ỦY BAN NHÂN DÂN TỈNH ĐỒNG THÁP	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 519 /KH-UBND	*Đồng Tháp, ngày 26 tháng 4 năm 2026*

KẾ HOẠCH
Tổ chức diễn tập thực chiến bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Đồng Tháp năm 2026

Căn cứ quy định của Trung ương về bảo đảm an toàn hệ thống thông tin[(1)]; Quyết định số 121/QĐ-UBND ngày 15/01/2026 của Ủy ban nhân dân tỉnh về ban hành Chương trình công tác của Ủy ban nhân dân tỉnh năm 2026;

Ủy ban nhân dân tỉnh xây dựng Kế hoạch tổ chức diễn tập thực chiến bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Đồng Tháp năm 2026 như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng trên địa bàn tỉnh, tăng cường bảo vệ cho hệ thống thông tin và giúp tuyên truyền cho cơ quan, tổ chức, người dân về công tác bảo đảm an toàn thông tin mạng.

- Kịp thời phát hiện các điểm yếu, lỗ hổng bảo mật về công nghệ, quy trình, con người nhằm có cơ sở đề ra các giải pháp phù hợp để bảo đảm an toàn thông tin cho hệ thống; giúp Đội Ứng cứu sự cố có kinh nghiệm xử lý sự cố đối với các hệ thống đang vận hành, từng bước nâng cao năng lực thực chiến.

- Đánh giá được năng lực của đơn vị giám sát hệ thống, năng lực ứng cứu sự cố của thành viên mạng lưới ứng cứu sự cố an toàn thông tin; phát huy vai trò, cải thiện năng lực cho Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh.

2. Yêu cầu

- Diễn tập trên hệ thống thật, không có kịch bản trước, có quy định giới hạn về mục tiêu, đối tượng tham gia, công cụ sử dụng, mức độ khai thác và khoảng thời gian diễn ra nhằm giảm thiểu rủi ro cho hệ thống.

- 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 nghiêm trọng 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.

[(1)]. Căn cứ Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ; Quyết định 05/2017/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; Thông tư 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; Chỉ thị 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Quyết định 1439/QĐ-BTTTT ngày 26/7/2022 của Bộ Thông tin và Truyền thông ban hành quy trình hướng dẫn diễn tập thực chiến.

- "Đội tấn công" và "Đội phòng thủ" bảo đảm đủ năng lực và có trách nhiệm thực hiện đúng, đầy đủ các nguyên tắc trong diễn tập thực chiến.

II. NỘI DUNG KẾ HOẠCH

1. Hệ thống thông tin được sử dụng để diễn tập

Hệ thống được chọn làm mục tiêu diễn tập là hệ thống thật đang được vận hành, sử dụng phục vụ hoạt động của các cơ quan, ban, ngành, địa phương trên địa bàn tỉnh. Hệ thống cụ thể sẽ được thông báo trong quá trình tổ chức thực hiện diễn tập thực chiến.

2. Nguyên tắc diễn tập

a) Nguyên tắc chung: Các Đội tấn công và Đội phòng thủ không được phép trao đổi thông tin liên quan đến việc tấn công và bảo vệ suốt thời gian diễn tập (*trừ trường hợp có yêu cầu từ Ban Tổ chức*).

b) Nguyên tắc tấn công

- Tuân thủ thời gian bắt đầu, kết thúc diễn tập;

- Cho phép sử dụng nhiều kỹ thuật khác nhau (bao gồm dò tìm tài khoản, khai thác lỗ hổng bảo mật, lừa đảo qua email,…) để tấn công chiếm quyền điều khiển hệ thống;

- Cho phép sử dụng các công cụ mã nguồn đóng, mở, công cụ chiếm quyền điều khiển hệ thống, công cụ khai thác lỗ hổng ứng dụng; các công cụ sử dụng phải đảm bảo không gây nguy hại đến hoạt động của hệ thống;

- Cho phép khai thác lỗ hổng bảo mật trên ứng dụng, Hệ thống thông tin cũng như hệ thống và hạ tầng mạng nằm trong phạm vi diễn tập;

- Cho phép thực hiện tấn công phishing để khai thác, thu thập thông tin từ người dùng nội bộ, phục vụ cho việc diễn tập tấn công;

- Không sử dụng các hình thức tấn công từ chối dịch vụ (DDOS) bằng cách làm nghẽn băng thông mạng;

- Không được thực thi các mã khai thác mà có thể gây khởi động lại hoặc làm gián đoạn quá trình hoạt động của máy chủ dịch vụ;

