UBND TỈNH QUẢNG NGÃI
SỞ KHOA HỌC VÀ CÔNG NGHỆ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 242 /QĐ-SKHCN

Quảng Ngãi, ngày 21 tháng 12 năm 2022

QUYẾT ĐỊNH
Ban hành Phương án Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống mạng LAN cơ quan Sở Khoa học và Công nghệ

GIÁM ĐỐC SỞ KHOA HỌC VÀ CÔNG NGHỆ TỈNH QUẢNG NGÃI

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng;

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; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của 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 Quyết định số 62/2021/QĐ-UBND ngày 08/11/2021 của UBND tỉnh Quảng Ngãi về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Khoa học và Công nghệ tỉnh Quảng Ngãi;

Căn cứ Quyết định số 1571/QĐ-UBND ngày 28/10/2019 của UBND tỉnh Quảng Ngãi về việc Ban hành Kế hoạch Ứng phó sự cố, bảo đảm an toàn, an ninh thông tin mạng trên địa bàn tỉnh Quảng Ngãi giai đoạn 2020 - 2025;

Căn cứ Quyết định số 164/QĐ-STTTT ngày 24/11/2021 của Giám đốc Sở Thông tin và Truyền thông tỉnh Quảng Ngãi về việc Phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống mạng LAN cơ quan Sở Khoa học và Công nghệ tỉnh Quảng Ngãi;

Thực hiện Công văn số 5609/UBND-KGVX ngày 03/11/2022 của Chủ tịch UBND tỉnh Quảng Ngãi tại về việc triển khai thực hiện Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ;

Theo đề nghị của Giám đốc Trung tâm Ứng dụng và Dịch vụ khoa học công nghệ.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Phương án Ứng phó sự cố, bảo đảm an toàn thông tin Hệ thống mạng LAN cơ quan Sở Khoa học và Công nghệ *(có Phương án kèm theo)*.

Điều 2. Các nội dung trong Phương án là căn cứ để Trưởng các phòng, đơn vị thuộc Sở chủ động chỉ đạo, điều hành các hoạt động ứng phó sự cố, bảo đảm an toàn thông tin mạng; bảo đảm hạn chế thấp nhất thiệt hại do sự cố mất an toàn an ninh thông tin mạng gây ra đối với Hệ thống mạng LAN cơ quan Sở Khoa học và Công nghệ.

Điều 3. Quyết định này có hiệu lực kể từ ngày ký.

Điều 4. Trưởng các phòng, đơn vị thuộc Sở và công chức, viên chức, người lao động thuộc Sở Khoa học và Công nghệ chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 4;
- UBND tỉnh (báo cáo);
- Sở Thông tin và Truyền thông;
- GĐ, các PGĐ Sở;
- Lưu: VT, HCTH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ KHOA HỌC VÀ CÔNG NGHỆ
TỈNH QUẢNG NGÃI

Trần Công Hòa

UBND TỈNH QUẢNG NGÃI
SỞ KHOA HỌC VÀ CÔNG NGHỆ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHƯƠNG ÁN
Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống mạng LAN của cơ quan Sở Khoa học và Công nghệ

(Ban hành kèm theo Quyết định số: /QĐ-SKHCN ngày 21/12/2022 của Giám đốc Sở Khoa học và Công nghệ)

I. MỤC ĐÍCH, YÊU CẦU

1. Công tác phòng ngừa, ứng phó sự cố hệ thống thông tin mạng LAN cơ quan Sở Khoa học và Công nghệ là nhiệm vụ quan trọng nhằm hạn chế đến mức thấp nhất thiệt hại về dữ liệu thông tin và tài sản của cơ quan.

2. Tăng cường thông tin, tuyên truyền, cảnh báo, hướng dẫn các biện pháp phòng, tránh và ứng phó sự cố hệ thống thông tin mạng nhằm phát huy ý thức tự giác, chủ động ứng phó của công chức, viên chức, người lao động tại Sở Khoa học và Công nghệ.

3. Các phòng, đơn vị thuộc Sở phải nỗ lực tổ chức phối hợp đồng bộ nhằm đưa công tác phòng ngừa, ứng phó sự cố, đảm bảo an toàn, an ninh thông tin mạng hiệu quả trong phạm vi quản lý theo quy định.

II. PHƯƠNG ÁN ỨNG PHÓ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

1. Nhận diện các nguy cơ, sự cố hệ thống thông tin mạng

Các nguy cơ, sự cố có khả năng ảnh hưởng đến hệ thống thông tin đối với Hệ thống mạng LAN cơ quan Sở Khoa học và Công nghệ như sau:

1.1. Sự cố do bị tấn công mạng:

+ 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 từ chối dịch vụ;

+ Tấn công giả mạo;

+ 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.

1.2. 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;

1.3. 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.

