BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 3024 /BTTTT-VNCERT	
V/v hướng dẫn một số giải pháp tăng cường bảo đảm an toàn cho hệ thống thông tin	*Hà Nội, ngày 01 tháng 9 năm 2016*

VĂN PHÒNG UBND TỈNH TÂY NINH
Số: 2928
ĐẾN Ngày: 05-9-16
Chuyển: ...

Kính gửi:

- Văn phòng Chủ tịch nước; Văn phòng Quốc hội;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- HĐND, UBND các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn kinh tế, Tổng công ty nhà nước, Tổ chức tài chính và Ngân hàng, các doanh nghiệp hạ tầng Internet, viễn thông.

Thực hiện Nghị quyết phiên họp Chính phủ thường kỳ tháng 7 năm 2016 số 71/NQ-CP ngày 05/8/2016 của Chính phủ, Bộ Thông tin và Truyền thông (TTTT) ban hành hướng dẫn và đề nghị các cơ quan Trung ương, các Bộ, Ngành, tỉnh, thành phố và các cơ quan, tổ chức, doanh nghiệp liên quan chỉ đạo, đôn đốc sát sao các cơ quan, đơn vị trực thuộc và các đơn vị vận hành hệ thống thông tin nghiêm túc, khẩn trương triển khai thực hiện một số giải pháp nhằm tăng cường đảm bảo an toàn thông tin mạng cho các hệ thống thông tin, cụ thể như sau:

1. Tổ chức triển khai hoạt động tổng kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho các hệ thống thông tin, máy chủ, máy trạm, thiết bị mạng, phần cứng, phần mềm hệ thống, phần mềm ứng dụng nhằm đánh giá tổng thể mức độ an toàn thông tin mạng, kịp thời phát hiện và xử lý sự cố, lỗ hổng, ngăn chặn, bóc gỡ mã độc tấn công vào hệ thống mạng theo quy trình tại Phụ lục 01 và 02. Đặc biệt chú trọng phát hiện và xử lý các mã độc, tấn công APT có tính chất nguy hiểm, tiềm ẩn sâu bên trong hệ thống và có khả năng gây rủi ro cao.

2. Chủ động xây dựng phương án, giải pháp kỹ thuật bảo đảm an toàn hệ thống thông tin theo hướng dẫn tại Phụ lục 03.

3. Thường xuyên tổ chức huấn luyện, diễn tập về ứng cứu sự cố, đảm bảo an toàn thông tin mạng cho các hệ thống thông tin theo quy trình tại Phụ lục 04, đặc biệt là trong các ngành, lĩnh vực hạ tầng trọng yếu quốc gia gồm: Chính phủ, chính quyền điện tử; thành phố thông minh; viễn thông; giao thông (đường sắt, đường bộ, đường thủy, hàng không, bến cảng); tài chính, ngân hàng; năng

lượng, điện, dầu, khí; thủy lợi, nước; thương mại điện tử và những ngành lĩnh vực trọng yếu khác.

Trường hợp xảy ra các sự cố, phát hiện các tấn công hoặc mã độc nguy hiểm cần kịp thời chủ động xử lý và thông báo cho các cơ quan chức năng có liên quan. Đầu mối thông báo sự cố, hỗ trợ kỹ thuật và điều phối, ứng cứu sự cố quốc gia: Cục An toàn thông tin, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), Bộ TTTT, 18 Nguyễn Du, Hà Nội; điện thoại: 04.3.640.4423, di động: 0934.424.009; thư điện tử: ir@vncert.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- PTTgCP Vũ Đức Đam (để b/c);
- Bộ trưởng Trương Minh Tuấn (để b/c);
- Các đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở TT&TT của các Tỉnh, thành phố trực thuộc Trung ương;
- Bộ TTTT: Cục ATTT, Trung tâm Thông tin;
- Lưu: VT, VNCERT (04b).

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Hưng

Phụ lục 01

QUY TRÌNH KIỂM TRA, RÀ SOÁT, ĐÁNH GIÁ BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

(Kèm theo Công văn số 3024 /BTTTT-VNCERT ngày 01 /9/2016 của Bộ Thông tin và Truyền thông)

1. Mục đích

Tài liệu này hướng dẫn các hoạt động thực hiện kiểm tra, rà soát, đánh giá đảm bảo an toàn thông tin mạng tại các tổ chức, cơ quan đơn vị bao gồm:

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho trang/cổng thông tin điện tử (Website);

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho hệ thống ứng dụng công nghệ thông tin;

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho máy trạm;

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho máy chủ;

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho thiết bị mạng.

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho các hệ thống thông tin khác.

2. Phạm vi áp dụng

Áp dụng cho tất cả các tổ chức, cơ quan, đơn vị có nhu cầu kiểm tra, rà soát, đánh giá đảm bảo an toàn thông tin mạng.

