UBND TỈNH THANH HOÁ
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

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

Số: 404 /QĐ-STNMT

Thanh Hoá, ngày 05 tháng 7 năm 2022

QUYẾT ĐỊNH
Phê duyệt Phương án ứng cứu sự cố, xử lý sự cố tấn công Hệ thống thông tin của Sở Tài nguyên và Môi trường Thanh Hoá

GIÁM ĐỐC SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 632/QĐ-TTg ngày 10 tháng 5 năm 2017 của Thủ tướng Chính phủ ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Quyết định số 2434/2003/QĐ-UB ngày 28/7/2003 của UBND tỉnh Thanh Hoá về việc thành lập Sở Tài nguyên và Môi trường Thanh Hoá;

Căn cứ Quyết định số 121/QĐ-STTTT ngày 16/4/2021 của Giám đốc Sở Thông tin truyền thông về việc phê duyệt cấp độ an toàn hệ thống thông tin Sở Tài nguyên và Môi trường Thanh Hoá;

Căn cứ Quyết định số 379/QĐ-STNMT ngày 28/6/2022 của Sở Tài nguyên và Môi trường Thanh Hoá về việc thành lập Tổ ứng cứu sự cố An toàn thông tin mạng Sở Tài nguyên và Môi trường;

Xét đề nghị của Giám đốc Trung tâm Công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Phương án ứng cứu sự cố, xử lý sự cố tấn công Hệ thống thông tin của Sở Tài nguyên và Môi trường Thanh Hoá".

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Chánh Văn phòng Sở, Giám đốc Trung tâm Công nghệ thông tin, Trưởng các đơn vị thuộc Sở, Tổ ứng cứu sự cố An toàn thông tin mạng của Sở và toàn thể cán bộ, công chức, viên chức thuộc Sở Tài nguyên và Môi trường Thanh Hóa chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Giám đốc Sở (b/c);
- Sở Thông tin và truyền thông (b/c);
- Cổng thông tin điện tử Sở;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH THANH HÓA

Phùng Đình Ảnh

PHƯƠNG ÁN
ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN HỆ THỐNG THÔNG TIN SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG THANH HOÁ

(Kèm theo Quyết định số /QĐ-STNMT ngày /7/2022 của Giám đốc Sở Tài nguyên và Môi trường)

1. Quy định chung

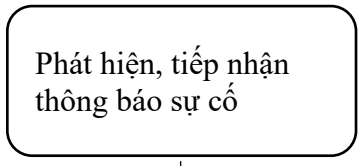
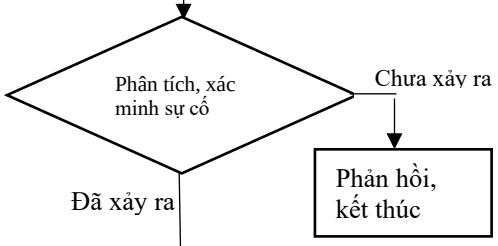
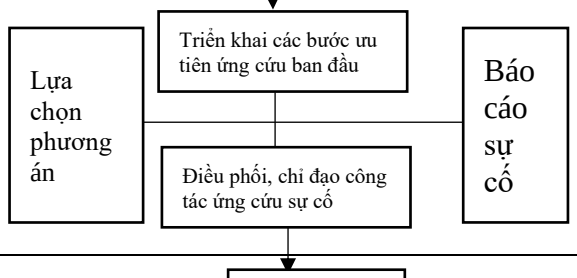
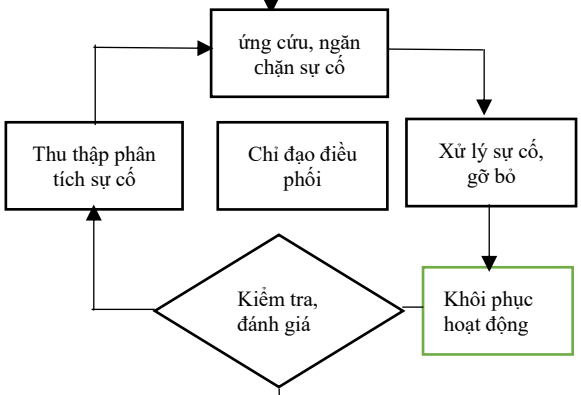
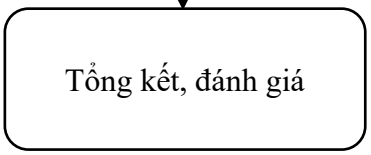
1.1. Các bên liên quan

