UBND TỈNH KHÁNH HÒA **BAN DÂN TỘC**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 12/KH-BDT	*Khánh Hòa, ngày 25 tháng 02 năm 2020*

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn, an ninh thông tin mạng trong hoạt động cơ quan Ban Dân tộc tỉnh Khánh Hoà năm 2020

Thực hiện Kế hoạch số 860/KH-UBND ngày 21/01/2020 của UBND tỉnh về việc ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2020; Ban Dân tộc tỉnh xây dựng và ban hành Kế hoạch ứng phó sự cố, bảo đảm an toàn, an ninh thông tin mạng trong hoạt động cơ quan Ban Dân tộc tỉnh Khánh Hoà năm 2020 như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Đảm bảo an toàn cho hệ thống thông tin mạng của cơ quan, đảm bảo khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin mạng; đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với lực lượng cán bộ, công chức, lao động trong cơ quan.

2. Yêu cầu

- Chủ động nghiên cứu các văn bản chỉ đạo, đánh giá các nguy cơ, sự cố an toàn thông tin mạng của toàn hệ thống để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời, phù hợp.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng cứu sự cố bảo đảm an toàn thông tin mạng.

II. NHIỆM VỤ

1. Triển khai nhiệm vụ khi chưa có sự cố

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

- Tổ chức tuyên truyền, phổ biến trên cổng thông tin điện tử, các cuộc họp giao ban các văn bản về an toàn thông tin như: Luật An toàn thông tin mạng, Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Thông tư số 121/2018/TT-BTC ngày 12/12/2018 của Bộ Tài chính quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng.

- Tạo điều kiện và cử cán bộ, công chức tham gia các lớp đào tạo, tập huấn đảm bảo an toàn thông tin mạng để nâng cao kỹ năng và công tác tham mưu triển khai, giám sát, đảm bảo an toàn thông tin.

1.2. Triển khai phòng ngừa sự cố, giám sát, phát hiện sớm sự cố

- Thường xuyên rà soát, báo cáo cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng (Sở Thông tin và Truyền thông, Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa) khi có nghi ngờ mã độc, 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.

1.3. Triển khai 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; chuẩn bị các điều kiện bảo đảm và tham gia các hoạt động sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

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

Tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng đối với hệ thống thông tin; đánh giá, dự báo các nguy cơ, sự cố tấn công mạng có thể xảy ra với 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 phục vụ đối phó, ứng cứu, khắc phục sự cố của cơ quan, đơn vị.

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

a) Xác định 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) Phối hợp với Sở Thông tin và Truyền thông, Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa trong việc đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.

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

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

- Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể từ các nguồn bên trong và bên ngoài; thu thập chứng cứ, xác định nguồn gốc sự cố.

- Tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo kế hoạch ứng phó sự cố theo hướng dẫn của Sở Thông tin và Truyền thông; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa.

- Lựa chọn phương án ngăn chặn và xử lý sự cố; báo cáo sự cố theo quy định tại Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông gửi Sở Thông tin và Truyền thông để tổng hợp báo cáo Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh Khánh Hòa.

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

Thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng; 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

- Kịp thời ngắt kết nối máy vi tính ra khỏi mạng LAN, Internet; sao chép các dữ liệu cần thiết ra thiết bị lưu ngoài (CD, USB, ổ cứng di động,...).

- Phối hợp với Sở thông tin và Truyền thông, Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh khẩn trương ngăn chặn sự cố, đồng thời 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.

- Phối hợp với các 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 của hệ thống thông tin.

- 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 theo quy định để xử lý dứt điểm, khôi phục hoạt động bình thường của hệ thống thông tin.

2.4. Tổng kết, đánh giá

Tổng hợp 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 Sở Thông tin và Truyền thông để tổng hợp, 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 ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2020 lồng ghép trong Kế hoạch ứng dụng công nghệ thông tin của cơ quan.

IV. TỔ CHỨC THỰC HIỆN

1. Văn phòng Ban có trách nhiệm đôn đốc, theo dõi, hướng dẫn, kiểm tra, giám sát việc thực hiện ứng phó sự cố đảm bảo an toàn thông tin mạng ở các phòng chuyên môn của Ban Dân tộc, báo cáo kết quả thực hiện theo quy định; tham mưu thực hiện việc xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 và Điều 15 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 và theo hướng dẫn tại Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

2. Cán bộ phụ trách CNTT chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của các thiết bị mạng theo đúng tiêu chuẩn kỹ thuật; xử lý, khắc

phục kịp thời khi xảy ra sự cố máy tính bị Vi rút xâm nhập; đảm bảo an toàn thông tin trước khi tiến hành các hoạt động quản lý, vận hành hệ thống thông tin. Tham mưu đề xuất Lãnh đạo Ban nâng cấp trang thiết bị, công cụ, phương tiện liên quan đến công tác đảm bảo an toàn thông tin, sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

3. Cán bộ, công chức thuộc Ban có trách nhiệm bảo vệ và bảo mật tài khoản, dữ liệu cá nhân và nghiêm túc triển khai thực hiện Kế hoạch này./.

Nơi nhận: (VBĐT)
- Sở TTTT;
- Lãnh đạo Ban;
- Các phòng chuyên môn thuộc Ban;
- Kế toán;
- Lưu: VT, VP.

TRƯỞNG BAN

CỘNG HÒA X.H.C.N VIỆT NAM
BAN DÂN TỘC
TỈNH KHÁNH HÒA

Ban Dân tộc
Ủy ban Nhân dân tỉnh Khánh Hòa
25.02.2020 10:03:26 +07:00

Đặng Văn Tuấn