- Nghiêm cấm thực hiện việc phá hủy hệ thống và dữ liệu; sử dụng các lỗi trên ứng dụng web để phát tán mã độc;

- Nghiêm cấm sử dụng các loại mã độc trong quá trình diễn tập như mã độc mã hoá dữ liệu, tống tiền, phần mềm gián điệp và các loại mã độc hại khác gây ảnh hưởng nghiêm trọng đến hệ thống;

- Cấm đánh cắp, chia sẻ làm lộ lọt thông tin;

- Chỉ được phép chia sẻ các thông tin về kết quả của việc tấn công cho Ban Tổ chức (BTC);

- Không được tấn công hệ thống không thuộc giới hạn, mục tiêu diễn tập;

Không sử dụng hệ thống nằm trong giới hạn, mục tiêu diễn tập để làm bàn đạp tấn công sang các hệ thống khác không thuộc giới hạn, mục tiêu diễn tập;

- Không được phép thực hiện tấn công làm thay đổi giao diện của Website/Cổng thông tin/Trang thông tin;

- Không sử dụng hoặc hạn chế sử dụng các công cụ rà quét (scan) có thể dẫn đến treo hệ thống;

- Nghiêm cấm việc lưu lại phần mềm, công cụ trên hệ thống bị xâm nhập để phục vụ cho các mục đích khác không liên quan đến diễn tập;

- Mỗi đội tấn công nếu phát hiện được lỗ hổng thì chỉ được phép khai thác một lần đối với lỗ hổng đó. Tuyệt đối không khai thác nhiều lần cùng một lỗ hổng nhằm tránh phát sinh nhiều giao dịch, gây khó khăn cho công tác đối soát dữ liệu sau diễn tập.

c) Nguyên tắc phòng thủ

- Cho phép triển khai các hệ thống Honeypot (là một hệ thống tài nguyên thông tin được xây dựng với mục đích giả dạng đánh lừa những kẻ sử dụng và xâm nhập không hợp pháp, thu hút sự chú ý của chúng, ngăn không cho chúng tiếp xúc với hệ thống thật) để đánh lạc hướng các Đội tấn công;

- Cho phép dải địa chỉ IP của các đội tham gia tấn công được truy cập tới các mục tiêu tấn công thông qua cổng dịch vụ mà tổ chức đang cung cấp;

- Thông báo dừng thực hiện tấn công, khai thác khi có yêu cầu của BTC;

- Thực hiện các biện pháp kỹ thuật, nghiệp vụ để giám sát, phát hiện và đánh chặn tấn công;

- Cho phép chặn địa chỉ IP gửi quá nhiều gói tin trong một khoảng thời gian (*theo yêu cầu của BTC*), để đảm bảo các đội còn lại không bị mất kết nối đến hệ thống mục tiêu;

- Theo dõi, giám sát, ngăn chặn các Đội tấn công vi phạm các nguyên tắc tấn công được quy định tại Kế hoạch này;

- Ghi nhận và theo dõi Đội tấn công đã tấn công thành công mục tiêu.

3. Hình thức, thời gian, địa điểm diễn tập

a) Hình thức: Thực hiện bán tập trung. Việc tấn công mục tiêu được các Đội tấn công thực hiện trực tuyến qua Internet từ bất kỳ nơi nào trong lãnh thổ Việt Nam; việc bảo vệ mục tiêu được thực hiện theo hình thức tập trung và giám sát bảo vệ từ xa.

b) Thời gian: Dự kiến từ 02 đến 03 ngày trong Quý III/2026. Ban Tổ chức sẽ bố trí thời gian cụ thể, phù hợp cho thành viên các đội tham gia diễn tập bảo đảm đạt hiệu quả cao nhất.

3. Quy trình tổ chức diễn tập thực chiến

Bước 1. Xây dựng phương án triển khai diễn tập thực chiến.

Bước 2. Thành lập Ban Tổ chức chương trình diễn tập thực chiến.

Bước 3. Xác định giới hạn diễn tập và ban hành Nội quy diễn tập.

Bước 4. Khai mạc diễn tập, công bố giới hạn, danh sách các đội, thời gian diễn tập.

Bước 5. Thực hiện diễn tập.

Bước 6. Đánh giá kết quả sau khi kết thúc diễn tập.

Bước 7. Bế mạc, tổng kết và đánh giá diễn tập.

Bước 8. Tổng hợp, gửi báo cáo kết quả tổ chức diễn tập.

4. Kinh phí thực hiện: Sử dụng từ nguồn kinh phí chi thường xuyên được bố trí trong dự toán chi ngân sách năm 2026 của Công an tỉnh.