- Đơn vị Chủ quản hệ thống thông tin: Sở Tài nguyên và Môi trường có thẩm quyền quản lý trực tiếp đối với hệ thông thông tin.
- Đơn vị vận hành hệ thống thông tin: Trung tâm Công nghệ thông tin.
- Bộ phận ứng cứu sự cố tại chỗ: là Tổ ứng cứu sự cố an toàn thông tin mạng Sở Tài nguyên và Môi trường (Tổ ứng cứu sự cố) do đơn vị 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 gồm: Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Thanh Hoá; Cục An toàn thông tin (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam VNCRET/CC)

1.2. Thông tin liên hệ:

- Tổ ứng cứu sự cố an toàn thông tin mạng Sở Tài nguyên và Môi trường
+ Địa chỉ: 14 Hạc Thành, phường Tân Sơn, thành phố Thanh Hoá
+ Số điện thoại: 0912.040.042 (Tổ trưởng - Tổ ứng cứu sự cố Sở)
- Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Thanh Hoá
+ Địa chỉ:
+ Website: https://attt.thanhhoa.gov.vn
+ Email: ungcuusuco@thanhhoa.gov.vn
+ Số điện thoại: 0916.422.583
- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCRET/CC)
+ Địa chỉ: Tầng 5, toà nhà 115 Trần Duy Hưng, Cầu Giấy, Hà Nội
+ Website: www.vncert.gov.vn
+ Email: ir@vncert.vn
+ Số điện thoại đường dây nóng: 0869100317

2. Lược đồ quy trình ứng cứu sự cố an toàn thông tin mạng theo sơ đồ như sau:

Thành phần	Quy trình	Ghi chú
Trung tâm Công nghệ thông tin, theo dõi Hệ thống thông tin (HTTT)		Thông tin sự cố có thể từ các nguồn: - Hệ thống theo dõi nội bộ của Trung tâm; - Thông tin thông báo từ các cơ quan, đơn vị -Thông tin mạng lưới - Nguồn tin xã hội
Trung tâm Công nghệ thông tin, Tổ ứng cứu sự cố an toàn thông tin mạng Sở và các bộ phân liên quan.		Doanh nghiệp viễn thông, ISP; thành viên mạng lưới; Cơ quan điều phối quốc gia phối hợp hỗ trợ
Tổ ưng cứu sự cố an toàn thông tin mạng Sở triển khai các bước ứng cứu, xử lý ban đầu; báo cáo sơ bộ sự cố.		Triển khai theo phương án đối phó, ứng cứu một số tình huống sự cố cụ thể.
Tổ ứng cứu sự cố an toàn thông tin mạng Sở, tổ chức triển khai phân tích, xác định nguồn gốc tấn công để tổ chức ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin - Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh chỉ đạo, điều phối ứng cứu sự cố.		Các thành phần tham gia ứng cứu sự cố căn cứ nội dung, nhiệm vụ được giao theo phân công, chỉ đạo tổ chức triển khai các quy trình, nghiệp vụ của mình. Quy trình này được triển khai liên tục, đảm bảo đến khi khôi phụ hoạt động của hệ thống thông tin trở lại bình thường.
Trung tâm Công nghệ thông tin; Tổ Ứng cứu sự cố an toàn thông tin mạng Sở.		

3. Mô tả các bước trong quy trình

3.1 Phát hiện, báo cáo sự cố

a) Bộ phận chủ trì: Trung tâm Công nghệ thông tin

b) Bộ phận phối hợp:

+ Tổ ứng cứu sự cố an toàn thông tin mạng Sở Tài nguyên và Môi trường

+ Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Thanh Hoá

+ Cục An toàn thông tin

c) Nội dung công việc:

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

+ 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 số phù hợp.

+ Báo cáo tình hình cho chủ quản hệ thống thông tin và Tổ ứng cứu sự cố an toàn thông tin mạng Sở Tài nguyên và Môi trường.

+ Báo cáo sự cố chi tiết về Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Thanh Hoá (theo hướng dẫn thực hiện yêu cầu phối hợp xử lý sự cố an toàn thông tin mạng tại Công văn số 675/STTTT-CNTT ngày 08/4/2021 của Sở Thông tin và Truyền thông).