3. Thuật ngữ và định nghĩa

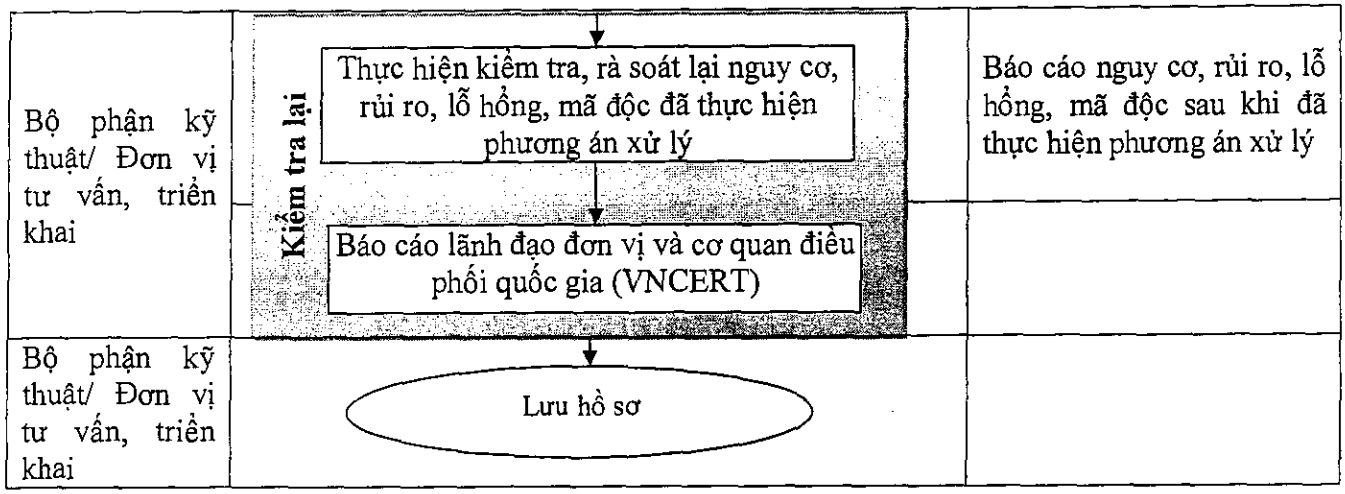
- Website: Trang/cổng thông tin điện tử

- CNTT: Công nghệ thông tin

4. Nội dung quy trình

4.1 Sơ đồ quy trình

Người chịu trách nhiệm	Trình tự công việc	Tài liệu liên quan
Lãnh đạo cơ quan, đơn vị	Yêu cầu kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng	
Lãnh đạo cơ quan, đơn vị	Phân công bộ phận kỹ thuật thực hiện hoặc lựa chọn đơn vị đủ năng lực để triển khai	
Bộ phận kỹ thuật/ Đơn vị tư vấn, triển khai	Xây dựng kế hoạch kiểm tra, rà soát, đánh giá bảo đảm ATTT mạng	Kế hoạch kiểm tra, rà soát, đánh giá bảo đảm ATTT mạng
Lãnh đạo cơ quan, đơn vị	Duyệt (-)	
Bộ phận kỹ thuật/ Đơn vị tư vấn, triển khai	(+) Thực hiện kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng	
Bộ phận kỹ thuật/ Đơn vị tư vấn, triển khai	Phân tích xác minh: Lập báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng	Báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng
	Xác minh (-) Loại bỏ các dữ kiện không đúng; (+)	Hồ sơ báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng
Bộ phận kỹ thuật/ Đơn vị tư vấn, triển khai	Tổng hợp báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng và đề xuất phương án xử lý, gửi lãnh đạo đơn vị, thông báo/cảnh báo đến các đơn vị liên quan và Cơ quan điều phối quốc gia (VNCERT)	Báo cáo kết quả kiểm tra, rà soát, đánh giá bảo đảm ATTT và đề xuất phương án xử lý
Lãnh đạo cơ quan đơn vị	Phân công bộ phận kỹ thuật thực hiện hoặc lựa chọn đơn vị đủ năng lực để triển khai các phương án xử lý đảm bảo ATTT	Kế hoạch thực hiện phương án xử lý
Lãnh đạo cơ quan đơn vị	Yêu cầu kiểm tra, rà soát, đánh giá lại sau thực hiện phương án xử lý	



4.2 Mô tả quy trình

4.2.1 Yêu cầu kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin

Căn cứ vào nhu cầu thực tế và tình hình an ninh, an toàn thông tin trong khu vực, Lãnh đạo cơ quan, đơn vị xác định yêu cầu kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng (bao gồm: đối tượng, phạm vi kiểm tra, rà soát, đánh giá an toàn bảo mật).

4.2.2 Phân công bộ phận kỹ thuật thực hiện hoặc lựa chọn đơn vị đủ năng lực để triển khai

Lãnh đạo cơ quan, đơn vị xem xét năng lực kỹ thuật của nhân sự trong cơ quan, đơn vị để phân công thực hiện hoặc có thể thuê đơn vị tư vấn phối hợp kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin.

4.2.3 Xây dựng kế hoạch kiểm tra, rà soát, đánh giá bảo đảm ATTT mạng

Bộ phận kỹ thuật /Đơn vị tư vấn, triển khai chịu trách nhiệm lập Kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin theo yêu cầu của cơ quan, đơn vị. Kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng phải bao gồm tối thiểu các nội dung sau:

- Mục đích kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng;
- Đối tượng kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin;
- Phạm vi, quy mô kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng;
- Tiêu chí, phương thức kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng;
- Nguồn lực kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng;
- Thời gian, kế hoạch thực hiện kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng.

4.2.4 Duyệt kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng

Lãnh đạo cơ quan, đơn vị xem xét và phê duyệt kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng để bộ phận kỹ thuật hoặc đơn vị tư vấn tiến hành triển khai thực hiện.

