

KẾ HOẠCH

Ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2018

Căn cứ Kế hoạch số 439/KH-UBND ngày 11/01/2018 của UBND tỉnh Khánh Hòa về Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2018;

Sở Công Thương xây dựng Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2018 trong hoạt động ứng dụng công nghệ thông tin của Sở như sau:

I. Mục đích

Đảm bảo an toàn thông tin cho các hệ thống thông tin đang được quản lý, sử dụng trong hoạt động của Sở Công Thương; đảm bảo các nguồn lực và điều kiện cần thiết để sẵn sàng triển khai và phối hợp triển khai có hiệu quả các phương án ứng cứu khẩn cấp sự cố an toàn thông tin mạng.

II. Nội dung

1. Thực hiện các nhiệm vụ khi chưa có sự cố xảy ra

a) Tuyên truyền, phổ biến Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 và các văn bản quy phạm pháp luật về an toàn thông tin mạng bằng cách đăng tải trên trang thông tin điện tử của Sở Công Thương tại địa chỉ <http://sct.khanhhoa.gov.vn>

- Thời gian thực hiện: Thường xuyên trong năm.

b) Tham gia huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; tham gia diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc và khắc phục sự cố an toàn thông tin mạng.

- Thời gian thực hiện: Theo hướng dẫn của Sở Thông tin và Truyền thông.

c) Kiểm tra, đánh giá an toàn thông tin mạng; rà quét, bóc gỡ, xử lý mã độc và phần mềm độc hại; áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin để giám sát, phòng ngừa, phát hiện sớm các nguy cơ, sự cố tấn công mạng.

- Thời gian thực hiện: Định kỳ hàng quý.

d) Trang bị và nâng cấp trang thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm (nếu có); dự phòng các nguồn lực và tài chính để sẵn sàng đối phó, ứng cứu, khắc phục sự cố an toàn thông tin mạng.

- Thời gian thực hiện: 6 tháng và hàng năm.



đ) Tổ chức đánh giá, dự báo các nguy cơ, sự cố tấn công mạng có thể xảy ra với các hệ thống thông tin; đánh giá, dự báo các hậu quả, thiệt hại có thể có; đánh giá hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ cho việc ứng cứu, khắc phục sự cố an toàn thông tin mạng.

- Thời gian thực hiện: Định kỳ hàng quý.

e) Xây dựng phương án đối phó, ứng cứu đối với một số tình huống, kịch bản cụ thể cho mỗi hệ thống thông tin và chương trình ứng dụng khi xảy ra sự cố an toàn thông tin mạng. Phương án đối phó, ứng cứu phải đảm bảo các nội dung và tiêu chí theo như Kế hoạch số 439/KH-UBND ngày 11/01/2018 của UBND tỉnh Khánh Hòa đề ra.

- Thời gian thực hiện: Thường xuyên trong năm.

2. Thực hiện các nhiệm vụ khi có sự cố xảy ra

a) Ứng cứu ban đầu và thông báo sự cố:

- Thường xuyên theo dõi, tiếp nhận và phân tích các cảnh báo, dấu hiệu của sự cố từ các nguồn bên trong và bên ngoài; tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc của sự cố.

- Sau khi đã xác định sự cố xảy ra, cán bộ chuyên trách công nghệ thông tin căn cứ vào bản chất, dấu hiệu của sự cố tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo hướng dẫn của Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh, lựa chọn phương án ứng cứu phù hợp với điều kiện hạ tầng kỹ thuật và các nguồn lực hiện có của Sở Công Thương.

- Sau khi triển khai các bước ưu tiên ứng cứu ban đầu, thông báo sự cố đến các tổ chức, cá nhân liên quan theo quy định tại Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12/09/2017 và quy định nội bộ (nếu có).

b) Xác định phạm vi và đối tượng bị ảnh hưởng bởi sự cố; 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.

c) Phối hợp với Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh và Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa thực hiện:

- Triển khai tiêu diệt, gỡ bỏ mã độc, phần mềm độc hại, khắc phục các điểm yếu về an toàn thông tin của hệ thống thông tin.

- 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 cho hệ thống thông tin.

- Triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa hoạt động ổn định, xác minh lại

nguyên nhân và tổ chức khắc phục dứt điểm, khôi phục lại hoạt động bình thường của hệ thống thông tin.

d) Tổng hợp toàn bộ các thông tin liên quan đến công tác triển khai ứng cứu sự cố, báo cáo Chủ quản hệ thống thông tin, Ban Chỉ đạo Ứng dụng công nghệ thông tin tỉnh Khánh Hòa và Cơ quan điều phối quốc gia; tổ chức phân tích nguyên nhân, rút kinh nghiệm và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai.

III. TỔ CHỨC THỰC HIỆN

Văn phòng Sở chủ trì, phối hợp với các phòng, ban, đơn vị thuộc Sở; các tổ chức và cá nhân liên quan thực hiện Kế hoạch này.

Trên đây là Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2018 của Sở Công Thương Khánh Hòa./. *pháo*

Nơi nhận:

- Sở TT và TT (thay b/cáo) (VBĐT);
- Các Phòng, đơn vị thuộc Sở (VBĐT);
- Lưu: VT, VP.

GIÁM ĐỐC



Lê Thu Hải



