Phụ lục 01

QUY TRÌNH PHỐI HỢP ỨNG CỨU, XỬ LÝ KHẨN CẤP SỰ CỐ TẤN CÔNG MẠNG

(Kèm theo công văn số 795/CATTT-VNCERTCC ngày 25/6/2021 của Cục An toàn thông tin)

1. Quy định chung

1.1. Các bên liên quan

- Chủ quản hệ thống thông tin là cơ quan báo chí có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin vận hành website, trang báo điện tử, tạp chí điện tử.

- Đơn vị vận hành hệ thống thông tin là tổ chức/doanh nghiệp/bộ phận được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin bị sự cố tấn công mạng.

- Bộ phận ứng cứu sự cố tại chỗ (gọi là bộ phận ứng cứu sự cố) là bộ phận do chủ quản hệ thống thông tin thành lập và giao nhiệm vụ ứng cứu, xử lý sự cố tấn công mạng.

- Mạng lưới Ứng cứu sự cố an toàn thông tin mạng quốc gia gồm các cơ quan, tổ chức, doanh nghiệp chịu sự điều phối ứng cứu sự cố của Cục An toàn thông tin (Cục ATTT) theo Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ.

1.2. Thông tin liên hệ Cục An toàn thông tin

Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC):

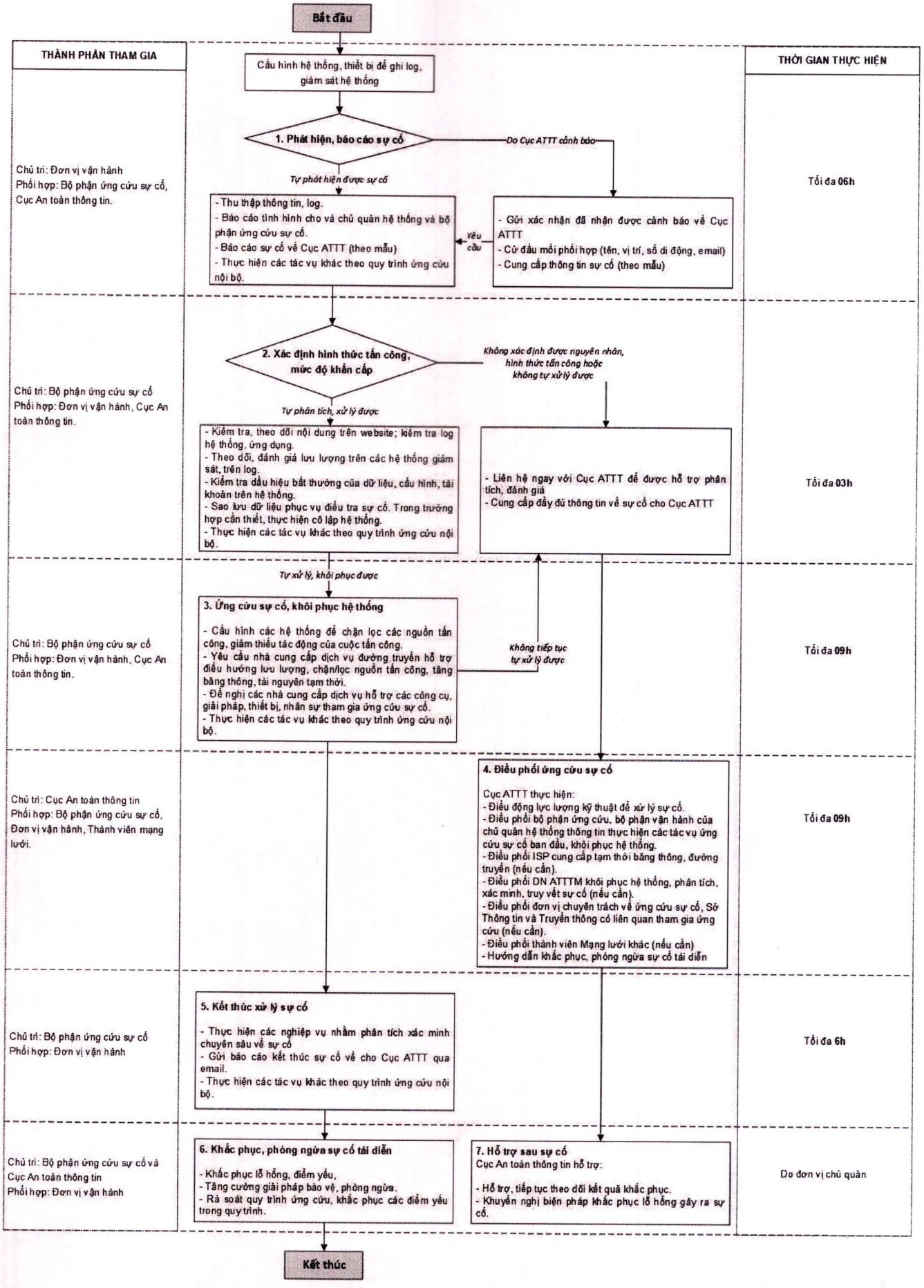
- Địa chỉ: Tầng 5, tòa nhà 115 Trần Duy Hưng, Cầu Giấy, Hà Nội

- Website: www.vncert.gov.vn.

