UBND TỈNH QUẢNG TRỊ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 34 /KH - STTTT

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

Quảng Trị, ngày 11 tháng 5 năm 2022

KẾ HOẠCH
Diễn tập thực chiến bảo đảm an toàn thông tin mạng tỉnh Quảng Trị năm 2022

Thực hiện Văn bản số 633/CATTT-VNCERT ngày 05/5/2021 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc đôn đốc thực hiện tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng; Sở Thông tin và Truyền thông tỉnh Quảng Trị xây dựng Kế hoạch diễn tập thực chiến bảo đảm an toàn thông tin mạng tỉnh Quảng Trị năm 2022 như sau:

I. CĂN CỨ LẬP KẾ HOẠCH

- Quyết định 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;

- Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ về phê duyệt Đề án "Đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố an toàn, tăng cường năng lực cho cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến năm 2020, định hướng đến 2025";

- Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng;

- Hướng dẫn số 01/HD-CATTT ngày 24/02/2022 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc hướng dẫn thực hiện hoạt động diễn tập thực chiến;

- Quyết định số 958/QĐ-UBND ngày 05/4/2022 của UBND tỉnh Quảng Trị về việc ban hành Kế hoạch và phê duyệt dự toán kinh phí đào tạo, bồi dưỡng cán bộ, công chức, viên chức tỉnh Quảng Trị năm 2022.

II. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Nâng cao năng lực bảo vệ an toàn thông tin, sẵn sàng ngăn chặn, xử lý và ứng cứu sự cố tấn công trên không gian mạng cho cán bộ chuyên trách hoặc phụ trách CNTT của các quan, đơn vị trên địa bàn tỉnh.

- Trang bị những kỹ năng cần thiết để kịp thời phối hợp ứng phó, giải quyết các vấn đề thông qua tình huống tấn công vào hệ thống thực khi khai thác các hệ thống thông tin trên môi trường mạng cho đội ngũ cán bộ chuyên trách hoặc phụ trách CNTT tại các Sở, ban, ngành, UBND các huyện, thị xã, thành phố trên địa bàn tỉnh Quảng Trị.

- Thực hiện đúng văn bản quy định, hướng dẫn của cấp trên về hoạt động diễn tập an toàn thông tin (Quy định tại Điều 1, mục II, khoản 4 của Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017: "Hàng năm mỗi bộ, tỉnh, thành phố tổ chức ít nhất 01 cuộc diễn tập chuyên đề an toàn thông tin, ứng cứu sự cố mạng trong phạm vi của bộ, ngành, địa phương mình; phối hợp, tham gia các cuộc diễn tập quốc gia và quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức).

2. Yêu cầu

- Triển khai hoạt động diễn tập thực chiến trên hệ thống đang vận hành như cổng thông tin điện tử, cổng dịch vụ công trực tuyến, hệ thống thư điện tử, hệ thống quản lý văn bản điều hành hoặc các hệ thống cần thiết khác; chú trọng diễn tập trên các hệ thống hiện diện trên mạng Internet, đặc biệt là các hệ thống, nền tảng phục vụ chính phủ điện tử, đô thị thông minh, chuyển đổi số. Các tình huống diễn tập phải đảm bảo hiệu quả, thiết thực, phù hợp với thực tế, tuân thủ các quy định về điều phối, ứng cứu sự cố an toàn thông tin theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 13/3/2017, Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017; Hướng dẫn số 1/HD-CATTT ngày 24/02/2022 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc hướng dẫn thực hiện hoạt động diễn tập thực chiến.

- Công tác tổ chức, chuẩn bị phải chu đáo, đảm bảo chất lượng về nội dung, thời gian, thành phần tham gia diễn tập; Bảo đảm hệ thống an toàn trong quá trình diễn tập; xây dựng phương án dự phòng xử lý rủi ro và sẵn sàng ứng cứu khi xảy ra sự cố trong quá trình diễn tập.

III. NỘI DUNG

1. Chủ đề diễn tập

Điều tra, xử lý và phòng chống các hoạt động tấn công không gian mạng như: làm mất kết nối Internet; giả mạo, đánh sập các website; phát tán mã độc tống tiền; tấn công có chủ đích…

Chi tiết nội dung tại Phụ lục kèm theo.

2. Thành phần tham gia

- Ban tổ chức: Sở Thông tin và Truyền thông tỉnh Quảng Trị

- Đội tấn công gồm: Thuê chuyên gia ATTT của VNCERT/CC.

- Đội phòng thủ gồm: Công chức chuyên trách CNTT các Sở, ban, ngành, UBND các huyện, thị xã, thành phố trên địa bàn tỉnh.

3. Thời gian

Thời gian: 05 ngày. Dự kiến tổ chức vào Quý III năm 2022.

