SỞ NÔNG NGHIỆP VÀ PTNT HẢI PHÒNG
BAN QUẢN LÝ CẢNG CÁ, BẾN CÁ

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

Số:01 /PA-QLCC

Hải Phòng, ngày 19 *tháng* 3 *năm 2024*

PHƯƠNG ÁN
Phối hợp ứng phó sự cố an toàn thông tin mạng

Thực hiện Phương án số 01/PA-SNN ngày 05/3/2024 của Sở Nông nhiệp và Phát triển nông thôn về phối hợp ứng phó sự cố an toàn, an ninh thông tin mạng và an ninh thông tin liên quan đến thiết bị camera giám sát của Sở Nông nghiệp và Phát triển nông thôn.

Ban Quản lý cảng cá, bến cá (dưới đây gọi là Ban Quản lý) xây dựng Phương án về phối hợp ứng phó sự cố an toàn thông tin mạng, cụ thể như sau:

1. Phạm vi và đối tượng áp dụng:

a) Viên chức, người lao động làm việc tại Ban Quản lý theo hợp đồng làm việc, hợp đồng lao động, bao gồm cả người lao động giao kết hợp đồng bằng miệng, người lao động làm việc bán thời gian.

b) Tổ chức, cá nhân có liên quan kết nối, sử dụng hệ thống thông tin làm việc, cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng (ATTT mạng) phục vụ hoạt động tại Ban Quản lý.

2. Đánh giá các nguy cơ, sự cố ATTT mạng:

a) Đánh giá khả năng bảo đảm ATTT mạng và dự báo nguy cơ, sự cố, tình huống tấn công mạng có thể xảy ra đối với các hệ thống thông tin và các đối tượng cần bảo vệ:

- Khả năng bảo đảm ATTT mạng: không có nhân lực chuyên trách về bảo vệ hệ thống thông tin mạng, do vậy, gặp nhiều khó khăn trong quá trình theo dõi, kiểm tra, đánh giá.

- Các nguy cơ và tình huống tấn công mạng có thể, bao gồm: tấn công từ chối dịch vụ (DDoS), xâm nhập hệ thống, lừa đảo, phần mềm độc hại, rò rỉ dữ liệu…

- Các đối tượng cần bảo vệ: văn bản mật; thông tin cá nhân của viên chức, người lao động; thông tin tài chính và giao dịch; hệ thống lưu trữ; mạng nội bộ…

b) Đánh giá, dự báo về hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố ATTT mạng:

- Mất mát hoặc dữ liệu quan trọng bị phá hủy, bao gồm: thông tin cá nhân của viên chức, người lao động; thông tin về tài chính và dữ liệu khác…

- Phải tiêu tốn một lượng lớn tài nguyên và chi phí để khắc phục và phục hồi sự cố, bao gồm: thời gian làm việc, công cụ và công nghệ mới.

- Có thể gây ra tổn thương nghiêm trọng đến uy tín và hình ảnh của Ban Quản lý trong mắt các ngư dân, doanh nghiệp đối tác, cơ quan cấp trên, ảnh hưởng đến việc xét duyệt thi đua trong quá trình làm việc.

- Sự cố có thể dẫn đến các hậu quả pháp lý, bao gồm các biện pháp pháp lý, khoản bồi thường và việc mất đi uy tín đối với ngư dân, doanh nghiệp đối tác.

c) Hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố ATTT mạng (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có):

- Ban Quản lý đang gián tiếp sử dụng các phần mềm kết nối với hệ thống mạng nội bộ được đảm bảo chế độ bảo mật thông qua sự quản lý của cơ quan cấp trên: quản lý văn bản điện tử (HP net), quản lý thông tin tàu cá (VNFisbase), hệ thống giám sát tàu cá, quản lý cán bộ (MISA), kê khai bảo hiểm xã hội điện tử, phần mềm kế toán (dùng cho kho bạc), phần mềm khai báo kho bạc, hoá đơn điện tử, thuế điện tử.

