Kế hoạch ứng phó sự cố ATTTM

Dự án: **Australian Government Cyber Security Training Development Program for Vietnam - Chương trình Phát triển Năng lực An toàn thông tin Việt Nam của Chính phủ Úc**

Tháng 1/2025

Liên hệ chính

Các bên liên quan chính			
Tên	**Chi tiết liên hệ**	**Chức danh**	**Trách nhiệm UCSC**
[Tên]	Điện thoại di động: Email: Vị trí:		

Bộ Thông tin và Truyền thông			
Tên	**Chi tiết liên hệ**	**Chức danh**	**Trách nhiệm UCSC**
[Tên]	Điện thoại di động: E-mail: Vị trí:		

Các bên liên quan bên ngoài			
Tên	**Chi tiết liên hệ**	**Chức danh**	**Trách nhiệm UCSC**
[Tên]	Điện thoại di động: E-mail: Vị trí:		

Nội dung

Danh mục các bảng

Danh mục các hình

1 Giới thiệu

1.1 Mục đích

Kế hoạch ứng phó sự cố ATTTM (Cyber Security Incident Response Plan - CSIRP) này hướng dẫn tổ chức ứng phó các sự cố ATTTM (sau đây gọi tắt là ATTTM). Quy trình sẽ xác định vai trò và trách nhiệm của những bên tham gia, phân loại các sự cố an toàn thông tin, các giai đoạn ứng phó sự cố và các yêu cầu báo cáo, hỗ trợ quản lý hiệu quả nhằm giảm mức độ nghiêm trọng, phạm vi và tác động của sự cố.

Tài liệu này được sử dụng khi có một hoặc một số các xảy ra bên dưới:

- Có nghi ngờ truy cập trái phép vào dữ liệu nhạy cảm.
- Lộ lọt dữ liệu đã được xác nhận.
- Tài sản vật lý hoặc kỹ thuật số bị mất/đánh cắp.
- Một sự cố an toàn thông tin đã được xác nhận bởi một nhà cung cấp dịch vụ.
- Phần mềm độc hại đã lây nhiễm vào mạng hoặc hệ thống.
- Hoạt động đáng ngờ hoặc có bất thường đã được phát hiện.
- Nhân viên báo cáo hoạt động đáng ngờ hoặc họ đã vô tình thực hiện hành động cần điều tra thêm.

1.2 Phạm vi

Kế hoạch này áp dụng cho hoạt động ứng phó và quản lý các sự cố ATTTM, liên quan đến hệ thống thông tin, dữ liệu và mạng; phù hợp để sử dụng cho tất cả các sự cố ATTTM. Tuy nhiên, nó không bao gồm các hoạt động ứng cứu sự cố kỹ thuật hoặc kịch bản cụ thể và không thay thế Quy trình ứng cứu sự cố đã được ban hành.

Sự cố ATTTM đề cập đến việc vi phạm chính sách bảo mật thông tin, chính sách sử dụng hoặc các biện pháp thực hành ATTTM theo tiêu chuẩn.

Kế hoạch không nhằm mục đích:

- Thay thế các tài liệu quản lý ứng cứu sự cố hiện có không liên quan đến mạng.
- Dùng để ứng cứu các sự cố ATTTM của tổ chức khác.

1.3 Đối tượng

Kế hoạch này dành cho các đối tượng sau:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC).
- Thành viên Mạng lưới ứng cứu sự cố ATTTM quốc gia.
- Các tổ chức, doanh nghiệp trong nước có nhu cầu tham khảo, áp dụng.

1.4 Thẩm quyền & Đánh giá

Tài liệu này sẽ được xem xét hàng năm hoặc mỗi khi có bất kỳ thay đổi lớn nào khác, bao gồm sự cố ATTTM nghiêm trọng hoặc những thay đổi quan trọng liên quan đến pháp lý.

1.5 Các tiêu chuẩn và khung tham chiếu

Các tiêu chuẩn và khuôn khổ sau đây đã được xem xét trong quá trình xây dựng tài liệu này:

- Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST): **Hướng dẫn Xử lý Sự cố Bảo mật Máy tính - Computer Security Incident Handling Guide**, tham khảo chi tiết tại https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- Trung tâm An ninh mạng Úc: **Hướng dẫn và Mẫu Kế hoạch Ứng cứu sự cố ATTTM - Cyber Incident Response Plan Guidance and Template**, tham khảo chi tiết tại https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-incident-response-plan
- Bộ Thông tin và Truyền thông Việt Nam: **Thông tư 20/2018/TT-BTTTT ngày 12?9/2017 Quy định về điều phối, ứng cứu sự cố ATTTM trên toàn quốc,** tham khảo chi tiết tại https://mic.mediacdn.vn/Upload/VanBan/20-2017-ttsigned.pdf

1.6 Sự cố ATTTM là gì?

Sự cố ATTTM là một sự kiện bất lợi xảy ra khi có hành vi xâm phạm vào hệ thống, vi phạm các chính sách bảo mật đã đặt ra và cần có hành động khắc phục. Sự cố ATTTM tiềm ẩn nhiều rủi ro nghiêm trọng, có thể gây tổn hại đến tính bảo mật, tính khả dụng và tính toàn vẹn của hệ thống thông tin.

Tham khảo Phụ lục A – Các loại sự cố ATTTM để biết thêm thông tin chi tiết

1.7 Các kiểu Tấn công phổ biến

Các kiểu tấn công là những con đường, phương thức hoặc kịch bản mà tin tặc có thể lợi dụng để thực hiện các cuộc tấn công ATTTM. Việc xác định được điểm vào hoặc lỗ hổng sẽ giúp chúng ta hiểu rõ hơn về các điểm yếu trong hệ thống và từ đó đưa ra các biện pháp bảo vệ hiệu quả.

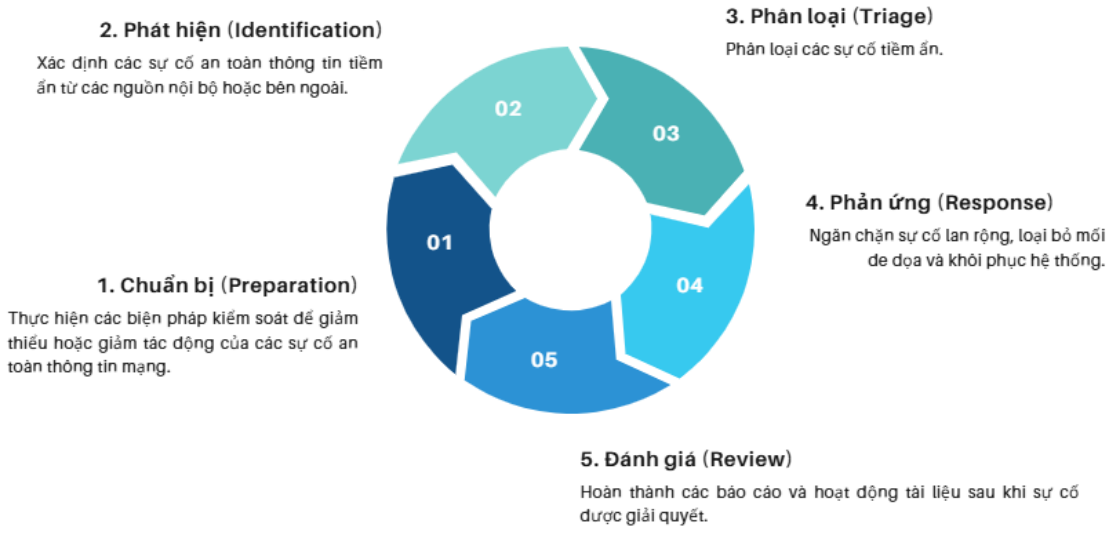
Tham khảo **Phụ lục B - Các kiểu tấn công phổ biến** để biết thêm thông tin chi tiết.

2 Tổng quan về ứng phó sự cố ATTTM

2.1 Tổng quan về Kế hoạch ứng phó sự cố ATTTM

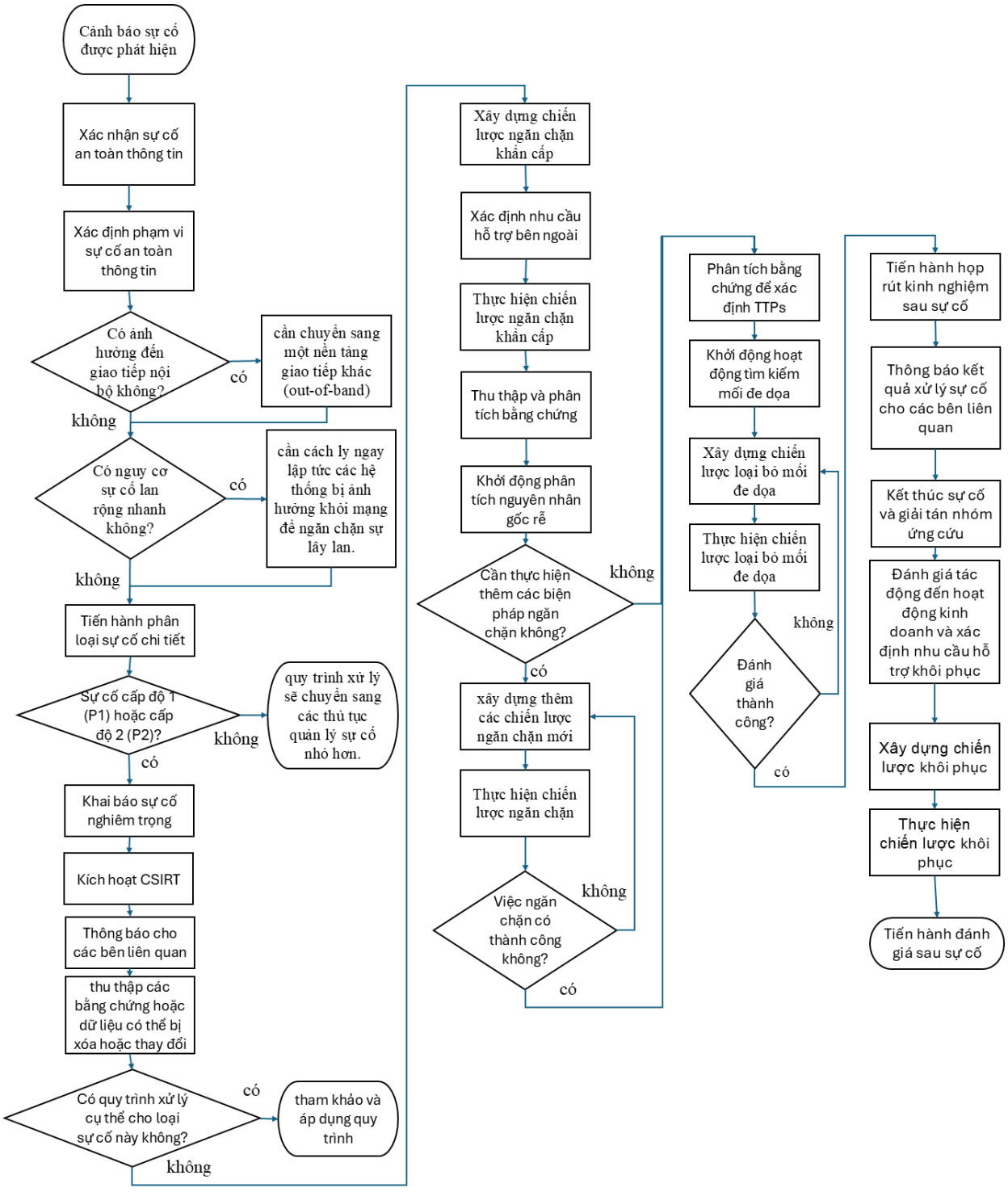
Vòng đời của Kế hoạch ứng phó sự cố ATTTM xác định các giai đoạn, công việc cần thiết để ứng phó với sự cố ATTTM. Các giai đoạn trong vòng đời được nêu trong Hình 1.

Việc hiểu rõ các giai đoạn trong vòng đời, bao gồm giai đoạn hiện tại là gì và giai đoạn nào trong tương lai, sẽ mang lại cách tiếp cận sáng suốt để ứng cứu với sự cố ATTTM.



Hình 1: Vòng đời Kế hoạch ứng phó sự cố ATTTM

2.2 Lưu đồ Kế hoạch ứng phó sự cố ATTTM



Hình 2: Lưu đồ Kế hoạch ứng phó sự cố ATTTM

3 Xếp loại

Trong ứng cứu sự cố ATTTM, phân loại (triage) là quá trình bao gồm việc xác định, phân loại và xếp mức ưu tiên ứng phó của sự cố. Việc xếp loại giúp các đội ứng cứu sự cố có hướng dẫn rõ ràng về cách thức và thời điểm cần thực hiện các hành động xử lý, đồng thời giúp các bên liên quan hiểu rõ mức độ nghiêm trọng của từng sự cố.

Quá trình xếploại dựa trên việc đánh giá tác động của sự cố đối với 6 yếu tố chính (xem Bảng 1) và phân sự cố từ cấp ưu tiên 4 (P4) - Sự cố nhỏ đến 1 (P1) - Sự cố thảm khốc (xem Bảng 2).

Yếu tố pháp lý	Yếu tố hoạt động	Yếu tố tài chính	Yếu tố Sức khỏe & An toàn	Yếu tố danh tiếng	Yếu tố CNTT & Mạng

Bảng 1: Phân loại yếu tố đánh giá

Sự cố nhỏ P4	Sự cố vừa phải P3	Sự cố lớn P2	Sự cố thảm khốc P1

Bảng 2: Bảng ưu tiên sự cố

Tham khảo Hành động 3 (A3) để biết hướng dẫn về cách thực hiện phân loại ứng cứu sự cố ATTTM.

4 Vai trò & Trách nhiệm

4.1 Đầu mối liên hệ để báo cáo sự cố ATTTM

Bảng dưới đây cung cấp danh sách các bên có thể liên quan đến việc báo cáo các sự cố ATTTM.

Tên	Chi tiết liên hệ	Cách liên lạc riêng	Chức vụ	Trách nhiệm
Đội ứng cứu sự cố …	<Nhập chi tiết liên hệ>	<Nhập chi tiết liên hệ>	<Nhập chi tiết>	<Nhập chi tiết>
Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam	<Nhập chi tiết liên hệ>	<Nhập chi tiết liên hệ>	<Nhập chi tiết>	<Nhập chi tiết>
<Nhập chi tiết liên hệ>				
<Nhập chi tiết liên hệ>				

Bảng 3: Các đầu mối liên hệ

KIẾN NGHỊ

Đầu mối liên hệ để báo cáo sự cố ATTTM phải bao gồm các bên liên quan chính bên trong và bên ngoài của tổ chức, những người sẽ cần tham gia vào trường hợp xảy ra sự cố ATTTM. Điều này nghĩa sẽ bao gồm quản lý cấp cao, nhân viên kỹ thuật, nhóm pháp lý, nhóm truyền thông và các bên liên quan quan trọng khác.

4.2 Ma trận RACI

Ma trận phân công trách nhiệm RACI (Responsibility Assignment Matrix) giúp xác định rõ ràng và minh bạch vai trò của từng cá nhân (hoặc vai trò) về người thực hiện trách nhiệm R (responsible), người chịu trách nhiệm chính A (accountable), người được tham khảo ý kiến C (consulted) hoặc người được thông báo I (informed). Ma trận này nâng cao hiệu suất làm việc thông qua việc trực quan hóa sự phân công công việc, quyền hạn và quy trình, giảm thiểu nguy cơ hiểu lầm hoặc không chắc chắn. Ma trận nên bao gồm tất cả các bên liên quan, đảm bảo sự rõ ràng giữa các bên liên quan nội bộ hoặc bên ngoài.

Tham khảo Error! Reference source not found. để biết thêm thông tin.

KIẾN NGHỊ

Ma trận RACI phải được phát triển, thống nhất và thử nghiệm nội bộ trước khi sử dụng trong sự cố ATTTM.

5 Báo cáo và xử lý bằng chứng

5.1 Báo cáo sự cố cho VNCERT/CC

Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC) chịu trách nhiệm điều phối và ứng cứu các sự cố ATTTM trên toàn quốc. VNCERT/CC có thể cung cấp lời khuyên,hỗ trợ chuyên môn thích hợp và có các nguồn lực có thể hỗ trợ ứng cứu sự cố ATTTM.

Nên tham khảo ý kiến của VNCERT/CC đối với các sự cố được phân loại từ P2 đến P1.

Xem **Phụ lục D - Báo cáo cho VNCERT/CC** để biết hướng dẫn về cách báo cáo cho VNCERT/CC.

5.2 Xử lý bằng chứng

Mặc dù việc thu thập bằng chứng trong một sự cố ATTTM nhằm mục đích chính để giải quyết sự cố, nhưng có thể cần sử dụng bằng chứng đó trong các thủ tục pháp lý về sau. Do đó, việc xử lý bằng chứng phải là một xem xét quan trọng trong suốt quá trình ứng cứu sự cố ATTTM.

Kế hoạch xử lý bằng chứng phải được phát triển, xem xét các yếu tố như giá trị của bằng chứng, tính biến động của bằng chứng và mức độ nỗ lực cần thiết để đạt được sự đồng thuận có căn cứ về những bằng chứng nào phải được thu thập.

Trong suốt tiến trình ứng phó sự cố, việc quan trọng là phải ghi chép rõ ràng cách thức bảo quản tất cả các bằng chứng, bao gồm cả các hệ thống bị xâm phạm. Tất cả các bằng chứng thu thập được phải

tuân thủ các quy trình chuỗi bảo quản có liên quan, có nghĩa là phải luôn được xác định rõ ràng; và bất cứ khi nào bằng chứng được chuyển giao từ người này sang người khác, các biểu mẫu chuỗi bảo quản, có trong **Phụ lục E -** Error! Reference source not found., phải chi tiết hóa việc chuyển giao và bao gồm chữ ký của mỗi bên.

Các ví dụ về bằng chứng có thể được thu thập:

- Các ảnh ổ cứng và các ảnh nguyên thuỷ.
- Các ảnh RAM.
- Các địa chỉ IP.
- Bắt và lưu chuyển gói mạng.
- Các sơ đồ mạng.
- Liên lạc với (các) kẻ tấn công.
- Các ghi chú điều tra.
- Các ảnh chụp màn hình.
- Các báo cáo và các cuộc họp.
- Tác động tài chính, vật lý và kinh doanh.
- Các tệp nhật ký và cấu hình.
- Phát hiện từ tình báo nguồn mở.

Bằng chứng phải được bảo vệ an toàn và quyền truy cập vào nó nên bị hạn chế đối với nhân viên được ủy quyền.

Tham khảo tài liệu *NIST SP 80-0-86 Hướng dẫn Tích hợp Kỹ thuật Điều tra vào Ứng phó sự cố - Guide to Integrating Forensic Techniques into Incident Response* để biết thêm hướng dẫn về thu thập và xử lý bằng chứng.

5.3 Bảo quản bằng chứng

Việc bảo quản và lưu giữ bằng chứng là quan trọng vì sau này nó có thể được yêu cầu cho việc thực thi pháp luật, thủ tục pháp lý và/hoặc các cuộc điều tra khác. Khi bắt đầu quá trình ứng phó sự cố ATTTM, cần có một nhân viên chịu trách nhiệm bảo quản bằng chứng.

Đơn vị phải xem xét và tuân thủ các quy định pháp luật và quy định có liên quan về việc bảo quản bằng chứng.

6 Hỗ trợ của bên thứ ba

6.1 Dịch vụ ứng cứu sự cố chuyên biệt

Các dịch vụ của bên thứ ba, như từ doanh nghiệp chuyên về an toàn an ninh mạng có thể cung cấp các dịch vụ để hỗ trợ quá trình ứng cứu sự cố.

Xem bảng bên dưới về liên hệ của bên thứ ba được đề xuất.

Nhà cung cấp	Dịch vụ	Liên hệ	Chi tiết
Ví dụ: Doanh nghiệp điều tra số và ứng phó sự cố	- Điều tra số - Ứng phó sự cố ATTTM	Điện thoại: <Nhập thông tin> Email: <Nhập thông tin> Di động: <Nhập thông tin>	<Nhập thông tin>
<Nhập thông tin>			

Bảng 4: Liên hệ hỗ trợ của bên thứ ba

KIẾN NGHỊ

Các dịch vụ hỗ trợ tiềm năng của bên thứ ba phải được tổ chức và thiết lập trước khi chúng được yêu cầu trong trường hợp khẩn cấp.

Phê duyệt việc sử dụng của bên thứ ba nên được sắp xếp càng sớm càng tốt, tránh phải thực hiện các quy trình phê duyệt trong tình huống khẩn cấp.

7 Giao tiếp

7.1 Liên lạc kênh riêng

Liên lạc kênh riêng là một phương thức giao tiếp diễn ra bên ngoài các kênh liên lạc thông thường trong doanh nghiệp. Đây là một kênh liên lạc biệt lập thường bao gồm:

- Mã hóa đầu cuối.
- Email không liên quan đến công việc (hoặc được kết nối).
- Chia sẻ tập tin được mã hóa.

Trong sự cố ATTTM, kẻ tấn công có thể đã truy cập rộng khắp vào hệ thống, mạng hoặc các tài khoản doanh nghiệp. Quyền truy cập và/hoặc kiểm soát này có thể xâm phạm đến tính bảo mật của liên lạc trong nội bộ và bên ngoài, nhất là email và các hệ thống khác của tổ chức được sử dụng để liên lạc nội bộ (chẳng hạn như Microsoft Teams).

Trong tình huống như vậy, nên xem xét liên lạc kênh riêng để ngăn chặn các kẻ tấn công có thể nhìn thấy được thông tin liên lạc trong nội bộ và bên ngoài. Trong một số trường hợp, việc không chuyển sang liên lạc kênh riêng có thể cung cấp cho kẻ tấn công thông tin liên quan đến sự cố, cho phép họ duy trì và/hoặc tăng quyền truy cập và/hoặc kiểm soát.

Kênh liên lạc riêng phải được sắp xếp trước và dựa trên nền tảng nhắn tin an toàn mà các bên liên quan chính sẽ có quyền truy cập kịp thời.

Việc lựa chọn nền tảng liên lạc riêng cần xem xét:

- Các bên liên quan có thể dễ dàng truy cập.
- Tách biệt với các kênh liên lạc chuẩn.
- Bảo mật của nền tảng.
- Dễ sử dụng cho các bên liên quan.

Sau khi lựa chọn phương thức liên lạc riêng, cần sắp xếp thành viên/quyền truy cập, đảm bảo các bên liên quan chính hiểu cách thức và thời điểm sử dụng nền tảng. Quyền truy cập và thành viên phải được cập nhật thường xuyên để đảm bảo thành viên là chính xác.

KIẾN NGHỊ

Kênh liên lạc riêng với các thành viên và các phương pháp sử dụng phải được sắp xếp trước. Có thể không thể thiết lập các kênh thay thế một cách an toàn khi sự cố đã xảy ra (hoặc đang diễn ra).

7.2 Chia sẻ tệp an toàn

Trong trường hợp xảy ra sự cố ATTTM, cùng với việc sử dụng kênh liên lạc riêng, cần thiết phải sử dụng tính năng chia sẻ tệp an toàn.

Chia sẻ tệp an toàn có thể liên quan đến việc sử dụng phần mềm của bên thứ ba cung cấp các giao thức và mã hóa bảo mật nâng cao để bảo vệ dữ liệu trong quá trình truyền.

KIẾN NGHỊ

Các phương pháp chia sẻ tệp an toàn nên được sắp xếp trước. Có thể không thiết lập được việc chia sẻ tệp an toàn khi sự cố đã xảy ra (hoặc đang diễn ra).

7.3 Đầu vào giao tiếp

Trong suốt vòng đời của sự cố ATTTM, thông tin sự cố phải được truyền đạt thường xuyên tới các bên liên quan chính bên trong và bên ngoài.

Tham khảo **Phụ lục F - Hướng dẫn giao tiếp** để biết them chi tiết.

8 Chuẩn bị

8.1 Đào tạo & Nhận thức

Đào tạo thường xuyên đóng vai trò quan trọng trong việc đảm bảo sẵn sàng của tổ chức nhằm phản ứng hiệu quả với các sự cố ATTTM. Các chương trình đào tạo trang bị cho nhân viên những kỹ năng và kiến thức cần thiết để xác định, ngăn chặn và giảm thiểu các mối đe dọa ATTTM. Đồng thời, việc nâng cao nhận thức của nhân viên về tầm quan trọng của ATTTM sẽ giúp tang cường khả năng nhận biết và báo cáo kịp thời các nguy cơ, góp phần xây dựng khuôn khổ ứng phó sự cố mạnh mẽ và chủ động hơn.

8.2 Kiểm tra Kế hoạch ứng phó sự cố ATTTM

Các hoạt động diễn tập ứng cứu sự cố ATTTM nên diễn ra hàng năm để đảm bảo kế hoạch và quy trình ứng cứu sự cố là phù hợp và khả thi. Việc kiểm tra cũng nhằm đảm bảo rằng nhân viên có liên quan hiểu được trách nhiệm của họ trong việc ứng phó khi xảy ra sự cố ATTTM và có kinh nghiệm thực hiện việc đó.

8.3 Duy trì và xem xét Kế hoạch ứng phó sự cố ATTTM

Việc duy trì và xem xét kế hoạch phải diễn ra hai năm một lần hoặc mỗi khi có sự tham gia của tổ chức/nhân sự quan trọng có thể ảnh hưởng đến khả năng và quy trình ứng cứu sự cố. Quy trình cũng có thể được cập nhật sau mỗi lần ứng phó sự cố hoặc có những thay đổi hữu ích sau ứng phó sự cố.

Phần ứng phó sự cố

Hướng dẫn tham khảo:

Liên hệ chính:

Tên	Chi tiết liên hệ	Liên hệ kênh riêng	Chức vụ
<Nhập chi tiết liên hệ>	Điện thoại: <Nhập thông tin> E-mail:<Nhập thông tin>	<Nhập thông tin>	:<Nhập thông tin>
<Nhập chi tiết liên hệ>			
<Nhập chi tiết liên hệ>			

Bảng 5: Liên hệ chính

9 Danh sách kiểm tra ứng cứu sự cố tổng hợp

Danh sách kiểm tra sau đây được thiết kế để đơn giản hóa việc quản lý ứng cứu sự cố và đảm bảo các hành động được thực hiện bởi các bên chịu trách nhiệm. Lưu ý rằng đây không phải là một quy trình tuyến tính, các bước có thể được thực hiện song song. Vui lòng tham khảo quy trình ứng cứu sự cố để biết hướng dẫn mang tính thủ tục.

	STT	Nhiệm vụ	Mô tả	Trạng thái
Phát hiện & Phân tích	A1	Xác nhận phát hiện sự cố ATTTM	Sau khi báo cáo hoặc nghi ngờ về một sự cố ATTTM, các bên liên quan về ATTTM cần phải đánh giá sự cố tiềm tàng.	
	A2	Thu thập và xác nhận thông tin đã biết	Theo dõi nguồn gốc của sự cố và tiến hành nghiên cứu thích hợp để hiểu rõ hơn về tính xác thực của sự cố.	
	A3	Phạm vi sự cố ATTTM	Xác định phạm vi và quy mô của (các) sự cố ATTTM.	
	A4	Xác định loại sự cố	Xác định loại sự cố ATTTM đã xảy ra.	
	A5	(Nếu có thể) Quyền truy cập và tính toàn vẹn của bản sao lưu	Cần kiểm tra tính toàn vẹn của các bản sao lưu để xác định xem chúng có bị xâm phạm hay không và dữ liệu/thông tin được lưu trữ có đủ để phục hồi sau sự cố hay không.	
	A6	Phân loại sự cố	Việc phân loại sự cố ATTTM đảm bảo tất cả các bên liên quan hiểu được mức độ nghiêm trọng của sự cố và phản ứng cần thiết.	
	A7	Tuyên bố sự cố	Tuyên bố về sự cố ATTTM.	
	A8	Triệu tập đội UCSC	Cần phải triệu tập đội ứng cứu sự cố để ứng phó với (các) sự cố an toàn thông tin đã được xác định.	
	A9	Thông báo cho các bên liên quan chính	Truyền đạt sự cố với các bên liên quan bên ngoài.	
	A10	Thu thập bằng chứng và dữ liệu dễ biến động	Thu thập và lưu trữ bằng chứng và dữ liệu dễ mất/thay đổi để hỗ trợ các hoạt động ứng phó sự cố, cùng với các tiến trình/điều tra pháp lý có thể phải tuân theo.	
	A11	Kích hoạt sổ tay ứng phó sự cố liên quan	Các sổ tay ứng phó cụ thể về sự cố có liên quan nên được kích hoạt để hỗ trợ ứng phó sự cố.	
	A12	Điều tra sự cố ATTTM	Thu thập bằng chứng về sự cố.	
	B1	Xây dựng chiến lược ngăn chặn	Xây dựng chiến lược ngăn chặn khẩn cấp với mục tiêu cách ly các hệ thống/máy chủ/thiết bị bị ảnh hưởng hoặc giảm thiểu sự cố.	

	B2	Xác định yêu cầu cần hỗ trợ từ bên thứ ba	Xem xét và đánh giá liệu có thể cần đến dịch vụ chuyên gia để ngăn chặn thành công sự cố hay không.	
	B3	(Nếu có thể) tham gia hỗ trợ của bên thứ ba	Nếu cần, đội ứng cứu sự cố sẽ sắp xếp bên thứ ba tham gia hỗ trợ ứng phó sự cố.	
	B4	Thực hiện chiến lược ngăn chặn	Thực hiện chiến lược và hành động ngăn chặn nhằm mục tiêu ngăn chặn sự cố.	
	C1	Xây dựng chiến lược xoá bỏ	Việc xây dựng chiến lược xoá bỏ sẽ tìm cách loại bỏ sự cố ATTTM. Chiến lược sẽ dựa trên loại tấn công, sử dụng những thông tin chi tiết thu thập được ở các giai đoạn trước.	
	C2	Thực hiện chiến lược xoá bỏ	Việc thực hiện chiến lược xoá bỏ sẽ tìm cách diệt trừ vĩnh viễn sự cố ATTTM.	
	C3	Tiến hành săn lùng mối đe dọa	Các hoạt động săn lùng mối đe dọa nhằm tìm kiếm các cơ chế tồn tại tiềm ẩn, hoặc chỗ đứng có thể truy cấp cho kẻ tấn công quyền truy cập và kiểm soát liên tục.	
	C4	Giao tiếp với các bên liên quan chính	Liên lạc trong khi ứng phó là bước quan trọng để cập nhật cho các bên liên quan về các hoạt động ứng phó sự cố.	
Sự phục hồi	D1	Thôi kích hoạt đội ứng cứu sự cố	Sau khi loại bỏ thành công sự cố ATTTM, đội ứng cứu sự cố sẽ ngừng hoạt động.	
	D2	Xây dựng chiến lược khôi phục	Chiến lược khôi phục sẽ hướng tới mục tiêu đưa hoạt động (kinh doanh) trở lại bình thường, đối với các hệ thống/dịch vụ bị ảnh hưởng.	
	D3	Thực hiện chiến lược khôi phục	Thực hiện các công việc khôi phục.	
	D4	Giao tiếp với các bên liên quan	Liên lạc thường xuyên trong khi ứng phó là bước quan trọng để cập nhật cho các bên liên quan về các hoạt động ứng phó sự cố.	

Bảng 6: Danh sách kiểm tra ứng cứu sự cố tổng hợp

10 Phát hiện, phân tích và xếp loại (triage)

Giai đoạn này bắt đầu bằng việc phát hiện một hoặc nhiều sự kiện bảo mật và kết thúc khi tuyên bố và phân loại sự cố bảo mật hoặc xác định là không phải là sự cố bảo mật, gồm phát hiện và phân tích các sự kiện bảo mật cũng như phân loại và ưu tiên tiếp theo.

STT	Nhiệm vụ	Nội dung
A1	Xác nhận phát hiện sự cố ATTTM	Khi có báo cáo hoặc nghi ngờ về một sự cố ATTTM, các bên liên quan về ATTTM nên đánh giá sự cố tiềm ẩn.
A2	Thu thập và xác nhận thông tin đã biết	Theo dõi nguồn gốc của sự cố và tiến hành nghiên cứu thích hợp để hiểu rõ hơn về tính xác thực của sự cố.
A3	Phạm vi sự cố ATTTM	Xác định phạm vi và quy mô của (các) sự cố ATTTM.
A4	Xác định loại sự cố	Xác định loại sự cố ATTTM đã xảy ra.
A5	(Nếu có thể) Quyền truy cập và tính toàn vẹn của bản sao lưu	Cần kiểm tra tính toàn vẹn của các bản sao lưu để xác định xem chúng có bị xâm phạm hay không và dữ liệu/thông tin được lưu trữ có đủ để phục hồi sau sự cố hay không.
A6	Phân loại sự cố	Việc phân loại sự cố ATTTM đảm bảo tất cả các bên liên quan hiểu được mức độ nghiêm trọng của sự cố và có phản ứng cần thiết.
A7	Tuyên bố sự cố	Tuyên bố sự cố ATTTM.
A8	Triệu tập đội UCSC	Cần phải triệu tập đội ứng cứu sự cố để phản ứng với (các) sự cố ATTTM đã được xác định.
A9	Thông báo cho các bên liên quan chính	Truyền đạt sự số với các bên liên quan bên ngoài.
A10	Thu thập bằng chứng và dữ liệu dễ biến động/mất	Thu thập và lưu trữ bằng chứng và dữ liệu dễ thay đổi/dễ mất để hỗ trợ các hoạt động ứng phó sự cố, cùng với các quy trình/điều tra pháp lý có thể phải tuân theo.
A11	Kích hoạt sổ tay ứng phó sự cố liên quan	Các sổ tay cụ thể về ứng phó sự cố có liên quan nên được kích hoạt để hỗ trợ ứng phó sự cố.
A12	Điều tra sự cố ATTTM	Thu thập bằng chứng về sự cố.

Bảng 7: Nhiệm vụ phát hiện, phân tích và xếp loại

Giai đoạn		Nội dung	
Phát hiện		Phát hiện xảy ra khi có báo cáo về sự cố bảo mật. Các dấu hiệu của sự cố an toàn thông tin thường được chia thành hai loại: tiền sự cố và các chỉ báo.	
#	**Nhiệm vụ**	**(Những) người chịu trách nhiệm**	**Mô tả hành động**

A1	Xác nhận sự cố an toàn thông tin	<Nhập Tên người chịu trách nhiệm>	Không có một quy trình duy nhất để phát hiện sự cố ATTTM. Việc phát hiện thường làm như sau:
			• Tiền sự cố (precursor): phát hiện rằng cuộc tấn công mạng có thể xảy ra trong tương lai, chẳng hạn như nhận được email đe dọa hoặc thông tin về các chiến dịch tấn công quy mô lớn bằng phần mềm độc hại/mã độc tống tiền. Tuy nhiên, hình thức phát hiện này hiếm gặp.
			• Chỉ báo: phát hiện rằng sự cố đã hoặc đang xảy ra, ví dụ: cảnh báo từ hệ thống phát hiện xâm nhập, tên tệp có ký tự lạ, thay đổi cấu hình.
			• Giám sát an toàn thông tin: Chuyển tiếp từ các đơn vị cung cấp dịch vụ quản lý bảo mật hoặc các tổ chức/các bên liên quan, cảnh báo về sự hiện diện của sự cố.
			Sự cố ATTTM có thể được phát hiện thông qua:
			• Tiền sự cố - Dấu hiệu cho thấy một cuộc tấn công ATTTM có thể xảy ra trong tương lai.
			• Chỉ báo - Dấu hiệu cho thấy một cuộc tấn công ATTTM có thể đã xảy ra hoặc hiện đang diễn ra.
			Tham khảo **Phụ lục F – Các Chỉ báo Phát hiện Sự cố** để biết danh sách các dấu hiệu tiền sự cố và các chỉ báo phổ biến có thể báo hiệu sự hiện diện của sự cố ATTTM:
			Một số kẻ tấn công có thể lợi dụng nỗi sợ về các cuộc tấn công mạng để đòi tiền chuộc một cách bất hợp pháp, ngay cả khi không xâm nhập vào hệ thống. Trong các trường hợp này, cần tiến hành điều tra kỹ lưỡng để xác minh tính xác thực của các yêu cầu.
			Đội UCSC cần xem xét:
			• Nạn nhân nhận ra hoặc được thông báo về vụ việc vào thời điểm nào?
			• Nếu đã nhận được tin nhắn, nó có bao gồm bất kỳ mối đe dọa, yêu cầu và bằng chứng xâm nhập nào không ?
			  ○ Những mối đe dọa này có chứa các tuyên bố có thể kiểm tra không?
			  ○ Tin nhắn có không đề cập đến tên cá nhân hoặc có bất kỳ tham chiếu nào đến tổ chức không?
			• Có thiết bị hoặc hệ thống nào bị mã hóa không?

			Sau khi xác nhận sự cố ATTTM, đội điều tra cần thu thập thông tin chi tiết về các dấu hiệu tiền sự cố và các chỉ báo đã phát hiện để phục vụ quá trình điều tra.
A2	Thu thập và xác nhận thông tin đã biết	<Nhập Tên người chịu trách nhiệm>	Việc thu thập tất cả các thông tin đã biết nên được thực hiện để đảm bảo hiểu đầy đủ về sự cố. Khi thu thập thông tin, cần xem xét những điều sau: • Khả năng của các giải thích thay thế. • Những hạn chế trong các bằng chứng hiện có. • Bất kỳ thông tin hành động nào được phát hiện trong quá trình điều tra có thể được khám phá thêm. Ngoài ra, thông tin cần được thu thập để hiểu các câu hỏi dưới đây: • Các dịch vụ và/hoặc hệ thống đã bị ảnh hưởng đến mức độ nào? • Những gì không thể truy cập được? • Đã không thể truy cập được trong bao lâu? • Sự cố có ảnh hưởng gì đến hoạt động của tổ chức? • Nếu tổ chức là một tổ chức trọng yếu, cuộc tấn công có cản trở khả năng thực hiện các dịch vụ thiết yếu của tổ chức không? • Những thành phần kiến trúc nào có thể gây ra các lỗi liên tiếp? Nếu sự cố liên quan đến việc bao gồm một 'ghi chú tống tiền', nhóm điều tra nên tìm cách xác định biến thể ransomware và yêu cầu tống tiền. Tham khảo **Phụ lục G – Các nguồn Ransomware** để biết các nguồn thông tim về ransomware. Tham khảo **Phụ lục B - Các yếu tố đe dọa phổ biến** để có cái nhìn tổng quan về các yếu tố đe dọa phổ biến cần được khám phá. Trong suốt quá trình này, điều quan trọng là phải ghi chép rõ ràng cách thức mà tất cả các bằng chứng đã được bảo quản, bao gồm các hệ thống bị xâm phạm. Tất cả các bằng chứng thu thập được phải tuân thủ các thủ tục bảo quản theo chuỗi, nghĩa là chúng phải luôn được ghi nhận. Bất kỳ nhật ký kiểm toán, báo cáo hoặc bằng chứng khác được thu thập phải được giữ lại và chia sẻ theo chỉ đạo của Đội trưởng Đội UCSC thông tin để bảo vệ chuỗi bảo quản. Nhật ký chi tiết phải được lưu giữ cho tất cả các bằng chứng, bao gồm các thông tin sau: • Thông tin nhận dạng (ví dụ: vị trí, số sê-ri, kiểu máy, tên máy chủ, địa chỉ kiểm soát truy cập phương tiện (MAC) và địa chỉ IP của máy tính);

			• Tên, chức danh và số điện thoại của từng cá nhân đã thu thập hoặc xử lý bằng chứng trong quá trình điều tra; • Thời gian và ngày (bao gồm múi giờ) của từng lần xử lý bằng chứng; và • Các vị trí nơi bằng chứng được lưu trữ. Bằng chứng phải được bảo vệ và truy cập vào nó nên được giới hạn cho nhân sự được ủy quyền. Tham khảo NIST SP 800-86, Hướng dẫn Tích hợp Kỹ thuật Điều tra Forensics vào Ứng phó Sự cố để có hướng dẫn thêm về thu thập và xử lý bằng chứng.
A3	Xác định phạm vi sự cố	<Nhập Tên người chịu trách nhiệm>	Mục đích của việc xác định phạm vi là: • Xác nhận xem sự cố bảo mật đã xảy ra hay vẫn đang xảy ra; • Chuẩn bị cho việc phân loại và mức ưu tiên sự cố; • Xác định tất cả thông tin, hệ thống và tài nguyên có thể đã bị xâm phạm; và • Thông báo các hành động ngăn chặn. Việc xác định phạm vi phải cung cấp đủ thông tin để đội UCSC đánh giá tác động và ưu tiên các hoạt động tiếp theo, chẳng hạn như ngăn chặn sự cố và phân tích sâu hơn về tác động của sự cố an toàn thông tin. Không cần phải xác minh đầy đủ phạm vi của sự cố và nên được chuyển qua khi tất cả các mục tiêu của phạm vi đã được đáp ứng. Thông tin có thể giúp xác định phạm vi là: • Xác định các tài sản thông tin bị ảnh hưởng. • Xác định mạng, hệ thống hoặc ứng dụng bị ảnh hưởng và cách thức như thế nào. • Xem xét liệu các ứng dụng hoặc hệ thống bị ảnh hưởng có khả năng gây ra vi phạm quyền riêng tư dữ liệu hoặc phản hồi về Kế hoạch kinh doanh/hoạt động liên tục hay không. • Xác định tài khoản bị xâm phạm (nếu có). • Xem xét các sự cố xảy ra đồng thời và liệu hoạt động này có liên quan hay duy nhất không. • Xác định nguồn gốc của sự kiện bảo mật.
A4	Xác định loại sự cố	<Nhập Tên người chịu trách nhiệm>	Dựa trên thông tin được thu thập trong A1-A3, nhóm ứng cứu sự cố phải xác định loại sự cố ATTTM. Tham khảo thêm ở Error! Reference source not found..
A5	(Nếu có thể) Quyền truy cập và tính toàn vẹn của bản sao lưu	<Nhập Tên người chịu trách nhiệm>	Cần kiểm tra tính toàn vẹn của các bản sao lưu để xác định xem chúng có bị xâm phạm hay không và dữ liệu/thông tin được lưu trữ có đủ để phục hồi sau sự cố hay không. Cụ thể, đội ứng cứu sự cố sẽ điều tra: • Các bản sao lưu có thể sử dụng được cho các dịch vụ hoặc hệ thống bị ảnh hưởng không?

			Nếu có: ○ Ước tính thời gian phục hồi là bao lâu? ○ Những giải pháp hiện có nào có thể được sử dụng để hỗ trợ các dịch vụ/hệ thống này? ○ Bản sao lưu đã hoàn tất chưa hay còn thiếu dữ liệu? **Nếu không**: ○ Các tùy chọn dự phòng là gì? ○ Điều này ảnh hưởng thế nào đến thời gian phục hồi? Ngoài ra, đội ứng cứu sự cố sẽ điều tra: • Tần suất và phạm vi hệ thống của các bản sao lưu là gì? • Các bản sao lưu đã được xác minh chưa? • Những bản sao lưu này có được cách ly khỏi mạng khi xảy ra sự cố không? Thêm vào đó, điều tra sẽ xem xét khoảng thời gian xảy ra sự xâm phạm, nếu sự cố này xảy ra từ nhiều tháng trước, có khả năng các bản sao lưu có thể đã vô tình sao lưu các tệp được mã hóa. Trong tình huống như vậy, các bản sao lưu cần được điều tra trước khi phục hồi.
A6	Phân loại sự cố	<Nhập Tên người chịu trách nhiệm>	Khi đã thu thập đủ thông tin, sự cố ATTTM nên được phân loại. Phân loại sự cố đảm bảo tất cả các bên liên quan hiểu được mức độ nghiêm trọng của sự cố và phản ứng cần thiết. Tham khảo Error! Reference source not found.**J–**Error! Reference source not found. để có ví dụ về khung phân loại sự cố.
A7	Tuyên bố sự cố	<Nhập Tên người chịu trách nhiệm>	Dựa trên các hoạt động được thực hiện trong A1 – A6, đội ứng cứu sự cố sẽ quyết định xem liệu các tình huống có phù hợp để tuyên bố sự cố mất an toàn hay không, bằng cách xem xét những điều sau: • Tính xác thực – xác nhận sự cố bảo mật không phải là dương tính giả (cảnh báo không đúng); • Tác động – đánh giá tác động trực tiếp, gián tiếp và tiềm ẩn của sự cố bảo mật; • Phản hồi bắt buộc – xác nhận các nguồn lực cần thiết để quản lý sự cố bảo mật; và • Khẩn cấp – xác nhận tốc độ và thời gian dự kiến của sự cố an toàn thông tin. Trước khi tuyên bố sự việc, cần phải tham khảo ý kiến của người điều hành cấp cao có liên quan. Tham khảo **Error! Reference source not found.**K đề xuất các câu hỏi điều hành trong một sự cố ATTTM.

			Sau đó, người lãnh đạo sẽ quyết định liệu sự cố có nên được tuyên bố là sự cố mất an toàn hay không. Lý do quyết định và bất kỳ tài liệu liên quan nào nên được ghi lại. Tuyên bố về sự cố nên có các thông tin sau: • Ngày và giờ xảy ra sự cố (thường là ngày và giờ sự việc được xác nhận). • Trạng thái của sự cố – ví dụ: mới/đang xảy ra/đã giải quyết. • Loại sự cố và phân loại – ví dụ: phần mềm độc hại / ransomware / DDoS, v.v. • Phạm vi – chi tiết về mạng, hệ thống và/hoặc ứng dụng bị ảnh hưởng. • Tác động – chi tiết về các thành phần / hệ thống bị ảnh hưởng bởi sự cố và mức độ ảnh hưởng của chúng. • Mức độ nghiêm trọng – chi tiết về tác động của sự cố đối với (các) tổ chức (ví dụ: dịch vụ kinh doanh nào bị ảnh hưởng?)
A8	Triệu tập đội ứng cứu sự cố	<Nhập Tên người chịu trách nhiệm>	Việc triệu tập đội ứng cứu sự cố sẽ thiết lập các nguồn lực cần thiết để tiếp tục quá trình ứng phó sự cố. Cần xem xét tầm quan trọng và quy mô của sự cố ATTTM, cùng với các kỹ năng và kinh nghiệm có thể cần thiết để có phản ứng đầy đủ. Nếu đội UCSC cần thêm nguồn lực, nên tìm kiếm sự hỗ trợ của bên thứ ba từ các chuyên gia ATTT và/hoặc hỗ trợ từ VNCERT/CC.
A9	Thông báo cho các bên liên quan chính	<Nhập Tên người chịu trách nhiệm>	Sau khi tuyên bố, các bên liên quan quan trọng trong nội bộ và bên ngoài nên được thông báo, cảnh báo về sự cố, cung cấp chi tiết về những gì đang xảy ra và cung cấp hướng dẫn rõ ràng về những gì cần làm. Trước khi thực hiện bước này, nhóm ứng cứu sự cố nên xem xét nhu cầu chuyển sang cách liên lạc dùng kênh riêng. Đội ứng cứu sự cố nên chọn ra một cá nhân hoặc một nhóm chịu trách nhiệm truyền đạt thông tin sự cố cho các bên liên quan nội bộ và bên ngoài. **Các bên liên quan trong nội bộ** Việc thông báo cho các bên liên quan nội bộ nên được thực hiện càng sớm càng tốt sau khi xác định được sự cố ATTTM. Việc trao đổi thông tin với các bên liên quan nội bộ cần tìm cách cung cấp: • Chuyện gì đang xảy ra? • Chúng ta đang làm gì ? • Những gì mà các bên liên quan trong nội bộ cần? • Các bên liên quan trong nội bộ có thể cập nhật thông tin ở đâu?

			Việc liên lạc với các bên liên quan trong nội bộ phải thường xuyên và trực tiếp, cung cấp thông tin cập nhật kịp thời về các hoạt động ứng cứu sự cố quan trọng. **Các bên liên quan bên ngoài** Trao đổi thông tin và thông báo cho các bên liên quan bên ngoài là một bước quan trọng để đảm bảo tiến trình ứng cứu sự cố hiệu quả. Khi cần, nhóm ứng cứu sự cố nên cân nhắc việc thông báo cho: • Cơ quan có thẩm quyền. • Cục An toàn thông tin. • <Nhập thêm các bên liên quan bên ngoài bổ sung> • <Nhập thêm các bên liên quan bên ngoài bổ sung> • <Nhập thêm các bên liên quan bên ngoài bổ sung>
A10	Thu thập và lưu trữ bằng chứng và dữ liệu dễ thay đổi/dễ mất	<Nhập Tên người chịu trách nhiệm>	Để hỗ trợ các hoạt động ứng phó sự cố, cùng với các quy trình/điều tra pháp lý có thể tiếp tục, việc thu thập và lưu trữ các bằng chứng và dữ liệu dễ thay đổi/mất là rất cần thiết. Nếu thu thập không thành công hoặc không thu thập, bằng chứng quan trọng này có thể bị mất trong khi thực hiện các hoạt động ngăn chặn. Đội UCSC sẽ thu thập và lưu trữ các thông tin sau (nếu có): • Dữ liệu chống virus. • Thông tin phát hiện của thiết bị điểm cuối. • Thông tin phòng chống xâm nhập. • Nhật ký tường lửa. • Phát hiện hành vi người dùng trước và sau. • Các nhật ký mạng có sẵn. • Nhật ký và dữ liệu bảo mật của Windows. • Tệp nhị phân ban đầu của mã độc. • (Các) địa chỉ IP ra lệnh và điều khiển bị nghi ngờ. • (Các) tệp thực thi đã được phục hồi. • Mẫu tập tin được mã hóa. • Tập lệnh PowerShell. • Ảnh bộ bộ nhớ đang hoạt động. • Tài khoản người dùng được tạo trong bất kỳ thư mục hoạt động nào. • Địa chỉ email/số điện thoại/hồ sơ mạng xã hội được những kẻ tấn công sử dụng để phát động cuộc tấn công. Nếu có thể, nhóm ứng cứu sự cố cũng sẽ thu thập thông tin liên quan đến: • Những tập tin đã được mã hóa. • Phần mở rộng tập tin của các tập tin được mã hóa. • Có bao nhiêu người dùng có thể bị ảnh hưởng. • Có bao nhiêu máy chủ đã bị ảnh hưởng. • Mức độ quan trọng của các hệ thống bị ảnh hưởng.

A11	Sử dụng Sổ tay ứng phó sự cố có liên quan	<Nhập Tên người chịu trách nhiệm>	Nếu có thể, các sổ tay cụ thể về ứng phó sự cố có liên quan nên được sử dụng để hỗ trợ ứng cứu sự cố. Các tình huống sự cố sau đây có các chiến lược khắc phục riêng biệt: • Tấn công tống tiền ransomware • Tấn công mã độc • Tấn công Từ chối dịch vụ; • Lộ lọt dữ liệu • Tài khoản email bị xâm nhập.

A12	Điều tra sự cố ATTTM	<Nhập Tên người chịu trách nhiệm>	Trong giai đoạn đầu ứng phó sự cố, có thể không thể hiện ngay lập tức rằng sự cố bảo mật đã xảy ra. Có nguy cơ là bằng chứng cần thiết có thể bị sai lệch hoặc bị tiêu hủy, dù cố ý hay vô tình trước khi nhận ra mức độ nghiêm trọng của vụ việc. Phải thu thập bằng chứng sự cố trong thời gian sớm nhất để xác định phạm vi của sự cố và xác định liệu sự cố đã, sẽ hoặc có thể ảnh hưởng đến các hệ thống khác và có thể ảnh hưởng đến quá trình ứng phó sự cố, bằng chứng cần thu thập và phương pháp thu thập bằng chứng.
			
			Nên tham khảo hướng dẫn điều tra dưới đây trong suốt quá trình điều tra:
			
			• Lấy và bảo quản một bản sao chính của bằng chứng gốc, bao gồm:
			  ○ Ảnh hoặc kết quả thu thập bằng chứng từ các điểm cuối bị ảnh hưởng
			  ○ Bản sao nhật ký tường lửa và các lưu lượng mạng khác
			  ○ Bản sao của nhật ký Windows và IIS
			  ○ Nếu cần giải quyết thời gian ngừng hoạt động, hãy ưu tiên bằng chứng từ các hệ thống quan trọng và bắt đầu phục hồi ngay khi có bằng chứng từ mỗi hệ thống.
			• Xác định nguyên nhân của sự cố, ví dụ: thông tin xác thực bị xâm phạm, lỗ hổng, phishing, v.v.
			• Xác định xem có bỏ sót bất kỳ phương pháp lưu giữ bổ sung nào hay không, ví dụ: các tài khoản hoặc quy trình mới được tạo, cửa hậu hoặc phần mềm độc hại.
			• Điều tra xem có hành vi di chuyển ngang (lateral movement) nào đã xảy ra không.
			• Xác định xem có bất kỳ thông tin cá nhân hoặc thông tin nhạy cảm nào được truy cập hay không, bao gồm:
			  ○ Bởi ai;
			  ○ Từ đâu; và
			  ○ Họ có được cấp quyền không?
			• Phát triển các chỉ số săn tìm dựa trên kết quả điều tra, chẳng hạn như tài khoản bị ảnh hưởng hoặc địa chỉ IP bên ngoài.

			Tham khảo Error! Reference source not found.**I-Hướng dẫn Điều tra Sâu** để được hướng dẫn thêm về các bước điều tra chuyên sâu.

Bảng 8: Quy trình phân tích phát hiện và phân loại

11 Ngăn chặn

Đội ứng cứu sự cố sẽ tìm cách ngăn chặn sự cố ATTTM để hạn chế tác động. Ngăn chặn sớm là chìa khóa để hạn chế các hậu quả của sự cố ATTTM.

STT	Hoạt động	Nội dung
B1	Xây dựng chiến lược ngăn chặn	Xây dựng chiến lược ngăn chặn khẩn cấp với mục tiêu cách ly các hệ thống/máy chủ/thiết bị bị ảnh hưởng hoặc giảm thiểu sự cố.
B2	Xác định yêu cầu cần hỗ trợ của bên thứ ba	Đánh giá và xem xét liệu có thể cần đến dịch vụ chuyên gia để ngăn chặn sự cố thành công hay không.
B3	(Nếu có thể) Yêu cầu sự hỗ trợ của bên thứ ba	Nếu được yêu cầu, Đội UCSC sẽ kết nối với bên thứ ba để hỗ trợ ứng cứu sự cố.
B4	Thực hiện chiến lược ngăn chặn	Chiến lược và hành động ngăn chặn sẽ được thực hiện với mục tiêu ngăn chặn sự cố.

Bảng 9: Nhiệm vụ ngăn chặn

Giai đoạn		Nội dung	
Ngăn chặn		Mục tiêu của đội ứng cứu sự cố là ngăn chặn sự cố an ATTTM để hạn chế ảnh hưởng. Ngăn chặn sớm sự cố là việc quan trọng để hạn chế ảnh hưởng bởi sự cố ATTTM. Các biện pháp ngăn chặn có thể được thực hiện liên tục trong quá trình ứng cứu khi có thêm thông tin về sự cố. Mục đích ngăn chặn giảm rủi ro và ngăn thiệt hại thêm nhằm cung cấp thêm thời gian cho đội UCSC phát triển chiến lược khắc phục phù hợp. Do áp lực thời gian trong các sự cố ATTTM, các chiến lược ngăn chặn nên được lập kế hoạch trước khi xảy ra sự cố nếu có thể. Một phần quan trọng của ngăn chặn là ra quyết định và những quyết định đó sẽ dễ dàng hơn nếu có các chiến lược và quy trình đã có sẵn.	
#	**Nhiệm vụ**	**(Những) người chịu trách nhiệm**	**Mô tả hành động**

B1	Xây dựng chiến lược ngăn chặn	<Nhập Tên người chịu trách nhiệm>	Ngăn chặn sẽ giới hạn mức độ tấn công và khả năng thiệt hại hoặc mất mát do sự cố ATTTM gây ra, cũng như cung cấp thời gian để phát triển các chiến lược loại bỏ và phục hồi. Chiến lược ngăn chặn sẽ thay đổi dựa trên loại sự cố ATTTM, ví dụ chiến lược ngăn chặn tấn công bằng mã độc sẽ khác với tấn công DDoS. Các hành động ngăn chặn có thể diễn ra trong suốt vòng đời của sự cố ATTTM khi biết thêm chi tiết mới. Chiến lược ngăn chặn sẽ cân nhắc các yếu tố sau: • Thiệt hại tiềm ẩn và tổn thất tài nguyên về dữ liệu, tài sản và danh tiếng. • Yêu cầu bảo quản bằng chứng. • Tính sẵn sàng của dịch vụ, ví dụ kết nối mạng, các dịch vụ cung cấp cho các bên bên ngoài. • Thời gian và tài nguyên cần để thực hiện chiến lược. • Hiệu quả của chiến lược, ví dụ ngăn chặn một phần, ngăn chặn đầy đủ. • Thời gian của giải pháp. Khi xác định mức độ hỗ trợ có thể cần thiết, đội ứng cứu sự cố sẽ xem xét các kỹ năng, nguồn lực và kinh nghiệm có thể cần để ngăn chặn sự cố ATTTM cụ thể. Ngoài ra, cần cân nhắc các bước ngăn chặn ngắn hạn và dài hạn. Việc cô lập và hạn chế thiệt hại trong quá trình ngăn chặn thường xảy ra thông qua: • Ngăn chặn ngắn hạn • Sao lưu hệ thống • Ngăn chặn dài hạn Ngăn chặn ngắn hạn không nhằm mục đích trở thành một giải pháp lâu dài cho vấn đề mà chỉ nhằm mục đích hạn chế sự cố trước khi nó trở nên tồi tệ hơn. Đội UCSC được khuyến nghị thực hiện các hành động cần thiết để cô lập (các) hệ thống/tài sản bị ảnh hưởng. Bước thứ hai là sao lưu hệ thống. Quá trình này cần xem xét cách thông tin cần được sao lưu và lưu lại để phân tích thêm sau này. Có thể cần thiết phải tạo một bản sao pháp y forensic trước khi xóa và tái tạo lại hệ thống bị ảnh hưởng. Mục đích của việc này là để chụp lại hệ thống bị ảnh hưởng như nó đã hoặc đang trong thời gian xảy ra sự cố. Bằng cách làm như vậy, bằng chứng có thể được sử dụng trong các thủ tục pháp lý nếu sự cố được coi là hành vi phạm tội. Bản sao pháp y forensic cũng có thể được sử dụng để quan sát cách hệ thống bị xâm phạm trong giai đoạn học hỏi bài học thu được. Bước cuối cùng là ngăn chặn dài hạn. Bước này tạm thời khắc phục (các) hệ thống bị ảnh hưởng để cho phép chúng tiếp tục được sử dụng (nếu cần), trong khi xây dựng lại hệ thống sạch. Mục đích của bước này là loại bỏ các cửa hậu không mong muốn do kẻ tấn công để lại, cài đặt các bản vá bảo mật và các

			nỗ lực giảm thiểu khác để hạn chế bất kỳ sự leo thang nào của sự cố trong khi thúc đẩy hoạt động/kinh doanh bình thường. Nếu đội UCSC không thể xác định chiến lược ngăn chặn phù hợp nhất do tính phức tạp, nguồn lực nội bộ hoặc khi thông tin đầu vào không đủ để hỗ trợ đánh giá, nên tham khảo ý kiến của bên thứ ba bên ngoài.
B2	Xác định yêu cầu cần hỗ trợ của bên thứ ba	<Nhập Tên người chịu trách nhiệm>	Dựa trên các hoạt động được thực hiện trước đó, đội UCSC nên xác định các yêu cầu cần hỗ trợ của bên thứ ba. Bên thứ ba có thể là một công ty tư nhân chuyên ứng cứu sự cố ATTTM hoặc một đơn vị khác của Nhà nước có thể cung cấp hỗ trợ kỹ thuật. Tham khảo Error! Reference source not found.**L- Hướng dẫn Đánh giá Bên Thứ ba** về các đề xuất cần xem xét khi đánh giá nhu cầu tiềm năng về hỗ trợ của bên thứ ba.
B3	(Nếu cần) Thuê/Mời hỗ trợ của bên thứ ba	<Nhập Tên người chịu trách nhiệm>	Đội UCSC cần đãm bảo rằng bên thứ ba được chọn có khả năng, kinh nghiệm và nguồn lực cần thiết để hỗ trợ cho các tiến trình ứng phó sự cố. Để hỗ trợ quá trình đánh giá, tham khảo Error! Reference source not found.**M- Các câu hỏi Hỗ trợ của Bên Thứ ba**.
B4	Thực hiện chiến lược ngăn chặn	<Nhập Tên người chịu trách nhiệm>	Sử dụng thông tin thu thập được, đội UCSC sẽ tiến hành một cách có hệ thống các bước ngăn chặn cần thiết để kiểm soát sự cố thành công. Điều quan trọng là các hành động ngăn chặn nên nhằm đạt được sự cô lập và hạn chế thiệt hại. Tham khảo **Phụ lục N – Hướng dẫn Ngăn chặn** để biết thêm các hướng dẫn về việc ngăn chặn.

Bảng 10: Dòng tiến trình ngăn chặn

12 Loại bỏ

Trong khi một sự cố đang được ngăn chặn và phân tích/truy lùng, việc loại bỏ có thể cần thiết để loại bỏ các thành phần của sự cố, chẳng hạn như xóa phần mềm độc hại và vô hiệu hóa các tài khoản người dùng bị xâm phạm, và sau đó, xác định và giảm thiểu bất kỳ lỗ hổng nào đã bị khai thác. Điều quan trọng là phải loại bỏ nguồn gốc và cơ chế duy trì của sự cố để ngăn chặn bất kỳ thiệt hại nào khác.

Cần lưu ý rằng một số hành động được thực hiện có thể thuộc nhiều giai đoạn, ví dụ hành động phục hồi từ bản sao lưu có thể được coi là hoạt động phục hồi và hoạt động loại bỏ. Tương tự, việc xóa một trang web tên miền công cộng trong một cuộc tấn công Từ chối dịch vụ (DoS) có thể là cả hoạt động ngăn chặn và hoạt động loại bỏ.

STT	Hoạt động	Nội dung
C1	Xây dựng chiến lược loại bỏ	Việc xây dựng chiến lược loại bỏ sẽ tìm cách loại bỏ sự cố ATTTM. Chiến lược sẽ dựa trên loại tấn công, sử dụng những hiểu biết thu thập được trong các giai đoạn trước đó.
C2	Thực hiện chiến lược loại bỏ	Việc triển khai chiến lược loại bỏ sẽ tìm cách loại bỏ hoàn toàn sự cố ATTTM.
C3	Tiến hành săn lùng mối đe dọa	Các hoạt động săn lùng mối đe dọa tìm cách xác định các cơ chế tồn tại tiềm ẩn hoặc chỗ đứng có thể cung cấp quyền truy cập và kiểm soát liên tục của kẻ tấn công.
C4	Giao tiếp với các bên liên quan chính	Liên lạc liên tục là một bước quan trọng để cập nhật cho các bên liên quan về các hoạt động ứng phó sự cố.

Bảng 11: Các nhiệm vụ Loại bỏ

Giai đoạn		Nội dung	
Loại bỏ		Việc loại bỏ đòi hỏi phải loại bỏ mối đe dọa và khôi phục các hệ thống bị ảnh hưởng về trạng thái trước đó, đồng thời giảm thiểu mất dữ liệu.	
#	**Nhiệm vụ**	**(Những) người chịu trách nhiệm**	**Mô tả hành động**
C1	Xây dựng Chiến lược Loại bỏ	<Nhập Tên người chịu trách nhiệm>	Quy trình loại bỏ phải dựa trên loại tấn công, mức độ ưu tiên và hệ thống cần phục hồi. Quy trình này sau đó sẽ đánh giá tác động tới tổ chức/doanh nghiệp; mọi thay đổi cấu hình cần thiết ở giai đoạn này (hoặc bất kỳ giai đoạn nào) của quy trình phải được thực hiện với sự chấp thuận của lãnh đạo. Trong kế hoạch loại bỏ, các hành động sau đây cần được xem xét để giảm thiểu các lỗ hổng đã được xác định: • Vá các hệ thống có lỗ hổng; • Khóa truy cập từ xa; • Cải thiện khả năng phát hiện mã độc; • Tăng cường cơ chế sao lưu; và

			• Hướng dẫn người dùng cách nhận diện email độc hại.
C2	Thực hiện Chiến lược Loại bỏ	<Nhập Tên người chịu trách nhiệm>	Việc triển khai chiến lược loại bỏ nên tìm cách loại bỏ vĩnh viễn kẻ tấn công khỏi các hệ thống bị khả năng gây gián đoạn của chúng. Các bước loại bỏ phải phản ánh loại sự cố cụ thể và mức độ thiệt hại gây ra. Tham khảo **Error! Reference source not found.**P- Hướng dẫn Loại bỏ để có hướng dẫn các bước.
C3	Tiến hành săn lùng mối đe dọa	<Nhập Tên người chịu trách nhiệm>	Các kẻ tấn công có thể cài đặt các cơ chế duy trì, hoặc điểm bám để có quyền truy cập liên tục và duy trì vào mạng bị xâm nhập. Khi hiểu rõ về chiến thuật, kỹ thuật và quy trình của kẻ tấn công thu được trong quá trình phân tích bằng chứng, chúng nên được xác định trên các hệ thống bị ảnh hưởng. Săn tìm mối đe dọa là phương pháp đạt được điều này. Săn tìm mối nguy nên bao gồm việc phân tích toàn diện các kỹ thuật liên quan đến sự cố đang được điều tra, trên tất cả các khu vực của mạng có thể bị ảnh hưởng bởi sự cố. Ngoài ra, cần cố xác định các hoạt động phổ biến khác của kẻ tấn công để đảm bảo phạm vi đầy đủ của sự cố đã được xác định trong phân tích trước đó. Khi săn tìm, điều quan trọng là phải quan tâm đến mọi hoạt động đáng ngờ. Ngay cả khi một số hoạt động này thoạt đầu không có vẻ liên quan đến sự cố đang diễn ra, nó có thể dẫn đến các phát hiện them về sự cố hoặc xác định được một sự cố riêng khác cũng đã xảy ra. Tiến trình săn lùng toàn diện là thành phần chính để đảm bảo loại bỏ hiệu quả các công cụ, kỹ thuật và quy trình của kẻ tấn công. Có thể sử dụng Khung MITER ATT&CK để trình bày các công cụ, kỹ thuật và quy trình của kẻ tấn công.
C4	Giao tiếp với các bên liên quan chính	<Tên người chịu trách nhiệm>	Việc trao đổi thông tin về các hoạt động Loại bỏ nên duy trì liên tục với các bên liên quan quan trọng, cung cấp các cập nhật và các kế hoạch khôi phục khi cần.

Bảng 12:Dòng tiến trình Loại bỏ

13 Khôi phục

Mục tiêu của giai đoạn khôi phục là đưa các hệ thống bị ảnh hưởng trở lại trạng thái hoạt động. Trước khi đưa các hệ thống này vào môi trường sản xuất, Đội trưởng đội UCSC cần tham khảo ý kiến của chủ sở hữu hệ thống và quản trị hệ thống để đảm bảo không gây ra các sự cố mới. Việc kiểm tra, giám sát và xác thực các hệ thống sau khi phục hồi là vô cùng quan trọng nhằm đảm bảo rằng chúng không bị tái nhiễm phần mềm độc hại hoặc bị xâm phạm trở lại bằng các cách khác.

STT	Hoạt động	Nội dung
D1	Dừng hoạt động đội ứng cứu sự cố	Sau khi loại bỏ thành công sự cố ATTTM, đội ứng cứu sự cố sẽ ngừng hoạt động.
D2	Xây dựng chiến lược phục hồi	Chiến lược phục hồi nên tìm cách mang trở lại các hoạt động kinh doanh như bình thường đối với các hệ thống/dịch vụ bị ảnh hưởng.
D3	Thực hiện chiến lược phục hồi	Việc triển khai các hành động khôi phục.
D4	Giao tiếp với các bên liên quan	Liên lạc liên tục là một bước quan trọng để cập nhật cho các bên liên quan về các hoạt động ứng cứu sự cố.

Bảng 13: Các nhiệm vụ khôi phục

Giai đoạn		Nội dung	
Khôi phục		Giai đoạn này bao gồm việc phục hồi các hệ thống bị ảnh hưởng trở lại trạng thái hoạt động.	
#	**Nhiệm vụ**	**(Những) người chịu trách nhiệm**	**Mô tả hành động**
D1	Dừng hoạt động đội ứng cứu sự cố	<Nhập Tên người chịu trách nhiệm>	Sau giai đoạn loại bỏ (hoặc ngăn chặn nếu không cần thiết phải loại bỏ) sự cố, đội ứng cứu sự cố sẽ chuyển sang hoạt động như thường lệ.
D2	Xây dựng chiến lược phục hồi	<Nhập Tên người chịu trách nhiệm>	Chiến lược khôi phục nên tìm cách cung cấp lại sự hoạt động bình thường cho các hệ thống/dịch vụ bị ảnh hưởng. Kế hoạch này nên xem xét các hoạt động theo thứ tự ưu tiên cần thực hiện hoàn trả lại hiệu quả nhất. Các nỗ lực khôi phục, đặc biệt là các nỗ lực không ưu tiên có thể diễn ra trong thời gian dài, nên có thể cần các dịch vụ dự phòng thay thế cho đến khi phục hồi hoàn toàn.
D3	Thực hiện chiến lược phục hồi	<Nhập Tên người chịu trách nhiệm>	Việc triển khai các hành động khôi phục. Ví dụ về các hành động khôi phục: • Khôi phục hệ thống từ các bản sao lưu sạch. • Xây dựng lại hệ thống từ đầu. • Thay thế các tập tin bị xâm phạm bằng các tập tin sạch. • Thay đổi hoặc làm mới các phương thức xác thực, chẳng hạn như thay đổi và luân phiên mật khẩu.

			• Các thay đổi về mạng, chẳng hạn như các thay đổi phân đoạn vi mô, tường lửa, thay ACL của bộ định tuyến. Khi phục hồi hệ thống, việc thẩm định cẩn thận phải đảm bảo rằng các yêu cầu, kiểm thử và quét lỗ hổng bảo mật được thực hiện.
D4	Giao tiếp với các bên liên quan	<Nhập Tên người chịu trách nhiệm>	Việc trao đổi thông tin về các hoạt động phục hồi nên duy trì liên tục với các bên liên quan quan trọng, cung cấp các thông tin cập nhật và các kế hoạch khôi phục theo yêu cầu.

Bảng 14: Dòng Tiến trình Khôi phục

14 Hoạt động sau sự cố

Sau khi sự cố được giải quyết, điều quan trọng thông báo đến tất cả các bên liên quan về việc sự cố đã kết thúc và bất kỳ công việc khắc phục nào chưa hoàn thành sẽ được thực hiện.

Đội trưởng Đội UCSC sẽ chuẩn bị Báo cáo Xử lý Sự cố, cung cấp góc nhìn theo thời gian về sự cố và xử lý đã thực hiện. Báo cáo nên nêu chi tiết những gì đã xảy ra, những gì đã được thực hiện, bởi ai và nhanh chóng như thế nào. Đội UCSC cũng nên xem xét quy trình ứng cứu sự cố hiện có, kế hoạch ứng phó sự cố ATTTM này là một hoạt động sau sự cố nhằm có thể sửa đổi, cải thiện hiệu quả và hiệu lực của các quy trình.

Điều quan trọng là tổ chức/doanh nghiệp nên thực hiện một phiên báo cáo và rút ra bài học kinh nghiệm với các bên liên quan để làm rõ những phát hiện liên quan đến việc xử lý sự cố. Các báo cáo này nên đảm bảo rằng tất cả các bên liên quan đều tin tưởng vào kết quả giải quyết sự cố và các bước tiếp theo nếu có.

Phần bên dưới cung cấp tổng quát về các hoạt động sau sự cố cần thiết và các email mẫu có thể được gửi đến các bên liên quan thông báo sự cố đã được giải quyết.

Người dùng nên thực hiện các hoạt động sau:

14.1 Huỷ kích hoạt trạng thái sự cố

Việc hủy kích hoạt là thông báo chính thức của đội trưởng đội UCSC đến tất cả các bên có liên quan rằng sự cố ATTTM đã được giải quyết hoặc đang được quản lý hiệu quả bằng các quy trình kinh doanh thường lệ.

14.1.1 Mẫu thông báo sự cố nội bộ

Mẫu thông báo dưới đây dành cho các nhân viên nội bộ, gồm cả những người liên quan trực tiếp đến sự cố và những người bị ảnh hưởng bởi sự cố.

Thông báo sự cố ATTTM đã giải quyết cho các bên liên quan chính
Kịch bản: Sự cố ATTTM đã được giải quyết và các bên liên quan chính trong nội bộ cần được thông báo.
Từ: Đội trưởng hoặc Đội phó đội ứng cứu sự cố **Đến:** Các bên liên quan chính trong nội bộ **Chủ đề:** Cập nhật sự cố an toàn thông tin mạng Kính gửi **<Nhập tên các phòng/bộ phận liên quan chính>**, <Nhập thông báo lỗi/hệ thống> hiện đã được giải quyết và mọi tính năng hiện đang hoạt động bình thường. Thông tin cập nhật về sự cố ATTTM như sau: • **Mô tả sự cố:** <Nhập mô tả ngắn gọn về sự cố>. • **Tác động đến hoạt động/kinh doanh:** <Nhập tác động đến hoạt động/kinh doanh và lý do tại sao xảy ra sự cố, nếu biết. Ví dụ: thông tin chi tiết về hệ thống, tài khoản, v.v. là đối tượng bị vi phạm bảo mật>.

- **Tóm tắt các hoạt động cho đến nay:** <Nhập tóm tắt ai đang làm gì để khôi phục sự cố>.
- **Trạng thái:**<Đã giải quyết hoặc chưa giải quyết, tại sao>.

Chúng tôi cảm ơn sự hỗ trợ và kiên nhẫn của bạn trong việc giải quyết sự cố này.

<Nhập tên đội> sẽ tiếp tục nỗ lực khắc phục mọi vấn đề tồn tại và rút kinh nghiệm từ sự cố này để chuẩn bị tốt hơn cho <Nhập tên tổ chức/doanh nghiệp> trong tương lai.

Trân trọng,

<Nhập tên đội>

Bảng 15: Thông báo đã giải quyết sự cố cho các bên liên quan trong nội bộ

14.1.2 Mẫu thông báo sự cố bên ngoài

Mẫu thông báo dưới đây dùng cho các bên liên quan bên ngoài, có thể là các cơ quan nhà nước, cơ quan quản lý và các đối tác hợp tác .

Lưu ý: mẫu báo cáo sự cố ATTTM cho cơ quan quản lý chuyên ngành tại địa phương và quốc gia vẫn áp dụng theo quy định hiện hành.

Thông báo đã giải quyết sự cố ATTTM cho các bên liên quan bên ngoài
Kịch bản: Sự cố ATTTM đã được giải quyết và các bên liên quan bên ngoài cần được thông báo.

Từ: Đội trưởng hoặc Đội phó đội ứng cứu sự cố

Đến: <Nhập các bên liên quan bên ngoài>

Chủ đề: Cập nhật sự cố ATTTM

Kính gửi <Nhập tên bên liên quan bên ngoài>

<Nhập thông báo lỗi/hệ thống> hiện đã được giải quyết và mọi tính năng hiện đang hoạt động bình thường.

Thông tin cập nhật về sự cố ATTTM như sau:

- **Mô tả sự cố:** <Nhập mô tả ngắn gọn về sự cố >.
- **Mức độ nghiêm trọng:** <SP1 – SP4>.
- **Tác động đến hoạt động/kinh doanh:** <Nhập tác động đến hoạt động/kinh doanh và lý do xảy ra sự cố, nếu biết. Ví dụ: thông tin chi tiết về hệ thống, tài khoản, v.v. đã bị vi phạm bảo mật>.
- **Tóm tắt các hoạt động cho đến nay:** <Nhập tóm tắt ai đang làm gì để khôi phục sự cố>.
- **Trạng thái:**<Đã giải quyết hoặc chưa giải quyết, tại sao>.

Chúng tôi cảm ơn sự hỗ trợ và kiên nhẫn của bạn trong việc giải quyết sự cố này.

<Nhập tên đội> sẽ tiếp tục nỗ lực khắc phục mọi vấn đề còn tồn tại và rút kinh nghiệm từ sự cố này để chuẩn bị tốt hơn cho <Điền tên tổ chức/doanh nghiệp> trong tương lai.

<Nhập tên doanh nghiệp> sẽ có một tóm tắt chính thức và bài học kinh nghiệm vào <Nhập thời gian dự kiến >.

Trân trọng,

<Nhập tên đội>

Bảng 16: Thông báo đã giải quyết sự cố ATTTM cho các bên liên quan bên ngoài

14.2 Tóm tắt Chính thức Sau Sự cố

Tóm tắt Chính thức Sau Sự cố cung cấp thông tin tổng quan về sự cố và kết luận. là một tài liệu chi tiết, tổng hợp toàn bộ quá trình điều tra và xử lý một sự cố an toàn thông tin. Báo cáo này sẽ được hoàn thành sau khi thu thập đầy đủ thông tin từ các cuộc phỏng vấn, các log hệ thống, dữ liệu giám sát và các nguồn dữ liệu khác. Báo cáo sẽ cung cấp một cái nhìn tổng quan về nguyên nhân, diễn biến, tác động của sự cố và các biện pháp khắc phục.

Bản tóm tắt chính thức sau sự cố cung cấp thông tin tổng quan về sự cố, khi sự cố kết thúc. Việc này nên thực hiện sau khi đã kết thúc tất cả các bước điều tra, đảm bảo mọi chi tiết liên quan đều có và có thể được đưa vào. Bản tóm tắt cung cấp cơ hội để tổ chức mô tả những gì đã xảy ra, lý do tại sao nó xảy ra và cách tổ chức xử lý.

Các cơ quan quản lý nhà nước có thể yêu cầu thêm thông tin qua email, tài liệu bổ sung hoặc qua các cuộc họp chính thức. *Lưu ý: báo cáo kết thúc sự cố gửi cho các cơ quan quản lý chuyên ngành ATTT vẫn thực hiện theo quy định hiện hành.*

Mẫu Tóm tắt Chính thức cho các bên liên quan bên ngoài

Từ: Đội trưởng hoặc Đội phó đội ứng cứu sự cố

Đến: <Nhập tên các bên liên quan bên ngoài>

Chủ đề: Cập nhật sự cố an toàn thông tin mạng

Kính gửi <Nhập tên bên liên quan bên ngoài>

Sự cố an toàn thông tin mạng [Nhập số tham chiếu] đã được giải quyết vào [Nhập ngày] của <Nhập hệ thống/khu vực bị ảnh hưởng> đã khôii phục lại chức năng bình thường.

<Nhập tên tổ chức/doanh nghiệp> đã chuẩn bị một bản tóm tắt sau sự cố. Bản tóm tắt này bao gồm phân tích chi tiết về sự cố đã xảy ra và trích các bài học kinh nghiệm.

<Nhập mô tả chi tiết về sự cố, dựa trên các câu hỏi thảo luận bên dưới>

• Nguyên nhân của sự cố là gì? Bao gồm:
  ○ Cách thức xâm phạm/thỏa hiệp?
  ○ (Nếu có) Các lỗ hổng bị khai thác.
• Tác động của sự cố là gì?
• Sự cố đã được giải quyết như thế nào?
• Những trở ngại nào đã gặp khi ứng phó với sự cố?
• Những chậm trễ và trở ngại nào đã xảy ra khi ứng phó?
	• Có bất kỳ điểm chuyển cấp nào không? Chẳng hạn như:
	  ○ Cơ quan thực thi pháp luật
	  ○ Những quản lý
	  ○ Hỗ trợ kỹ thuật bên ngoài
	  ○ Các cơ quan khác
	• (Nếu có thể) việc chuyển cấp có cản trở tiến trình ứng phó không?

• <Nhập tên tổ chức/doanh nghiệp> đã được chuẩn bị đầy đủ cho sự cố chưa? • Đội UCSC có đủ nhân lực và nguồn lực để ứng phó không?	• Các tổ chức truyền thông có hỏi bất kỳ điều gì trước, trong hoặc sau sự kiện này không? ○ (Nếu có thể) Bản chất của các câu hỏi là gì, có dẫn đến công bố công khai nào về (các) sự cố hay không?

<Điền tên doanh nghiệp> hy vọng rằng các thông tin ở trên cung cấp đến <Nhập tên bên liên quan bên ngoài> những thông tin cần thiết. Nếu bạn cần thêm thông tin, vui lòng liên hệ với đại diện của <Điền tên doanh nghiệp> qua số điện thoại di động: <Nhập số điện thoại di động> và/hoặc E-mail: <Nhập email>.

Trân trọng,

<Nhập tên đội>

Bảng 17: Mẫu Tóm tắt Chính thức cho các bên liên quan bên ngoài

14.3 Bài học kinh nghiệm

Sau khi xảy ra sự cố ATTTM, việc rút ra bài học kinh nghiệm là vô cùng cần thiết, cung cấp cơ hội để xem xét những gì đã xảy ra và đã ứng phó như thế nào.

Tổ chức / doanh nghiệp sẽ tiến hành đánh giá, tập trung vào việc hiểu:

- Chính xác những gì đã xảy ra và vào những thời điểm nào nào?
- Nhân viên và cấp quản lý đã thư thế nào với sự cố ATTTM? Các thủ tục ghi chép lại có được tuân theo không? Chúng có đầy đủ không
- Thông tin nào cần có sớm hơn?
- Có bất kỳ bước nào hoặc hành động nào đã làm có thể cản trở việc khôi phục không?
- Nhân viên và cấp quản lý sẽ làm những gì khác đi nếu có một sự cố ATTTM tương tự xảy ra lần tới?
- Làm thế nào để có thể cải thiện việc chia sẻ thông tin với các tổ chức khác?
- Các hành động khắc phục nào có thể ngăn chặn các sự cố ATTTM tương tự trong tương lai?
- Những dấu hiệu hoặc chỉ số nào cần theo dõi để phát hiện sự cố tương tự?
- Chúng ta cần những công cụ và tài nguyên bổ sung nào giúp phát hiện, phân tích và giảm thiểu các sự cố trong tương lai?

Một báo cáo theo dõi sẽ được tạo cho mỗi sự cố ATTTM có mức độ ưu tiên P1 và P2. Báo cáo cung cấp một tham khảo có thể dung để hỗ trợ xử lý các sự cố tương tự.

Việc tạo ra một trình tự các sự kiện chính thức và ước tính thiệt hại sẽ hỗ trợ trong trường hợp có các thủ tục pháp lý.

Phụ lục A. Các loại sự cố ATTTM

Bảng dưới đây cung cấp danh sách các kiểu tấn công phổ biến.

#	Loại/Mô tả	Ứng phó ban đầu để giảm thiểu tác hại tiềm tàng
1	**Mã độc tống tiền ransomware:** công cụ để mã hoá hoặc khoá dữ liệu nạn nhân cho đến khi trả tiền chuộc.	Ngay lập tức loại thiết bị nhiễm ra khỏi mạng để hạn chế phát tán ransomware. Thu thập tất cả nhật ký liên quan đến thiết bị. Cách ly thiết bị trong khi thực hiện ngăn chặn và loại bỏ.
2	**Nhiễm mã độc:** vi-rút, sâu, trojan hoặc các loại mã độc hại khác xâm nhập vào hệ thống.	Ngay lập tức loại thiết bị bị nhiễm ra khỏi mạng để hạn chế phát tán mã độc. Thu thập tất cả nhật ký liên quan đến thiết bị. Cách ly thiết bị trong khi xác nhận đã ngăn chặn và cố gắng diệt trừ mã độc.
3	**Tấn công từ chối dịch vụ (DoS) hoặc từ chối dịch vụ phân tán (DDoS):** làm quá tải mạng với lượng lưu lượng mà nó không thể xử lý, đôi khi gây ra sự cố mạng.	Yêu cầu nhà cung cấp dịch vụ cổng xác định bản chất của DoS/DDoS, cách thức tấn công và triển khai các giải pháp phù hợp. Phối hợp với dịch vụ cổng và nhóm mạng để triển khai các bộ lọc ở biên mạng và/hoặc tăng dung lượng.
4	**Lừa đảo và Kỹ thuật xã hội:** được thiết kế các giao tiếp đánh lừa để lấy thông tin nhạy cảm của người dùng (bao gồm thông tin đăng nhập mạng)	Xem xét nhật ký của người dùng bị ảnh hưởng (nhật ký web và email) để xác định xem các liên kết/tệp đính kèm độc hại có được truy cập hay không. Tư vấn cho người dùng để xác nhận các hành động họ đã thực hiện và liệu có bất kỳ thông tin cá nhân/nhạy cảm nào được cung cấp cho nỗ lực lừa đảo/kỹ thuật xã hội. Xem xét việc đặt lại mật khẩu của người dùng và giám sát các tài khoản để phát hiện bất kỳ truy cập trái phép nào.
5	**Vi phạm dữ liệu:** Truy cập trái phép vào thông tin nhạy cảm hoặc thông tin nhận dạng cá nhân.	Kiềm chế sự mất mát dữ liệu càng sớm càng tốt. Cảnh báo cho các đội về riêng tư, pháp lý và truyền thông/truyền thông. Điều tra nguyên nhân của việc mất mát dữ liệu.

Bảng 18: Các loại sự cố ATTTM

Phụ lục B. Các Kiểu Nguy cơ Phổ biến

Các phương thức tiềm ẩn gây nguy hại phổ biến gồm:

#	Loại	Nội dung
1	Ổ đĩa lắp ngoài / di động	Tấn công thực hiện từ USB chứa mã độc.
2	Tiêu hao	Tấn công DDoS qua mạng hoặc hệ thống quan trọng.
3	Web	Chuyển hướng lưu lượng web đến URL độc hại để cài mã độc lên thiết bị của nạn nhân.
4	E-mail	Tấn công giả mạo phishing nhằm đánh cắp thông tin và/hoặc chạy mã độc trên thiết bị của nạn nhân.
5	Mạo danh	Ví dụ tạo một tên miền bắt chước tên miền của tổ chức/doanh nghiệp/cá nhân nhằm lừa dối nạn nhân (thường liên quan đến các cuộc tấn công lừa đảo).
6	Sử dụng sai cách	Lỗi do con người dẫn đến vi phạm chính sách ATTT; hoặc tấn công từ người nội bộ độc hại dẫn đến sự cố ATTTM.

Bảng 19: Các Kiểu Nguy cơ Phổ biến

Phụ lục C. Ví dụ ma trận RACI

[R] Responsible (Chịu trách nhiệm thực hiện): Người trực tiếp thực hiện công việc. Họ là những người được giao nhiệm vụ hoàn thành công việc hoặc đưa ra quyết định.
[A] Accountable (Chịu trách nhiệm cuối cùng): Người chịu trách nhiệm cuối cho việc hoàn thành nhiệm vụ. Lý tưởng nhất chỉ là một người, thường là giám đốc điều hành hoặc nhà tài trợ chương trình.
[C] Consulted (Được tư vấn ý kiến): Những người cung cấp thông tin, thường là những người có chuyên môn hoặc kiến thức liên quan đến nhiệm vụ, cần được tham khảo ý kiến trước khi quyết định, được gọi là chuyên gia về chủ đề.
[I] Informed (Được thông báo): Những người được cập nhật tiến độ, là những người bị ảnh hưởng bởi kết quả của các hoạt động và cần được cập nhật thông tin.

Kích hoạt/Nhiệm vụ	Giám đốc điều hành	CISO	Nhóm CNTT	Đội trưởng đội UCSC	Pháp chế	Đội Truyền thông	Nhân viên VNCERT/CC
Khủng ATTTM tiềm ẩn mạng được báo cáo	I	R	C	I	C	R	I
Dữ liệu đã được truy cập hoặc lộ lọt	A	R	C	C	C	R	I
Kẻ tấn công vẫn còn hoạt động trong hệ thống	A	C	C	I	C	R	I
Bằng chứng về sự tham gia của tấn công APT	I	C	C	I	I	I	I
Kẻ tấn công triển khai ransomware, gây gián đoạn hoạt động	C	C	C	C	C	R	I
Kẻ tấn công đã liên hệ với các bên liên quan chính	A	I	I	C	C	R	I
Kẻ tấn công leo thang và phát hành các trích xuất dữ liệu hoặc cảnh báo trực tuyến	A	C	C	C	C	R	I
Liên lạc với kẻ tấn công được tiết lộ	A	I	I	C	C	R	I

Bảng 20 : Ví dụ Ma trận RACI

KIẾN NGHỊ

Ma trận RACI mẫu phải được thiết kế để phù hợp với mục đích đáp ứng các yêu cầu cụ thể của tổ chức/doanh nghiệp.

Phụ lục D. Báo Sự cố cho VNCERT/CC

Để báo cáo sự cố hoặc vi phạm ATTTM cho VNCERT/CC qua các kênh sau:

- Gửi đến địa chỉ: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - Tầng 5, 115 Trần Duy Hưng, Trung Hoà, Cầu Giấy, Hà Nội
- Gửi Email: **ir@vncert.vn**
- Gửi trên website: **https://vncert.vn/page/154/bao-cao-su-co**
- Gửi trên IRLab: **https://irlab.vn/report/#/new-case**
- Gọi số hotline: 0869100317

Phụ lục E. Mẫu Sổ đăng ký bằng chứng

NGÀY, THỜI GIAN VÀ ĐỊA ĐIỂM THU THẬP	THU THẬP BỞI (Tên, chức danh, số liên lạc và số điện thoại)	CHI TIẾT CÁC MỤC (Địa chỉ IP, Địa chỉ Mac, Số kiểu máy, Tên máy chủ, Số sê-ri, Tên tệp, v.v.)	VỊ TRÍ LƯU TRỮ VÀ SỐ NHÃN	TRUY CẬP (Ngày, Giờ, Người, lý do truy cập sau khi thu thập)

Bảng 21: Đăng ký bằng chứng

KIẾN NGHỊ

Mẫu Đăng ký Bằng chứng phải được thiết kế phù hợp với mục đích của tổ chức/doanh nghiệp cụ thể.

Phụ lục F. Hướng dẫn Truyền thông

Yếu tố	Câu hỏi chỉ định	(Các) hành động

Sự kiện/Kịch bản	• Các sự kiện chính của sự cố ATTTM là gì?
	  ○ Những hệ thống nào bị ảnh hưởng hoặc có khả năng bị ảnh hưởng?
	  ○ Thông tin nào đã hoặc có thể đã bị xâm phạm?
	• Những cân nhắc chính:
	  ○ Sự cố này đã được công khai hay đã có rò rỉ không?
	  ○ Đây có phải là sự cố của bên thứ ba không?
	  ○ Có bằng chứng về ransomware, tống tiền qua mạng hoặc tống tiền dữ liệu bị đánh cắp không?
	  ○ Có biết kẻ tấn công không?
		• Soạn thảo bản tóm tắt sự cố. Lưu ý: Đảm bảo rằng các thông tin liên lạc với các bên liên quan chỉ nêu những sự kiện đã biết và có thể xác minh được, và không chứa các suy đoán.

Những bên liên quan chính trong nội bộ nhận thông tin truyền thông	• Ai cần tham gia vào việc phát triển chiến lược truyền thông trong khủng hoảng này?
	• Xem xét:
	  ○ Yêu cầu quy định.
	  ○ Sự tham gia của Bộ.
	  ○ Đầu vào và rủi ro pháp lý.
	  ○ Tuân thủ và các tác động của rủi ro.
	  ○ Tác động hoạt động.
	  ○ Tác động khách hàng.
	  ○ Tác động bảo hiểm.
	  ○ Sự tham gia của Truyền thông và quan hệ Doanh nghiệp.
		• Liên hệ với các bên liên quan quan trọng trong nội bộ.

Thông điệp chiến lược tổng thể	• Có bất kỳ thông điệp chiến lược bao quát nào sẽ cung cấp thông tin đến các bên liên quan không? Chúng có cụ thể cho từng bên liên quan không?	• Xác định thông điệp chiến lược.
Hỗ trợ pháp lý	• Có đang tìm kiếm lời khuyên pháp lý về sự cố này không (lời khuyên có thể là để xác định hậu quả pháp lý của việc quản lý sự cố theo một cách cụ thể hoặc hậu quả pháp lý của sự cố nếu nó ảnh hưởng đến	• Xác định xem có cần tư vấn pháp lý hay không, bảo vệ liên lạc liên quan đến tư vấn pháp lý đó, tìm kiếm đánh giá pháp lý về liên lạc nếu có rủi ro pháp lý trong những liên lạc đó.

	thông tin cá nhân của khách hàng về sản phẩm hoặc dịch vụ không)? • Có bất kỳ liên lạc bổ sung nào (ngoài các thông điệp chính đã được phê duyệt) cần đóng góp từ từ pháp lý không?	
Các kênh truyền thông	• Thông tin sẽ được truyền đạt đến các bên liên quan như thế nào? • Có các kênh truyền thông cụ thể nào cần để thực hiện chiến lược truyền thông không? Cần nhắc: ○ Các kênh có sẵn đã sở hữu và các kênh có thể được yêu cầu, chẳng hạn như các cuộc họp báo với truyền thông bên ngoài.	• Xác định các kênh liên lạc trong khi ứng phó sự cố. • Thiết lập trang web đặc biệt để cập nhật thông tin về sự cố. ngoài trang web chính • Xem lại các kênh để xác định xem có kênh nào đang ngoại tuyến hay không.
Nhịp điệu liên lạc	• Tần suất thông tin sẽ được truyền đạt sau khi nhận diện sự kiện là bao lâu? Cân nhắc các liên lạc ngắn hạn, trung hạn và dài hạn.	• Xác định tần suất được thỏa thuận để truyền đạt đến các nhóm các bên liên quan chính cả trong và ngoài tổ chức.

Bảng 22: Hướng dẫn truyền thông

Phụ lục G. Các Chