UBND TỈNH KHÁNH HÒA **SỞ CÔNG THƯƠNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 15 /KH-SCT	*Khánh Hòa, ngày 05 tháng 6 năm 2019*

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2019 Sở Công Thương Khánh Hòa

Triển khai thực hiện Kế hoạch số 3669/KH-UBND ngày 19/4/2019 của UBND tỉnh Khánh Hòa về Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2019, Sở Công Thương xây dựng Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2019 tại cơ quan như sau:

I. MỤC ĐÍCH.

- Chuẩn bị các điều kiện và nguồn lực cần thiết để ứng phó sự cố mất an toàn thông tin mạng xảy ra trong quá trình quản lý, vận hành các hệ thống thông tin tại Sở Công Thương.

- Đảm bảo các phương án, giải pháp ứng cứu được triển khai kịp thời, hiệu quả; giảm thiểu tối đa các mối nguy cơ, đe dọa đến an toàn, an ninh thông tin trên môi trường mạng.

II. NỘI DUNG THỰC HIỆN.

1. Chuẩn bị các điều kiện và nguồn lực cần thiết.

a. Tuyên truyền, phổ biến 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 121/2018/TT-BTC ngày 12/12/2018 của Bộ Tài chính Quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng và các văn bản quy phạm pháp luật về an toàn thông tin mạng trên Trang thông tin điện tử Sở Công Thương.

** Thời gian thực hiện: Tháng 6/2019.*

b. Tham gia chương trình huấn luyện, đào tạo, bồi dưỡng, diễn tập các phương án đối phó, ứng cứu sự cố, nâng cao kỹ năng, nghiệp vụ phối hợp, chống tấn công, xử lý mã độc và khắc phục sự cố do Sở Thông tin và Truyền thông chủ trì, tổ chức.

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

c. Xây dựng, phổ biến các quy định nội bộ về an toàn thông tin mạng; sử dụng phần mềm diệt virus có bản quyền rà quét, bóc gỡ, xử lý mã độc và phần mềm độc hại trên các máy tính.

** Thời gian thực hiện: Thường xuyên trong năm.*

d. Đầu tư nâng cấp trang thiết bị công nghệ thông tin và gia hạn bản quyền phần mềm có liên quan đến bảo mật, có khả năng phòng ngừa, ngăn chặn các nguy cơ, sự cố mất an toàn thông tin trên môi trường mạng.

** Thời gian thực hiện: Thường xuyên trong năm.*

e. Tổ chức đánh giá các nguy cơ, sự cố an toàn thông tin mạng đối với các hệ thống thông tin.

** Thời gian thực hiện: Dự kiến Quý III/2019.*

f. Phương án đối phó, ứng cứu đối với tình huống mất an toàn thông tin mạng thường gặp:

Tình huống, sự cố mất an toàn thông tin mạng Sở Công Thương thường gặp là bị tấn công mạng

- Tiêu chí xác định tính chất, mức độ nghiêm trọng của sự cố:

➢ Dịch vụ, tiện ích của hệ thống không hoạt động theo yêu cầu của người sử dụng.

➢ Xuất hiện nhiều tập tin lạ.

➢ Hệ thống tự động shutdown/restart/logoff hoặc tự động thay đổi thông tin, cấu hình ban đầu mà không có sự can thiệp của người quản trị, vận hành hệ thống.

➢ Giao diện hệ thống tự động thay đổi mà không có sự điều chỉnh của người sử dụng.

➢ Dữ liệu người sử dụng bị mất hoặc thay đổi, không còn nguyên vẹn.

- Nguyên nhân, nguồn gốc sự cố:

➢ Người sử dụng truy cập website có tiềm ẩn nguy cơ, khả năng tấn công từ chối dịch vụ/tấn công sử dụng mã độc/tấn công truy cập trái phép, chiếm quyền điều khiển/tấn công thay đổi giao diện/tấn công phá hoại thông tin, dữ liệu, phần mềm,…

➢ Hệ điều hành máy tính không có bản quyền dẫn đến hệ thống bảo mật không đủ mạnh để phòng chống sự xâm nhập từ môi trường mạng.