1.4. Sự cố liên quan đến các thảm họa tự nhiên: Bão, lụt, động đất, hỏa hoạn,...

2. Ứng phó sự cố an toàn hệ thống thông tin mạng

Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm virus, nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu,…), cần phải thực hiện các bước như sau:

- Bước 1. Khoanh vùng cô lập sự cố

+ Sau khi phát hiện sự cố, công chức, viên chức và người lao động tại các phòng, đơn vị thực hiện khoanh vùng cô lập máy tính bị sự cố, như: ngắt kết nối máy tính khỏi hệ thống thông tin mạng LAN của cơ quan (tắt máy, rút dây mạng…).

+ Báo cáo ngay Lãnh đạo phòng các dấu hiệu sự cố; đồng thời thông báo kịp thời về Trung tâm Ứng dụng và Dịch vụ khoa học công nghệ (Thành viên Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi) để cử công chức phối hợp kiểm tra, xử lý.

- Bước 2. Thu thập thông tin phục vụ phân tích sự cố:

+ Trung tâm Ứng dụng và Dịch vụ khoa học công nghệ (Thành viên Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi) sẽ phối hợp với công chức, viên chức và người lao động tại các phòng, đơn vị kiểm tra máy tính đang bị sự cố để nắm bắt thông tin ban đầu về sự cố.

+ Các thông tin thu thập gồm: Thông tin hệ thống; chức năng của hệ thống; cấu hình của hệ thống (OS, servise, version, network, …); Thu thập chứng cứ; Thu thập bộ nhớ; Thu thập trạng thái network và các kết nối; Thu thập các tiến trình đang chạy; Thu thập hard drive media; Thu thập removeble media; Thu thập Log file…).

- Bước 3. Phân tích sự cố

+ Kiểm tra máy tính đang bị sự cố để phân tích nguyên nhân ban đầu về sự cố.

+ Các thông tin phân tích gồm: 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.

- Bước 4. Xử lý sự cố:

+ Trường hợp sự cố có khả năng kiểm soát, xử lý được: Sẽ tiến hành xử lý sự cố bao gồm các bước: Gỡ bỏ sự cố; Xác định và gỡ bỏ các 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.

+ Trường hợp sự cố ngoài khả năng kiểm soát, không xử lý được (sự cố có tính chất nghiêm trọng): Triển khai ngay các biện pháp xử lý ngăn chặn tấn công tránh lây nhiễm sự cố các máy tính khác trên hệ thống mạng và báo cáo đề xuất Giám đốc Sở có văn bản đề nghị Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để kịp thời hỗ trợ, xử lý.

- Bước 5. Tổng hợp báo cáo:

+ Sau khi triển khai các giải pháp ứng cứu sự cố, tham mưu Giám đốc Sở tổ chức họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp ứng cứu cho các sự cố tương tự.

+ Tham mưu báo cáo kết quả ứng cứu sự cố xảy ra về Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để biết, theo dõi.

- Bước 6. Lưu hồ sơ:

Toàn bộ các hồ sơ trong quá trình xử lý sự cố sẽ được lưu trữ phục vụ các hoạt động quản lý và theo dõi, kiểm tra định kỳ.

III. PHÂN CÔNG NHIỆM VỤ

1. Trách nhiệm của Trung tâm Ứng dụng và Dịch vụ khoa học công nghệ (Thành viên Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi)

- Làm đầu mối ứng cứu sự cố đối với hệ thống mạng LAN cơ quan Sở Khoa học và Công nghệ theo đúng quy trình ứng cứu sự cố dựa trên tính chất, mức độ, phạm vi và nguyên nhân xảy ra sự cố; bảo đảm nhanh chóng, chính xác, kịp thời, an toàn và hiệu quả.

- Phối hợp với các phòng, đơn vị thuộc Sở kiểm tra, rà soát đánh giá an toàn thông tin thường xuyên, định kỳ hoặc đột xuất khi có các yếu tố quan trọng, đặc biệt thay đổi để kịp thời phát hiện các lỗ hổng đang tồn tại, các nguy cơ mất an toàn thông tin mạng.

- Phối hợp với phòng Hành chính - Tổng hợp tham mưu Giám đốc Sở chỉ đạo triển khai các nội dung sau:

+ Tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin cho công chức, viên chức, người lao động tại Sở.

+ Cử công chức, viên chức, người lao động tại Sở tham dự các lớp kỹ năng bảo vệ hệ thống thông tin do các cơ quan chức năng tổ chức.

- Phối hợp với phòng Hành chính - Tổng hợp thực hiện việc đảm bảo an toàn thông tin Hệ thống mạng LAN cơ quan Sở Khoa học và Công nghệ:

+ Về cơ sở hạ tầng: Đảm bảo việc lắp đặt thiết bị chống sét, thiết bị cảnh báo phòng chống cháy, nổ tại trụ sở để bảo vệ hệ thống, thiết bị công nghệ thông tin.