4.2.5 Thực hiện kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin

Bộ phận kỹ thuật hoặc đơn vị tư vấn, triển khai tiến hành kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng các đối tượng:

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho trang/cổng thông tin điện tử (Website);
- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho hệ thống ứng dụng công nghệ thông tin;
- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho máy trạm;
- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho máy chủ;
- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho thiết bị mạng.
- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho các hệ thống thông tin khác.

4.2.6 Phân tích xác minh

Bộ phận kỹ thuật hoặc đơn vị tư vấn, triển khai lập báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng.

Chuyên gia kỹ thuật đọc phân tích,xem xét báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng để xác nhận lại có đúng nguy cơ mất an toàn thông tin không. Nếu không đúng tiến hành loại bỏ các dữ liệu sự kiện không chính xác. Nếu đúng tiến hành tổng hợp báo cáo nguy cơ, lỗ hổng, mã độc gây mất an toàn thông tin mạng và đề xuất phương án xử lý.

4.2.7 Tổng hợp báo cáo nguy cơ, lỗ hổng, mã độc gây mất an toàn thông tin mạng và đề xuất phương án xử lý

Bộ phận kỹ thuật hoặc đơn vị tư vấn, triển khai tổng hợp kết quả dựa trên kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng, tổng hợp báo cáo nguy cơ, lỗ hổng, mã độc gây mất an toàn thông tin mạng và đề xuất phương án xử lý, gửi lãnh đạo đơn vi, đồng thời thông báo/cảnh báo đến các đơn vị liên quan và báo cáo Cơ quan điều phối quốc gia VNCERT.

4.2.8 Phân công bộ phận kỹ thuật thực hiện hoặc lựa chọn đơn vị đủ năng lực để triển khai các phương án xử lý đảm bảo an toàn thông tin mạng

Cơ quan, đơn vị sau khi nhận báo cáo sẽ xem xét kết quả kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng , nếu cơ quan chủ quản còn có những vấn đề vướng mắc thì liên hệ với Bộ phận kỹ thuật hoặc đơn vị tư vấn, triển khai để làm rõ kết quả. Nếu không vướng mắc tiến hành phân công bộ phận kỹ thuật hoặc lựa chọn đơn vị đủ năng lực để tiến hành khắc phúc các biện pháp nhằm đảm bảo an toàn thông tin.

4.2.9 Yêu cầu kiểm tra, rà soát, đánh giá lại sau thực hiện phương án xử lý

Lãnh đạo cơ quan đơn vị yêu cầu bộ phận kỹ thuật hoặc đơn vị tư vấn triển khai tiến hành kiểm tra, rà soát, đánh giá lại các nguy cơ mất an toàn thông tin sau khi thực hiện phương án xử lý.

4.2.10 Kiểm tra lại

Bộ phận kỹ thuật hoặc đơn vị tư vấn thực hiện kiểm tra, rà soát lại nguy cơ, lỗ hổng, mã độc đã thực hiện phương án xử lý để đảm bảo an toàn bảo mật các đối tượng được kiểm tra, rà soát đánh giá như kế hoạch.

Sau khi rà soát tiến hành báo cáo cho lãnh đạo đơn vị, các đơn vị liên quan và cơ quan điều phối quốc gia VNCERT về kết quả kiểm tra, rà soát, đánh giá.

4.2.11 Lưu hồ sơ

Toàn bộ các hồ sơ trong quá trình kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng được lưu trữ phục vụ các hoạt động quản lý và theo dõi định kỳ.

5. Hồ sơ lưu trữ

stt	Tên hồ sơ	Đơn vị lưu trữ
1.	Kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng	Bộ phận kỹ thuật/Đơn vị tư vấn, triển khai
2.	Báo cáo nguy cơ, lỗ hổng, mã độc gây mất an toàn thông tin mạng	
3.	Hồ sơ báo cáo nguy cơ, lỗ hổng, mã độc gây mất an toàn thông tin mạng	
4.	Báo cáo kết quả kiểm tra, rà soát, đánh giá bảo đảm ATTT và đề xuất phương án xử lý	
5.	Báo cáo nguy cơ, lỗ hổng, mã độc sau khi đã thực hiện phương án xử lý	

Phụ lục 02

QUY TRÌNH XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

(Kèm theo Công văn số 3024 /BTTTT-VNCERT ngày 01 /9/2016 của Bộ Thông tin và Truyền thông)

1. Mục đích

Tài liệu này hướng dẫn các bước thực hiện xử lý sự cố an toàn thông tin tại các tổ chức, cơ quan, đơn vị khi có phát sinh.

2. Phạm vi áp dụng

Áp dụng cho tất cả các tổ chức, cơ quan, đơn vị.