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

(c2) Đối với sự cố do Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Thanh Hoá; Cục ATTT cảnh báo:

+ Gửi xác nhận đã nhận được cảnh báo về đơn vị cảnh báo.

+ 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.

- Các loại sự cố chính thường xảy ra:

+ Sự cố do bị tấn công mạng.

+ Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc lỗi đường điện, đường truyền ....

+ Sự cố của người quản trị, vận hành hệ thống.

+ Sự cố liên quan đến các thảm họ tự nhiên như bão, lụt, động đất, hoả hoạn,...

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

a) Bộ phận chủ trì: Tổ ứng cứu sự cố.

b) Đơn vị phối hợp: Trung tâm Công nghệ thông tin, Đơn vị thương trực về ứng cứu sự cố của tỉnh.

c) Nội dung công việc

- *Trường hợp Tổ ứng cứu sự cố tự phân tích, xử lý được:*

+ Kiểm tra, theo dõi nội dung trên hệ thống, 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, tài 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.

- *Trường hợp Tổ ứng cứu sự cố không tự phân tích, xử lý được:*

+ Liên hệ ngay với Đơn vị trường trực về ứng cứu sự cố của tỉnh.

+ Cung cấp đầy đủ các thông tin về sự cố theo yêu cầu của Đơn vị trường trực về ứng cứu sự cố của tỉnh.

d) Thời gian thực hiện: Tối đa 03 giờ.

3.3. Thông báo, báo cáo sự cố:

Sau khi triển khai các bước ưu tiên ứng cứu ban đầu, Trung tâm Công nghệ thông tin tổ chức thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan trong và ngoài cơ quan quy định. Cụ thể như sau:

- Báo cáo sự cố ngay tới Lãnh đạo Sở.

- Thông báo sự cố tới Tổ ứng cứu sự cố an toàn thông tin mạng Sở.

- Thông báo sự cố tới Đơn vị thường trực về ứng cứu sự cố của tỉnh chậm nhất 03 ngày kể từ khi phát hiện sự cố; trường hợp sự cố có thể vượt khả năng xử lý, Trung tâm Công nghệ thông tin phải báo cáo ban đầu sự cố bằng văn bản gửi về Đơn vị thường trực về ứng cứu sự cố của tỉnh. Hình thức gửi báo cáo:

+ Qua đường văn bản: Gửi về Trung tâm Công nghệ thông tin và Truyền thông Thanh Hoá.

+ Qua hộp thư điện tử: ungcuusuco@thanhhoa.gov.vn

4. Triển khai ứng cứu, ngăn chặn sự cố

Tổ ứng cứu sự cố phối hợp với Đơn vị thường trực về ứng cứu sự cố của tỉnh 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 tại ***Phụ lục II***. Trong đó tập trung nguồn lực thực hiện:

4.1. 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 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 hard drive media;

+ Thu thập log file;

+ Thu thập các cổng đang mở của hệ thống.

4.2. 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.

5. Xử lý sự cố, gỡ bỏ và khôi phục

5.1. Xử lý sự cố, gỡ bỏ

Sau khi đã triển khai ngăn chặn sự cố, Tổ ứng cứu sự cố, Đơn vị thường trực về ứng cứu sự cố của tỉnh và các đơn vị liên quan tiến hành 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.

5.2. Khôi phục

Trung tâm Công nghệ thông tin và Tổ ứng cứu sự cố phối hợp với các đơn vị liên quan triển khai 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.

5.3. Kiểm tra, đánh giá hệ thống thông tin

Trung tâm Công nghệ thông tin và Tổ ứng cứu sự cố phối hợp với các đơn vị liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống 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.

6. Tổng kết, đánh giá

6.1. Tổng kết, đúc rút nghiệm nghiệm:

Trung tâm Công nghệ thông tin và Tổ ứng cứu sự cố phối hợp với Đơn vị thường trực về ứng cứu sự có của tỉnh 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 của tỉnh; 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 trong tương lai...

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

Trung tâm Công nghệ thông tin, Tổ ứng cứu sự cố và Đơn vị thường trực về ứng cứu sự có của tỉnh 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 úug cứu sự cố, trong vòng 10 ngày Trung tâm Công nghệ thông tin phải xây dựng báo cáo kết thúc ứng phó sự số, gửi về Cơ quan chuyên trách an toàn thông tin của tỉnh.

