

Số: 734 /KH-PTTH

Hà Tĩnh, ngày 22 tháng 9 năm 2023

KẾ HOẠCH

Ứng phó sự cố, bảo đảm an toàn thông tin mạng

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ 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;

Căn cứ Thông tư số 12/2022-TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định 01/2021/QĐ-UBND ngày 19/01/2021 của Ủy ban nhân dân tỉnh về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh;

Đài Phát thanh và Truyền hình xây dựng Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng, an ninh hệ thống thông tin, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Đảm bảo an toàn thông tin cho các hệ thống thông tin của Đài; đảm bảo khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên mạng; đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

- Tạo chuyên biến mạnh mẽ trong nhận thức về an toàn thông tin đối với cán bộ, viên chức và người lao động của Đài;

- 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 an toàn thông tin mạng.

2. Yêu cầu

- Căn cứ trên kết quả khảo sát, đánh giá các nguy cơ, sự cố mất an toàn thông tin mạng của hệ thống thông tin của Đài để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời, phù hợp.

- Có phương án đối phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra.

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

II. NHIỆM VỤ TRIỂN KHAI

1. Triển khai các nhiệm vụ khi chưa có sự cố xảy ra

- Tuyên truyền, phổ biến các văn bản quy phạm pháp luật về an toàn thông tin mạng cho toàn thể cán bộ, viên chức và người lao động của Đài.

- Tổ chức tuyên truyền, phổ biến, hướng dẫn nội dung của Luật An toàn thông tin mạng, Quyết định số 05/2017/QĐ-TTg, Quyết định số 1017/QĐ-TTg và các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng trên cổng thông tin điện tử của Đài, trong các hội nghị, các buổi chào cờ đầu tháng...

- Triển khai các chương trình đào tạo, bồi dưỡng kỹ năng đánh giá, ứng phó sự cố. Tham gia các khóa đào tạo, bồi dưỡng nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố theo hướng dẫn của Sở Thông tin và Truyền thông.

- Triển khai giám sát, phát hiện sớm các nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc; phòng ngừa sự cố, quản lý rủi ro; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Nghiên cứu, tham mưu, đề xuất trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng các nguồn lực và tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

- Tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng đối với hệ thống thông tin; đánh giá, dự báo các nguy cơ, sự cố tấn công mạng có thể xảy ra với hệ thống thông tin; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể nếu có xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực phục vụ đối phó, ứng cứu, khắc phục sự cố (nếu có).

- Đối với mỗi hệ thống thông tin và chương trình ứng dụng triển khai tại Đài, cần dự kiến tình huống, 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 nghiêm trọng của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung theo hướng dẫn của cơ quan chuyên môn.

2. Triển khai các nhiệm vụ khi có sự cố xảy ra

- Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể từ các nguồn bên trong và bên ngoài. Khi phân tích, xác minh sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố.

- Sau khi đã xác định sự cố xảy ra, đơn vị sử dụng, vận hành hệ thống thông tin cần căn cứ vào dấu hiệu, cảnh báo, hướng dẫn của cơ quan chuyên môn để tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố.

- Căn cứ theo các cảnh báo, hướng dẫn của Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh để lựa chọn phương án ngăn chặn và xử lý sự cố. Báo cáo, đề xuất Ban Giám đốc xin ý kiến chỉ đạo.

- Triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng; phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

- Sau khi đã triển khai ngăn chặn sự cố, Tổ Quản trị mạng khẩn trương tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.

- Triển khai các hoạt động khôi phục hệ thống thông tin, dữ liệu và kết nối; cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng, phần mềm bảo đảm an toàn thông tin của hệ thống thông tin.

- Bộ phận sử dụng, quản lý, vận hành hệ thống thông tin và các phòng chuyên môn liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố.

II. KINH PHÍ THỰC HIỆN

Căn cứ tình hình thực tế, Tổ Quản trị mạng phối hợp với phòng Hành chính – Tổng hợp tham mưu Ban Giám đốc đề xuất kinh phí trong quá trình triển khai phương án ứng cứu sự cố.

IV. TỔ CHỨC THỰC HIỆN

- Phòng Hành chính - Tổng hợp phối hợp với Tổ Quản trị mạng và các phòng chuyên môn phổ biến Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng của Đài trên cổng thông tin điện tử của Đài và trong toàn thể cán bộ viên chức và người lao động.

- Tổ Quản trị mạng là bộ phận đầu mối về ứng cứu sự cố an toàn thông tin mạng của Đài. Theo chức năng nhiệm vụ được phân công, chủ động phối hợp thực hiện các nội dung của Kế hoạch đảm bảo yêu cầu, hiệu quả. Trong quá trình thực hiện có gì vướng mắc cần sửa đổi, bổ sung thì tham mưu Ban giám đốc xem xét, quyết định.

Nơi nhận:

- Sở Thông tin và Truyền thông;
- Ban Giám đốc;
- Các phòng chuyên môn (thực hiện);
- Lưu: VT, TC./.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Nguyễn Văn Hiền