III. NHIỆM VỤ BAN TỔ CHỨC, BAN GIÁM KHẢO, CÁC ĐỘI THAM GIA DIỄN TẬP

1. Nhiệm vụ của Ban Tổ chức: Chủ trì điều phối, bảo đảm việc thực hiện các nội dung, nhiệm vụ của Ban Giám khảo, các đội tham gia diễn tập theo Kế hoạch.

2. Nhiệm vụ của Ban Giám khảo

- Công bố phương thức đánh giá, xếp loại các Đội tham gia.

- Thực hiện đánh giá công bằng, khách quan các Đội tấn công và phòng thủ dựa trên tổng hợp báo cáo do Ban Tổ chức cung cấp; gửi kết quả đánh giá về Ban Tổ chức.

- Tuân thủ các yêu cầu bảo mật thông tin (về lỗ hổng, điểm yếu hệ thống và các thông tin nhạy cảm khác) trong và sau thời gian diễn tập.

3. Nhiệm vụ của Đội tấn công

- Đăng ký thông tin về thành viên tham dự theo yêu cầu của Ban Tổ chức, thông tin về địa chỉ IP được sử dụng để diễn tập cho Ban Tổ chức.

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

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

- Lưu vết và đưa ra các bằng chứng (evidence) tấn công.

- Tuân thủ theo thời gian bắt đầu và thời gian kết thúc tấn công do Ban Tổ chức đưa ra.

- Hạn chế hoặc không sử dụng các công cụ rà quét (scan) có thể dẫn đến hỏng hoặc treo hệ thống.

- Tuân thủ nội quy, nguyên tắc khi thực hiện tấn công.

- Báo cáo về Ban Tổ chức phương pháp, tên công cụ và kết quả của việc tấn công (bao gồm cả các điểm yếu nghiêm trọng và không nghiêm trọng) theo các quy tắc: Đúng thời hạn và bảo vệ kết quả báo cáo bằng việc mã hóa hoặc đặt mật khẩu.

- Cam kết tuân thủ bảo mật thông tin và các yêu cầu khác của Ban Tổ chức.

4. Nhiệm vụ của Đội phòng thủ

- Tổ chức phòng thủ phải đảm bảo yêu cầu quy trình ứng phó sự cố, bảo đảm an toàn thông tin mạng theo hướng dẫn tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017, Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017.

- Phân công vai trò, trách nhiệm mỗi thành viên, nhóm liên quan thực hiện công tác phòng thủ theo hướng dẫn và quy định của Ban Tổ chức.

- Rà soát và thực thi tăng cường phương án dự phòng, sao lưu dữ liệu và hệ thống trước khi bắt đầu thực hiện diễn tập.

- Theo dõi các hoạt động dò quét, thăm dò, khai thác lỗ hổng trên hệ thống mục tiêu được lựa chọn tổ chức diễn tập.

- Thực hiện các phân tích, điều tra chuyên sâu các hoạt động liên quan đến tấn công, xâm nhập hệ thống.

- Rà soát và thực thi tăng cường phương án giám sát hệ thống mục tiêu diễn tập thực chiến (bao gồm cả các hệ thống nằm ngoài mục tiêu diễn tập), phát hiện khi các hệ thống bị tấn công nằm ngoài giới hạn, phạm vi diễn tập. Báo cáo Ban Tổ chức khi phát hiện các vi phạm của Đội tấn công vi phạm nội quy.

- Thực hiện các biện pháp khắc phục sự cố, vá lỗ hổng, điểm yếu được phát hiện.

- Lưu giữ các nhật ký, dữ liệu, bằng chứng bảo vệ hệ thống trong quá trình diễn tập.

- Ngăn chặn địa chỉ IP, nguồn tấn công nếu thấy gây phương hại hoặc ảnh hưởng đến hoạt động bình thường của hệ thống.

- Báo cáo về Ban Tổ chức kết quả của việc giám sát, phát hiện, ngăn chặn theo quy tắc: đúng thời hạn và bảo vệ kết quả báo cáo bằng việc mã hóa hoặc đặt mật khẩu.

- Tuân thủ bảo mật thông tin và các yêu cầu khác của Ban Tổ chức.

5. Nhiệm vụ của Đội Chuyên gia

- Hướng dẫn, hỗ trợ chuyên môn, kỹ thuật cho Đội tấn công và Đội phòng thủ; có ý kiến chuyên môn về các vấn đề bảo đảm an toàn, an ninh cho Ban Tổ chức Diễn tập.