- Email: **ir@vncert.vn**.

- Số điện thoại đường dây nóng **0869 100317** (thoại, sms, viber, zalo).

2. Lược đồ quy trình ứng cứu, xử lý khẩn cấp sự cố tấn công mạng



3. Mô tả các bước trong quy trình ứng cứu, xử lý sự cố tấn công mạng

Hệ thống thông tin phải thường xuyên rà quét và thực hiện cấu hình hệ thống, thiết bị để lưu nhật ký (log), giám sát hệ thống.

1.1 Phát hiện, báo cáo sự cố

a) Bộ phận chủ trì: Đơn vị vận hành

b) Bộ phận phối hợp: Bộ phận ứng cứu sự cố tại chỗ, Cục An toàn thông tin.

c) Nội dung công việc:

(c1) Đối với sự cố tự phát hiện được, thực hiện:

+ Thu thập thông tin, log: dấu hiệu sự cố, thu thập log (ứng dụng, thiết bị mạng, thiết bị bảo mật,…) phục vụ xác định nguyên nhân, nguồn gốc và đưa ra giải pháp xử lý sự cố.

+ Báo cáo tình hình cho chủ quản hệ thống thông tin và bộ phận ứng cứu sự cố.

+ Báo cáo sự cố chi tiết về Cục ATTT (Mẫu báo cáo khẩn cấp sự cố tấn công mạng tham khảo kèm theo).

+ Thực hiện các tác vụ khác theo quy trình ứng cứu sự cố nội bộ.

(c2) Đối với sự cố Cục ATTT cảnh báo:

+ Gửi xác nhận đã nhận được cảnh báo về Cục ATTT.

+ Cử đầu mối phối hợp (họ tên, chức vụ, số di động, email).

+ Thực hiện các hoạt động như nội dung tại (c1).

d) Thời gian thực hiện: tối đa **06 giờ (h)**.

1.2 Xác định hình thức tấn công, mức độ khẩn cấp

a) Bộ phận chủ trì: Bộ phận ứng cứu sự cố

b) Bộ phận phối hợp: Đơn vị vận hành, Cục ATTT.

c) Nội dung công việc:

(c1) Trường hợp bộ phận ứng cứu tự phân tích, xử lý được:

- Kiểm tra, theo dõi nội dung trên hệ thống, website; kiểm tra log (ứng dụng, thiết bị mạng, thiết bị bảo mật,…).

- Theo dõi, đánh giá lưu lượng trên các hệ thống giám sát, trên log để đánh giá tình hình, phát hiện sự bất thường.

- Rà soát, kiểm tra dấu hiệu bất thường của dữ liệu, cấu hình, tải khoản trên hệ thống.

- Trên cơ sở đó xác định hình thức tấn công và mức độ khẩn cấp của sự cố.

- Sao lưu dữ liệu phục vụ xác minh, truy vết sự cố. Trong trường hợp cần thiết, thực hiện cô lập hệ thống.

- Thực hiện các nội dung khác theo quy trình nội bộ.

(c2) Trường hợp bộ phận ứng cứu sự cố không tự phân tích, xử lý được:

- Liên hệ ngay với Cục ATTT để được hỗ trợ phân tích.

- Cung cấp đầy đủ các thông tin về sự cố theo yêu cầu của Cục ATTT.

d) Thời gian thực hiện: tối đa **03h**

1.3 Ứng cứu sự cố, khôi phục hệ thống

a) Bộ phận chủ trì: Bộ phận ứng cứu sự cố

b) Bộ phận phối hợp: Đơn vị vận hành, Cục ATTT.

(c1) Trường hợp tiếp tục tự xử lý được

- Căn cứ vào sự cố và hình thức tấn cống thực hiện cấu hình các hệ thống để chặn lọc các nguồn tấn công, giảm thiểu tác động của cuộc tấn công và khôi phục lại hệ thống.

- Đề nghị các nhà cung cấp dịch vụ vận hành, an toàn thông tin,…có liên quan hỗ trợ các công cụ, giải pháp, thiết bị, nhân sự tham gia ứng cứu sự cố.