IV. KINH PHÍ THỰC HIỆN Thực hiện theo Quyết định số 958/QĐ-UBND ngày 05/4/2022 của UBND tỉnh Quảng Trị về việc ban hành Kế hoạch và phê duyệt dự toán kinh phí đào tạo, bồi dưỡng cán bộ, công chức, viên chức tỉnh Quảng Trị năm 2022.

V. TỔ CHỨC THỰC HIỆN

1. Trung tâm Công nghệ thông tin và Truyền thông

- Chủ trì tham mưu, xây dựng chương trình diễn tập, phối hợp chuyên gia ATTT và Đơn vị cung cấp dịch vụ VNPT, Viettel Quảng Trị tổ chức, triển khai diễn tập.

- Phối hợp với Phòng Bưu chính, Viễn thông - Công nghệ thông tin, Văn phòng Sở chuẩn bị các điều kiện phục vụ diễn tập.

- Tham mưu lập ban hành Giấy mời và các tài liệu phục vụ diễn tập.

- Tổng hợp báo cáo kết quả diễn tập để báo cáo về UBND tỉnh, các cơ quan, đơn vị sau khi kết thúc diễn tập.

2. Văn phòng, Phòng Bưu chính, Viễn thông - Công nghệ thông tin

- Chủ trì, phối hợp với các phòng, Trung tâm Công nghệ thông tin và Truyền thông chuẩn bị các điều kiện phục vụ diễn tập (hội trường, khánh tiết, đón tiếp đại biểu).

- Hỗ trợ Trung tâm Công nghệ thông tin và Truyền thông thực hiện và điều hành diễn tập.

3. Đề nghị các sở, ban, ngành, UBND cấp huyện

- Đề nghị các cơ quan, đơn vị tạo điều kiện và cử cán bộ chuyên trách, phụ trách CNTT tham gia đầy đủ, đúng thời gian.

- Các thành viên tham gia diễn tập chịu sự phân công nhiệm vụ của Ban tổ chức diễn tập.

Trên đây là Kế hoạch diễn tập thực chiến bảo đảm an toàn thông tin mạng tỉnh Quảng Trị năm 2022./.

Nơi nhận:
- Cục An toàn thông tin - Bộ Thông tin và Truyền thông;
- UBND tỉnh (*Báo cáo*);
- Các sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Lưu: VT, BCVT&CNTT.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG TRỊ

Nguyễn Văn Tường

Phụ lục

Nội dung diễn tập thực chiến bảo đảm an toàn thông tin mạng tỉnh Quảng Trị

(Kèm theo Kế hoạch số /KH-STTTT ngày 11/5/2022 của Sở Thông tin và Truyền thông Quảng Trị)

Thời gian	Nội dung	Thực hiện
Ngày 1	Tổng quan tình hình ATTT	- Tình hình an toàn thông tin - Các kỹ thuật tấn công diện rông, tấn công có chủ đích - Tấn công có chủ đích sử dụng mã độc - Tổng quan về phân tích mã độc - Phân tích mã độc trong ứng cứu sự cố - Môi trường phân tích mã độc. *Thực hành: tấn công có chủ đích sử dụng mã độc; xây dựng môi trường phân tích, xử lý, bóc gỡ.*
Ngày 2	Điều tra, phân tích mã độc và biện pháp ngăn chặn	- Kỹ thuật phân tích tĩnh cơ bản - Kỹ thuật phân tích động cơ bản và nâng cao - Kỹ thuật điều tra, phân tích gói tin - Sử dụng thiết bị giám sát, điều tra, ngăn chặn - Gia cố hệ thống máy chủ - Gia cố cơ sở dữ liệu - Chống tấn công lây lan, phát tán. *Thực hành: cách thức thu thập, phân tích, bóc gỡ mã độc bằng các công cụ chuyên dụng.*
Ngày 3	Ứng cứu sự cố tấn công bằng mã độc	- Phương án và Quy trình ứng cứu sự cố - Tổ chức hoạt động ứng cứu sự cố - Triển khai ứng cứu sự cố - Tổng kết, đánh giá và rút kinh nghiệm. *Thực hành: xây dựng quy trình ứng cứu sự cố; ứng cứu sự cố mã độc.*
Ngày 4	Hướng dẫn sử dụng các công cụ trong bài diễn tập	- Công cụ bảo mật WireShark - Sử dụng Burp Suite đánh giá bảo mật ứng dụng.
Ngày 5	Diễn tập	Các cơ quan, đơn vị tham dự
	Tổng kết diễn tập và trao đổi kinh nghiệm ứng cứu sự cố giữa các đơn vị	Các cơ quan, đơn vị tham dự