UỶ BAN NHÂN DÂN **XÃ KỲ KHANG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:197 /QĐ-UBND	*Kỳ Khang, ngày 20 tháng 12 năm 2023*

QUYẾT ĐỊNH
Về việc ban hành Phương án bảo đảm, ứng phó, khắc phục sự cố an toàn, an ninh mạng đối với các hệ thống thông tin của xã Kỳ Khang

ỦY BAN NHÂN DÂN XÃ

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

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

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về 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 01/2021/QĐ-UBND ngày 19/01/2021 của Ủy ban nhân dân tỉnh Hà Tĩnh về Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh;

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 19/6/2015;Luật sửa đổi, bổ sung một số điều của Luật tổ chức Chính phủ và Luật tổ chức Chính quyền địa phương ngày 22/11/2019;

Theo đề nghị của công chức Văn hóa - Xã hội (chuyên trách CNTT) xã,

QUYẾT ĐỊNH:

Điều 1: Ban hành kèm Quyết định này Phương án bảo đảm, ứng phó, khắc phục sự cố an toàn, an ninh mạng đối với các hệ thống thông tin UBND xã Kỳ Khang

Điều 2: Quyết định có hiệu lực kể từ ngày ban hành.

Điều 3: Công chức Văn phòng - Thống kê, Công chức Văn hóa - Xã hội (chuyên trách CNTT), các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận: - Như Điều 3; - Các PCT UBND xã; - Lưu: VT, VP.	**TM. ỦY BAN NHÂN DÂN** **CHỦ TỊCH** **Hồ Xuân Trính**

ỦY BAN NHÂN DÂN
XÃ KỲ KHANG

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

PHƯƠNG ÁN
Bảo đảm, ứng phó, khắc phục sự cố an toàn, an ninh mạng đối với các hệ thống thông tin của xã Kỳ Khang

(Ban hành kèm theo Quyết định số /QĐ-UBND, ngày tháng 12 năm 2023)

I. PHƯƠNG ÁN BẢO ĐẢM AN TOÀN, AN NINH MẠNG ĐỐI VỚI CÁC HỆ THỐNG THÔNG TIN CỦA XÃ KỲ KHANG

1. Hồ sơ, tài liệu quản lý

a) Lập hồ sơ, tài liệu hệ thống như tài liệu thiết kế, triển khai, quản trị, vận hành, bảo đảm an toàn thông tin.

b) Lưu trữ, bảo quản hồ sơ, tài liệu, xác định phạm vi phổ biến, sử dụng của tài liệu.

c) Thực hiện cập nhật tài liệu thường xuyên khi có thay đổi, xem xét định kỳ hàng năm.

2. Kiểm tra, đánh giá an toàn, an ninh mạng

a) Thực hiện kiểm tra, đánh giá chức năng và an toàn, an ninh mạng các hệ thống thông tin trước khi đưa vào sử dụng, khi triển khai hệ thống mới hoặc nâng cấp hệ thống có thay đổi kiến trúc của hệ thống.

b) Thực hiện kiểm tra, đánh giá chức năng và an toàn, an ninh mạng trước khi đưa vào sử dụng đối với các phần mềm thuê khoán, khi xây dựng phần mềm mới hoặc khi thay đổi phần mềm, thay đổi mã nguồn mà có ảnh hưởng đến kiến trúc của phần mềm.

c) Chuẩn bị hồ sơ, thực hiện các bước, quy trình kiểm tra, đánh giá an toàn, an ninh mạng theo quy định, quy trình, hướng dẫn của Trung Tâm CNTT và Truyền thông (đơn vị chuyên trách về ATTT của Sở Thông tin và Truyền thông).

3. Giám sát an toàn, an ninh mạng

a) Triển khai giám sát 24/7 đối với các hệ thống thông tin.

b) Các yêu cầu giám sát cơ bản gồm: trạng thái hoạt động up/down; lưu lượng mạng, dịch vụ. Ngoài ra, thực hiện giám sát an toàn thông tin theo hướng dẫn tại Thông tư số 31/2017/TT-BTTTT. Tùy vào điều kiện, nguồn lực và mức độ quan trọng của các hệ thống thông tin, có thể triển khai thêm các phương án giám sát khác để giám sát bất thường, nguy cơ, rủi ro hoặc dấu hiệu an toàn, an ninh mạng của hệ thống thông tin.

c) Xây dựng các quy trình xử lý đối với các sự cố an toàn, an ninh mạng

được phát hiện qua công tác giám sát. Đối với các sự cố chưa có trong quy trình, có khả năng ảnh hưởng nguy hiểm tới các hệ thống thông tin quan trọng thì thực hiện cung cấp thông tin kịp thời cho đơn vị chuyên trách an toàn, an ninh mạng của tỉnh để phối hợp điều tra, phân tích và xử lý.

d) Thực hiện báo cáo định kỳ, báo cáo khi có sự cố xảy ra hoặc báo cáo đột xuất theo yêu cầu của các cấp có thẩm quyền.

