

KẾ HOẠCH
Ứng phó sự cố bảo đảm an toàn thông tin mạng
trên địa bàn xã Thanh An

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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;

Công văn số 1737/UBND-KGVX ngày 05/4/2024 của Chủ tịch UBND tỉnh Quảng Ngãi về việc tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ trên địa bàn tỉnh;

Ủy ban nhân dân xã Thanh An xây dựng kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Phối hợp với Đội ứng phó sự cố huyện, đề ra các phương án ứng phó kịp thời khi gặp sự cố mất an toàn thông tin (ATTT) mạng. Bảo đảm ATTT mạng cho hệ thống thông tin của UBND xã

- Bảo đảm nhân lực, vật lực, tài lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng cứu sự cố ATTT mạng.

2. Yêu cầu

- Hệ thống thông tin phải được đánh giá hiện trạng và khả năng bảo đảm ATTT mạng, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra để đưa ra phương án ứng phó, ứng cứu sự cố kịp thời, phù hợp.

- Công tác ứng phó sự cố ATTT mạng phải tuân thủ theo quy chế, quy định pháp luật; tổ chức ứng phó kịp thời, nhanh chóng, đồng bộ và hiệu quả.

- Hoạt động ứng cứu sự cố an toàn thông tin mạng phải chuyển từ bị động sang chủ động, bao gồm: Chủ động thực hiện sẵn lòng mỗi nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý.

II. NHIỆM VỤ

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

- Tuyên truyền, phổ biến các văn bản chỉ đạo trên Trang thông tin điện tử của xã Chỉ thị số 14/CT-TTg ngày 07/6/2014 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng an toàn

thông minh của xã, huyện, tỉnh Quảng Ngãi; Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng Quốc gia; Thông tư 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ thông tin và truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về nâng cao năng lực phòng chống phần mềm độc hại; văn bản số 476/BTTTT-CATTT ngày 30/3/2024 của Bộ Thông tin và Truyền thông về tăng cường bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin.

- Phối hợp tham gia triển khai thực hiện các phương án, chương trình huấn luyện, diễn tập đối phó, ứng cứu sự cố 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.

- Giám sát, phát hiện sớm các nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin mạng và rà quét, xử lý mã độc; phòng ngừa sự cố, quản lý rủi ro; cảnh báo sự cố, nghiên cứu, phân tích, xác minh phần mềm độc hại; 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.

- Triển khai các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố như: 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; 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.

- Tổ chức kiểm tra, đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin; dự báo các nguy cơ, sự cố tấn công mạng có thể xảy ra và các hậu quả, thiệt hại, tác động nếu có; 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 các nhà thầu đã ký hợp đồng cung cấp dịch vụ).

- Xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng đối với mỗi hệ thống thông tin, chương trình ứng dụng. Phải đặt ra các tiêu chí để xác định được tính chất, mức độ nghiêm trọng khi sự cố xảy ra. Các cơ quan, đơn vị sử dụng, vận hành hệ thống thông tin, chương trình ứng dụng phải xây dựng phương án đối phó, ứng cứu sự cố.

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

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 của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố và tuân thủ theo các quy định, hướng dẫn của Bộ thông tin và Truyền thông đảm bảo các nội dung sau:

- a) Quy trình triển khai và các bước ưu tiên ứng cứu ban đầu khi hệ thống thông tin gặp sự cố, có phân theo các loại sự cố thực hiện theo mục 3, Phần III. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố của Kế hoạch

này.

b) 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. Các sự cố thường gặp:

- 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, 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 và các sự cố gây mất ATTT mạng khác.

c) Phương án đối phó, khắc phục sự cố đối với một hoặc nhiều tình huống.

- 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 ATTT;
- + 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 thiên tai, thảm họa tự nhiên, như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

d) Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, các tổ chức trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.

- Đơn vị chủ trì: Ban Chỉ đạo chuyển đổi số xã

- Đơn vị phối hợp: Văn phòng Thống kê xã; Phòng Văn hóa và Thông tin huyện, Đội ứng cứu sự cố ATTT mạng của huyện; các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên hàng năm.

đ) 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.

- Đơn vị chủ trì: Các ban, ngành, Hội đoàn thể xã.

- Đơn vị phối hợp: Văn phòng Thống kê xã; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên hàng năm.

3. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố

3.1. Thông báo, báo cáo sự cố ATTT mạng:

- Khi có sự cố xảy ra, các ban ngành, hội đoàn thể xã có báo ngay về Văn phòng Thống kê xã để có phương án hỗ trợ, xử lý.

- Thời gian thực hiện: Thường xuyên, ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

3.2. Phát hiện, tiếp nhận, xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng: Văn phòng Thống kê xã chủ trì phối hợp Đội ứng cứu sự cố an toàn thông tin huyện; Phòng Văn hoá và Thông tin hướng dẫn, xử lý khắc phục những sự cố nhỏ hoặc liên hệ ngay với Sở Thông tin và Truyền thông để Đội ứng cứu sự cố tỉnh có hướng dẫn, xử lý khắc phục...

- Đơn vị chủ trì: Văn phòng Thống kê xã.

- Thời gian thực hiện: Ngay sau khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố của tổ chức, cá nhân.

III. TỔ CHỨC THỰC HIỆN

1. Công chức VH – XH xã:

- Phối hợp với các ngành có liên quan triển khai thực hiện Kế hoạch; hướng dẫn các cơ quan, đơn vị trên địa bàn xã trong công tác đảm bảo an toàn thông tin mạng. Tổng hợp, báo cáo kết quả thực hiện Kế hoạch về UBND xã, Phòng Văn hóa – Thông tin huyện theo đúng quy định

2. Công chức Văn phòng - Thống kê xã:

- Chủ trì, thực hiện cảnh báo; phối hợp với các đơn vị có liên quan xử lý tình huống khi xảy ra sự cố.

- Tham gia đầy đủ các lớp tập huấn Ứng phó sự cố, bảo đảm an toàn thông tin mạng do tỉnh tổ chức.

- Phối hợp các cơ quan đơn vị mở lớp tập huấn Ứng phó sự cố, bảo đảm an toàn thông tin mạng triển khai đến các cơ quan, đơn vị, địa phương.

3. Công chức Tài chính – Kế toán xã:

Phối hợp với các đơn vị liên quan tham mưu UBND xã bố trí kinh phí thực hiện Kế hoạch theo đúng quy định.

4. Đài truyền thanh xã:

Thông tin, tuyên truyền công tác đảm bảo an toàn thông tin mạng rộng rãi trên hệ thống Đài truyền thanh xã.

5. Các cơ quan, đơn vị, ban, ngành, đoàn thể đóng trên địa bàn xã:

Tổ chức thực hiện Kế hoạch tại cơ quan, đơn vị. Bố trí cán bộ, công chức, viên chức của cơ quan, đơn vị phụ trách công tác đảm bảo an toàn thông tin tại cơ quan, đơn vị.

Trên đây là Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn xã Thanh An năm 2024. Trong quá trình thực hiện nếu có khó khăn, vướng mắc, các cơ quan, đơn vị phản ánh về Công chức VH – XH xã để tổng hợp, báo cáo UBND xã xem xét, giải quyết./

Nơi nhận:

- UBND huyện;
- Phòng VH&TT huyện;
- Thường trực ĐU, HĐND xã;
- CT, các PCT UBND xã;
- Trang tin điện tử xã;
- Lưu: VT.

CHỦ TỊCH

Đinh Văn Dục