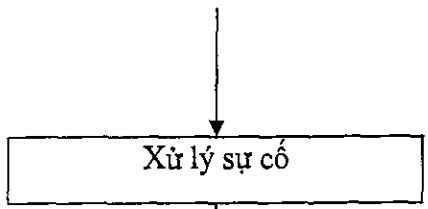
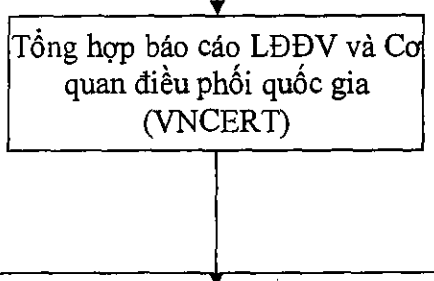
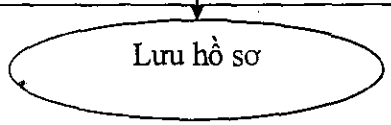
3. Thuật ngữ và định nghĩa

- **CERT:** Computer Emergency Response Team (Đội ứng cứu sự cố khẩn cấp).
- **LĐĐV:** Lãnh đạo đơn vị.
- **Phishing:** là hành vi giả mạo như là một thực thể đáng tin cậy (website của các cơ quan, tổ chức, các website xã hội phổ biến, các trung tâm chi trả trực tuyến,...) để lấy cắp thông tin nhạy cảm như tên người dùng, mật khẩu, các chi tiết thẻ tín dụng... thông qua các giao tiếp trên mạng.
- **Deface**: Là tấn công thay đổi nội dung website của nạn nhân thông qua lỗ hổng bảo mật.
- **Phát tán Malware:** là hành vi phát tán các phần mềm độc hại (virus, trojan, backdoor...) qua môi trường internet.
- **DoS** (Denial of Service) - tấn công từ chối dịch vụ bằng cách chiếm dụng một lượng lớn tài nguyên mạng, tài nguyên hệ thống như băng thông, bộ nhớ, khả năng xử lý ... và làm mất khả năng đáp ứng yêu cầu dịch vụ từ các khách hàng khác.

4. Nội dung quy trình

4.1Sơ đồ quy trình

Người chịu trách nhiệm	Trình tự công việc	Tài liệu liên quan
CERT tại cơ quan, đơn vị	Tiếp nhận sự cố	- Cảnh báo sự cố (Công văn, email, điện thoại, website) - Phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá
CERT tại cơ quan, đơn vị/ Đơn vị tư vấn, triển khai	Xác min/xác nhận sự cố -	- Xem xét tình trạng, mức độ, phạm vi và độ ưu tiên xử lý
CERT tại cơ quan, đơn vị/ Đơn vị tư vấn, triển khai	+ Phân loại sự cố	- Sự cố về tấn công thay đổi giao diện (deface) - Sự cố về tấn công lừa đảo - Sự cố về tấn công phát tán mã độc (malware) - Sự cố về một số tấn công mạng - Sự cố có yếu tố nước ngoài - Sự cố tấn công khác
Lãnh đạo đơn vị (LĐĐV)	Báo cáo LĐĐV và Cơ quan điều phối quốc gia (VNCERT)	- Chỉ đạo xử lý và phân công trách nhiệm xử lý
CERT tại cơ quan, đơn vị/ Đơn vị tư vấn, triển khai	Thu thập thông tin 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 đang chạy - Thu thập hard drive media - Thu thập removeble media - Thu thập log file
CERT tại cơ quan, đơn vị/ Đơn vị tư vấn, triển khai	Phân tích sự cố	- 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 ...

CERT tại cơ quan, đơn vị/ Đơn vị tư vấn, triển khai		- Gỡ bỏ sự cố - Xác định và gỡ bỏ các backdoors - Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi - Khôi phục dữ liệu - Thu thập các tập tin, hình ảnh, email, … bị xóa, thời gian bị xóa - Tìm kiếm các tập tin không thể khôi phục - Khôi phục các tập tin phù hợp
CERT tại cơ quan, đơn vị/ Đơn vị tư vấn, triển khai		- Báo cáo kết quả phân tích sự cố: mô tả chi tiết các bước quan trọng khi thực hiện xử lý sự cố. - Tổng hợp báo cáo gửi Lãnh đạo cơ quan, tổ chức và các bên liên quan đến sự cố - Rút kinh nghiệm và ứng dụng cho các sự cố tương tự
CERT tại cơ quan, đơn vị, VNCERT, Các bên liên quan		

4.2 Mô tả quy trình

4.2.1 Tiếp nhận sự cố

Đội CERT của cơ quan, đơn vị tiếp nhận thông tin về sự cố qua các phương thức: Email, điện thoại, công văn … Bên cạnh đó CERT nhận được các thông báo sự cố từ các hệ thống giám sát của các cơ quan nhà nước có thẩm quyền (VNCERT) hoặc các đơn vị quản lý ISP.

4.2.2 Xác minh/xác nhận sự cố

Đội CERT của cơ quan, đơn vị hoặc Đơn vị tư vấn, triển khai tiến hành Xác minh/xác nhận sự cố bao gồm các thông tin như sau:

- Tình trạng (Sự cố sẽ xãy ra; Sự cố đang xảy ra; Sự cố đã xảy ra);
- Mức độ (Sự cố nghiêm trọng; Sự cố bình thường);
- Phạm vi (Sự cố diện rộng; Sự cố mạng máy tính; Sự cố một máy tính);
- Và địa điểm xảy ra sự cố.

4.2.3 Phân loại sự cố

Sau khi xác nhận được sự cố, Đội CERT của cơ quan, đơn vị hoặc Đơn vị tư vấn, triển khai có trách nhiệm phân loại các sự cố theo hình thức như sau

- Sự cố về tấn công thay đổi giao diện (deface);
- Sự cố về tấn công lừa đảo (phishing);
- Sự cố về tấn công phát tán mã độc (malware);
- Sự cố về tấn công từ chối dịch vụ (DoS/DDoS);
- Sự cố có yếu tố nước ngoài (hợp tác quốc tế);
- Sự cố tấn công khác.

