ỦY BAN NHÂN DÂN THÀNH PHỐ CẦN THƠ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 104 /KH-UBND	*Cần Thơ, ngày 09 tháng 5 năm 2025*

KẾ HOẠCH
Rà soát, đánh giá và nâng cao hiệu quả công tác đảm bảo an toàn các hệ thống thông tin trên địa bàn thành phố Cần Thơ năm 2025

Thực hiện Công văn số 02/VPBCĐ ngày 06 tháng 01 năm 2025 của Ban Chỉ đạo An toàn, an ninh mạng quốc gia về việc rà soát đánh giá và xử lý các hoạt động tấn công mạng, gián điệp mạng, Ủy ban nhân dân thành phố xây dựng Kế hoạch kiểm tra công tác đảm bảo an toàn hệ thống thông tin trên địa bàn thành phố Cần Thơ năm 2025, như sau:

I. MỤC ĐÍCH VÀ YÊU CẦU

1. Mục đích

a) Kiểm tra, đánh giá tổng thể mức độ an toàn, bảo mật của hệ thống thông tin tại các cơ quan hành chính, đơn vị sự nghiệp trên địa bàn thành phố Cần Thơ nhằm phát hiện sớm các lỗ hổng bảo mật, nguy cơ mất an ninh mạng có thể bị tin tặc khai thác, từ đó có biện pháp xử lý kịp thời, ngăn chặn các rủi ro;

b) Hỗ trợ các cơ quan, đơn vị nâng cao năng lực bảo vệ dữ liệu, triển khai các biện pháp tăng cường bảo mật thông tin nhằm đảm bảo hoạt động ổn định của hệ thống. Nâng cao nhận thức, trách nhiệm của các cơ quan, đơn vị về công tác an toàn mạng, tăng cường khả năng ứng phó với các cuộc tấn công mạng;

c) Tạo tiền đề cho việc xây dựng, triển khai các giải pháp đảm bảo an ninh mạng đồng bộ, phù hợp với định hướng chuyển đổi số của thành phố. Đảm bảo việc tuân thủ nghiêm ngặt các quy định của pháp luật về bảo vệ dữ liệu cá nhân, an toàn mạng và an ninh quốc gia.

2. Yêu cầu

a) Công tác rà quét, đánh giá phải được thực hiện một cách khách quan, khoa học, đảm bảo độ tin cậy và không gây ảnh hưởng đến hoạt động thường xuyên của các hệ thống thông tin;

b) Các cơ quan, đơn vị có liên quan phải chủ động phối hợp, cung cấp thông tin trung thực, đầy đủ, chính xác và kịp thời để phục vụ công tác kiểm tra, đánh giá. Đảm bảo tính bảo mật thông tin, tuyệt đối không để lộ, lọt thông tin trong quá trình rà soát, kiểm tra;

c) Rà soát phải được thực hiện trên phạm vi rộng, bao gồm tất cả các hệ thống thông tin, cổng/trang thông tin điện tử, phần mềm nội bộ, hệ thống lưu trữ dữ liệu và các thiết bị kết nối mạng tại các cơ quan, đơn vị. Các cơ quan, đơn vị phải cam kết thực hiện đầy đủ các giải pháp khắc phục được đề xuất sau rà quét, đồng thời có kế hoạch dài hạn để đảm bảo an ninh mạng bền vững.

II. NỘI DUNG THỰC HIỆN

1. Thu thập thông tin về hệ thống thông tin thuộc các cơ quan, đơn vị (đối tượng cần rà soát)

Các cơ quan, đơn vị chủ quản, vận hành hệ thống thông tin cung cấp danh mục hệ thống thông tin đang quản lý, phát triển hoặc được giao quản lý, bao gồm:

a) Danh sách website, hệ thống phần mềm nội bộ, hệ thống lưu trữ dữ liệu;

b) Thông tin về domain, địa chỉ IP, máy chủ;

c) Các giải pháp bảo mật đang áp dụng (firewall, IDS/IPS, giải pháp mã hóa dữ liệu,...) và hệ thống sao lưu, phục hồi dữ liệu và các quy trình ứng phó sự cố an ninh mạng;

d) Số lượng thiết bị đang phục vụ cho hệ thống thông tin tại cơ quan, đơn vị;

đ) Nhân sự phụ trách quản lý hệ thống thông tin và trình độ đào tạo về công nghệ thông tin và an ninh mạng (đầu mối trao đổi, liên lạc trong việc triển khai, thực hiện Kế hoạch).

2. Rà soát, kiểm tra và đánh giá an toàn hệ thống

a) Kiểm tra tổng thể mức độ an toàn của hệ thống, bao gồm hạ tầng mạng, phần mềm ứng dụng, cơ sở dữ liệu và khả năng chống chịu trước các hình thức tấn công mạng như tấn công từ chối dịch vụ (DDoS), xâm nhập trái phép (hacking), mã độc (malware)...;

b) Đánh giá mức độ tuân thủ các tiêu chuẩn an ninh mạng theo quy định pháp luật, thực hiện kiểm thử xâm nhập (Penetration Testing) để xác định và phân loại mức độ nghiêm trọng của các lỗ hổng bảo mật.

