

Phụ lục IX
Quy trình quản lý sự cố an toàn thông tin
(Kèm theo Quyết định số /QĐ-BNV ngày / /2024
của Bộ trưởng Bộ Nội vụ)

I. Giải thích từ ngữ

Cơ quan điều phối quốc gia: Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (Trung tâm VnCert) là cơ quan điều phối quốc gia về ứng cứu sự cố.

Đơn vị chuyên trách về ứng cứu sự cố: là Trung tâm Thông tin.

Cơ quan thường trực: là Bộ Thông tin và Truyền thông, giúp việc cho Ban Chỉ đạo quốc gia.

Bộ phận tác nghiệp ứng cứu khẩn cấp, bao gồm: Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam VnCert; Cục An toàn thông tin - Bộ Thông tin và Truyền thông; Cục An ninh mạng, Cục Cảnh sát phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an; Cục Công nghệ thông tin, Bộ Tổng tham mưu - Bộ Quốc phòng.

II. Nội dung Quy trình quản lý sự cố an toàn thông tin

Quy trình quản lý sự cố an toàn thông tin được thực hiện theo Điều 14, Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia, cụ thể:

Bước 1: Phát hiện, tiếp nhận, sự cố

Đơn vị chủ trì: Đơn vị vận hành hệ thống thông tin; Cơ quan điều phối quốc gia.

Đơn vị phối hợp: Đơn vị chuyên trách về ứng cứu sự cố; Chủ quản hệ thống thông tin.

Nội dung thực hiện: Đơn vị vận hành hệ thống thông tin chịu trách nhiệm liên tục theo dõi, phát hiện các tấn công, sự cố đối với hệ thống thông tin được giao quản lý, vận hành. Cơ quan điều phối quốc gia là đơn vị đầu mối tổ chức các hoạt động theo dõi, giám sát, phát hiện các sự cố và tiếp nhận thông báo về sự cố an toàn thông tin mạng từ các nguồn khác nhau.

Bước 2: Xác minh, phân tích, đánh giá và phân loại sự cố

Đơn vị chủ trì: Cơ quan điều phối quốc gia.

Đơn vị phối hợp: Chủ quản hệ thống thông tin; Đơn vị chuyên trách về ứng cứu sự cố; Đơn vị vận hành hệ thống thông tin.

Nội dung thực hiện:

a) Cơ quan điều phối quốc gia phối hợp cùng chủ quản hệ thống thông tin (hoặc đơn vị phụ trách về ứng cứu sự cố hoặc đơn vị vận hành hệ thống thông tin) xác minh sự cố bao gồm các thông tin sau: Tình trạng sự cố; mức độ sự cố; phạm vi ảnh hưởng của sự cố; đối tượng, địa điểm xảy ra sự cố.

b) Sau khi xác minh được sự cố, Cơ quan điều phối quốc gia có trách nhiệm phân loại sự cố và triển khai tiếp như sau:

- Trường hợp sự cố được phân loại thông thường thì Cơ quan điều phối quốc gia thông báo cho các bên liên quan để tiếp tục triển khai theo phương án ứng cứu sự cố an toàn thông tin mạng thông thường;

- Trường hợp sự cố được phân loại nghiêm trọng thì Cơ quan điều phối quốc gia báo cáo Cơ quan thường trực về sự cố nghiêm trọng cùng với các đề xuất: Phương án ứng cứu; các đơn vị tham gia lực lượng ứng cứu; nguồn lực cần thiết để ứng cứu sự cố; dự kiến triệu tập bộ phận tác nghiệp ứng cứu khẩn cấp và thực hiện tiếp Bước 3.

Bước 3: Cơ quan thường trực quyết định lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp

Đơn vị chủ trì: Cơ quan thường trực.

