mạng đối với chủ quản hệ thống thông tin quan trọng cấp sở, ban, ngành, địa phương

(Ban hành kèm theo Kế hoạch số 79 /KH-UBND ngày 05/9/2025 của UBND tỉnh Đồng Nai)



I. TỔ CHỨC ỨNG CỨU SỰ CỐ CẤP TỈNH

1. Đội ứng cứu sự cố An toàn thông tin cấp tỉnh (Đội UCSC)

- Đội trưởng: Phó Giám đốc Công an tỉnh Đồng Nai.

- Thành viên:

+ Các sở, ban, ngành trực thuộc tỉnh.

+ Các cơ quan ngành dọc trên địa bàn tỉnh.

+ UBND các xã/phường.

+ Các trường đại học, cao đẳng, học viện tại địa bàn.

+ Đại diện các doanh nghiệp viễn thông đang triển khai dịch vụ trong tỉnh.

+ Đại diện Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ).

+ Cán bộ kỹ thuật an toàn thông tin (do các đơn vị giới thiệu).

- Thường trực Đội UCSC cấp tỉnh: Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh), cử cán bộ chuyên trách là Thư ký Đội UCSC và làm đầu mối điều phối.

2. Nhiệm vụ Đội UCSC cấp tỉnh

- Công an tỉnh (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao): Chủ trì điều phối, có quyền yêu cầu hỗ trợ từ các đơn vị và doanh nghiệp trong tỉnh.

- Các sở, ngành, địa phương: Phối hợp cung cấp thông tin, hỗ trợ điều tra.

- Các trường Đại hoc: Hỗ trợ kỹ thuật, giảng viên chuyên ngành làm lực lượng hỗ trợ ứng cứu khi cần.

- Các doanh nghiệp viễn thông: Đảm bảo kết nối, hỗ trợ truy vết, phân tích mạng.

- Tổng đài hỗ trợ 24/7: Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* cử cán bộ túc trực nhận báo cáo sự cố - Số điện thoại: 02513.685.134.

- Điều phối lực lượng và nguồn lực kỹ thuật UCSC trên toàn tỉnh;

- Đề xuất phương án kỹ thuật, phối hợp điều tra số, giám định và phục hồi hệ thống;

- Triệu tập đội phản ứng nhanh, hỗ trợ khẩn cấp cho đơn vị bị tấn công;

- Báo cáo định kỳ hoặc khẩn cấp về Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (Bộ Công an) và Trung tâm điều hành quốc gia.

II. TỔ ỨNG CỨU SỰ CỐ CẤP ĐƠN VỊ

1. Mỗi sở, ban, ngành, cơ quan, đơn vị, trường học, UBND các xã, phường… trước mắt phân công ít nhất 01 cán bộ, công chức, viên chức chuyên trách về ATTT làm đầu mối phối hợp xử lý sự cố, sau khi đơn vị được bổ sung nhân sự về công nghệ thông tin/an toàn thông tin phải thành lập Tổ/Đội UCSC nội bộ, gồm các thành viên sau:

- 01 đầu mối điều phối;

- 01 cán bộ kỹ thuật (công nghệ thông tin/an toàn thông tin);

- 01 cán bộ phụ trách quản lý hệ thống/ứng dụng.

2. Trách nhiệm:

- Phát hiện, xử lý ban đầu các sự cố;

- Báo cáo kịp thời về Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* khi vượt quá khả năng xử lý;

- Tham gia phối hợp ứng cứu, khắc phục, thu thập dữ liệu phục vụ điều tra.

III. QUY TRÌNH ỨNG CỨU SỰ CỐ

1. Bước 1. Phát hiện và báo cáo

- Ngay khi phát hiện sự cố, đơn vị phải:

- Báo cáo về Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* chậm nhất 24 giờ (qua Email, Hotline, hoặc Cổng báo cáo chính thức);

- Báo cáo ban đầu phải gồm: đơn vị, thời gian, biểu hiện sự cố, mức độ ảnh hưởng, đầu mối liên hệ, biện pháp đã thực hiện.

2. Bước 2. Ứng phó ban đầu

- Cô lập hệ thống bị tấn công, không tắt nguồn;

- Thu thập log, dữ liệu RAM, ổ đĩa, IP truy cập;

- Khôi phục từ bản sao lưu sạch nếu cần thiết.

3. Bước 3. Phân loại sự cố

- Mức 1: Cục bộ, không ảnh hưởng nghiêm trọng – đơn vị xử lý nội bộ, báo cáo tổng kết.

- Mức 2: Ảnh hưởng một phần, nghi ngờ mã độc/lộ lọt – phối hợp với Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* điều tra, phục hồi.

- Mức 3: Tấn công có chủ đích, lộ tài liệu mật, lan rộng – Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* điều phối toàn diện, có thể huy động doanh nghiệp ATTT hỗ trợ.