PHƯƠNG ÁN
ĐỐI PHÓ, ỨNG CỨU MỘT SỐ TÌNH HUỐNG CỤ THỂ

(Kèm theo Quyết định số /QĐ-STNMT ngày /7/2022 của Giám đốc Sở Tài nguyên và Môi trường)

Bước	Nội dung tham khảo thực hiện	Bộ phận thực hiện
1. Tấn công gây rò rỉ dữ liệu		
Dấu hiệu	- Dữ liệu của cơ quan, đơn vị bị rò rỉ, phát tán trên không gian mạng - Tài khoản truy cập vào các hệ thống phần mềm dùng chung bị chiếm đoạt, khai thác trái phép. - Dữ liệu bị thay đổi, xóa bỏ, lấy cắp trái phép.	Bộ phận trực/giám sát hệ thống
Xử lý ưu tiên, ban đầu	- Thông báo Tổ ứng cứu sự cố an toàn thông tin mạng Sở - Ưu tiên cô lập hệ thống: Tách máy tính, thiết bị nghi ngờ rò rỉ dữ liệu ra khỏi hệ thống mạng nội bộ và ngắt kết nối Internet. - Tiến hành xác minh nhanh dữ liệu bị rò rỉ, xác định mức độ và phạm vi rò rỉ dữ liệu.	
Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu.	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc ban đầu của cuộc tấn công. - Thông báo với các đơn vị liên quan mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố. - Đánh giá sơ bộ về thiệt hại hoặc mức độ ảnh hưởng của sự cố	Trung tâm Công nghệ thông tin / Tổ ứng cứu sự cố an toàn thông tin mạng Sở/ Các đơn vị liên quan
Cô lập hệ thống	- Thực hiện cô lập hệ thống bị tấn công để tránh bị thay đổi hiện trường. - Thông báo tới các cơ quan chức năng và đối tác để hỗ trợ.	
Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Rà soát hệ thống để phát hiện các lỗ hổng có thể bị khai thác tấn công vào cơ sở dữ liệu. - Rà soát khả năng lộ mật khẩu của các tài khoản quản trị, tài khoản có quyền quản trị cơ sở dữ liệu. - Rà quét và xử lý mã độc trên máy tính của người sử dụng các tài khoản này này, thay đổi mật khẩu các tài khoản.	
Khôi phục hệ thống	- Xác định được lỗ hổng mà hacker đã sử dụng để tấn công, vá các lỗ hổng này. - Rà soát và vá các lỗ hổng ở module khác của hệ thống. - Sử dụng các công cụ rà quét mạng để phát hiện bất kỳ truy cập nào trái phép hoặc phát hiện sự quay trở lại của hacker.	
Kiện toàn hệ thống	- Điều tra chi tiết hơn về sự cố để mở rộng phạm vi và chống các ảnh hưởng tiềm tàng khác. - Ghi lại toàn bộ các thông tin liên quan đến sự cố như	Trung tâm Công nghệ thông tin

