Người ký: Ủy ban nhân dân tỉnh Tây Ninh
Cơ quan: Tỉnh Tây Ninh
Thời gian ký: 27.01.2021 09:33:21 +07:00

ỦY BAN NHÂN DÂN **TỈNH TÂY NINH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 231 /KH- UBND	*Tây Ninh, ngày 25 tháng 01 năm 2021*

KẾ HOẠCH

Đảm bảo an toàn an ninh thông tin các hệ thống thông tin của tỉnh trong thời gian Đại hội lần thứ XIII của Đảng và các dịp lễ, tết năm 2021

Nhằm tăng cường bảo đảm an toàn, an ninh mạng, không để bị động, bất ngờ với mọi tình huống tấn công mạng và phát tán thông tin xấu độc trong thời gian diễn ra các sự kiện lớn của đất nước. Đặc biệt là Đại hội đại biểu toàn quốc lần thứ XIII của Đảng, Tết Nguyên đán Tân Sửu và các ngày lễ trong năm, Ủy ban nhân dân tỉnh ban hành kế hoạch đảm bảo an toàn an ninh thông tin, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Quy định trình tự, cách thức thực hiện, kiểm soát việc xử lý sự cố khi bị tấn công mạng hoặc xảy ra sự cố đối với hệ thống thông tin gây ảnh hưởng đến hoạt động (gọi chung là sự cố an toàn thông tin mạng) nhằm giảm thiểu tác động của sự cố một cách nhanh chóng, kịp thời và hiệu quả.

- Đảm bảo hoạt động ổn định xuyên suốt các trang thông tin, hệ thống phần mềm dùng chung của tỉnh và các hệ thống phần mềm của các Sở, ban, ngành đang vận hành tại Trung tâm tích hợp dữ liệu (TTTHDL) của tỉnh trong thời gian Đại hội lần thứ XIII của Đảng, các dịp lễ, tết năm 2021.

2. Yêu cầu

- Khắc phục sự cố và phục hồi hoạt động của hệ thống thông tin một cách nhanh nhất (nếu hệ thống bị phá hoại). Hoặc duy trì hoạt động bình thường của hệ thống thông tin với sự giám sát an ninh ở mức độ cao (trường hợp hệ thống không bị phá hoại mà chỉ lộ lọt thông tin).

- Cơ sở vật chất, nguồn lực phải được ưu tiên cho công tác xử lý sự cố.

- Báo cáo ngay Lãnh đạo UBND tỉnh ngay khi xảy ra sự cố gây mất an toàn thông tin trên địa bàn tỉnh

II. NỘI DUNG

1. Tuyên truyền, phổ biến các văn bản quy phạm pháp luật; tập huấn nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng

- Tổ chức hội nghị tuyên truyền, phổ biến về Luật An toàn thông tin mạng; Luật An ninh mạng; 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; Quyết định

số 05/2017/QĐ-TTg ngày 16/3/2017 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; Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ; Thông tư số 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.

- Tập huấn nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng cho cán bộ, công chức, viên chức.

- Đơn vị chủ trì: Sở Thông tin và Truyền thông.

- Đơn vị phối hợp: Các sở, ban, ngành tỉnh; UBND các huyện, thị xã, thành phố; các đơn vị có liên quan của tỉnh.

2. Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu 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.

- Đơn vị thực hiện: Các sở, ban, ngành tỉnh; UBND các huyện, thị xã, thành phố.

- Đơn vị phối hợp: Đơn vị chuyên trách ứng cứu sự cố (Sở Thông tin và Truyền thông); Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh; các đơn vị liên quan khác.

3. Xây dựng phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

Đối với mỗi 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, 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 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 niềm, 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: Sở Thông tin và Truyền thông;

- Đơn vị phối hợp: Các sở, ban, ngành tỉnh; UBND các huyện, thị xã, thành phố; Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh;

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

Triển khai các hoạt động thuộc trách nhiệm của các cơ quan, đơn vị liên quan theo quy định tại Điều 11, Điều 12, Điều 13, Điều 14 và các nội dung liên quan khác thuộc Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 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 (sau đây gọi tắt là Quyết định số 05/2017/QĐ-TTg).

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 khi có sự cố xảy ra.

a) Báo cáo sự cố an toàn thông tin mạng theo quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg, Điều 9 Thông tư 20/2017/TT-BTTTT.

- Đơn vị thực hiện:

+ Đơn vị vận hành hệ thống thông tin (các Sở, ngành; UBND cấp huyện) báo cáo cơ quan Chủ quản hệ thống thông tin, Sở Thông tin và Truyền thông.

+ Sở Thông tin và Truyền thông báo cáo cơ quan UBND tỉnh, Ban Chỉ đạo xây dựng chính quyền điện tử tỉnh, Cơ quan điều phối quốc gia và báo cáo Cơ quan thường trực và Ban Chỉ đạo quốc gia về ứng cứu sự cố.