Nội dung thực hiện:

a) Cơ quan thường trực căn cứ theo báo cáo của Cơ quan điều phối quốc gia xem xét quyết định lựa chọn phương án ứng cứu khẩn cấp quốc gia và triệu tập bộ phận tác nghiệp ứng cứu khẩn cấp để ứng cứu, xử lý sự cố.

b) Nguyên tắc phân công nhiệm vụ triển khai các biện pháp ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia như sau:

- Chỉ đạo điều hành hoạt động ứng cứu và giám sát cơ chế phối hợp, chia sẻ thông tin: Bộ Thông tin và truyền thông;

- Thu thập, tổng hợp thông tin và chia sẻ, báo cáo; Cơ quan điều phối quốc gia, chủ quản hệ thống thông tin (qua đơn vị vận hành hệ thống thông tin và đơn vị chuyên trách ứng cứu sự cố);

- Phân tích thông tin: Cơ quan điều phối quốc gia, đơn vị vận hành hệ thống thông tin, đơn vị chuyên trách ứng cứu sự cố và các đơn vị tham gia tác nghiệp ứng cứu khẩn cấp;

- Ngăn chặn, xử lý sự cố: Đơn vị vận hành hệ thống thông tin, đơn vị chuyên trách ứng cứu sự cố, Cơ quan điều phối quốc gia và các đơn vị tham gia tác nghiệp ứng cứu khẩn cấp;

- Khắc phục, gỡ bỏ, khôi phục dữ liệu và hoạt động bình thường: Chủ quản hệ thống thông tin, các đơn vị được chủ quản hệ thống thông tin lựa chọn;

- Xử lý hậu quả: Chủ quản hệ thống thông tin, các đơn vị tham gia tác nghiệp ứng cứu khẩn cấp;

- Công bố và xử lý khủng hoảng thông tin: Cơ quan thường trực, Cơ quan điều phối quốc gia.

Bước 4: Triển khai phương án ứng cứu ban đầu

Đơn vị chủ trì: Cơ quan điều phối quốc gia; Chủ quản hệ thống thông tin.

Nội dung thực hiện: Cơ quan điều phối quốc gia nhanh chóng phối hợp với chủ quản hệ thống thông tin tiến hành ngay các biện pháp ứng cứu ban đầu, bao gồm:

a) Xác định phạm vi, đối tượng, mục tiêu cần ứng cứu:

- Các sự cố liên quan đã xảy ra;
- Đối tượng đang bị ảnh hưởng;
- Phạm vi bị ảnh hưởng;
- Các mục tiêu ưu tiên trong khắc phục sự cố (khôi phục hoạt động, bảo đảm bí mật dữ liệu; bảo đảm tính toàn vẹn dữ liệu);
- Diễn biến tình hình và phương thức thủ đoạn tấn công;
- Dự đoán các diễn biến tiếp theo có thể xảy ra.

b) Điều phối các hoạt động ứng cứu ban đầu: Cơ quan thường trực chỉ đạo Cơ quan điều phối quốc gia thực hiện điều phối và chia sẻ thông tin, tài liệu liên quan đến tình huống ứng cứu cho các thành viên tham gia theo chức năng, nhiệm vụ được giao.

c) Cảnh báo sự cố trên mạng lưới ứng cứu quốc gia: Cơ quan điều phối quốc gia thực hiện cảnh báo cho các thành viên mạng lưới và các đối tượng có liên quan hoặc có khả năng xảy ra các sự cố tương tự.

d) Tiến hành các biện pháp khôi phục tạm thời:

Căn cứ vào mục tiêu được ưu tiên trong khắc phục sự cố, Chủ quản hệ thống thông tin phối hợp với Cơ quan điều phối quốc gia, các nhà cung cấp dịch vụ và các cơ quan chức năng khác tiến hành khôi phục một số hoạt động, dữ liệu hoặc kết nối cần thiết nhất để giảm thiểu thiệt hại đối với hệ thống thông tin, ảnh hưởng uy tín của cơ quan chủ quản, quản lý hệ thống hoặc gây ảnh hưởng xấu tới xã hội.