4.2.4 Báo cáo LĐĐV, xin ý kiến chỉ đạo

Ngay sau khi phân loại được sự cố Đội ứng cứu sự cố có trách nhiệm báo cáo Lãnh đạo đơn vị để xem xét loại sự cố và tuỳ theo đối tượng sẽ tiến hành phân công cho các thành viên trong tổ ứng cứu sự cố và báo cáo Cơ quan điều phối Quốc gia (VNCERT).

Các trường hợp phức tạp không tự xử lý được, gửi công văn nhờ sự hỗ trợ của các đơn vị quản lý ISP và cơ quan quản lý nhà nước về Ứng cứu và điều phối sự cố an toàn thông tin mạng như VNCERT (Bộ Thông tin truyền thông)

4.2.5 Thu thập thông tin phục vụ phân tích sự cố

Đội CERT của cơ quan, đơn vị hoặc Đơn vị tư vấn, triển khai phối hợp các đơn vị liên quan tiến hành thu thập các thông tin:

- 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 đang chạy
- Thu thập hard drive media
- Thu thập removeble media
- Thu thập Log file

4.2.6 Phân tích sự cố

Đội CERT của cơ quan, đơn vị hoặc Đơn vị tư vấn, triển khai tiến hành phân tích sự cố, bao gồm các thông tin sau:

- 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
- Kiểm tra sự thay đổi cấu hình
- Kiểm tra hệ thống tập tin có bị mã độc
- Kiểm tra tập tin Internet history và các tập tin history khác
- Kiểm tra Registry và tiến trình
- Quan sát các tập tin, tiến trình lúc khởi động
- Phân tích log file

4.2.7 Xử lý sự cố

Đội CERT của cơ quan, đơn vị hoặc Đơn vị tư vấn, triển khai tiến hành xử lý sự cố bao gồm các bước:

- Gỡ bỏ sự cố
- Xác định và gỡ bỏ các backdoors
- Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi
- Khôi phục dữ liệu
- Thu thập các tập tin, hình ảnh, email, ... bị xóa, thời gian bị xóa
- Tìm kiếm các tập tin không thể khôi phục
- Khôi phục các tập tin phù hợp

4.2.8 Tổng hợp báo cáo

Đội CERT của cơ quan, đơn vị hoặc Đơn vị tư vấn, triển khai tiến hành tổng hợp kết quả phân tích và báo cáo kết quả với lãnh đạo, trong đó mô tả chi tiết các bước thực hiện, giải pháp xử lý sự cố, kết quả khắc phục hiện tại.

Đội Ứng cứu sự cố tiến hành tổng hợp toàn bộ các báo cáo phân tích có liên quan đến sự có để báo cáo với lãnh đạo đơn vị và Cơ quan điều phối Quốc gia (VNCERT). Họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp ứng dụng cho các sự cố tương tự.

4.2.9 Lưu hồ sơ

Toàn bộ các hồ sơ trong quá trình xử lý sự cố được lưu trữ phục vụ các hoạt động quản lý và theo dõi định kỳ.

5. Hồ sơ lưu trữ

STT	Tên hồ sơ	Đơn vị lưu trữ
1.	Thông báo sự cố	Đội CERT tại cơ quan, đơn vị
2.	Kế hoạch xử lý sự cố	
3.	Hồ sơ xử lý sự cố	
4.	Báo cáo phân tích kết quả điều tra xử lý sự cố	
5.	Báo cáo thống kê hàng năm	

Phụ lục 03

HƯỚNG DẪN XÂY DỰNG PHƯƠNG ÁN, GIẢI PHÁP KỸ THUẬT BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN

(Kèm theo Công văn số 3024 /BTTTT-VNCERT ngày 01 /9/2016 của Bộ Thông tin và Truyền thông)

1. Giải thích từ ngữ

- **Chủ quản hệ thống thông tin** là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. Đối với cơ quan, tổ chức nhà nước, chủ quản hệ thống thông tin là các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương hoặc là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin đó.

- **Đơn vị vận hành hệ thống thông tin** là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin. Trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ

- **Đơn vị chuyên trách về công nghệ thông tin** là đơn vị chuyên trách về công nghệ thông tin của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ; Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc trung ương hoặc đơn vị chuyên trách về công nghệ thông tin của chủ quản hệ thống thông tin do chủ quản hệ thống thông tin chỉ định.

- **Đơn vị chuyên trách về an toàn thông tin** là đơn vị có chức năng, nhiệm vụ bảo đảm an toàn thông tin của chủ quản hệ thống thông tin.

- **Bộ phận chuyên trách về an toàn thông tin** là bộ phận do chủ quản hệ thống thông tin thành lập hoặc chỉ định để thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng.

2. Xây dựng phương án, giải pháp kỹ thuật bảo đảm an toàn cho HTTT

a. Chủ quản hệ thống thông tin chỉ đạo các đơn vị chuyên môn tham mưu, phối hợp với các tổ chức tư vấn, cung cấp dịch vụ để triển khai các biện pháp bảo đảm an toàn cho các hệ thống thông tin sau đây:

+ Xác định các hệ thống thông tin quan trọng và có thể trở thành mục tiêu tấn công của tin tặc cần được quan tâm bảo vệ.

