

Số: 93/KH-VPUB

Hưng Yên, ngày 10 tháng 5 năm 2022

KẾ HOẠCH

Ứng phó sự cố an toàn thông tin mạng trong hoạt động của Văn phòng UBND tỉnh

1. Phạm vi điều chỉnh

Kế hoạch quy định về ứng phó sự cố an toàn thông tin mạng (ATTT) trong hoạt động ứng dụng công nghệ thông tin của các phòng, ban, đơn vị thuộc Văn phòng UBND tỉnh Hưng Yên.

2. Đối tượng áp dụng

Các phòng, ban, đơn vị thuộc Văn phòng UBND tỉnh; cán bộ, công chức, viên chức, người lao động thuộc Văn phòng UBND tỉnh và tổ chức, cá nhân khác liên quan.

3. Nguyên tắc, phương châm ứng phó sự cố

Phân nhóm sự cố an toàn thông tin (ATTT) mạng đáp ứng các tiêu chí sau:

Hệ thống thông tin cần ứng phó khi bị một trong các sự cố sau:

- Hệ thống bị gián đoạn dịch vụ.
- Dữ liệu thuộc danh mục bí mật nhà nước có khả năng bị tiết lộ.
- Dữ liệu quan trọng của hệ thống không đảm bảo tính toàn vẹn và không có khả năng khôi phục được.
- Hệ thống bị mất quyền điều khiển.
- Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền.
- Chủ quản hệ thống thông tin không đủ khả năng kiểm soát, xử lý được sự cố.

4. Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

a) Đánh giá hiện trạng và khả năng đảm bảo ATTT mạng của các hệ thống thông tin và các đối tượng cần bảo vệ.

b) Đánh giá, dự báo nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ.

c) Đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố.

d) 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 nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

5. 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 sự cố ATTT mạng phải đặt ra các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố ATTT mạng cần đảm bảo các nội dung sau:

a) 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.

- Sự cố do bị tấn công mạng.
- Sự cố do lỗi 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 liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn,...

b) Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tình huống sau:

** 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 mạng 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 an toàn thông tin;
- 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 liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn, ...*

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

d) 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.

6. Quy trình ứng cứu sự cố an toàn thông tin mạng

- Đối với sự cố an toàn thông tin mạng thông thường: Cán bộ chuyên trách an toàn thông tin của Văn phòng UBND tỉnh (thuộc Trung tâm Thông tin - Hội nghị tỉnh) có thể tự triển khai xử lý sự cố theo các văn bản hướng dẫn quy định tại Quyết định 05/2017/QĐ-TTg ngày 16/03/2017 về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 về quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

- Đối với sự cố an toàn thông tin mạng nghiêm trọng không tự xử lý được, cán bộ chuyên trách an toàn thông tin của Văn phòng UBND tỉnh phối hợp với Sở Thông tin và Truyền thông, đội ứng cứu sự cố của tỉnh xử lý sự cố và gửi văn bản đề nghị sự hỗ trợ của các đơn vị quản lý ISP và Cục An toàn thông tin (Bộ Thông tin và Truyền thông).

***Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng bao gồm các bước như sau:**

Thứ nhất, phát hiện hoặc tiếp nhận sự cố: Cán bộ chuyên trách về an toàn thông tin của Văn phòng UBND tỉnh (thuộc Trung tâm Thông tin - Hội nghị tỉnh) chịu trách nhiệm tiếp nhận thông tin hoặc liên tục theo dõi, phát hiện các tấn công, sự cố đối với hệ thống mình được giao quản lý, vận hành qua các phương thức: Email, điện thoại, công văn...

Thứ hai, báo cáo Lãnh đạo Văn phòng UBND tỉnh, xin ý kiến chỉ đạo

Ngày sau khi phân loại được sự cố, cán bộ chuyên trách về an toàn thông tin có trách nhiệm báo cáo Lãnh đạo Văn phòng UBND tỉnh để xem xét loại sự cố và tùy theo đối tượng sẽ tiến hành phân công cho các thành viên trong tổ chuyên trách ứng cứu sự cố và báo cáo cho Đội ứng cứu sự cố của tỉnh, Sở Thông tin và Truyền thông.

Thứ ba, xác minh và phân loại sự cố: cán bộ chuyên trách về an toàn thông tin hoặc đơn vị tư vấn triển khai tiến hành xác minh sự cố gồm các thông tin như sau: tình trạng (Sự cố sẽ xảy ra; sự cố đang xảy ra; sự cố đã xảy ra); mức độ (Sự cố nghiêm trọng; sự cố bình thường); phạm vi (sự cố có diện rộng; sự cố mạng máy tính; sự cố một máy tính); địa điểm xảy ra sự cố.

Sau khi xác minh được sự cố, cán bộ chuyên trách về an toàn thông tin hoặc đơn vị tư vấn, triển khai có trách nhiệm phân loại các sự cố theo hình thức như sau: sự cố về tấn công thay đổi giao diện; sự cố về tấn công lừa đảo; sự cố về tấn công phát tán mã độc; sự cố về tấn công từ chối dịch vụ; sự cố có yếu tố nước ngoài; sự cố tấn công khác.

Thứ tư, thu thập thông tin phục vụ phân tích sự cố

Cán bộ chuyên trách về an toàn thông tin hoặc đơn vị tư vấn, triển khai phối hợp các đơn vị liên quan tiến hành thu thập các thông tin:

- + Thông tin về đầu mối liên hệ.
- + Thu thập thông tin hệ thống.
- + Thu thập chức năng của hệ thống.
- + Thu thập cấu hình của hệ thống.
- + Thu thập chứng cứ.
- + Thu thập bộ nhớ.
- + Thu thập trạng thái network và các kết nối.
- + Thu thập tiến trình đang chạy.
- + Thu thập hard drive media.
- + Thu thập Log file...

