TRUNG TÂM Y TẾ MỸ HÀO

KỊCH BẢN
PHÒNG NGỪA KHẮC PHỤC SỰ CỐ HỆ THỐNG

TRUNG TÂM Y TẾ MỸ HÀO

KỊCH BẢN
PHÒNG NGỪA KHÁC PHỤC SỰ CỐ HỆ THỐNG

	Người lập	Người xem xét	Người phê duyệt
Họ tên	**Phạm Việt Đức**	**Lê Thị Mai**	**Bùi Quang Trọng**
Ký tên	Đức		
Chức vụ	Nhân viên CNTT	Trưởng phòng Kế hoạch - Nghiệp vụ - Điều dưỡng	Giám đốc
Ngày	18/8/2025	18/8/2025	18/8/2025

Số: 37../QĐ-TTYT Ngày ban hành: 18/8/2025

Đường Hào, tháng 8/2025

KỊCH BẢN PHÒNG NGỪA KHẮC PHỤC SỰ CỐ HỆ THỐNG CÔNG NGHỆ THÔNG TIN TẠI TRUNG TÂM Y TẾ MỸ HÀO

1. MỤC ĐÍCH, YÊU CẦU

1.1. Mục đích

Bảo đảm an toàn thông tin mạng của Trung tâm Y tế Mỹ Hào, trong đó tập trung an toàn thông tin cho các hệ thống thông tin quan trọng của trung tâm, có khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin mạng. Đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

Nâng cao năng lực, hiệu quả hoạt động của Tổ Công nghệ thông tin ứng cứu sự cố an toàn thông tin mạng, nội bộ, gắn kết với các đơn vị cung cấp phần mềm, hợp tác, kết nối chặt chẽ, điều phối kịp thời, phối hợp đồng bộ, hiệu quả của các lực lượng để ứng cứu sự cố mạng, chống tấn công mạng.

Bảo đảm các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng cứu sự cố bảo đảm an toàn thông tin mạng.

1.2 Yêu cầu

- Phải khảo sát, đánh giá các nguy cơ, sự cố an toàn thông tin mạng của hệ thống thông tin đưa ra phương án đối phó, ứng cứu sự cố phù hợp, kịp thời

- Phương án đối phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra.

2. NHIỆM VỤ TRIỂN KHAI

2.1. Đánh giá các nguy cơ, sự cố an toàn thông tin mạng:

Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá; dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (*bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có*).

2.2 . Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

Đối với mỗi hệ thống thông tin cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được các tiêu chí để có thể nhanh chóng xác đinh được tính chất, mức độ nghiệm trọng của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung sau:

2.2.1. Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp.

- Sự cố do bị tấn công mạng;

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

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

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

2.2.2. Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tình huống sau:

STT	Tình huống	Cách phòng ngừa
I. Tình huống sự cố do bị tấn công mạng		
1	***Tấn công từ chối dịch vụ:*** Là một loại hình tấn công nhằm ngăn chặn những người dùng hợp lệ được sử dụng một dịch vụ nào đó, Các cuộc tấn công có thể đươc thực hiện nhằm vào bất kì một thiết bị mạng nào bao gồm là tấn công vào các thiết bị định tuyến, web, thư điện tử và hệ thống DNS, …	- Cài đặt và duy trì phần mềm chống virus. - Cài đặt tường lửa và cấu hình nó để giới hạn lưu lượng đến và đi từ máy tính của bạn. - Làm theo các hướng dẫn thực hành an toàn về phân phối địa chỉ email. - Dùng các bộ lọc email để giúp bạn quản lý lưu lượng không mong muốn. - Nâng cao ý thức của người sử dụng khi tham gia vào hệ thông thông tin trung tâm. - Ban hành quy chế đảm bảo an toàn an ninh thông tin trong toàn trung tâm.
2	***Tấn công giả mạo:*** Là một hành vi giả mạo các ý nhằm lấy được các thông tin nhạy cảm như tên người dùng, mật khẩu và các chi tiết thẻ tín dụng bằng cách giả dạng thành một chủ thể tin cậy trong một giao dịch điện tử. Các giao dịch thường dùng để đánh lừa những người ít dùng ít đa nghi là các giao dịch có vẻ xuất phát từ các	- Tập huấn, tuyên truyền nâng cao nhận thức về công nghệ thông tin cho cán bộ nhân viên trung tâm về phát hiện các tình huống giả mạo. - Triển khải một bộ lọc SPAM để phát hiện virus, người gửi trống cho toàn bộ hệ thống mail cũng như các hệ thống công nghệ thông tin của trung tâm. - Giữ tất cả các hệ thống hiện tại với các bản vá lỗi bảo mật và cập nhật mới nhất. Cài đặt một giải pháp chống virus, lên