- Mạng nội bộ tại Ban Quản lý có chế độ bảo mật riêng, được kiểm tra định kỳ về tình trạng kết nối, các trang thiết bị thông tin đặc biệt trang thiết bị phục vụ lưu trữ chỉ được cấp quyền truy cập cho 01 cá nhân, máy tính đang sử dụng tại các phòng, cảng cá đều cài đặt phần mềm diệt virus, phòng chống mã độc.

3. Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể:

a) Tiêu chí xây dựng phương án đối phó, ứng cứu sự cố ATTT mạng:

Xác định nhanh chóng, kịp thời, nguyên nhân, nguồn gốc các loại sự cố có thể xảy ra, phân loại chúng theo mức độ nghiêm trọng và ảnh hưởng đến hệ thống, dữ liệu 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.

b) Phương án đối phó, ứng cứu, khắc phục sự cố ATTT mạng:

- 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 ATTT mạng 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 ATTT mạng 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 ATTT mạng liên quan đến các thảm họa tự nhiên như: bão, lụt, động đất, hỏa hoạn…

4. Phối hợp thực hiện phòng ngừa, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố ATTT mạng:

a) Nội dung, nhiệm vụ nhằm phòng ngừa sự cố ATTT mạng và 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 ATTT mạng, phần mềm độc hại;

- Áp dụng quy trình, quy định, tiêu chuẩn ATTT mạng;

- Tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

b) Nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố ATTT mạng:

- 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 ATTT mạng;

- Chuẩn bị nguồn lực để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố ATTT mạng xảy ra.

- Ứng phó ngay khi có sự cố ATTT mạng xảy ra, bao gồm cách thức xử lý, giải quyết sự cố.

- Đánh giá mức độ nghiêm trọng, xác định nguyên nhân và phạm vi ảnh hưởng đến hệ thống và dữ liệu của sự cố ATTT mạng.

- Cách ly hệ thống hoặc dữ liệu bị ảnh hưởng để ngăn chặn sự lan rộng của sự cố ATTT mạng và bảo vệ các phần khác của mạng.

- Phối hợp với cơ quan chuyên môn có thẩm quyền thực hiện các biện pháp khắc phục để khôi phục hệ thống về trạng thái bình thường một cách an toàn, nhanh chóng.

- Ghi nhận lại các chi tiết về sự cố và các biện pháp ứng phó, từ đó cải thiện cách thức ứng phó trong tương lai.

- Tiến hành kiểm tra và đánh giá để đảm bảo rằng hệ thống đã được khôi phục một cách an toàn và không có hậu quả tiêu cực nào.

- Dựa trên các kinh nghiệm từ sự cố, cập nhật và cải thiện kế hoạch ứng phó để nâng cao khả năng đáp ứng và bảo vệ trước sự cố ATTT mạng.

5. Tổ chức thực hiện:

a) Các phòng, cảng cá triển khai thực hiện Kế hoạch số 13/KH-QLCC ngày 14/3/2024 của Ban Quản lý cảng cá, bến cá về An toàn thông tin mạng năm 2024 và các năm tiếp theo.

b) Mọi viên chức, người lao động chủ động thực hiện nghiêm quy định về sử dụng mạng internet, các quy định về bảo đảm ATTT mạng, chịu trách nhiệm trước lãnh đạo Ban Quản lý nếu để xảy ra mất ATTT mạng, an ninh thông tin, làm lộ, lọt bí mật nhà nước.

c) Thủ trưởng các phòng, cảng cá triển khai Phương án này đến 100% viên chức, người lao động thuộc thẩm quyền quản lý.

d) Giao Phòng Hành chính giúp Giám đốc Ban Quản lý: triển khai, kiểm tra, giám sát và tổng hợp, báo cáo việc thực hiện Phương án này./.

Nơi nhận:
- Sở NN-PTNT; (để b/c)
- GĐ, các PGĐ Ban QLCC;
- Các phòng, CC;
- Lưu: VT, PHC.

GIÁM ĐỐC

SỞ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN TỈNH PHÚ YÊN
BAN QUẢN LÝ CẢNG CÁ, BẾN CÁ

Đỗ Đức Hưng