+ Quản lý hệ thống mạng nội bộ: Mạng nội bộ của Sở khi kết nối với mạng Internet phải thông qua thiết bị tường lửa Sophos do Sở Thông tin và Truyền thông tỉnh lắp đặt để kiểm soát, hạn chế việc truy cập trái phép từ bên ngoài. Các máy chủ, máy trạm trên hệ thống phải được cài đặt phần mềm diệt virus có bản quyền.

+ Quản lý hệ thống mạng không dây (wifi): Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ.

+ Quản lý truy cập từ xa vào mạng nội bộ: Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

+ Bảo mật truy cập: Các chương trình, phần mềm được được bàn giao cho công chức, viên chức và người lao động sử dụng phải được thiết lập mật khẩu theo quy định. Kịp thời điều chỉnh vị trí công tác cho người sử dụng (khi có sự thay đổi); xóa khỏi hệ thống các tài khoản người dùng đã về hưu hoặc chuyển công tác.

+ Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

+ Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng hệ thống thông tin trong phạm vi quản lý tối thiểu 6 tháng/01 lần.

2. Trách nhiệm của Trưởng các phòng, đơn vị

- Trưởng các phòng, đơn vị thuộc Sở tăng cường công tác tuyên truyền, phổ biến các văn bản, quy định về an toàn thông tin đến công chức, viên chức, người lao động nhằm nâng cao ý thức trách nhiệm về đảm bảo an toàn, an ninh thông tin mạng.

- Thường xuyên chỉ đạo công chức, viên chức, người lao động thực hiện nghiêm các quy định bảo đảm an toàn thông tin hệ thống mạng LAN cơ quan.

- Phối hợp với Trung tâm Ứng dụng và Dịch vụ khoa học công nghệ trong công tác kiểm tra, phát hiện, xử lý kịp thời các sự cố về an toàn thông tin mạng.

3. Trách nhiệm của công chức, viên chức, người lao động tại các phòng, đơn vị thuộc Sở

- Có trách nhiệm quản lý tài khoản, mật khẩu đăng nhập vào các phần mềm dùng chung được triển khai tại cơ quan, đơn vị. Thường xuyên thay đổi mật khẩu đủ mạnh (ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt) để đảm bảo an toàn, an ninh thông tin.

- Có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính. Tuyệt đối không chia sẻ thư mục, dữ liệu cá nhân trên hệ thống mạng LAN cơ quan, đơn vị.

- Có trách nhiệm tuân thủ các biện pháp theo hướng dẫn cảnh báo về lỗ hổng bảo mật, cảnh báo nguy cơ tấn công của cơ quan có thẩm quyền nhằm rà soát, giám sát, ngăn chặn, phòng ngừa, xử lý kịp thời hạn chế đến mức thấp nhất nguy cơ gây mất an toàn an ninh thông tin. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài (USB, ổ cứng di động, thẻ nhớ...) đều phải được quét, diệt virus trước khi sao chép vào máy. Không truy cập vào các Website, đường dẫn liên kết không rõ ràng; không truy cập vào các link hoặc tải về các file tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

- Tự quản lý, bảo quản thiết bị công nghệ thông tin như: Máy tính, máy in, máy scan, máy photocopy,... mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Thực hiện tiếp nhận, xử lý, phát hành, quản lý và lưu trữ văn bản, hồ sơ điện tử trên phần mềm quản lý văn bản đúng quy định trên môi trường mạng và ký số cá nhân, đảm bảo theo đúng quy định pháp luật hiện hành. Không sử dụng gmail, yahoo… để gửi, nhận văn bản giữa các cơ quan nhà nước.

- Không được tự ý cài đặt phần mềm download trên mạng khi chưa có sự đồng ý hoặc tự gỡ bỏ phần mềm diệt vius đã được cài đặt trên máy trạm.

- Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm virus, nhiễm mã độc trên máy trạm (Ví dụ: Máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu,…), người sử dụng phải báo ngay cho lãnh đạo phòng, đơn vị để phối hợp với Trung tâm Ứng dụng và Dịch vụ khoa học công nghệ xử lý kịp thời, tránh lây lan đến các máy trạm khác.

IV. TỔ CHỨC THỰC HIỆN

1. Các phòng thuộc Sở trong phạm vi nhiệm vụ, quyền hạn của mình, có trách nhiệm phối hợp với Trung tâm Ứng dụng và Dịch vụ khoa học công nghệ trong quá trình tham gia ứng phó sự cố an toàn thông tin mạng khi xảy ra sự cố.

2. Trung tâm Ứng dụng và Dịch vụ khoa học công nghệ; Phòng Hành chính - Tổng hợp căn cứ chức năng, nhiệm vụ quyền hạn được giao phân công công chức, viên chức, người lao động thực hiện công tác đảm bảo an toàn, an ninh thông tin tại đơn vị.

3. Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung; Trưởng các phòng, đơn vị thuộc Sở kịp thời phản ánh về Trung tâm Ứng dụng và Dịch vụ khoa học công nghệ để tổng hợp báo cáo Giám đốc Sở xem xét sửa đổi, bổ sung cho phù hợp./.