BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 60 /CT-BTTTT

Hà Nội, ngày 16 tháng 9 năm 2021

CHỈ THỊ

Về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng

Bảo đảm an toàn thông tin mạng là nhiệm vụ then chốt, liên quan mật thiết tới sự phát triển bền vững của quá trình chuyển đổi số. Việc đảm bảo an toàn thông tin mạng gắn liền với việc nâng cao năng lực chuyên môn của đội ứng cứu sự cố của cơ quan, tổ chức, doanh nghiệp.

Thời gian vừa qua, hoạt động diễn tập bảo đảm an toàn thông tin, ứng cứu sự cố mạng (gọi tắt là diễn tập) đã được một số cơ quan, tổ chức, doanh nghiệp triển khai nhưng số lượng vẫn còn rất ít, nặng về hình thức, "diễn" nhiều hơn "tập", thường theo những kịch bản có sẵn và thực hiện trên các hệ thống mô phỏng, giả lập. Hạn chế của hình thức diễn tập này là các đội ứng cứu sự cố không có nhiều cơ hội cọ sát thực tế, năng lực cải thiện không đáng kể, phần lớn chưa có khả năng đối phó với các cuộc tấn công phức tạp, quy mô, kéo dài.

Trong khi đó, nguy cơ các hệ thống thông tin của bộ, ngành, địa phương, doanh nghiệp bị tấn công, khai thác là hiện hữu. Để các đội ứng cứu sự cố có đủ năng lực xử lý sự cố xảy ra trong hệ thống của mình, hoạt động diễn tập cần chuyển sang hình thức diễn tập thực chiến, với phương thức, phạm vi, tính chất mới. Diễn tập thực chiến được thực hiện trên hệ thống thật, không có kịch bản trước nhưng được quy định về mục tiêu, đối tượng tham gia, công cụ sử dụng, mức độ khai thác và thời gian diễn ra nhằm giảm thiểu rủi ro.

Diễn tập thực chiến gắn hoạt động diễn tập vào chính hệ thống mà đội ứng cứu sự cố có trách nhiệm bảo vệ, qua đó kinh nghiệm xử lý sự cố của đội ứng cứu sự cố đối với các hệ thống đang vận hành càng được nâng cao.

Diễn tập thực chiến chuyển diễn tập từ trạng thái "tĩnh" sang "động", thay vì có kịch bản trước, giới hạn trong thời gian ngắn thì diễn ra không cần kịch bản, trong thời gian đủ dài để thành viên tham gia có thể phát huy các kỹ năng tấn công và đưa đội ứng cứu vào trạng thái luôn thường trực, sẵn sàng xử lý sự cố, như các cuộc tấn công trong thực tế.

Diễn tập thực chiến chuyển từ diễn tập "ít" sang "nhiều", từ diễn tập sự vụ sang các đợt kéo dài, diễn ra càng thường xuyên thì khả năng phòng thủ, ứng

cứu lại càng được cải thiện, rủi ro càng được giảm thiểu, diễn tập mở rộng cho nhiều đối tượng tham gia, qua đó càng có nhiều cơ hội phát hiện điểm yếu, lỗ hổng đang tồn tại trong công nghệ, quy trình, con người để kịp thời xử lý.

Trên cơ sở đó, để triển khai hoạt động diễn tập thực chiến trong thời gian tới, Bộ trưởng Bộ Thông tin và Truyền thông chỉ thị:

1. Đơn vị chuyên trách về an toàn thông tin của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ; Sở Thông tin và Truyền thông của các tỉnh, thành phố trực thuộc Trung ương

a) Tham mưu cho các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương về kế hoạch, bố trí kinh phí hàng năm để tổ chức ít nhất 01 cuộc diễn tập thực chiến chuyên đề an toàn thông tin, ứng cứu sự cố mạng trong phạm vi của bộ, ngành, địa phương mình theo chỉ đạo của Thủ tướng Chính phủ tại Nhiệm vụ 4, Mục II, Quyết định 1622/QĐ-TTg 25 tháng 10 năm 2017 phê duyệt đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025 và Quyết định 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (gọi tắt là Quyết định 05).

b) Triển khai hoạt động diễn tập thực chiến trên hệ thống đang vận hành, cung cấp dịch vụ 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, thành phố thông minh, chuyển đổi số.

c) Chuẩn bị kỹ lưỡng, bài bản, sẵn sàng các phương án bảo vệ nhằm giảm thiểu rủi ro, bảo đảm hệ thống luôn được an toàn trong quá trình diễn tập; phải xác định rõ hệ thống là mục tiêu diễn tập, công cụ, kỹ thuật được sử dụng để không gây hậu quả hoặc hậu quả xảy ra trong giới hạn cho phép; 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.

d) Tự tổ chức hoạt động diễn tập thực chiến hoặc lựa chọn tổ chức, doanh nghiệp có đủ năng lực để triển khai diễn tập thực chiến.