4. Bước 4. Điều tra và thu thập dữ liệu

- Thực hiện pháp y số theo yêu cầu của Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)*;

- Giữ nguyên hiện trạng hệ thống đến khi có chỉ đạo;

- Phối hợp xử lý đúng quy định về bảo vệ dữ liệu cá nhân, tài liệu mật.

5. Bước 5. Làm sạch và phục hồi

- Gỡ mã độc, vá lỗ hổng, thay đổi mật khẩu/tài khoản bị xâm nhập;

- Kiểm tra hệ thống phục hồi trước khi vận hành lại.

6. Bước 6. Báo cáo hoàn tất và rút kinh nghiệm

- Báo cáo kết thúc gửi về Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* và lưu trữ tối thiểu 03 năm;

- Đơn vị bị sự cố phải tổ chức họp rút kinh nghiệm, cập nhật quy trình nội bộ.

IV. CƠ CHẾ PHỐI HỢP

1. Công an tỉnh *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)*: Chủ trì điều phối, có quyền yêu cầu hỗ trợ từ các đơn vị và doanh nghiệp trong tỉnh.

2. Các sở, ban, ngành, địa phương: Phối hợp cung cấp thông tin, hỗ trợ điều tra.

3. Các trường Đại học: Hỗ trợ kỹ thuật, giảng viên chuyên ngành làm lực lượng hỗ trợ ứng cứu khi cần.

4. Các doanh nghiệp viễn thông: Đảm bảo kết nối, hỗ trợ truy vết, phân tích mạng.

5. Tổng đài hỗ trợ 24/7: Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* cử cán bộ túc trực nhận báo cáo sự cố - Số điện thoại: 02513.685.134.

V. KỊCH BẢN ỨNG PHÓ SỰ CỐ CỤ THỂ

KỊCH BẢN 1*: Tấn công mã độc tống tiền (Ransomware) vào hệ thống tài chính – kế toán tại Sở Tài chính*

1. Tình huống giả định: *Ngày X, nhân viên kế toán tại Sở Tài chính phát hiện không thể mở tệp dữ liệu kế toán. Tất cả File có phần mở rộng lạ, hiển thị thông báo yêu cầu trả tiền chuộc bằng tiền điện tử để khôi phục dữ liệu.*

2. Hành động cấp tốc

- Tổ UCSC nội bộ ngắt kết nối toàn bộ máy tính khỏi mạng LAN/Internet.

- Không tắt máy, giữ nguyên trạng thái máy bị nhiễm để phân tích pháp y.

- Báo cáo ngay về Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* qua Hotline và Email.

3. Vai trò các đơn vị

- Sở Tài chính: Cung cấp toàn bộ log, nhật ký hệ thống, lịch sử kết nối USB/Email.

- Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* : Cử Tổ kỹ thuật xuống trực tiếp phân tích pháp y số, cô lập lây nhiễm.

- Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ): Đánh giá mức độ lây nhiễm qua hệ thống mạng chung, hỗ trợ phục hồi hạ tầng.

- Doanh nghiệp ATTT (nếu huy động): Gỡ mã độc, khôi phục dữ liệu từ bản sao lưu an toàn.

4. Biện pháp khắc phục

- Cách ly hoàn toàn hệ thống nhiễm độc.

- Phục hồi hệ thống từ bản sao lưu "sạch" có kiểm tra tính toàn vẹn.

- Tổ chức diễn tập, đào tạo lại cho người dùng, rà soát chính sách bảo mật.

5. Báo cáo và hậu kiểm

- Gửi báo cáo hoàn chỉnh trong vòng 05 ngày, gồm: phân tích nguyên nhân, lỗ hổng, thiệt hại, hướng khắc phục lâu dài.

KỊCH BẢN 2*: Tấn công làm thay đổi giao diện (Deface) Cổng thông tin điện tử của các sở, ban, ngành, UBND xã, phường.*

1. Tình huống giả định: *Người dân phản ánh Website đơn vị A hiển thị nội dung phản cảm, hình ảnh chống phá Nhà nước.*

2. Hành động cấp tốc

- Tổ CNTT của đơn vị A ngắt kết nối website, kiểm tra máy chủ.

- Gửi báo cáo khẩn về Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* trong vòng 01 giờ kể từ phát hiện.

- Lưu giữ bản sao toàn bộ File Website bị thay đổi.

3. Vai trò các đơn vị

- Đơn vị A: Cung cấp mã nguồn, tài khoản quản trị bị xâm nhập.

- Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)*: Điều tra IP, cách thức tấn công (webshell, SQLi…).

- Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ): Khôi phục giao diện, thiết lập lại trạng thái ban đầu.

4. Biện pháp khắc phục

- Đổi toàn bộ tài khoản quản trị.

