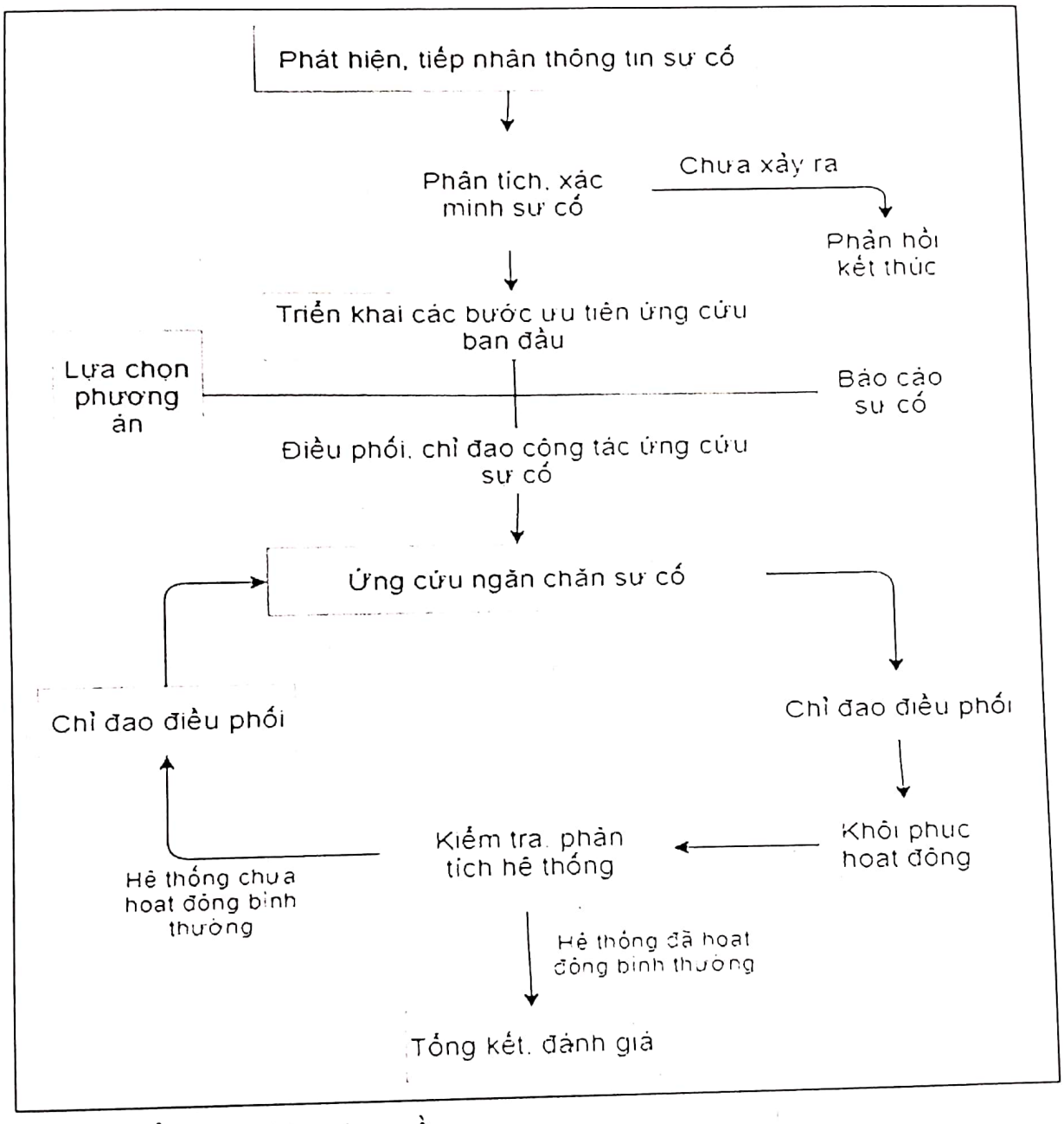
HỌC VIỆN CHÍNH TRỊ QUỐC GIA
HỒ CHÍ MINH
HỌC VIỆN BÁO CHÍ VÀ TUYÊN TRUYỀN
*

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày ... tháng.... năm .....

QUY TRÌNH ỨNG PHÓ SỰ CỐ CNTT

Công tác ứng cứu, xử lý sự cố CNTT cần được thực hiện khoa học, hiệu quả và thường nằm trong quy trình xử lý sự cố an toàn thông tin, được mô tả tại Hình sau:



Các bước triển khai chính, bao gồm:

1. Phát hiện, tiếp nhận, ứng cứu ban đầu và thông báo sự cố

1.1. Phát hiện, tiếp nhận, xác minh sự cố

Đơn vị vận hành hệ thống thông tin chủ trì, phối hợp với Đơn vị thường trực về ứng cứu sự cố của Học viện và các tổ chức liên quan tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài (cảnh báo sự cố: Văn bản, email, điện thoại, website, mạng xã hội...; phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá). Khi xác định được sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp.

Các loại sự cố chính, bao gồm:

- Sự cố do bị tấn công hệ thống mạng;
- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền...;
- Sự cố do lỗi của người quản trị, vận hành hệ thống;
- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn,...