+ Khảo sát và lập kế hoạch kiểm tra, rà quét, đánh giá an toàn thông tin cho các hệ thống thông tin quan trọng hoặc có nguy cơ bị tấn công cao. Các cơ quan nhà nước cần lưu ý các hệ thống thông tin cung cấp dịch vụ sau đây: Cổng thông tin điện tử, thư điện tử, dịch vụ công trực tuyến v.v...

+ Thực hiện kế hoạch kiểm tra, rà quét, đánh giá an toàn thông tin theo hướng dẫn tại Phục lục 01 kèm theo công văn này để phát hiện ra các điểm yếu an toàn thông tin đang tồn tại, khả năng xảy ra các sự cố an toàn thông tin mạng.

+ Xây dựng và triển khai các phương án khắc phục điểm yếu (nếu có), bảo vệ hoặc phòng ngừa để giảm thiểu thiệt hại khi có tấn công, sự cố an toàn thông tin mạng.

+ Kiểm tra rà quét để phát hiện, xử lý hoặc loại bỏ mã độc hoặc phần mềm độc hại đang có trong hệ thống mạng, máy tính.

+ Thường xuyên cập nhật các bản vá, phiên bản mới để hạn chế bị tấn công và khai thác lỗ hổng "Zero day" cho thiết bị mạng, máy tính, máy chủ. Chỉ cài đặt và sử dụng các phần mềm đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết. Không sử dụng các phần mềm đã được cảnh báo không an toàn hoặc không được nhà sản xuất hỗ trợ kỹ thuật khi không thực sự cần thiết.

+ Triển khai các biện pháp sao lưu dự phòng để nâng cao khả năng phục hồi hoạt động khi xảy ra sự cố;

+ Thiết lập, các biện pháp quản lý truy cập an toàn, phù hợp, hạn chế tối đa việc sử dụng tài khoản vượt quyền hạn so với nhu cầu. Sử dụng và quản lý mật khẩu an toàn theo hướng dẫn của Trung tâm VNCERT (xem tại: http://www.vncert.gov.vn/files/Huong_dan_su_dung_mat_khau_an_toan.pdf).

+ Thực hiện cấu hình hoạt động hệ thống thư điện tử theo hướng dẫn số 430/BTTTT-CATTT ngày 09 tháng 02 năm 2015 của Cục An toàn thông tin "về việc hướng dẫn bảo đảm ATTT cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước" và sử dụng an toàn hòm thư điện tử công vụ theo hướng dẫn tại công văn số 244/VNCERT-KTHT ngày 12/9/2013 của Trung tâm VNCERT (xem tại:

www.vncert.gov.vn/files/huongdansudungantoanthudientucongvu.pdf).

+ Việc triển khai các hệ thống thông tin, thiết bị, phần mềm cần tuân thủ theo các hướng dẫn và quy định về bảo đảm an toàn do nhà sản xuất công bố.

+ Rà soát, cập nhật các quy định, quy trình về bảo đảm an toàn thông tin để phát hiện ra các sai sót, bất cập, điều chỉnh bổ sung phù hợp. Xem xét áp dụng các tiêu chuẩn về quản lý rủi ro an toàn thông tin như: tiêu chuẩn TCVN ISO/IEC 27001:2009 và bộ tiêu chuẩn ISO/IEC 27001.

b. Các đơn vị vận hành hệ thống thông tin cần nâng cao tinh thần cảnh giác, chủ động thực hiện các nhiệm vụ sau:

+ Tăng cường theo dõi, giám sát các hoạt động của hệ thống thông tin để phát hiện ra các vấn đề bất thường, dấu hiệu tấn công, sự cố an toàn thông tin mạng. Khi phát hiện sự cố an toàn thông tin, thực hiện xử lý quy trình xử lý được hướng dẫn tại Phụ lục 02.

+ Thực hiện đúng công tác thông báo sự cố theo điều 7 Thông tư số 27/2011/TT-BTTTT ngày 4/10/2011 của Bộ Thông tin và Truyền thông về việc "Quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam".

b. Đơn vị chuyên trách về an toàn thông tin có trách nhiệm:

- Tổ chức kiểm tra đánh giá trình độ của bộ phận chuyên trách về an toàn thông tin. Xây dựng kế hoạch phát triển đội ngũ kỹ thuật và tổ chức đào tạo, huấn luyện nâng cao trình độ để có thể đáp ứng yêu cầu thực tế.

- Chỉ đạo và cử cán bộ tham gia đầy đủ và nghiêm túc các hoạt động diễn tập và huấn luyện về an toàn thông tin do các đơn vị chức năng thuộc Bộ Thông tin và Truyền thông tổ chức.

- Tuyên truyền, phổ biến và nâng cao nhận thức cho cán bộ, công chức và người lao động về an toàn thông tin mạng. Tăng cường đào tạo, hướng dẫn các kỹ năng sử dụng máy tính an toàn cho người sử dụng máy tính.

- Tăng cường chia sẻ, trao đổi kinh nghiệm trong công tác bảo đảm an toàn thông tin.

Phụ lục 04

QUY TRÌNH HƯỚNG DẪN DIỄN TẬP AN TOÀN THÔNG TIN MẠNG

(Kèm theo Công văn số 3024 /BTTTT-VNCERT ngày 01 /8/2016 của Bộ Thông tin và Truyền thông)

1. Mục đích

Tài liệu này hướng dẫn các bước thực hiện diễn tập an toàn thông tin tại các tổ chức, cơ quan, đơn vị có ứng dụng Công nghệ thông tin trong các hoạt động.