STT	Tình huống	Cách phòng ngừa
	website xã hội phổ biến, các trung tâm chi trả trực tuyến hoặc các quản trị mạng.	lịch cập nhật chữ ký, và theo dõi trạng thái chống virus trên tất cả các thiết bị. - Thực hiện chế độ mã hóa tất cả thông tin nhạy cảm, quan trọng của trung tâm để lưu trữ an toàn.
3	***Tấn công sử dụng mã độc:*** Một khái niệm chung dùng để chỉ các phần mềm độc hại được viết với mục đích có thể lây lan phát tán (hoặc không lây lan, phát tán) trên hệ thống máy tính và internet, nhằm thực hiện các hành vi bất hợp pháp nhằm vào người dùng cá nhân, cơ quan, tổ chức. Thực hiện các hành vi chuộc lợi cá nhân, kinh tế, chính trị hoặc đơn giản là để thỏa mãn ý tưởng và sở thích của người viết.	- Luôn luôn cài đặt, cập nhật và sử dụng một phần mềm diệt virus có bản quyền để bảo vệ các máy tính. - Xây dựng chính sách với các thiết bị PnP. - Thiết lập quy tắc đối xử với các file. - Truy cập web an toàn. - Cập nhật máy tính, phần mềm. - Thành lập tổ chức xử lý các sự cố về công nghệ thông tin để kịp thời phối hợp xử lý khi phát hiện mã độc.
4	***Tấn công truy cập trái phép, chiếm quyền điều khiển***: Truy cập vào dữ liệu, chiếm đoạt quyền truy cập và leo theo đặc quyền.	- Với kiểu tấn công vào mật khẩu: Đặt mật khẩu mạnh. Không sử dụng mật khẩu ở dạng bản rõ cả khi lưu trữ hoặc truyền trên mạng. Trong các khuyến nghị về chính sách an ninh mạng, đều yêu cầu phải ghi lại nhật ký hệ thống. Bằng cách xem xét các bản ghi nhật ký, admin có thể biết được các thông tin và số lần truy cập không thành công. Nếu phát hiện từ một địa chỉ IP có số lần truy cập không thành công vượt quá giới hạn cho phép thì đây rất có thể là do tấn công vào mật khẩu. Ví dụ về việc phân tích nhật ký hệ thống, để phát hiện tấn công mật khẩu. Để xử lý, admin cần cấu hình giới hạn về số lần đăng nhập, ví dụ trong bài viết này. - Với kiểu tấn công lợi dụng sự tin cây, admin cần giảm thiểu việc cấu hình trust giữa các hệ thống, Ví dụ, khi bạn dùng trình duyệt IE trên máy chủ windows

STT	Tình huống	Cách phòng ngừa
		Server, mỗi khi bạn vào một website thì IE đều hỏi bạn xem có trust cái site đó không. - Với kiểu tấn công MITM: vì kẻ đứng giữa cần nhân bản dữ liệu mà hắn chặn bắt, do vậy sẽ tiêu tốn nhiều băng thông. Admin cần có công cụ giám sát băng thông để phát hiện ra việc này. Ví dụ về các phần mềm giám sát hoặc phần mềm giám sát băng thông. - Với kiểu tấn công tràn bộ đệm, bạn cần có công cụ giám sát trạng thái của các tiến trình đang chạy trong hệ thống, ví dụ 2 công cụ Event Viewer kết hợp với Performance Monitor trên Windows.
5	Tấn công thay đổi giao diện.	- Xem những thông tin nhật ký, file log của máy chủ và truy tìm xem, hacker đã làm gì và làm như thế nào trên hệ thống của mình.
6	Tấn công mã hóa phần mềm, dữ liệu, thiết bị.	- Cài đặt và duy trì phần mềm chống virus. - Công cụ chống phần mềm độc hại.
7	Tấn công phá hoại thông tin, dữ liệu, phần mềm.	- Cài đặt và duy trì phần mềm chống virus. - Công cụ chống phần mềm độc hại.
8	Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu. Tấn công tổng hợp sử dụng kết hợp nhiều hình thức.	- Cập nhật máy tính, phần mềm. - Cài đặt và duy trì phần mềm chống virus trên các máy tính. - Công cụ chống phần mềm độc hại.
II. Tình huống sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật		
1	Sự cố nguồn điện.	- Sử dụng bộ lưu điện UPS. - Sử dụng nguồn điện dự phòng.
2	Sự cố đường kết nối Internet.	- Sử dụng nhiều đường kết nối internet của nhiều nhà cung cấp dịch vụ.

STT	Tình huống	Cách phòng ngừa
3	Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin.	- Sao lưu hệ thống hằng ngày. - Lưu trữ dự phòng ở nhiều nơi.
4	Sự cố liên quan đến quá tải hệ thống.	- Kiểm tra hệ thống thường xuyên. - Nâng cấp hệ thống để phù hợp với từng giai đoạn của trung tâm.
III. Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống		
1	Lỗi trong cập nhật, thay đổi, cấu hình phần cứng. Lỗi trong cập nhật, thay đổi, cấu hình phần mềm. Lỗi liên quan đến chính sách và thủ tục an toàn thông tin. Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc. Lỗi khách liên quan đến người quản trị, vận hành hệ thống.	- Backup dự phòng trước khi cập nhật, thay đổi cấu trúc hệ thống.
IV. Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn, ...		
1	Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn, …	Trung tâm thuê hệ thống lưu trữ dự phòng tại các trung tâm dữ liệu đạt tiêu chuẩn do Bộ TTTT công bố để lưu các bản sao dữ liệu.