- Tuân thủ bảo mật thông tin và các yêu cầu khác của Ban Tổ chức.

IV. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh

- Chủ trì triển khai thực hiện các nội dung kế hoạch nhằm đạt được các mục tiêu đề ra. Thành lập Ban Tổ chức, Ban Giám khảo, Đội phòng thủ và Đội tấn công.

- Chủ trì, phối hợp các đơn vị có liên quan lựa chọn thành viên có năng lực, kinh nghiệm trong việc tổ chức, tác chiến để tham gia Ban Tổ chức, Ban Giám khảo, Đội tấn công và Đội phòng thủ theo nội dung diễn tập.

- Cử lực lượng tại chỗ (*lực lượng nội bộ*), thành viên Đội Ứng cứu sự cố của tỉnh và các chuyên gia bảo mật an toàn thông tin đang cung cấp dịch vụ giám sát, đảm bảo an ninh mạng của tỉnh tham gia vào hoạt động phòng thủ.

- Hướng dẫn Đội tấn công và Đội phòng thủ thực hiện bảo mật thông tin liên quan đến diễn tập theo quy định được Ban Tổ chức đưa ra.

- Xây dựng kế hoạch, chương trình diễn tập rõ ràng, chỉ công bố cho các bên liên quan.

- Xây dựng và phổ biến nội quy diễn tập thực chiến an toàn thông tin.

- Tổ chức, chỉ đạo và giám sát công tác diễn tập bảo đảm tuân thủ đúng quy định, nội quy đã ban hành; cho phép chặn các địa chỉ IP gửi quá nhiều gói tin trong một khoảng thời gian, nếu xét thấy có nguy cơ làm ảnh hưởng đến hoạt động hoặc kết nối bình thường đến hệ thống; không cho phép Đội tấn công và Đội phòng thủ trao đổi thông tin liên quan đến việc tấn công và bảo vệ hệ thống mục tiêu trong suốt thời gian diễn tập (trừ trường hợp có yêu cầu của Ban Tổ chức).

- Tiếp nhận, tổng hợp kết quả báo cáo gửi về từ các Đội tấn công và Đội phòng thủ; gửi kết quả diễn tập và kết quả theo dõi quá trình diễn tập của mỗi Đội cho Ban Giám khảo thực hiện đánh giá.

- Báo cáo Chủ quản hệ thống thông tin để kịp thời tổ chức khắc phục, vá các lỗ hổng do các Đội tấn công phát hiện trong quá trình diễn tập.

- Báo cáo tình hình diễn tập và đánh giá kết quả về cho Trung tâm An ninh mạng quốc gia - Bộ Công an, Uỷ ban nhân dân tỉnh.

- Phối hợp Sở Tài chính và các đơn vị liên quan dự trù kinh phí thực hiện và quyết toán đúng quy định.

2. Sở Khoa học và Công nghệ

- Phối hợp Công an tỉnh lựa chọn mục tiêu tổ chức diễn tập thực chiến, bảo đảm mục tiêu được lựa chọn là hệ thống thật, đang hoạt động phục vụ yêu cầu công tác của các cơ quan đơn vị trên địa bàn tỉnh.

- Bảo đảm duy trì hoạt động của hệ thống thông tin được sử dụng để diễn tập; lên phương án phòng ngừa rủi ro, ứng cứu sự cố; chịu trách nhiệm trong thực hiện bảo đảm an toàn cho hệ thống trong quá trình diễn tập, thiết lập hệ

thống dự phòng song song hoặc thực hiện sao lưu toàn bộ hệ thống trước khi tiến hành diễn tập.

- Phân công đơn vị vận hành hệ thống được chọn diễn tập và nhân sự có liên quan để thực hiện nhiệm vụ của Đội phòng thủ.

3. Sở Tài chính

Tổng hợp, cân đối nguồn kinh phí trình cấp có thẩm quyền xem xét, bố trí kinh phí cho Công an tỉnh để tổ chức thực hiện.

Trong quá trình triển khai thực hiện Kế hoạch nếu có khó khăn, vướng mắc đề nghị các cơ quan, đơn vị, địa phương kịp thời báo cáo về Ủy ban nhân dân tỉnh *(qua Công an tỉnh)* để hướng dẫn thực hiện./.

Nơi nhận:
- Cục ANM&PCTPSDCNC - Bộ Công an;
- Các PCT UBND tỉnh;
- Như Mục IV;
- Tiểu ban An ninh mạng tỉnh;
- VPUB: CVP, các PCVP;
- Lưu: VT, KGVX (vttoan).

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Phạm Thành Ngại