2. Phạm vi áp dụng

Áp dụng cho tất cả các tổ chức, cơ quan, đơn vị.

3. Thuật ngữ và định nghĩa

- **CERT**: Computer Emergency Response Team (Đội ứng cứu sự cố khẩn cấp/Tổ phản ứng nhanh an toàn thông tin mạng).

- **LĐ**: Lãnh đạo.

- **Phishing** là hành vi giả mạo như là một thực thể đáng tin cậy (website của các cơ quan, tổ chức, các website xã hội phổ biến, các trung tâm chi trả trực tuyến,...) để lấy cắp thông tin nhạy cảm như tên người dùng, mật khẩu, các chi tiết thẻ tín dụng... thông qua các giao tiếp trên mạng.

- **Deface** là tấn công thay đổi nội dung website của nạn nhân thông qua lỗ hổng bảo mật.

- **Phát tán Malware** là hành vi phát tán các phần mềm độc hại (virus, trojan, backdoor...) qua môi trường internet.

- **DoS** (Denial of Service) - tấn công từ chối dịch vụ bằng cách chiếm dụng một lượng lớn tài nguyên mạng, tài nguyên hệ thống như băng thông, bộ nhớ, khả năng xử lý ... và làm mất khả năng đáp ứng yêu cầu dịch vụ từ các khách hàng khác.

4. Nội dung quy trình

4.1 Sơ đồ quy trình

Người chịu trách nhiệm	Trình tự công việc	Tài liệu liên quan
Bộ phận kỹ thuật/CERT của cơ quan, đơn vị	Xác định nhu cầu diễn tập	- Quy trình xử lý sự cố (nếu có)
Bộ phận kỹ thuật/CERT của cơ quan, đơn vị hoặc đơn vị tư vấn, triển khai	Đề xuất chủ đề, nội dung diễn tập	- Xác định mục tiêu diễn tập - Đối tượng diễn tập
Lãnh đạo	Xem xét (-, +)	
Bộ phận kỹ thuật/CERT của cơ quan, đơn vị hoặc đơn vị tư vấn, triển khai	Xây dựng kế hoạch diễn tập	- Xây dựng kịch bản diễn tập, nội dung huấn luyện trước diễn tập và tài liệu liên quan - Lựa chọn hình thức diễn tập - Thời gian diễn tập - Kênh liên lạc: web, mail, chat
Lãnh đạo	Xem xét (-, +)	- Thông tin về đầu mối - Địa điểm và thời gian xử lý
Lãnh đạo	Ký duyệt kế hoạch	
Bộ phận kỹ thuật/CERT của cơ quan, đơn vị hoặc đơn vị tư vấn, triển khai	Diễn tập: Kiểm tra kênh liên lạc trước diễn tập	- Kênh liên lạc sử dụng trong diễn tập - Quy tắc trong diễn tập
	Diễn tập: Huấn luyện, diễn tập theo kịch bản	- Thành phần Tổ chức - Thành phần Giám sát,điều phối người chơi - Thành phần tham gia diễn tập.
	Diễn tập: Tổng hợp, đánh giá	- Kịch bản,phản ứng với từng tình huống của cán bộ tham gia diễn tập - Đánh giá, phản hồi của cán bộ tham gia diễn tập
Bộ phận kỹ thuật/CERT của cơ quan, đơn vị	Lưu hồ sơ	

4.2 Mô tả quy trình

4.2.1 Nhận biết nguy cơ tấn công mạng

- Tất cả các sự cố có thể xảy ra với hệ thống thông tin của đơn vị;

- Những nguy cơ tấn công mạng có thể xảy ra.

4.2.2 Xác định nhu cầu thực tiễn

Bộ phận kỹ thuật/CERT của cơ quan, đơn vị có trách nhiệm nhận biết nguy cơ, rủi ro tấn công mạng từ đó xác nhu cầu thực tiễn phải tiến hành chương trình diễn tập như sau:

- Các sự cố có thể xảy ra đối với hệ thống thông tin của cơ quan tổ chức:

+ Sự cố về tấn công thay đổi giao diện (Deface);

+ Sự cố về tấn công lừa đảo (Phishing);

+ Sự cố về tấn công phát tán mã độc (Malware);

+ Sự cố về một số tấn công từ chối dịch vụ (DoS, DDoS);

+ Sự cố tấn công mạng khác.

- Hậu quả, mức độ thiệt hại nếu sự cố xảy ra;

- Nếu có chuẩn bị trước thì có thể giảm được thiệt hại đến mức nào.

4.2.3 Đề xuất diễn tập

Bộ phận kỹ thuật/CERT của cơ quan, đơn vị và đơn vị tư vấn (nếu có) có trách nhiệm đề xuất chương trình diễn tập với Lãnh đạo đơn vị gồm ít nhất những nội dung như sau:

- Mục tiêu của diễn tập;

- Đối tượng tham gia chương trình diễn tập;

- Mong muốn đạt được sau chương trình diễn tập;

- Mức độ cần thiết phải thực hiện chương trình diễn tập;

- Bước đầu xác định chủ đề diễn tập.