- Yêu cầu nhà cung cấp dịch vụ đường truyền hỗ trợ điều hướng lưu lượng, chặn/lọc nguồn tấn công, tăng băng thông, tài nguyền tạm thời (nếu cần).

- Thực hiện các nội dung khác theo quy trình nội bộ.

(c2) Trường hợp không tiếp tục tự xử lý được

- Liên hệ ngay với Cục ATTT để được hỗ trợ phân tích, đánh giá tình trạng.

- Cung cấp đầy đủ các thông tin về sự cố theo yêu cầu của Cục ATTT.

- Thời gian thực hiện: Tối đa **09h**.

1.4 Điều phối ứng cứu sự cố

Trong trường hợp cần thiết, Cục ATTT thực hiện điều phối ứng cứu sự cố.

a) Bộ phận chủ trì: Cục ATTT.

b) Bộ phận phối hợp: Bộ phận ứng cứu sự cố, Đơn vị vận hành, Thành viên mạng lưới.

c) Nội dung công việc:

Căn cứ trên tình hình thực tế, Cục ATTT sẽ:

- Điều động lực lượng kỹ thuật của Cục ATTT để hướng dẫn các tác nghiệp ứng cứu, xử lý sự cố, khôi phục hệ thống từ xa hoặc thực hiện ứng cứu, xử lý sự cố, khôi phục hệ thống ngay tại hiện trường.

- Điều phối các đơn vị chuyên trách về ứng cứu sự cố có liên quan trực tiếp thực hiện ứng cứu khẩn cấp sự cố.

- Điều phối đơn vị vận hành, bộ phận ứng cứu (gồm cả các doanh nghiệp/tổ chức cung cấp dịch vụ) cung cấp thông tin, thực hiện các tác nghiệp ứng cứu, xử lý sự cố và khôi phục hệ thống.

- Điều phối thành viên Mạng lưới là các doanh nghiệp cung cấp hạ tầng Internet có liên quan để hỗ trợ tạm thời băng thông, đường truyền (nếu cần).

- Điều phối thành viên Mạng lưới là các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng tham gia công tác ứng cứu, xử lý, khôi phục hệ thống, phân tích, xác minh, truy vết sự cố (nếu cần).

- Điều phối thành viên Mạng lưới là Sở TT&TT tỉnh, thành phố liên quan; các đơn vị chuyên trách về ứng cứu sự cố và các thành viên Mạng lưới khác tham gia ứng cứu, xử lý sự cố (nếu cần).

- Hướng dẫn khắc phục, phòng ngừa sự cố tái diễn.

d) Thời gian thực hiện: Tối đa trong **09h**.

1.5 Kết thúc xử lý sự cố

a) Bộ phận chủ trì: Bộ phận ứng cứu sự cố.

b) Bộ phận phối hợp: Đơn vị vận hành.

c) Nội dung công việc:

- Thực hiện các nghiệp vụ nhằm phân tích xác minh chuyên sâu về sự cố.

- Gửi báo cáo kết thúc sự cố về cho Cục ATTT qua email. Báo cáo gồm các thông tin: diễn biến sự cố, cách thức xử lý sự cố và thời gian xử lý xong sự cố

- Thực hiện các tác vụ khác theo quy trình ứng cứu nội bộ.

d) Thời gian thực hiện: Tối đa trong **06h**.

1.6 Khắc phục, phòng ngừa sự cố tái diễn.

a) Bộ phận chủ trì: Bộ phận ứng cứu sự cố

b) Bộ phận phối hợp: Đơn vị vận hành

c) Nội dung công việc:

- Triển khai các biện pháp khắc phục lỗ hổng, điểm yếu.

- Tăng cường giải pháp bảo vệ, phòng ngừa.

- Rà soát quy trình ứng cứu, khắc phục các điểm yếu trong quy trình.

d) Thời gian thực hiện: Do đơn vị chủ quản.

3.7. Hỗ trợ sau sự cố

a) Bộ phận chủ trì: Cục ATTT

b) Bộ phận phối hợp: Bộ phận ứng cứu sự cố, đơn vị vận hành

c) Nội dung công việc:

- Tiếp tục theo dõi kết quả, hỗ trợ khắc phục sự cố trong thời gian tiếp theo.

- Khuyến nghị các biện pháp bảo đảm an toàn, an ninh mạng cần triển khai để khắc phục các lỗ hổng dẫn tới sự cố.

d) Thời gian thực hiện: trong vòng 01 tuần sau kết thúc xử lý sự cố.

Mẫu báo cáo khẩn cấp sự cố tấn công mạng

BÁO CÁO KHẨN CẤP SỰ CỐ TẤN CÔNG MẠNG

(Ngày..... tháng..... năm.....)

1. Thông tin về cơ quan báo chí gặp sự cố

(1) Tên cơ quan báo cáo sự cố (*) .....

