UBND TỈNH TUYÊN QUANG
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

Số: 331/STTTT-CNTT
V/v hướng dẫn một số giải pháp tăng cường đảm bảo an toàn cho hệ thống thông tin

*Tuyên Quang, ngày 22 tháng 9 năm 2016*

UP 26/9

Kính gửi:
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành;
- Uỷ ban nhân dân các huyện, thành phố.

Thực hiện Văn bản số 3024/BTTTT-VNCERT ngày 01/9/2016 của Bộ Thông tin và Truyền thông về việc hướng dẫn một số giải pháp tăng cường đảm bảo an toàn cho hệ thống thông tin;

Sở Thông tin và Truyền thông hướng dẫn và đề nghị các sở, ban, ngành và Ủy ban nhân dân các huyện, thành phố 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.

Trong 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 Sở Thông tin và Truyền thông (điện thoại: 0276.251.788), đồng thời thông báo cho Cục An toàn thông tin hoặc Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), Bộ Thông tin và Truyền thông, 18 Nguyễn Du, Hà Nội; điện thoại: 04.3.640.4423, di động: 0934.424.009, thư điện tử ir@vncert.gov.vn để có phương án xử lý có hiệu quả.

Trân trọng./.

***Nơi nhận:***
- Như kính gửi;
- UBND tỉnh (báo cáo);
- Giám đốc Sở (báo cáo);
- Ban biên tập Website Sở;
- Lưu: VT, CNTT.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TUYÊN QUANG

**Vũ Tuấn**

**Phụ lục 01**

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

*( Kèm theo Công văn số 331/STTTT-CNTT, ngày 22/9/2016 của Sở 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 ưa, 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 ví 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 vả định nghĩa

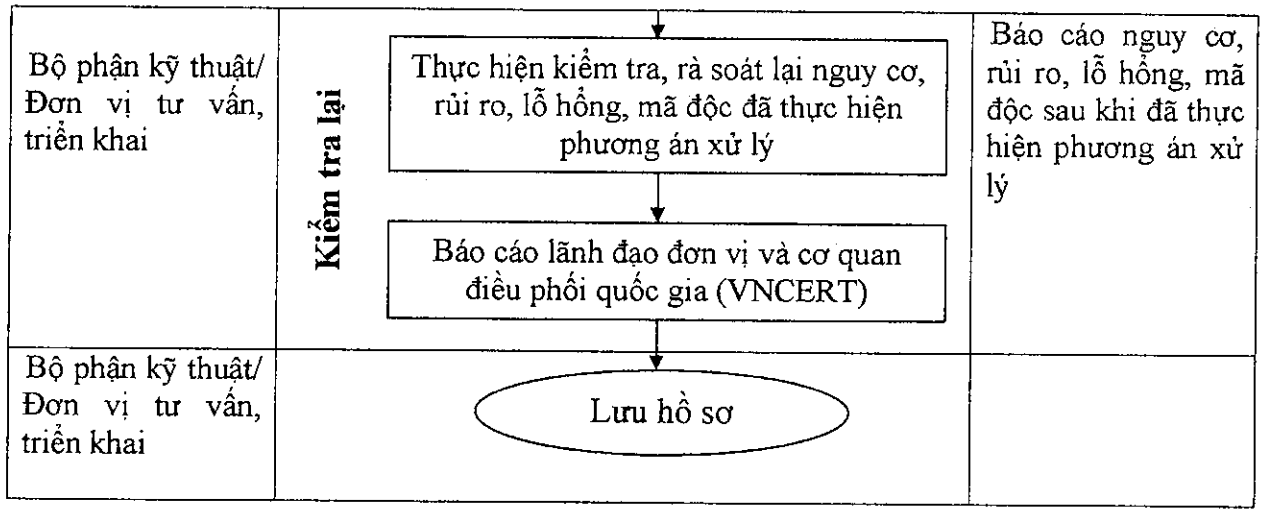
- Website: Trang/cổng thông tin điện tử

- CNTT: Công nghệ thông tin

## 4. Nội dung quy trình

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; Xác minh; Loại bỏ các dữ kiện không đúng | Báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất ATTT mạng<br>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 bảo 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 khi 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 vị, 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 phục 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 để 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 1731/STTTT-CNTT, ngày 22../9/2016 của Sở 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 cổ khẩn cấp).
- **LĐĐV**: Lãnh đạo đơn vị.
- **Phishing**: là hành vi giả mạo như là một thực thế 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 tải 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**

Sơ 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 cáo sự cố (Công văn, email, điện thoại, website)<br>- 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 minh/ xác nhận sự cố | - Xem xét tình trạng, mức độ vi phạm 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)<br>- Sự cố về tấn công lừa đảo<br>- Sự cố về tấn công phát tán mã độc<br>- Sự cố về một số tấn công mạng<br>- Sự cố có yếu tố nước ngoài<br>- Sự cố tấn công khác |
| Lãnh đơn vị (LĐĐV) | Báo cáo LĐĐV và VNCERT | - Chỉ đạo xử lý 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<br>- Thu thập thông tin hệ thống<br>- Thu thập chức năng của hệ thống<br>- Thu thập cấu hình của hệ thống (OS, servise, version, network, ...)<br>- Thu thập chứng cứ<br>- Thu thập bộ nhớ<br>- Thu thập trạng thái network và các kết nối<br>- Thu thập các tiến trình đang chạy<br>- Thu thập hard drive media<br>- Thu thập removeble media<br>- 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<br>- Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi<br>- Thời gian thực hiện các cập nhật lớn đối với hệ thống<br>- Thời điểm mà hệ thống sử dụng lần cuối cùng<br>- Phân tích dữ liệu... |
| CERT tại cơ | | - Gỡ bỏ sự cố |

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

### 4.1. Mô tả quy trình

#### 4.1.1. 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.

#### 4.1.2. Xác minh/xác nhận sự cố

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

- Tình trạng (Sự cố sẽ xảy 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 cố 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.

| 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 thông 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 331/STTTT-CNTT, ngày 22/9/2016 của Sở 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".

c. 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, cử cán bộ tham gia đầy đủ và nghiêm túc các hoạt động diễn tập, 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 tinh 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.