➢ Phần mềm diệt virus không có bản quyền hoặc chưa được cấu hình đầy đủ chức năng để chống lại mã độc trong quá trình truy cập mạng.

- Phương án đối phó, ứng cứu, khắc phục sự cố:

➢ Bật tường lửa của hệ điều hành (nếu đã tắt); sử dụng phần mềm diệt virus có bản quyền để quét toàn bộ hệ thống nhằm phát hiện và tiêu diệt mã độc, ngăn chặn sự tấn công và phạm vi ảnh hưởng của sự cố.

➢ Rà soát lại các trường hợp mất an toàn thông tin mạng đã được Sở Thông tin và Truyền thông cảnh báo, hướng dẫn để áp dụng khắc phục sự cố nếu có tính chất, mức độ tương tự.

➢ Nếu cả hai cách trên đều không khắc phục được, Quản trị mạng phải trang bị phần mềm hệ điều hành và phần mềm diệt virus có bản quyền cho tất cả máy tính trong hệ thống thông tin, tìm kiếm giải pháp đồng thời thông báo sự cố cho Sở Thông tin và Truyền thông được biết để có hướng dẫn đối phó, ứng cứu ban đầu. Kinh phí trang bị phần mềm có bản quyền trong dự toán chi thường xuyên của Sở.

2. Ứng cứu khi có sự cố xảy ra.

a. Tiếp nhận và xác minh sự cố:

- Quản trị mạng có trách nhiệm tiếp nhận thông tin sự cố, tiến hành kiểm tra, xác minh sự cố bằng cách thu thập bằng chứng từ hệ thống thông tin đang vận hành, sử dụng chuyên môn nghiệp vụ để phân tích, xác định nguyên nhân, nguồn gốc của sự cố để bắt đầu triển khai phương án ứng cứu, khắc phục.

- Trường hợp không thể xác định được nguyên nhân, nguồn gốc sự cố phải thông báo ngay lập tức cho Sở Thông tin và Truyền thông biết để có hướng dẫn kịp thời.

b. Xác định phạm vi bị ảnh hưởng bởi sự cố, thông báo cho các cá nhân liên quan trong hệ thống thông tin biết và đề nghị phối hợp khắc phục sự cố.

c. Quản trị mạng triển khai phương án đối phó, ứng cứu, khắc phục sự cố đã được chuẩn bị và hướng dẫn cho các cá nhân có liên quan thực hiện.

d. Sau khi triển khai phương án ứng cứu, khắc phục, Quản trị mạng kiểm tra, đánh giá lại hoạt động của toàn bộ hệ thống thông tin, nếu hệ thống chưa hoạt động ổn định, phải phối hợp với Sở Thông tin và Truyền thông xác minh lại chính xác nguyên nhân sự cố để xử lý dứt điểm, tiêu diệt, gỡ bỏ mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của toàn bộ hệ thống trong thời gian nhanh nhất.

3. Tổng hợp, báo cáo sự cố.

Quản trị mạng tổng hợp toàn bộ các thông tin liên quan đến quá trình triển khai ứng cứu sự cố, phân tích nguyên nhân và báo cáo kết quả khắc phục sự cố, trong đó nêu rõ biện pháp khắc phục cố cho Sở Thông tin và Truyền thông được biết để tổng hợp báo cáo lên cơ quan cấp trên.

III. TỔ CHỨC THỰC HIỆN.

Văn phòng Sở chủ trì, phối hợp với các phòng, đơn vị, 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 2019 của Sở Công Thương Khánh Hòa./.

Nơi nhận: *(VBĐT)*
- Sở Thông tin và Truyền thông;
- BGĐ Sở;
- Các phòng, đơn vị;
- Lưu: VT, VP.

GIÁM ĐỐC

Sở Công thương tỉnh Khánh Hòa
Ủy ban Nhân dân tỉnh Khánh Hòa
05.06.2019 09:30:15 +07:00

Lê Thu Hải
05.06.2019 09:12:36 +07:00

Lê Thu Hải