BỘ TƯ PHÁP
CỤC CÔNG NGHỆ THÔNG TIN

Số: 05 /KH-CNTT

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

Hà Nội, ngày 06 tháng 5 năm 2024

KẾ HOẠCH
Tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng tại Bộ Tư pháp năm 2024

Căn cứ Quyết định số 05/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ 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;

Căn cứ Quyết định số 1468/QĐ-BTP ngày 29/6/2018 của Bộ trưởng Bộ Tư pháp quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Công nghệ thông tin;

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

Căn cứ Quyết định số 3131/QĐ-BTP ngày 29/12/2023 của Bộ Tư pháp Phê duyệt Kế hoạch công tác năm 2024 của Cục Công nghệ thông tin.

Cục Công nghệ thông tin xây dựng Kế hoạch diễn tập thực chiến bảo đảm an toàn thông tin mạng năm 2024, cụ thể như sau:

I. NỘI DUNG

1. Mục đích, yêu cầu

a, Mục đích:

Việc triển khai diễn tập thực chiến nhằm nâng cao nhận thức, trách nhiệm đồng thời phát triển năng lực, kinh nghiệm điều phối, ứng cứu sự cố an toàn thông tin mạng của Cục Công nghệ thông tin cũng như các đơn vị tham gia vận hành hệ thống thông tin.

Trang bị những kỹ năng cần thiết cho cán bộ chuyên trách ATTT, kịp thời ứng phó, giải quyết các vấn đề mất an toàn thông tin thông qua tình huống giả định tấn công vào mạng máy tính và các hệ thống thông tin tại Trung tâm dữ liệu điện tử Bộ Tư pháp.

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

+ Mục tiêu tấn công: ban tổ chức lựa chọn các thành phần trong hệ thống thông tin.

+ Thời lượng tấn công và bảo vệ mục tiêu: dự kiến kéo dài trong 01 ngày.

+ Ngưỡng tấn công:

✓ Không sử dụng hệ thống mục tiêu để làm bàn đạp tấn công các mục tiêu khác.

✓ Chiếm được quyền điều khiển hệ thống phải dừng cuộc tấn công hoặc chuyển phương án tấn công mới (nếu có), không tấn công leo thang đặc quyền hệ thống (điều kiện này có thể áp dụng hoặc không áp dụng tùy thuộc vào từng cuộc diễn tập cụ thể).

✓ Không tấn công từ chối dịch vụ; tấn công phá hủy hệ thống hoặc dữ liệu; khởi động lại hoặc tắt máy chủ dịch vụ; khai thác lỗ hổng bảo mật để phát tán mã độc, đánh cắp, chia sẻ làm lộ lọt thông thông; sử dụng các loại mã độc mã hóa dữ liệu, đòi tiền chuộc và các loại tấn công khác làm ngưng trệ hệ thống và để lại hậu quả về sau.

- Lên phương án phòng ngừa rủi ro, ứng cứu sự cố hệ thống.

- Xây dựng kế hoạch, chương trình diễn tập và công bố công khai, rõ ràng.

- Xác định hình thức diễn tập:

+ Hình thức tập trung: các đội thực hiện tấn công/phòng thủ tại một địa điểm do Ban tổ chức lựa chọn.

+ Hình thức bán tập trung: Việc tấn công mục tiêu được các đội tấn công thực hiện trực tuyến qua Internet từ bất kỳ nơi nào. Việc bảo vệ mục tiêu được thực hiện theo hình thức tập trung và giám sát bảo vệ từ xa.

- Lựa chọn nhân sự, phân công, tổ chức các đội tham gia.

- Xây dựng và phổ biến Quy chế diễn tập thực chiến an toàn thông tin.

- Chỉ đạo, tổ chức, giám sát diễn tập đúng quy định tại Quy chế.

b, Nhiệm vụ của đội tấn công

- Phân công vai trò, trách nhiệm mỗi đội, mỗi thành viên trong đội thực hiện việc tấn công mục tiêu theo hướng dẫn và Quy chế của Ban tổ chức.

- Sử dụng tùy chọn các công cụ, kỹ thuật khác nhau (technical và on-technical) hoặc các công cụ, kỹ thuật được Ban tổ chức quy định cụ thể khai thác lỗ hổng bảo mật, tấn công hệ thống.

- Lưu vết hoặc đưa ra các bằng chứng tấn công.

- Tuân thủ theo thời gian bắt đầu và thời gian kết thúc tấn công đã được xác định trong giới hạn diễn tập (bao gồm mục tiêu diễn tập, ngưỡng tấn công, thời gian diễn tập).

- Báo cáo về Ban tổ chức phương pháp, tên công cụ và kết quả của việc tấn công theo các quy định: đúng thời hạn và bảo vệ kết quả báo cáo bằng việc mã hóa hoặc đặt mật khẩu.

- Không sử dụng các công cụ rà quét có thể dẫn đến hỏng hoặc treo hệ

5	Lên phương án phòng ngừa rủi ro, ứng cứu sự cố hệ thống	Cục Công nghệ thông tin	- Các đơn vị thuộc Bộ - Các đơn vị chuyên trách về An toàn thông tin	Quý IV/2024
6	Thử nghiệm hệ thống, phổ biến quy chế diễn tập thực chiến	Cục Công nghệ thông tin	- Các đơn vị thuộc Bộ - Các đơn vị chuyên trách về An toàn thông tin	Quý IV/2024
7	Triển khai chính thức	Cục Công nghệ thông tin	- Các đơn vị thuộc Bộ - Các đơn vị chuyên trách về An toàn thông tin	Quý IV/2024
8	Tổng kết đánh giá, rút kinh nghiệm	Cục Công nghệ thông tin	- Các đơn vị thuộc Bộ - Các đơn vị chuyên trách về An toàn thông tin	Quý IV/2024

5. Kinh phí thực hiện

Nguồn kinh phí hoạt động cho Đội ứng cứu sự cố an toàn thông tin Bộ Tư pháp.

II. TỔ CHỨC THỰC HIỆN

Cục Công nghệ thông tin chủ trì, phối hợp với các đơn vị liên quan tổ chức triển khai diễn tập thực chiến đảm bảo an toàn thông tin mạng tại Bộ Tư pháp năm 2024./.

Nơi nhận:
- Như trên;
- Thứ trưởng Mai Lương Khôi (để b/c);
- Cục trưởng (để b/c);
- Cục ATTT, Bộ TTTT (để b/c);
- Lưu: VT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA XHCN VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ TƯ PHÁP

Tạ Thành Trung