UBND TỈNH THÁI BÌNH
SỞ LAO ĐỘNG
THƯƠNG BINH VÀ XÃ HỘI

Số: 150 / SLĐTBXH-VP

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

Thái Bình, ngày 18 *tháng* 01 *năm 2021*

KỊCH BẢN
Về phối hợp ứng phó sự cố an toàn thông tin mạng trong hoạt động của Sở Lao động – Thương binh và Xã hội.

CHƯƠNG I
CÁC QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

Các phòng , đơn vị trực thuộc Sở, cán bộ công chức, viên chức, người lao động thuộc quản lý của Sở Lao động – Thương binh và Xã hội.

Điều 2. 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 bị một số trong các sự cố sau:
  + Hệ thống bị gián đoạn dịch vụ.
  + Dữ liệu tuyệt mật hoặc 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 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.

Điều 3. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các lực lượng tham gia ứng phó sự cố:

Văn phòng Sở là bộ phận chuyên trách ứng cứu sự cố ATTT mạng của Sở có trách nhiệm: Tham gia hoạt động ứng cứu khẩn cấp bảo đảm ATTT mạng nội bộ khi có yêu cầu từ các phòng, đơn vị trực thuộc Sở.

Các phòng, đơn vị trực thuộc có trách nhiệm cử cán bộ, công chức phụ trách ATTT tham gia ứng cứu sự cố ATTT khi xảy ra sự cố.

CHƯƠNG II
ĐÁNH GIÁ CÁC NGUY CƠ, SỰ CỐ AN TOÀN THÔNG TIN MẠNG

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

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

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

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

4. Đánh giá về hiện trạng phương tiên, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

CHƯƠNG III

PHƯƠNG ÁN ĐỐI PHÓ, ỨNG CỨU SỰ CỐ ĐỐI VỚI MỘT SỐ TÌNH HUỐNG SỰ CỐ CỤ THỂ

Điều 5. Tiêu chí xây dựng phương án đối phó, ứng cứu sự cố ATTT mạng.

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 sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung sau:

1. 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 ….

2. 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 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 v.v....

3. 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.

CHƯƠNG IV

TRIỂN KHAI PHÒNG NGỪA SỰ CỐ, GIÁM SÁT PHÁT HIỆN, BẢO ĐẢM CÁC ĐIỀU KIỆN SẴN SÀNG ĐỐI PHÓ, ỨNG CỨU, KHẮC PHỤC SỰ CỐ.

Điều 6. Thực hiện xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố, có nội dung bao gồm:

1. Các nội dung, nhiệm vụ nhằm phòng ngừa sự cốvà phát hiện sớm:

- 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 an toàn thông tin mạng, phần mềm độc hại

- 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.

2. Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố.

- 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; thuê dịch vụ bảo đảm an toàn thông tin

- Chuẩn bị các nguồn lực để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.
- Tham gia các hoạt động của mạng lưới ứng cứu sự cố.

CHƯƠNG V

TỔ CHỨC THỰC HIỆN

Điều 7. Trách nhiệm của Văn phòng Sở.

- Chủ trì, phối hợp với các phòng, đơn vị trực thuộc ban hành kế hoạch, phương án cụ thể thực hiện các nội dung tại Điều 4 và Điều 5, Điều 6 của Kịch bản này.

- Làm 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 trực thuộc tiến hành kiểm tra các công tác bảo đảm ATTT mạng định kỳ hàng năm hoặc theo hướng dẫn của cơ quan chuyên môn.

- Tham mưu đưa nội dung dự phòng kinh phí, nhân lực, vật lực thường trực sẵn sàng ứng cứu sự cố; triển khai điều hành phối hợp tổ chức ứng cứu và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố vào các hoạch về bảo đảm ATTT mạng, ứng dụng CNTT.

Điều 8. Trách nhiệm của các phòng, đơn vị thuộc Sở.

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

- Chủ động bố trí kinh phí trang bị phần mềm chống virus, thiết bị tường lửa cho hệ thống máy tính, hệ thông mạng, hệ thống thông tin tại đơn vị mình.

- Phối hợp các đơn vị liên quan thực hiện công tác ứng phó khi sự cố ATTT mạng tại đơn vị mình.

Trong quá trình thực hiện Kịch bản này nếu có vấn đề vướng mắc, phát sinh, các phòng, đơn vị trực thuộc phán ánh kịp thời về Văn phòng Sở để tổng hợp báo cáo./.

Nơi nhận:
- Ban giám đốc;
- Các phòng CMNV, đơn vị trực thuộc;
- Lưu VT.

KT. GIÁM ĐỐC

PHÓ GIÁM ĐỐC

SỞ LAO ĐỘNG THƯƠNG BINH VÀ XÃ HỘI TỈNH THÁI BÌNH

Phạm Quang Hòa