	cách thức phát hiện, đánh giá, xử lý sự cố và khôi phục hệ thống để làm tài liệu tham khảo cho các lần sau. - Phối hợp các cơ quan chức năng để phối hợp mở rộng phạm vi.	
2. Sự cố tấn công thay đổi giao diện		
Dấu hiệu	Trang thông tin điện tử của cơ quan, đơn vị bị thay đổi trái phép nội dung toàn bộ hoặc một phần.	Bộ phận trực/giám sát hệ thống
Xử lý ưu tiên, ban đầu	- Thông báo Tổ ứng cứu sự cố an toàn thông tin mạng Sở - Ưu tiên cô lập hệ thống cung cấp dịch vụ Website - Kích hoạt hệ thống dự phòng hoặc trang thông báo lỗi, bảo trì.	
Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc ban đầu của cuộc tấn công. - Kiểm tra xem tên miền có trỏ đúng vào máy chủ web hay không, liên hệ với đơn vị quản lý tên miền để xác định trạng thái tài khoản quản lý tên miền. - Trong trường hợp tên miền không bị chiếm quyền điều khiển: Thực hiện thay thế nội dung trang chủ bằng thông báo bảo trì, nâng cấp hệ thống. - Trong trường hợp tên miền bị chiếm quyền điều khiển: + Yêu cầu lấy lại quyền điều khiển tên miền + Cấu hình tên miền trỏ đúng về địa chỉ máy chủ web. + Yêu cầu khóa tài khoản quản lý tên miền này, không cho phép cập nhật các thông tin liên quan. - Thông báo với các đơn vị liên quan mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố.	Trung tâm Công nghệ thông tin / Tổ ứng cứu sự cố an toàn thông tin mạng Sở/ Các đơn vị liên quan
Cô lập hệ thống và kích hoạt hoạt động hệ thống dự phòng	- Thực hiện cô lập hệ thống bị tấn công để tránh bị thay đổi hiện trường. - Rà soát khả năng bị tấn công khai thác của hệ thống dự phòng và chuyển đổi sang hệ thống dự phòng. - Trong trường hợp hệ thống dự phòng cũng bị tấn công, thực hiện trỏ tên miền tới trang Cổng thông tin điện tử của tỉnh đồng thời thực hiện xây dựng hệ thống mới. - Tạm ngắt các tài khoản quản trị, tài khoản có quyền đăng bài lên website. - Thông báo tới các cơ quan chức năng và đối tác để hỗ trợ.	
Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Điều tra, phân tích hệ thống để tìm kiếm các shell, file lạ, phân tích hành vi và xác định nguyên nhân của cuộc tấn công. - Thu thập tất cả các thành phần file độc hại và phối hợp với các đối tác phân tích, điều tra. - Phân tích các hành vi của shell và mã độc. - Xác định và xử lý được đầy đủ các thành phần của mã độc	

	+ File shell hacker đã tải lên server + Tiến trình của mã độc + File của mã độc + Thành phần đăng ký khởi động cùng server của mã độc - Rà soát khả năng lộ mật khẩu của các user quản trị, user có quyền đăng bài lên website. - Rà quét và xử lý mã độc trên máy tính của user này, sau đó đổi mật khẩu các user.	
Kiện toàn hệ thống	- Điều tra chi tiết hơn về sự cố để mở rộng phạm vi và chống các ảnh hưởng tiềm tàng khác. - Ghi lại toàn bộ các thông tin liên quan đến sự cố như cách thức phát hiện, đánh giá, xử lý sự cố và khôi phục hệ thống để làm tài liệu tham khảo cho các lần sau. - Phối hợp các cơ quan chức năng để phối hợp mở rộng phạm vi.	Trung tâm Công nghệ thông tin
3. Tấn công mã độc		
Dấu hiệu	Hệ thống thông tin/máy tính trong Sở bị tấn công bởi các dạng mã độc khác nhau.	Bộ phận trực/giám sát hệ thống
Xử lý ưu tiên, ban đầu	- Thông báo Tổ ứng cứu sự cố an toàn thông tin mạng Sở - Ưu tiên cô lập toàn bộ các máy bị lây nhiễm hoặc có dấu hiệu bất thường. - Kiểm tra các máy tính có dữ liệu quan trọng, cô lập và có biện pháp sao lưu dữ liệu.	
Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc ban đầu của cuộc tấn công. - Xác định cấu phần thuộc hệ thống bị ảnh hưởng/phạm vi bị ảnh hưởng. - Thông báo với các đơn vị liên quan mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố.	Trung tâm Công nghệ thông tin / Tổ ứng cứu sự cố an toàn thông tin mạng Sở/ Các đơn vị liên quan
Cô lập hệ thống	- Thực hiện cô lập hệ thống bị tấn công để tránh bị thay đổi hiện trường và thông báo về khoảng thời gian tạm dừng hệ thống dự kiến. - Thông báo tới các cơ quan chức năng và đối tác để hỗ trợ.	
Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Điều tra, phân tích hệ thống để tìm kiếm các shell, file lạ, phân tích hành vi của nó và xác định nguyên nhân của cuộc tấn công. - Thu thập tất cả các thành phần file độc hại và phối hợp với các đối tác phân tích, điều tra. - Phân tích các hành vi của shell và mã độc. - Xác định và xử lý được đầy đủ các thành phần của mã độc *+ File shell hacker đã tải lên server* *+ Tiến trình của mã độc* *+ File của mã độc*	