Chủ quản hệ thống thông tin phải phối hợp chặt chẽ, cung cấp đầy đủ thông tin để Cơ quan điều phối quốc gia thực hiện giám sát, theo dõi quá trình phục hồi và các tấn công, ảnh hưởng trong thời gian chưa khắc phục triệt để sự cố.

đ) Xử lý hậu quả ban đầu: Chủ quản hệ thống thông tin cần nhanh chóng tiến hành các biện pháp khắc phục khẩn cấp các hậu quả, thiệt hại do tấn công mạng gây ra làm ảnh hưởng đến người dân, xã hội, cơ quan, tổ chức khác theo yêu cầu của Cơ quan thường trực.

e) Ngăn chặn, xử lý các hành vi đã được phát hiện: Cơ quan thường trực điều phối chỉ đạo Cơ quan điều phối quốc gia thực hiện điều phối các cơ quan chức năng triển khai hỗ trợ phát hiện và xử lý các nguồn phát tán tấn công, ngăn chặn các tấn công từ bên ngoài vào hệ thống thông tin bị sự cố. Cơ quan thường trực cung cấp hoặc chỉ đạo cung cấp các thông tin, chứng cứ liên quan đến các hành vi vi phạm pháp luật có yếu tố cấu thành tội phạm (nếu có) để các cơ quan chức năng thuộc Bộ Công an tiến hành điều tra, xác minh và ngăn chặn tội phạm.

Bước 5: Triển khai phương án ứng cứu khẩn cấp

a) Chỉ đạo xử lý sự cố

Đơn vị chủ trì: Cơ quan thường trực.

Nội dung thực hiện: Căn cứ theo phương án ứng cứu được lựa chọn, Cơ quan thường trực chỉ đạo chủ quản hệ thống thông tin, Cơ quan điều phối quốc gia, bộ phận tác nghiệp ứng cứu sự cố triển khai công tác ứng cứu, xử lý sự cố. Trong quá trình ứng cứu, tùy thuộc vào diễn biến tình hình thực tế, Cơ quan thường trực có thể quyết định bổ sung thành phần tham gia tác nghiệp ứng cứu khẩn cấp.

b) Điều phối công tác ứng cứu

Đơn vị chủ trì: Cơ quan điều phối quốc gia.

Nội dung thực hiện: Căn cứ theo phương án ứng cứu được lựa chọn, Ban Điều phối ứng cứu quốc gia hoặc Cơ quan điều phối quốc gia thực hiện công tác điều phối ứng cứu theo chức năng nhiệm vụ của mình và giám sát cơ chế phối hợp, chia sẻ thông tin.

c) Phát ngôn và công bố thông tin

Cơ quan thường trực chịu trách nhiệm chỉ định người phát ngôn, cung cấp thông tin; quyết định địa điểm, nội dung, thời điểm phát ngôn, cung cấp thông tin cho các cơ quan thông tin đại chúng, các cá nhân và tổ chức có liên quan đến sự cố.

d) Thu thập thông tin

Đơn vị chủ trì: Cơ quan điều phối quốc gia; chủ quản hệ thống thông tin.

Nội dung thực hiện: Căn cứ theo yêu cầu cung cấp thông tin cho các đơn vị thuộc thành phần tác nghiệp ứng cứu khẩn cấp, cơ quan điều phối quốc gia cùng chủ quản hệ thống thông tin phối hợp tiến hành thu thập, tổng hợp và chia sẻ, cung cấp thông tin.

đ) Phân tích, giám sát tình hình liên quan sự cố

Cơ quan điều phối quốc gia chủ trì, phối hợp với chủ quản hệ thống thông tin thực hiện giám sát liên tục diễn biến sự cố và thông báo, cập nhật đến các đơn vị trong bộ phận tác nghiệp ứng cứu khẩn cấp.

Các đơn vị thuộc bộ phận tác nghiệp ứng cứu khẩn cấp dựa trên các thông tin thu thập được, sử dụng các nguồn lực, phương tiện và các quy trình nghiệp vụ của mình để tiến hành phân tích sự cố. Kết quả phân tích sự cố được báo cáo Cơ quan thường trực, Cơ quan điều phối quốc gia và chia sẻ trong bộ phận tác nghiệp ứng cứu khẩn cấp để phục vụ ứng cứu, khắc phục sự cố.

e) Khắc phục sự cố, gỡ bỏ mã độc

Đơn vị chủ trì: Chủ quản hệ thống thông tin.