(2) Tên lãnh đạo cơ quan gặp sự cố (*).....

(3) Địa chỉ: (*) .....

(4) Điện thoại (*) .....

(5) Email (*).....

2. Đầu mối ứng cứu sự cố

(6) Họ và tên (*) .....

(7) Chức vụ:.....

(8) Điện thoại (*) .....

(9) Email (*).....

3. Mức độ chia sẻ thông tin về sự cố

(10) Thông tin sự cố chỉ được chia sẻ cho các đối tượng nào dưới đây (*)
(*Đánh dấu vào các đối tượng sẵn sàng chia sẻ thông tin để hỗ trợ công tác xử lý, truy vết sự cố*):

☐ Cục An toàn thông tin (Trung tâm VNCERT/CC)

☐ Đơn vị vận hành cho hệ thống bị sự cố

☐ Đơn vị đảm bảo an toàn thông tin cho hệ thống bị sự cố

☐ Các doanh nghiệp về an toàn thông tin để được hỗ trợ xử lý sự cố

☐ Tất cả cộng đồng.

4. Thông tin chi tiết về hệ thống xảy ra sự cố

(11)Tên đơn vị vận hành hệ thống thông tin (*): .....

(12)Cơ quan chủ quản (*):.....

(13)Lãnh đạo cơ quan chủ quản (Tên, số điện thoại) (*):.....

(14)Tên hệ thống bị sự cố:.....

- Địa chỉ IP: .....
- Tên miền: .....

(15)Tổ chức cung cấp dịch vụ an toàn thông tin (nếu có):.....

Đầu mối liên hệ:

- Họ và tên (*) .....
- Chức vụ: .....

- Điện thoại (*).....
- Email (*).....

(16)Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có).....

Đầu mối liên hệ:

- Họ và tên (*) .....
- Chức vụ: .....
- Điện thoại (*).....
- Email (*).....

(17)Dải địa chỉ Public IP kết nối với hệ thống bên ngoài:

.....

.....

(18)Mô tả sơ bộ quá trình xảy ra sự cố (*)

.....

.....

.....

(19)Thời gian phát hiện sự cố (*): .....giờ.... phút ngày ...../...../.....

(20)Cách thức phát hiện (*) (Đánh dấu những cách thức được sử dụng để phát hiện sự cố)

☐ Qua hệ thống phát hiện xâm nhập

☐ Kiểm tra dữ liệu lưu lại (Log File)

☐ Nhận được thông báo từ: .....

☐ Khác, đó là .....

(21)Đã gửi thông báo sự cố cho (*)

☐ ISP đang trực tiếp cung cấp dịch vụ

☐ Tổ chức cung cấp dịch vụ vận hành hệ thống

☐ Tổ chức cung cấp dịch vụ vận hành an toàn thông tin

☐ Cục An toàn thông tin

☐ Đơn vị khác:.....

(22)Hệ điều hành (*).....Version.....

(23)Các dịch vụ có trên hệ thống (*)

(Đánh dấu những dịch vụ được sử dụng trên hệ thống)

☐ Web server

☐ Mail server

☐ Database server

☐ Dịch vụ khác, đó là .....

(24)Các biện pháp an toàn thông tin đã triển khai (*)

(Đánh dấu những biện pháp đã triển khai)

☐ Giải pháp an toàn cho thiết bị đầu cuối (Endpoint), tên giải pháp .....

☐ Firewall, tên giải pháp .....

☐ Hệ thống phát hiện xâm nhập (IDS/IPS), tên giải pháp .....

☐ Hệ thống SIEM, tên giải pháp .....

☐ Hệ thống chống DDoS, tên giải pháp .....

☐ Hệ thống chống tấn công APT, tên giải pháp .....

☐ Khác: .....

(25)Các địa chỉ IP của hệ thống (Liệt kê địa chỉ IP sử dụng trên Internet) (*):

.....

.....

(26)Các tên miền của hệ thống (*): .....

(27)Mục đích chính sử dụng hệ thống(*): .....

(28)Thông tin gửi kèm

☐ Mô hình kết nối hệ thống (*)

☐ Nhật ký hệ thống (*), bao gồm .....

☐ Mẫu virus / mã độc

☐ Khác (nếu có):.....

(29) Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật (*):

☐ Có

☐ Không

(30)Kiến nghị, đề xuất hỗ trợ: .....

.....

.....

.....

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁT LUẬT

(Ký tên, đóng dấu)

Chú thích: 1. Phần (*) là những thông tin bắt buộc. Các phần còn lại có thể loại bỏ nếu không có thông tin.

2. Sử dụng tiêu đề (subject) bắt đầu bằng "[TBSC]" khi gửi thông báo qua email