	+ Thành phần đăng ký khởi động cùng server của mã độc - Rà soát khả năng lộ mật khẩu của các tài khoản quản trị, tài khoản có quyền trên hệ thống. - Rà quét và xử lý mã độc trên máy tính của các người dùng sử dụng tài khoản này, thay đổi mật khẩu các tài khoản.	
Khôi phục hệ thống	- Xác định được lỗ hổng mà hacker đã sử dụng để tấn công, vá các lỗ hổng này. - Rà soát và vá các lỗ hổng ở module khác của hệ thống. - Thực hiện ngăn chặn mã hash, C&C server (nếu có) trên hệ thống Antivirus, Firewall, IPS. - Đưa hệ thống chính quay lại hoạt động. - Sử dụng các công cụ rà quét mạng để phát hiện bất kỳ truy cập nào trái phép hoặc phát hiện sự quay trở lại của hacker.	
Kiện toàn hệ thống	- Điều tra chi tiết hơn về sự cố để mở rộng phạm vi và chống các ảnh hưởng tiềm tàng khác. - Ghi lại toàn bộ các thông tin liên quan đến sự cố như cách thức phát hiện, đánh giá, xử lý sự cố và khôi phục hệ thống để làm tài liệu tham khảo cho các lần sau. - Phối hợp các cơ quan chức năng để phối hợp mở rộng phạm vi.	Trung tâm Công nghệ thông tin
4. Tấn công từ chối dịch vụ		
Dấu hiệu	Toàn bộ các truy cập vào dịch vụ tại Sở cung cấp ngoài Internet không truy cập được hoặc truy cập chậm, gián đoạn.	Bộ phận trực/giám sát hệ thống
Xử lý ưu tiên, ban đầu	- Thông báo Tổ ứng cứu sự cố an toàn thông tin mạng - Thông báo tới nhà cung cấp dịch vụ và Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh. - Kích hoạt hệ thống dự phòng (nếu có)	Trung tâm Công nghệ thông tin / Tổ ứng cứu sự cố an toàn thông tin mạng Sở/ Các đơn vị liên quan
Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc ban đầu của cuộc tấn công. - Thông báo với các đơn vị liên quan mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố.	
Kích hoạt hoạt động hệ thống dự phòng	- Rà soát khả năng bị tấn công khai thác của hệ thống dự phòng và chuyển đổi sang hệ thống dự phòng. - Trong trường hợp hệ thống dự phòng cũng bị tấn công, thực hiện trỏ tên miền hệ thống thông báo dịch vụ. Đồng thời thực hiện triển khai hệ thống mới tách biệt với hệ thống hiện có về đường truyền, bảo đảm cung cấp các dịch vụ thiết yếu trong thời gian khôi phục hệ thống chính. - Thông báo tới các cơ quan chức năng và đối tác để hỗ trợ.	

Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Trường hợp các nhà cung cấp dịch vụ Internet, phân giải tên miền bị tấn công từ chối dịch vụ, thực hiện chuyển sang các đường truyền của nhà cung cấp dịch vụ khác. - Liệt kê các địa chỉ IP thực hiện tấn công từ chối dịch vụ và chặn trên hệ thống Firewall. Trong trường hợp dịch vụ cung cấp phần lớn là khách hàng ở Việt Nam, phối hợp với các ISP hoặc cấu hình trên hệ thống Firewall ngăn chặn truy cập có IP nguồn từ nước ngoài để giảm thiểu nguồn tấn công. - Rà soát hệ thống để phát hiện các lỗ hổng có thể bị khai thác tấn công từ chối dịch vụ. - Phối hợp với ISP, đối tác để hỗ trợ xử lý sự cố.	
Khôi phục hệ thống	- Xác định được lỗ hổng mà hacker đã sử dụng để tấn công, vá các lỗ hổng này. - Rà soát và vá các lỗ hổng ở module khác của hệ thống. - Đưa hệ thống chính quay lại hoạt động. - Sử dụng các công cụ rà quét mạng để phát hiện bất kỳ truy cập nào trái phép hoặc phát hiện sự quay trở lại của hacker.	
Kiện toàn hệ thống	- Điều tra chi tiết hơn về sự cố để mở rộng phạm vi và chống các ảnh hưởng tiềm tàng khác. - Ghi lại toàn bộ các thông tin liên quan đến sự cố như cách thức phát hiện, đánh giá, xử lý sự cố và khôi phục hệ thống để làm tài liệu tham khảo cho các lần sau. - Phối hợp các cơ quan chức năng để phối hợp mở rộng phạm vi.	Trung tâm Công nghệ thông tin