UBND TỈNH KHÁNH HÒA
BAN QLDA ĐẦU TƯ XÂY DỰNG CÁC CÔNG TRÌNH NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN

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

Số: 303 /KH-BQLNN

Khánh Hòa, ngày 30 tháng 5 năm 2019

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng của Ban quản lý dự án đầu tư xây dựng các công trình Nông nghiệp và Phát triển nông thôn tỉnh Khánh Hòa năm 2019

Căn cứ Kế hoạch số 3669/KH-UBND ngày 19/04/2019 của Ủy ban nhân dân tỉnh Khánh Hòa về việc ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2019,

Thực hiện Công văn số 753/STTTT-CNTT ngày 02/5/2019 của Sở Thông tin và Truyền thông tỉnh Khánh Hòa về việc triển khai thực hiện Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2019,

Ban quản lý dự án đầu tư xây dựng các công trình Nông nghiệp và Phát triển nông thôn tỉnh Khánh Hòa xây dựng và triển khai Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng của Ban năm 2019, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích:

- Tập trung đảm bảo an toàn thông tin cho các hệ thống thông tin quan trọng của Ban, đảm bảo các khả năng xử lý một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên mạng. Đề ra các giải pháp ứng phó và hướng khắc phục khi gặp sự cố mất an toàn thông tin mạng.

- Phổ biến mức độ rủi ro và nâng cao nhận thức về an toàn thông tin đối với cán bộ công chức, viên chức và người lao động trong cơ quan. Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố bảo đảm an toàn thông tin mạng.

2. Yêu cầu:

- Căn cứ trên kết quả khảo sát, đánh giá các nguy cơ, sự cố mất an toàn thông tin mạng trên hệ thống thông tin của các cơ quan Nhà nước trên địa bàn tỉnh và trên cơ sở đó đối chiếu với tình hình thực tế của Ban trong thời gian qua, để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời và phù hợp.

- Có phương án đối phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra được các tiêu chí rõ ràng để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra.

- Đảm bảo nguồn lực, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, đảm bảo khả thi, hiệu quả.

II. NHIỆM VỤ TRIỂN KHAI

1. Triển khai các nhiệm vụ khi chưa có sự cố xảy ra

1.1 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

- **Nội dung thực hiện**: Tổ chức tuyên truyền, phổ biến trên trang Thông tin điện tử của Ban, Hệ thống phần mềm Quản lý văn bản E-Office của Ban và trên bản tin chung của Ban… đến tất cả các cán bộ công chức, viên chức và người lao động thuộc Ban về Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 và các văn bản quy phạm pháp luật về an toàn thông tin mạng.

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

1.2. Phối hợp tham gia triển khai các phương án, chương trình huấn luyện, diễn tập

- **Nội dung thực hiện**: Phối hợp 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 do các cơ quan chuyên môn thực hiện; huấn luyện, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố.

- **Thời gian thực hiện**: Theo kế hoạch của cơ quan chuyên trách ứng cứ sự cố an toàn thông tin mạng của tỉnh (Sở Thông tin và Truyền thông).

1.3. Triển khai các phương án, hướng dẫn phòng ngừa sự cố, giám sát, phát hiện sớm sự cố

- **Nội dung thực hiện**: Thực hiện việc giám sát, phát hiện sớm các nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin 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.

- **Thời gian thực hiện**: Định kỳ hàng quý.

1.4. Triển khai các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

- **Nội dung thực hiện**: Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, gia hạn bản quyền các phần mềm; chuẩn bị các điều kiện bảo đảm, dự phòng các nguồn lực và tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; thuê dịch vụ kỹ thuật, chuyên gia ứng cứu sự cố và sự hỗ trợ, phối hợp của các cơ quan, đơn vị liên quan khi tổ chức tham gia các hoạt động ứng cứu sự cố.

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

1.5. Kiểm tra, đánh giá các nguy cơ, sự cố an toàn thông tin mạng

- **Nội dung thực hiện**: Thực hiện việc kiểm tra, đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin; 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, tác động có thể nếu có xảy ra sự cố; đánh giá về

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 (*bao gồm của Đơn vị đã ký hợp đồng cung cấp dịch vụ nếu có*).

- **Thời gian thực hiện**: Định kỳ hàng quý.

1.6. Xây dựng các phương án đối phó, ứng cứu; dự báo, đưa ra các biện pháp khắc phục đối với một số tình huống sự cố cụ thể

- **Nội dung thực hiện**: Đối với hệ thống thông tin, chương trình ứng dụng, cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được 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:

a. 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 của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền...;

- 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 v.v...

b. 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....

c) 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;

d) Phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ, và dự kiến kinh phí để thực hiện, đối phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể.