Thứ năm, phân tích sự cố

Cán bộ chuyên trách về an toàn thông tin hoặc đơn vị tư vấn, triển khai tiến hành phân tích sự cố, bao gồm các thông tin sau:

- + Phân tích dòng thời gian.
- + Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi.
- + Thời gian thực hiện các cập nhật lớn đối với hệ thống.
- + Thời điểm mà hệ thống sử dụng lần cuối cùng.
- + Phân tích dữ liệu.
- + Kiểm tra sự thay đổi cấu hình.
- + Kiểm tra hệ thống tập tin có bị mã độc.
- + Kiểm tra tập tin Internet history và các tập tin history khác.
- + Kiểm tra Registry và tiến trình.
- + Quan sát các tập tin, tiến trình lúc khởi động.
- + Phân tích log file.

Thứ sáu, xử lý sự cố gồm: Cán bộ chuyên trách về an toàn thông tin hoặc đơn vị tư vấn, triển khai tiến hành xử lý sự cố gồm các bước: gỡ bỏ sự cố; xác định và gỡ bỏ backdoors; phân tích và kiểm tra lỗ hổng sau khi thực hiện các

bản vá lỗi; khôi phục dữ liệu; thu thập các tập tin, hình ảnh, email... bị xóa, thời gian bị xóa; tìm kiếm các tập tin không thể khôi phục; khôi phục các tập tin phù hợp.

Thứ bảy, tổng hợp báo cáo: cán bộ chuyên trách an toàn thông tin hoặc đơn vị tư vấn, triển khai tiến hành tổng hợp kết quả phân tích và báo cáo kết quả với lãnh đạo Văn phòng UBND tỉnh, trong đó mô tả chi tiết các bước thực hiện, giải pháp xử lý sự cố, kết quả khắc phục hiện tại. Họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất biện pháp ứng dụng cho các sự cố tương tự.

Thứ tám, kết thúc lưu hồ sơ: Toàn bộ các hồ sơ trong quá trình xử lý sự cố được lưu trữ phục vụ các hoạt động quản lý và theo dõi định kỳ: Lưu hồ sơ, tài liệu lưu trữ; xây dựng, đúc rút các bài học, kinh nghiệm; đề xuất các kiến nghị về kỹ thuật, chính sách để hạn chế thiệt hại khi xảy ra các tấn công tương tự.

7. Các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, đảm bảo các điều kiện sẵn sàng ứng phó, khắc phục sự cố

a) Các nội dung nhằm phát hiện sớm và phòng ngừa sự cố

- Thực hiện nghiêm công tác giám sát, phát hiện sớm nguy cơ sụp đổ.
- 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 về ATTT; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố tấn công mạng.

b) Các nội dung nhằm đảm bảo các điều kiện sẵn sàng ứng phó, khắc phục sự cố

- Trang bị, nâng cấp thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm phục vụ việc ứng cứu, khắc phục sự cố.
- Thuê dịch vụ đảm bảo ATTT, chuẩn bị các nguồn lực sẵn sàng để ứng phó, khắc phục khi sự cố xảy ra.
- Tham gia các lớp tập huấn, các hoạt động của mạng lưới ứng cứu sự cố.

8. Tổ chức thực hiện

a) Trung tâm Thông tin - Hội nghị tỉnh

- Là đơn vị chủ trì, phối hợp với các phòng, đơn vị thuộc Văn phòng triển khai thực hiện các nội dung về ứng cứu sự cố.
- Là đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về ATTT mạng trong hoạt động của cơ quan.
- Chủ trì, phối hợp với các phòng, đơn vị thuộc Văn phòng tiến hành kiểm tra công tác đảm bảo ATTT mạng định kỳ hàng năm hoặc theo hướng dẫn của cơ quan chuyên môn.

- Xây dựng các nội dung thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố vào các Kế hoạch về đảm bảo ATTT mạng, Kế hoạch ứng dụng công nghệ thông tin.

b) Phòng Hành chính - Quản trị

Tham mưu nội dung dự phòng kinh phí, nhân lực, vật lực thường trực sẵn sàng ứng cứu sự cố.

c) Trách nhiệm của các phòng, ban, đơn vị thuộc Văn phòng UBND tỉnh

- Quan tâm, chú trọng đến công tác đảm bảo ATTT mạng cho hệ thống thông tin tại phòng, ban, đơn vị mình.

- Chủ động cài đặt phần mềm diệt virus, tường lửa cho hệ thống máy tính, hệ thống mạng, hệ thống thông tin tại phòng, ban, đơn vị mình.

- Phối hợp với Trung tâm Thông tin - Hội nghị tỉnh và các đơn vị liên quan thực hiện công tác ứng phó sự cố ATTT mạng tại phòng, ban, đơn vị mình.

Trên đây là Kế hoạch phối hợp ứng phó sự cố an toàn thông tin mạng trong hoạt động của Văn phòng năm 2022. Yêu cầu các phòng, ban, đơn vị triển khai thực hiện theo đúng Kế hoạch./.

Nơi nhận:

- Lãnh đạo Văn phòng UBND tỉnh;
- Sở Thông tin và Truyền thông;
- Các phòng, ban, đơn vị thuộc Văn phòng UBND tỉnh;
- Lưu: VT, TTHN.

**KT. CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG**



Ký bởi: Ủy ban nhân dân tỉnh Hưng
Yên
Cơ quan: Tỉnh Hưng Yên
Thời gian ký: 10/05/2022 13:48:42

Trần Văn Thắng