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

b) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Điều 10 Thông tư 20/2017/TT-BTTTT của Bộ Thông tin và Truyền thông.

- Đơn vị chủ trì: Sở Thông tin và Truyền thông; đơn vị vận hành hệ thống thông tin (các sở, ban, ngành tỉnh; UBND các huyện, thị xã, thành phố).

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam –VNCERT/CC); tổ chức, cá nhân gửi thông báo, báo cáo sự cố; đơn vị cung cấp dịch vụ an toàn thông tin mạng (nếu có); các đơn vị chức năng liên quan.

- 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.

c) Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Điều 11 Thông tư 20/2017/TT-BTTTT của Bộ Thông tin và Truyền thông.

5. Triển khai huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố, cụ thể bao gồm:

a) Triển khai các chương trình huấn luyện, diễn tập.

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; 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; tham gia huấn luyện, diễn tập vùng, miền, quốc gia, quốc tế.

- Đơn vị chủ trì: Sở Thông tin và Truyền thông; Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh.

- Đơn vị phối hợp: Đơn vị vận hành hệ thống thông tin (các sở, ban, ngành tỉnh; UBND các huyện, thị xã, thành phố); Cơ quan điều phối quốc gia (Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam – VNCERT/CC); các đơn vị chức năng liên quan.

b) Các nội dung, nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố

Giám sát, phát hiện sớm nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin mạng và rà quét, bóc gỡ, phân tích, xử Iý 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.

- Đơn vị chủ trì: Sở Thông tin và Truyền thông; đơn vị vận hành hệ thống thông tin (các sở, ban, ngành tỉnh; UBND các huyện, thị xã, thành phố); Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam – VNCERT/CC); các đơn vị chức năng liên quan.

c) 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 hoạt động của đội ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- Đơn vị chủ trì: Sở Thông tin và Truyền thông; đơn vị vận hành hệ thống thông tin (các sở, ban, ngành tỉnh; UBND các huyện, thị xã, thành phố); Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam – VNCERT/CC); các đơn vị chức năng liên quan.

III. TỔ CHỨC THỰC HIỆN

1. Các sở ban, ngành tỉnh; UBND các huyện, thị xã, thành phố

- Xây dựng nội dung để triển khai các nhiệm vụ được giao tại Kế hoạch này.

- Phân công lãnh đạo phụ trách và thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về an toàn thông tin mạng của cơ quan, đơn vị.

- Thông báo, phối hợp với các đơn vị có liên quan khi xảy ra sự cố gây mất an toàn thông tin.

2. Sở Thông tin và Truyền thông

- Xây dựng kế hoạch đảm bảo an toàn thông tin, đảm bảo hoạt động tại Trung tâm tích hợp dữ liệu tỉnh.

- Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về ATTT mạng trên địa bàn tỉnh.

- Tham mưu, hướng dẫn tổ chức thực hiện, đôn đốc, kiểm tra, đánh giá, giám sát công tác bảo đảm an toàn thông tin theo Kế hoạch này.

- Theo dõi, hướng dẫn, kiểm tra, giám sát việc thực hiện ứng phó sự cố đảm bảo an toàn thông tin mạng ở các sở, ban, ngành tỉnh và Ủy ban nhân dân các huyện, thị xã, thành phố.

3. Công an tỉnh

- Phối hợp với Sở Thông tin và Truyền thông tham mưu UBND tỉnh ban hành kế hoạch, phương án ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh.

- Tổ chức, chỉ đạo, triển khai công tác phòng, chống, điều tra tội phạm lợi dụng hệ thống mạng để xâm phạm an ninh quốc gia, gây mất an toàn thông tin mạng, mất trật tự an toàn xã hội.

- Phối hợp với Sở Thông tin và Truyền thông kiểm tra, xử lý các vi phạm về an toàn thông tin mạng theo quy định.

- Hỗ trợ các cơ quan, đơn vị đánh giá nguy cơ mất an toàn thông tin mạng khi có yêu cầu.

Trên đây là Kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Tây Ninh; Ủy ban nhân dân tỉnh yêu cầu Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch UBND các huyện, thị xã, thành phố nghiêm túc triển khai thực hiện. Trong quá trình thực hiện nếu có khó khăn, vướng mắc đề nghị các đơn vị, địa phương phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp báo cáo Ủy ban nhân dân tỉnh chỉ đạo giải quyết./.

Nơi nhận:
- CT, các PCT;
- Văn phòng Tỉnh ủy;
- Các sở, ban, ngành tỉnh;
- UBND các huyện, thị xã, thành phố;
- LĐVP;
- Phòng KGVX;
- Lưu: VT, VP UBND tỉnh.

Trinh

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

ỦY BAN NHÂN DÂN TỈNH TÂY NINH

Trần Văn Chiến