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

2. Triển khai các nhiệm vụ, biện pháp khắc phục khi có sự cố xảy ra:

2.1. Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố

a. Tiếp nhận, xác minh sự cố

- **Nội dung thực hiện**: Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể xảy ra từ các nguồn bên trong và bên ngoài. Khi phân tích, xác minh sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác minh nguồn gốc sự cố.

b. Triển khai các bước ưu tiên ứng cứu ban đầu

- **Nội dung thực hiện**: Sau khi xác định sự cố xảy ra, đơn vị sử dụng, vận hành hệ thống thông tin căn cứ vào dấu hiệu, cảnh báo, hướng dẫn của cơ quan chuyên môn để tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo Kế hoạch ứng phó sự cố đã được cấp thẩm quyền phê duyệt hoặc làm theo hướng dẫn của cơ quan chuyên trách ứng cứu sự cố an toàn thông tin trên địa bàn tỉnh.

c. Triển khai lựa chọn các phương án ứng cứu

- **Nội dung thực hiện**: Căn cứ theo Kế hoạch ứng phó sự cố của Ban, hướng dẫn của cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh để lựa chọn phương án ngăn chặn và xử lý sự cố; Báo cáo, đề xuất đơn vị quản lý hệ thống thông tin để xin ý kiến chỉ đạo nếu cần.

d. Chỉ đạo xử lý sự cố (*nếu cần*)

- **Nội dung thực hiện**: Căn cứ theo báo cáo, đề xuất của các cán bộ, công chức, viên chức và người lao động trong Ban, Lãnh đạo Ban chỉ đạo cho cán bộ chuyên trách CNTT và các Lãnh đạo các phòng chuyên môn kiểm tra ngăn chặn và xử lý sự cố, đồng thời tổng hợp báo cáo lên Cơ quan chuyên trách ứng cứ sự cố an toàn thông tin mạng của tỉnh (Sở TTTT) hoặc Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa để được hướng dẫn triển khai công tác ứng cứu, xử lý sự cố; chỉ đạo, phân công cán bộ cung cấp thông tin. Trong quá trình ứng cứu, tùy thuộc vào diễn biến tình hình thực tế, cán bộ chuyên trách ứng cứu sự cố an toàn thông tin mạng sẽ điều chỉnh phương án ứng cứu sự cố.

đ. Báo cáo sự cố

- **Nội dung thực hiện**: Sau khi đã triển khai các bước ưu tiên ứng cứu ban đầu, sau đó tổ chức thông báo, báo cáo sự cố đến các cá nhân liên quan bên trong và bên ngoài cơ 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).

e. Công tác phối hợp trong ứng cứu

- **Nội dung thực hiện**: Căn cứ vào tính chất sự cố, đề nghị hỗ trợ của các đơn vị sử dụng, vận hành hệ thống thông tin và cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng, các cơ quan, đơn vị liên quan tích cực thực hiện công tác phối hợp, hỗ trợ và tạo điều kiện thuận lợi để thực hiện công tác ứng cứu, xử lý sự cố.

2.2. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- **Nội dung thực hiện**: Triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng; 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.

2.3. Xử lý sự cố, gỡ bỏ và khôi phục

a. Xử lý sự cố, gỡ bỏ

Nội dung thực hiện: Sau khi đã triển khai ngăn chặn sự cố, Lãnh đạo Cơ quan chỉ đạo cán bộ chuyên trách và những cá nhân có liên quan đến việc sử dụng, quản lý, vận hành hệ thống thông tin phối hợp với cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng triển khai biện pháp tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.

b. Khôi phục

- **Nội dung thực hiện**: Cán bộ chuyên trách vận hành hệ thống thông tin chủ trì phối hợp với các Phòng, đơn vị liên quan triển khai các hoạt động 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.

c. Kiểm tra, đánh giá hệ thống thông tin

- **Nội dung thực hiện**: Cán bộ chuyên trách vận hành hệ thống thông tin phối hợp các cơ quan, đơn vị liên quan 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, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ chức các bước tương ứng tại Khoản 2.2 và Khoản 2.3 của Kế hoạch này để khôi phục hoạt động bình thường của hệ thống thông tin.

2.5. Tổng kết, đánh giá

- **Nội dung thực hiện**: Cán bộ chuyên trách Công nghệ thông tin của đơn vị bị sự cố phối hợp với cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng của tỉnh triển khai tổng hợp toàn bộ các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai phương án ứng cứu sự cố báo cáo cho chủ quản hệ thống thông tin và Ban Chỉ đạo Ứng dụng công nghệ thông tin tỉnh Khánh Hòa để tổ chức phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện theo dự toán chi phí Ban 2019.

IV. TỔ CHỨC THỰC HIỆN

1. Các phòng nghiệp vụ triển khai thực hiện các nhiệm vụ sau:

Phối hợp với Phòng Tài chính - Tổng hợp và cán bộ phụ trách công nghệ thông tin trao đổi, xử lý những vấn đề có liên quan đến việc ứng dụng công nghệ thông tin của Ban, đảm bảo hoạt động có hiệu quả.

2. Trong quá trình tổ chức thực hiện kế hoạch này, nếu có khó khăn vướng mắc, đề nghị các phòng đóng góp ý kiến qua phòng Tài chính - Tổng hợp để tổng hợp báo cáo Lãnh đạo Ban xem xét, quyết định.

Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, các Phòng nghiệp vụ trong Ban liên hệ trực tiếp đến phòng Tài chính – Tổng hợp xem xét, sửa đổi và điều chỉnh cho phù hợp./.

Nơi nhận:
- UBND tỉnh (để b/cáo);
- Sở TTTT (để biết);
- Tất cả CCVC và Phòng nghiệp vụ của Ban;
- Lưu:VT, A.Phong.

GIÁM ĐỐC

ỦY BAN NHÂN DÂN TỈNH KHÁNH HÒA
BAN QUẢN LÝ DỰ ÁN ĐẦU TƯ XÂY DỰNG CÁC CÔNG TRÌNH NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN T. KHÁNH HÒA

Quách Thanh Sơn
BQLDA đầu tư xây dựng các công trình NN và PTNT, Tỉnh Khánh Hòa
30/01/2019 11:35:26 +07:00

Quách Thanh Sơn