đ) Phối hợp với Cục An toàn thông tin trong quá trình diễn tập để đánh giá hiệu quả diễn tập, đánh giá rủi ro và hỗ trợ điều phối ứng cứu khi xảy ra sự cố.

e) Đảm bảo vừa nâng cao năng lực cho đội ứng cứu sự cố, vừa tăng cường bảo vệ cho hệ thống thông tin đồng thời giúp tuyên truyền cho cơ quan, tổ chức, người dân về công tác đảm bảo an toàn thông tin mạng trong quá trình tổ chức diễn tập.

g) Tham gia đầy đủ vào các chương trình diễn tập thực chiến an toàn thông tin, ứng cứu sự cố mạng do Bộ Thông tin và Truyền thông (Cục An toàn thông tin) tổ chức; đôn đốc đội ứng cứu sự cố thuộc phạm vi quản lý của mình tham gia tích cực vào các hoạt động diễn tập thực chiến do đơn vị khác tổ chức nhằm nâng cao năng lực.

2. Các tổ chức, doanh nghiệp là thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia

a) Hàng năm tổ chức ít nhất 01 cuộc diễn tập thực chiến an toàn thông tin, ứng cứu sự cố mạng đối với các hệ thống thông tin thuộc phạm vi quản lý của mình.

b) Triển khai hoạt động diễn tập thực chiến trên các hệ thống đang vận hành, cung cấp dịch vụ; chú trọng diễn tập trên các hệ thống hiện diện trên mạng Internet.

c) Thực hiện các nội dung tại Khoản c, d, đ, g Mục 1 của Chỉ thị này.

d) Phối hợp, hỗ trợ các cơ quan, tổ chức, doanh nghiệp khác trong quá trình diễn tập thực chiến, sẵn sàng tham gia ứng cứu, xử lý sự cố khi các đơn vị diễn tập gặp rủi ro trong quá trình diễn tập.

3. Cục An toàn thông tin

a) Hướng dẫn thực hiện hoạt động diễn tập thực chiến.

b) Đôn đốc, kiểm tra cơ quan, tổ chức, doanh nghiệp là thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia triển khai hoạt động diễn tập thực chiến.

c) Sử dụng kết quả diễn tập thực chiến là một trong những tiêu chí để đánh giá năng lực đội ứng cứu sự cố của thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia.

d) Chủ trì tổ chức các chương trình diễn tập thực chiến an toàn thông tin, ứng cứu sự cố mạng cấp quốc gia hàng năm.

e) Tổ chức đánh giá kết quả diễn tập thực chiến của thành viên Mạng lưới và báo cáo kết quả hàng năm cho Bộ trưởng Bộ Thông tin và Truyền thông; đề xuất các biện pháp nhằm cải tiến hoạt động diễn tập thực chiến.

4. Tổ chức thực hiện

Các cơ quan, tổ chức, doanh nghiệp là thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia căn cứ nội dung tại Chỉ thị, tập trung triển khai các nhiệm vụ nhằm nâng cao hiệu quả trong công tác diễn tập thực chiến.

Cục An toàn thông tin có trách nhiệm theo dõi, đôn đốc các cơ quan, tổ chức, doanh nghiệp triển khai hiệu quả nhiệm vụ được giao. Định kỳ hàng năm tổng hợp báo cáo Bộ trưởng tình hình, kết quả thực hiện Chỉ thị./.

BỘ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Mạnh Hùng

Nơi nhận:
- Thủ tướng Chính phủ (để b/c);
- Các Phó Thủ tướng Chính phủ (để b/c);
- Văn phòng Chính phủ;
- Bộ TT&TT: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ, Cổng TTĐT;
- Cơ quan, tổ chức, doanh nghiệp là thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia;
- Các hội, hiệp hội hoạt động trong ngành TT&TT;
- Lưu: VT, Cục ATTT.