- Vá lỗ hổng, kiểm tra upload File trái phép.

- Giám sát log hệ thống 07 ngày sau khi phục hồi.

5. Báo cáo và hậu kiểm

- Báo cáo chi tiết gửi về Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* và Chủ tịch UBND tỉnh (qua Văn phòng UBND tỉnh).

KỊCH BẢN 3*: Lộ lọt dữ liệu cá nhân qua hệ thống phần mềm nội bộ tại Bệnh viện tuyến tỉnh.*

1. Tình huống giả định: *Một đường link chứa dữ liệu bệnh án (gồm cả thông tin CCCD, BHYT, chẩn đoán...) bị rò rỉ trên nhóm mạng xã hội.*

2. Hành động cấp tốc

- Tổ CNTT Bệnh viện xác minh tính xác thực, lập tức khóa hệ thống phát sinh dữ liệu.

- Báo cáo khẩn cho Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* và Sở Y tế.

3. Vai trò các đơn vị

- Bệnh viện: Xác định người/thiết bị truy xuất dữ liệu gần nhất.

- Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)*: Truy nguồn IP tải/xuất dữ liệu, yêu cầu nhà mạng phối hợp.

- Sở Y tế: Phối hợp xác minh trách nhiệm và chỉ đạo khắc phục.

4. Biện pháp khắc phục

- Ngăn truy cập tệp dữ liệu.

- Rà soát lại toàn bộ phân quyền hệ thống HIS, LIS.

- Gửi thông báo đến người bị ảnh hưởng theo quy định Luật Bảo vệ dữ liệu cá nhân (nếu có).

5. Báo cáo và hậu kiểm

- Hồ sơ lưu 03 năm.

- Gửi báo cáo đến Bộ Y tế và Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* theo thẩm quyền.

KỊCH BẢN 4*: Tấn công từ chối dịch vụ (DDoS) vào Cổng dịch vụ công tỉnh*

1. Tình huống giả định: *Cổng Dịch vụ công tỉnh bị quá tải truy cập bất thường, không thể truy cập trong giờ hành chính.*

2. Hành động cấp tốc

- Trung tâm Khoa học và Công nghệ (Sở Khoa học và Công nghệ) xác nhận lưu lượng tăng đột biến từ các IP quốc tế.

- Bật chế độ bảo vệ (Anti-DDoS), lọc IP tại tường lửa.

- Báo cáo Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)* trong vòng 30 phút.

3. Vai trò các đơn vị

- Trung tâm Khoa học và Công nghệ: Triển khai CDN, tăng cường khả năng chịu tải.

- Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)*: Xác minh nguồn tấn công, liên hệ các ISP để chặn IP; Yêu cầu nhà cung cấp phải báo cáo thời gian DDOS, lưu lượng tấn công và các biện pháp khắc phục.

- Doanh nghiệp viễn thông: Thiết lập lọc lưu lượng ở tầng mạng (L3-L4).

4. Biện pháp khắc phục

- Chuyển máy chủ sang máy chủ đệm dự phòng.

- Bổ sung hạ tầng phòng chống DDoS vĩnh viễn.

- Điều chỉnh SLA với nhà cung cấp dịch vụ Cloud hoặc Hosting.

5. Báo cáo và hậu kiểm

- Lập báo cáo gửi Chủ tịch UBND tỉnh và Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)*.

KỊCH BẢN 5*: Tấn công có chủ đích (APT) vào hệ thống văn bản điều hành tại một Sở chủ lực.*

1. Tình huống giả định: Hệ thống văn bản điều hành liên tục bị gián đoạn, phát hiện tiến trình lạ và kết nối ra nước ngoài từ máy chủ.

2. Hành động cấp tốc

- Dừng hệ thống ngay lập tức.

- Gửi Log và ổ đĩa chứa phần mềm điều hành cho Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)*.

- Không khôi phục từ bản cũ trước khi pháp y hoàn tất.

3. Vai trò các đơn vị

- Sở bị tấn công: Cung cấp toàn bộ quyền truy cập để điều tra.

- Thường trực Đội UCSC *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)*: Trực tiếp điều tra số, giám định, theo dõi hành vi di chuyển ngang hàng trong mạng.

- Doanh nghiệp ATTT (nếu cần): Tiến hành rà quét rootkit, malware, RAT và truy nguyên nguồn lây lan.

4. Biện pháp khắc phục

- Tạo lại toàn bộ server mới từ bản sạch.

- Đổi toàn bộ mật khẩu Email, SSO, Active Directory.

- Hạn chế truy cập từ các quốc gia lạ.

5. Báo cáo và hậu kiểm

Gửi báo cáo toàn diện *(định danh mã độc, nhóm APT nếu xác định được)*, đề xuất kiến nghị UBND tỉnh hỗ trợ chi phí nâng cấp bảo mật./.