4. Quản lý rủi ro

a) Thực hiện đánh giá rủi ro đối với các hệ thống thông tin.

b) Nội dung đánh giá rủi ro tập trung xác định các điểm yếu, mối đe dọa đối với tài sản của các hệ thống thông tin, từ đó xác định hậu quả và mức độ ảnh hưởng. Đồng thời đưa ra biện pháp để xử lý rủi ro bảo đảm cân đối giữa nguồn lực và giá trị mang lại.

5. Kết thúc vận hành, khai thác, sửa chữa, thanh lý, hủy bỏ

a) Thực hiện hủy bỏ toàn bộ thông tin, dữ liệu trên hệ thống với sự xác nhận của đơn vị chủ quản hệ thống thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin. Trong trường hợp thông tin, dữ liệu của hệ thống thông tin lưu trữ trên tài sản vật lý, đơn vị chủ quản hệ thống thông tin thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bảo đảm không có khả năng phục hồi. Với trường hợp đặc biệt không thể tiêu hủy được thông tin, dữ liệu thì sử dụng biện pháp tiêu hủy cấu trúc phần lưu trữ dữ liệu trên tài sản đó.

b) Đối với các hệ thống thông tin có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; Có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ dịch vụ sửa chữa thiết bị lưu trữ dữ liệu.

II. PHƯƠNG ÁN ỨNG PHÓ, KHẮC PHỤC SỰ CỐ AN TOÀN, AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN CỦA UBND XÃ KỲ KHANG

1. Nguyên tắc thực hiện

Phương án ứng phó, khắc phục sự cố an toàn, an ninh mạng được thực hiện theo nguyên tắc: Phát hiện hoặc tiếp nhận sự cố; xác minh, phân tích, đánh giá và phân loại sự cố; quyết định lựa chọn phương án và phối hợp các đơn vị liên quan; Ứng cứu sự cố, khôi phục hệ thống; điều phối, ứng cứu sự cố; kết thúc sự cố; khắc phục, phòng ngừa sự cố tái diễn; Hỗ trợ sau sự cố (chi tiết tại Phụ lục I).

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

a) Thực hiện đánh giá, xác định nguy cơ, sự cố an toàn, an ninh mạng trong hoạt động quản trị, vận hành các hệ thống thông tin.

b) Đơn vị, cá nhân vận hành hệ thống thông tin chủ trì, phối hợp với

chuyên trách an toàn thông tin của xã và Tổ ứng cứu sự cố của Huyện và các cơ quan, tổ chức liên quan tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài (cảnh báo sự cố: Văn bản, email, điện thoại, website, mạng xã hội...; phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá). Khi xác định được sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp.

Các loại sự cố chính, bao gồm:

- Sự cố do bị tấn công hệ thống mạng;

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

- Sự cố do lỗi của người quản trị, vận hành hệ thống;

- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn,...

c) Triển khai, lựa chọn các bước ưu tiên ứng cứu ban đầu:

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

d) Thông báo, báo cáo sự cố:

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

Thông báo sự cố tới Tổ ứng cứu sự cố của Huyện chậm nhất 03 ngày kể từ khi phát hiện sự cố; trường hợp xác định sự cố có thể vượt khả năng xử lý, tổ ứng cứu sự cố của Huyện thực hiện báo cáo ban đầu sự cố bằng văn bản về đơn vị thường trực về ứng cứu sự cố của tỉnh.

đ) Điều phối công tác ứng cứu

- Căn cứ vào tính chất sự cố, đề nghị hỗ trợ của Bộ phận vận hành hệ thống thông tin, bộ phận chuyên trách về an toàn thông tin thực hiện công tác điều phối, giám sát cơ chế phối hợp, chia sẻ thông tin theo phạm vi, chức năng, nhiệm vụ của mình để huy động nguồn lực ứng cứu sự cố.

- Trường hợp sự cố vượt quá khả năng ứng cứu của UBND xã thì thực hiện báo cáo về phòng Tổ ứng cứu của Huyện và Trung tâm CNTT và Truyền thông tỉnh Hà Tĩnh (đơn vị chuyên trách về an toàn thông tin của Sở Thông tin và Truyền thông) để đề nghị điều phối ứng cứu sự cố.

3. Triển khai ứng cứu, ngăn chặn sự cố

Đơn vị, cá nhân vận hành hệ thống phối hợp với chuyên trách an toàn

thông tin của xã 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:

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

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

+ Thông tin về đầu mối liên hệ;

+ Thu thập thông tin hệ thống;

+ Thu thập chức năng của hệ thống;

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

+ Thu thập chứng cứ;

+ Thu thập bộ nhớ;

+ Thu thập trạng thái network và các kết nối;

+ Thu thập các tiến trình đang chạy;

+ Thu thập hard drive media;

+ Thu thập log file;

+ Thu thập các cổng đang mở của hệ thống.

b) 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

4. Xử lý sự cố, gỡ bỏ và khôi phục

a) Xử lý sự cố, gỡ bỏ

Sau khi đã triển khai ngăn chặn sự cố, bộ phận vận hành hệ thống thông tin, tổ ứng cứu sự cố và các cá nhân có liên quan triển khai tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.