4.2.4 Xây dựng kế hoạch diễn tập

Ngay sau khi được Lãnh đạo đồng ý, bộ phận kỹ thuật/CERT của cơ quan, đơn vị và đơn vị tư vấn, triển khai (nếu có) phải lên kế hoạch chi tiết để thực hiện chương trình diễn tập gồm tối thiểu những nội dung sau:

a) Xác định chủ đề và thiết kế kịch bản diễn tập:

- Lựa chọn chủ đề;

- Thiết kế và xây dựng kịch bản diễn tập: kịch bản diễn tập chia thành các phần nhỏ và nối tiếp nhau để mô tả tình huống, sự cố sát với thực tế. Thông thường kịch bản của một chương trình diễn tập có từ 8-10 pha/tình huống mô tả các giai đoạn tấn công mạng với mức độ tăng dần.

- Một số sự cố có thể xây dựng kịch bản diễn tập gồm:

+ Sự cố tấn công từ chối dịch vụ vào trang, cổng thông tin điện tử (DDoS);

+ Sự cố tấn công thay đổi giao diện website (Deface);

+ Sự cố tấn công lừa đảo (Phishing);

+ Sự cố tấn công mã độc trên hệ thống mạng nội bộ của các đơn vị;

+ Sự cố tấn công mạng khác.

Các sự cố tấn công trong thực tế thường kết hợp nhiều hình thức tấn công nên trong quá trình thiết kế kịch bản diễn tập cần phải có những tình huống kết hợp giữa các tấn công này.

b) Nội dung huấn luyện theo kịch bản

Để kết quả diễn tập được hiệu quả, cần xây dựng nội dung huấn luyện theo nguyên tắc: nội dung diễn tập như nào thì nội dung huấn luyện như vậy.

c) Xác định các khung thời gian diễn tập

- Thời gian đăng ký diễn tập;

- Thời gian thử nghiệm kênh liên lạc;

- Thời gian huấn luyện theo kịch bản;

- Thời gian diễn tập chính thức;

- Thời gian báo cáo sau diễn tập.

c) Lên danh sách cán bộ tham gia diễn tập

- Gửi thông báo về chương trình diễn tập tới các đơn vị:

+ Thời gian;

+ Chủ đề;

+ Quy tắc.

- Tổng hợp danh sách cán bộ tham gia diễn tập.

Thông thường các đơn vị có thể phối hợp với các đơn vị liên quan đến việc xử lý sự cố để thực hiện chương trình diễn tập như: đơn vị quản lý ISP, Công ty hosting, công ty, doanh nghiệp làm về an toàn thông tin và cơ quan

quản lý nhà nước về Ứng cứu và điều phối sự cố an toàn thông tin mạng như VNCERT;

4.2.5 Kiểm tra kênh liên lạc trước diễn tập

- Kênh thư điện tử:

+ Gửi email cho các đơn vị theo mẫu: tiêu điều, nội dung, chữ ký...

+ Hỗ trợ và xác nhận các đơn vị phản hồi mail

- Kênh web:

+ Gửi thông tin website và tài khoản đăng nhập

+ Hỗ trợ và xác nhận các đơn vị đăng nhập và phản hồi trên web.

- Kênh chat:

+ Gửi thông tin để đăng nhập kênh chat qua email

+ Hỗ trợ và xác nhận các đơn vị đăng nhập và sử dụng kênh chat

4.2.6 Diễn tập theo kịch bản

Thông trường trong diễn tập có các vai trò sau được thể hiện rõ:

Thành phần Tổ chức (Excon): Là một nhóm thực hiện các thực hiện nhiệm vụ để điều khiển chương trình diễn tập như lên kế hoạch thời gian, kịch bản và hỗ trợ trong suốt quá trình diễn tập. Tùy thuộc vào tình huống của diễn tập họ có thể là Mục tiêu của tấn công, ISP, Cơ quan chính phủ để đảm bảo tình huống trong diễn tập sát với thực tế.

Thành phần Điều phối - Giám sát người chơi (Observers) của mỗi đội: thường là người có vai trò quản lý, điều phối hoạt động của Người chơi trong đội của mình. Thành phần này chịu trách nhiệm tương tác trực tiếp với thành phần Tổ chức và trao đổi thông tin với các nhóm khác về mọi vấn đề trong đội của mình như: kịch bản tình huống, thời gian, tiến độ và kết quả phản ứng tình huống trong suốt diễn tập.

Thành phần Người tham gia diễn tập(Player): tham gia trực tiếp vào diễn tập, tiếp nhận kịch bản cho từng tình huống và đưa ra phản ứng dưới kiểm soát của người điều phối - giám sát

4.2.7 Tổng hợp đánh giá

Bộ phận kỹ thuật/CERT của cơ quan, đơn vị có trách nhiệm phối hợp với đơn vị tư vấn (nếu có) thực hiện tổng hợp đánh giá kết quả diễn tập, và áp dụng các kết quả, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp ứng dụng cho các sự cố tương tự.

4.2.8 Lưu hồ sơ

Toàn bộ các hồ sơ trong quá trình diễn tập được lưu trữ phục vụ các hoạt động quản lý và theo dõi.

5. Hồ sơ lưu trữ

STT	Tên hồ sơ	Đơn vị lưu trữ
1.	Kế hoạch diễn tập	Bộ phận kỹ thuật/CERT của cơ quan, đơn vị
2.	Tổng hợp,đánh giá sau diễn tập	