3. Đề xuất giải pháp và khuyến nghị

a) Xây dựng danh sách các lỗ hổng bảo mật và phân loại theo mức độ ưu tiên xử lý, đề xuất biện pháp khắc phục phù hợp cho từng lỗ hổng;

b) Đưa ra các giải pháp kỹ thuật nhằm bảo vệ hệ thống thông tin như cập nhật bản vá bảo mật, nâng cấp phần mềm, triển khai hệ thống tường lửa (firewall), hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS), mã hóa dữ liệu và giám sát an ninh mạng. Thực hiện kiểm tra, rà quét hệ thống thông tin tại đơn vị định kỳ **03 tháng/lần**;

c) Kiến nghị tổ chức đào tạo chuyên sâu cho đội ngũ cán bộ công nghệ thông tin, diễn tập xử lý sự cố an ninh mạng để nâng cao khả năng ứng phó với các tình huống tấn công mạng.

4. Báo cáo kết quả rà quét và kiến nghị biện pháp xử lý

a) Tổng hợp và phân tích kết quả rà quét, đưa ra đánh giá chi tiết về mức độ an toàn của từng hệ thống thông tin, từ đó đề xuất phương án xử lý cụ thể đối với các lỗ hổng bảo mật phát hiện được, đảm bảo việc khắc phục được thực hiện kịp thời và hiệu quả;

b) Báo cáo đơn vị có trách nhiệm để triển khai các biện pháp hỗ trợ, giám sát việc thực hiện các đề xuất khắc phục, đảm bảo các đơn vị tuân thủ nghiêm ngặt các yêu cầu về an ninh mạng.

III. TỔ CHỨC THỰC HIỆN

1. Thời gian thực hiện

a) Kế hoạch được triển khai thực hiện xuyên suốt và liên tục trong năm 2025;

b) Các hoạt động rà quét, kiểm tra sẽ được thực hiện theo từng giai đoạn, đảm bảo tính thường xuyên và cập nhật kịp thời để ứng phó với các nguy cơ tấn công an ninh mạng;

c) Báo cáo định kỳ sẽ được thực hiện để tổng hợp kết quả đánh giá và kịp thời đề xuất biện pháp xử lý phù hợp.

2. Phương pháp thực hiện

a) Áp dụng các biện pháp nghiệp vụ chuyên sâu kết hợp với các phương pháp kỹ thuật tiên tiến để rà quét, đánh giá an toàn thông tin;

b) Sử dụng hệ thống công cụ phân tích, giám sát an ninh mạng hiện đại tại Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an thành phố nhằm phát hiện kịp thời các lỗ hổng bảo mật và nguy cơ tấn công mạng;

c) Thực hiện kiểm thử xâm nhập định kỳ để đánh giá khả năng phòng thủ của hệ thống thông tin và đề xuất các biện pháp tăng cường bảo mật;

d) Tăng cường phối hợp với các đơn vị chuyên trách về an ninh mạng để hỗ trợ xử lý các sự cố an toàn thông tin và hướng dẫn các đơn vị triển khai biện pháp khắc phục hiệu quả.

3. Kinh phí thực hiện

a) Kinh phí từ nguồn kinh phí đảm bảo an toàn thông tin năm 2025;

b) Các cơ quan, đơn vị chủ động bố trí kinh phí để thực hiện các biện pháp khắc phục lỗ hổng bảo mật theo kiến nghị của Công an thành phố;

c) Việc sử dụng kinh phí phải đảm bảo đúng mục đích, hiệu quả và tuân thủ quy định tài chính hiện hành.

4. Trách nhiệm thực hiện

a) Công an thành phố chủ trì, phối hợp với cơ quan, đơn vị liên quan tổ chức triển khai, rà quét, chịu trách nhiệm tổng thể trong việc thực hiện nhiệm vụ trong Kế hoạch, bảo đảm chất lượng, tiến độ; tổng hợp báo cáo kết quả, các khó khăn, vướng mắc, tham mưu, đề xuất Ủy ban nhân dân thành phố chỉ đạo thực hiện;

b) Các cơ quan, đơn vị trên địa bàn thành phố có trách nhiệm cung cấp thông tin chi tiết về hệ thống thông tin đang quản lý *(được nêu tại mục 1, phần II - Kế hoạch này)*; đồng thời, xây dựng kế hoạch triển khai thực hiện gửi về Ủy ban nhân dân thành phố *(qua Công an thành phố, địa chỉ liên hệ: Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an thành phố, số 9A,*

đường Trần Phú, phường Cái Khế, quận Ninh Kiều, thành phố Cần Thơ) **trong tháng 5 năm 2025** để tổng hợp, báo cáo Ủy ban nhân dân thành phố. Báo cáo kết quả thực hiện, gửi về Công an thành phố trước **ngày 10 tháng 10 năm 2025** để tổng hợp, gửi Ban Chỉ đạo An toàn, an ninh mạng quốc gia. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các cơ quan, đơn vị trao đổi với Công an thành phố để phối hợp thực hiện.

Trên đây là Kế hoạch rà soát, đánh giá và nâng cao hiệu quả công tác đảm bảo an toàn các hệ thống thông tin trên địa bàn thành phố Cần Thơ năm 2025./.

Nơi nhận:
- Ban Chỉ đạo AT, ANM quốc gia;
- Cục ANM và PCTPSDCNC, Bộ Công an;
- CT, PCT UBND TP;
- Công an thành phố;
- Sở, ban, ngành thành phố;
- UBND quận, huyện;
- UBND xã, phường, thị trấn;
- VP UBND TP (2,3E,7);
- Lưu: VT, M.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Trương Cảnh Tuyên