Đơn vị phối hợp: Cơ quan điều phối quốc gia, các đơn vị khác thuộc Bộ phận tác nghiệp ứng cứu khẩn cấp.

Nội dung thực hiện:

Sao lưu hệ thống trước và sau khi xử lý sự cố;

- Tiêu diệt các mã độc, phần mềm độc hại;
- Khôi phục hệ thống, dữ liệu và kết nối;
- Cấu hình hệ thống an toàn;
- Kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố;
- Khắc phục các điểm yếu an toàn thông tin;
- Bổ sung các thiết bị, phần cứng, phần mềm bảo đảm an toàn thông tin cho hệ thống;
- Triển khai theo dõi, giám sát, ngăn chặn khả năng lặp lại sự cố hoặc xảy ra các sự cố tương tự.

g) Ngăn chặn, xử lý hậu quả

Chủ quản hệ thống thông tin có trách nhiệm xử lý các hậu quả do sự cố hệ thống thông tin của mình gây ra ảnh hưởng đến người dân, cơ quan, tổ chức khác.

Các đơn vị thuộc thành phần tham gia tác nghiệp ứng cứu khẩn cấp, dựa trên các kết quả phân tích, điều tra, sử dụng các nguồn lực, phương tiện và nghiệp vụ của mình để tiến hành ngăn chặn các hành vi gây ra sự cố và hỗ trợ xử lý hậu quả.

h) Xác minh nguyên nhân và truy tìm nguồn gốc

Các đơn vị tham gia tác nghiệp ứng cứu khẩn cấp sau khi phân tích sự cố, tham khảo các kết quả phân tích sự cố của các đơn vị khác, sử dụng các nguồn tin và quy trình nghiệp vụ của mình, chủ động điều tra chi tiết nguyên nhân và truy tìm nguồn gốc, gửi Cơ quan thường trực, Cơ quan điều phối quốc gia để tổng hợp, xác minh, báo cáo Ban Chỉ đạo quốc gia các thông tin liên quan, cụ thể bao gồm:

- Đối tượng bị tấn công;
- Phương thức thủ đoạn tấn công (quy trình, kỹ thuật, mẫu mã độc, phần mềm độc hại);
- Thời gian tấn công;
- Các thiệt hại đã xảy ra;
- Đối tượng tấn công;
- Dự đoán khả năng xảy ra các tấn công tương tự và thiệt hại.

Bước 6: Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

Đơn vị chủ trì: Ban Chỉ đạo quốc gia

Nội dung thực hiện: Cơ quan thường trực tổng hợp toàn bộ các báo cáo phân tích có liên quan đến triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia để báo cáo với Ban Chỉ đạo quốc gia và họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung cho các sự cố tương tự.

Bước 7: Kết thúc

Đơn vị chủ trì: Cơ quan điều phối quốc gia

Đơn vị phối hợp: Chủ quản hệ thống thông tin, các đơn vị thuộc Bộ phận tác nghiệp ứng cứu khẩn cấp.

Nội dung thực hiện: Cơ quan điều phối quốc gia căn cứ kết quả đánh giá của Ban Chỉ đạo quốc gia sẽ thực hiện hoàn tất các nhiệm vụ sau khi kết thúc hoạt động ứng cứu sự cố khẩn cấp:

- Lưu hồ sơ, tài liệu lưu trữ;
- Xây dựng, đúc rút các bài học, kinh nghiệm;
- Đề xuất các kiến nghị về kỹ thuật, chính sách để hạn chế thiệt hại khi xảy ra các tấn công tương tự;
- Báo cáo cơ quan cấp trên, tổ chức họp báo hoặc gửi thông tin cho truyền thông nếu cần thiết.