b) Khôi phục

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

c) Kiểm tra, đánh giá hệ thống thông tin

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

5. Tổng kết, đánh giá

a) Tổng kết, đúc rút kinh nghiệm:

Bộ phận vận hành hệ thống thông tin bị sự cố phối hợp với chuyên trách an toàn thông tin tại xã 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 huyện và 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 tương tự trong tương lai...

b) Xây dựng báo cáo kết thúc ứng phó sự cố:

Bộ phận vận hành hệ thống thông tin bị sự cố, chuyên trách an toàn thông tin cấp xã triển khai tổng hợp và xây dựng báo cáo kết thúc ứng phó sự cố, trong đó trình bày chi tiết quá trình xử lý sự cố, tóm tắt tổng quát về tình hình sự cố và đề xuất cách thức triển khai điều phối, ứng cứu sự cố nhằm xử lý nhanh, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự.

Sau khi kết thúc ứng cưu sự cố, trong vòng 10 ngày chuyên trách về an toàn thông tin của xã phải xây dựng báo cáo kết thúc ứng phó sự cố, gửi về cơ quan chuyên trách về an toàn thông tin khi có yêu cầu.

Phụ lục 1:QUY TRÌNH ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Thành phần	Quy trình	Ghi chú
Bộ phận vận hành hệ thống thông tin (HTTT)	Phát hiện, tiếp nhận thông báo sự cố	Thông tin sự cố có thể từ các nguồn: -Hệ thống theo dõi nội bộ -Đơn vị thường trực về ƯCSC -Thông tin mạng lưới -Nguồn tin xã hội
Bộ phận vận hành hệ thống thông tin , Cán bộ quản trị mạng	Phân tích, xác minh sự cố Phản hồi, kết thúc	Doanh nghiệp cung cấp viễn thông, ISP; thành viên mạng lưới; Trung tâm CNTT và Truyền thông hỗ trợ
- Bộ phận vận hành HTTT, cán bộ Quản trị mạng triển khai các bước ứng cứu ban đầu; báo cáo sự cố - Đội ứng cứu sự cố của Huyện chỉ đạo điều phối ứng cứu sự cố	Triển khai các bước ưu tiên ứng cứu ban đầu Lựa chọn phương án Điều phối chỉ đạo công tác ứng cứu Điều phối chỉ đạo công tác ứng cứu	Triển khai theo phương án đối phó, ứng cứu một số tình huống sự cố cụ thể hoặc theo hướng dẫn của đơn vị có chức năng đảm bảo ATTT
-Bộ phận vận hành HTTT, cán bộ Quản trị mạng, 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 -Chuyên trách về an toàn thông tin phối hợp với tổ ứng cứu của huyện trong công tác ứng cứu sự cố an toàn thông tin mạng của xã.	Triển khai các bước ưu tiên ứng cứu ban đầu Triển khai các bước ưu tiên ứng cứu ban đầu Triển khai các bước ưu tiên ứng cứu ban đầu Khôi phục hoạt động Kiểm tra, đánh giá	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 phục hoạt động của hệ thống thông tin trở lại bình thường
Bộ phận vận hành HTTT; cán bộ quản trị mạng; Tổ ứng cứu sự cố an toàn thông tin mạng của Huyện	Tổng kết, đánh giá	

Phụ lục 2:
PHƯƠNG ÁN ĐỐI PHÓ, ỨNG CỨU MỘT SỐ TÌNH HUỐNG CỤ THỂ

1. Sự cố gây rò rỉ dữ liệu

Bước	Nội dung tham khảo thực hiện
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.
Xử lý ưu tiên, ban đầu	- Bộ phận vận hành hệ thống cùng với đơn vị vận hành báo cáo lãnh đạo và liên hệ Tổ Ứng cứu sự cố an toàn thông tin mạng của đơn vị Huyện - 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
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, 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 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

Bước	Nội dung tham khảo thực hiện
Dấu hiệu	Trang thông tin điện tử của cơ quan, đơn vị bị thay đổi trái phép nội dung toàn bộ hoặc một phần.
Xử lý ưu tiên, ban đầu	- Triệu tập Tổ Ứng cứu sự cố an toàn thông tin mạng - 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.
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 thông tin điện tử của Sở 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.

3. Tấn công mã độc

Bước	Nội dung tham khảo thực hiện
Dấu hiệu	Hệ thống thông tin/máy tính trong cơ quan, đơn vị bị tấn công bởi cácdạng mã độc khác nhau.
Xử lý ưu tiên, ban đầu	- Triệu tập Tổ Ứng cứu sự cố an toàn thông tin mạng - 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.
Cô lập hệ thống	- Thực hiện cô lập hệ thống bị tấn công để tránh bị thay đổi hiện trườngvà 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 hoặc máy trạm bị lây nhiễm* *+ Tiến trình của mã độc* *+ File của mã độc* *+ Thành phần đăng ký khởi động 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 bảo mật tại đơn vị như: 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.