1.2. Triển khai, lựa chọn các bước ưu tiên ứng cứu ban đầu:

Sau khi đã xác định sự cố xảy ra, đơn vị vận hành hệ thống thông tin tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo phương án đối phó, ứng cứu một số tình huống sự cố cụ thể hoặc theo tư vấn, hướng dẫn của Đơn vị thường trực về ứng cứu sự cố.

1.3. Thông báo, báo cáo sự cố:

Sau khi triển khai các bước ưu tiên ứng cứu ban đầu, đơn vị vận hành hệ thống thông tin tổ chức thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan, tổ chức theo quy định. Cụ thể:

- Thông báo sự cố tới Đơn vị thường trực về ứng cứu sự cố chậm nhất 03 ngày kể từ khi phát hiện sự cố; trường hợp xác định sự cố có thể vượt khả năng xử lý, đơn vị vận hành hệ thống thông tin phải báo cáo ban đầu sự cố bằng văn bản về Đơn vị thường trực về ứng cứu sự cố.

1.4. Điều phối công tác ứng cứu

- Căn cứ vào tính chất sự cố, đề nghị hỗ trợ của Đơn vị vận hành hệ thống thông tin và báo cáo ban đầu của Đơn vị thường trực về ứng cứu sự cố. Đội ứng cứu sự cố thực hiện công tác điều phối, giám sát cơ chế phối hợp, chia sẻ thông tin

theo phạm vi, chức năng, nhiệm vụ của mình để huy động nguồn lực ứng cứu sự cố.

- Hướng dẫn thực hiện yêu cầu điều phối xử lý sự cố tới các thành viên trong Đội ứng cứu sự cố.

2. Triển khai ứng cứu, ngăn chặn sự cố

Đơn vị vận hành hệ thống phối hợp với Đơn vị thường trực về ứng cứu sự cố và các đơn vị liên quan tiến hành triển khai theo phương án đối phó, ứng cứu một số tình huống sự cố cụ thể. Trong đó, tập trung nguồn lực thực hiện:

2.1. Triển khai thu thập chứng cứ, xác định phạm vi, đối tượng bị ảnh hưởng.

- Thu thập thông tin ban đầu để phục vụ phân tích sự cố:

+ Thông tin về đầu mối liên hệ;

+ Thu thập thông tin hệ thống;

+ Thu thập chức năng của hệ thống;

+ Thu thập cấu hình của hệ thống (OS, Servise, version, network...):

+ Thu thập chứng cứ;

+ Thu thập bộ nhớ;

+ Thu thập trạng thái network và các kết nối:

+ Thu thập các tiến trình dang chạy:

+ Thu thập hard drive media;

+ Thu thập log file;

+ Thu thập các cổng đang mở của hệ thống.

2.2. Triển khai phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

- Phân tích sự cố, xác định nguồn gốc tấn công

+ Phân tích dòng thời gian;

+ Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi.

+ Thời gian thực hiện các cập nhật lớn đối với hệ thống;

+ Thời điểm mà hệ thống sử dụng lần cuối cùng;

+ Phân tích dữ liệu

+ Phân tích hệ thống quản lý tệp (File System)

+ Phân tích Resgitry

- Phân tích Windows
- Phân tích kết nối mạng

3. Xử lý sự cố, gỡ bỏ và khôi phục

3.1. Xử lý sự cố, gỡ bỏ

Sau khi đã triển khai ngăn chặn sự cố, đơn vị vận hành hệ thống thông tin, Đơn vị thường trực về ứng cứu sự cố và các đơn vị liên quan triển khai tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.

3.2. Khôi phục

Đơn vị vận hành hệ thống chủ trì phối hợp với các đơn vị liên quan triển khai các hoạt động khôi phục hệ thống thông tin dữ liệu và kết nối; cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng phần mềm bảo đảm an toàn thông tin cho hệ thống thông tin.

3.3. Kiểm tra, đánh giá hệ thống thông tin

Đơn vị vận hành hệ thống và các đơn vị liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ chức các bước tương ứng để xử lý dứt điểm, khôi phục hoạt động bình thường của hệ thống thông tin.

4. Tổng kết, đánh giá

4.1. Tổng kết, đúc rút kinh nghiệm:

Đơn vị vận hành hệ thống thông tin bị sự cố phối hợp với Đơn vị thường trực về ứng cứu sự cố triển khai tổng hợp tất cả các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai, báo cáo Cơ quan chuyên trách về an toàn thông tin; tổ chức phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai...

4.2. Xây dựng báo cáo kết thúc ứng phó sự cố:

Đơn vị vận hành hệ thống thông tin bị sự cố, Đơn vị thường trực về ứng cứu sự cố triển khai tổng hợp và xây dựng báo cáo kết thúc ứng phó sự cố, trong đó trình bày chi tiết quá trình xử lý sự cố, tóm tắt tổng quát về tình hình sự cố và đề

xuất cách thức triển khai điều phối, ứng cứu sự cố nhằm xử lý nhanh, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự.

Sau khi kết thúc ứng cứu sự cố, trong vòng 10 ngày đơn vị vận hành hệ thống thông tin phải xây dựng báo cáo kết thúc ứng phó sự cố, gửi về Cơ quan chuyên trách về an toàn thông tin./.

BỘ PHẬN CNTT&TBDH

Vũ Hữu Thu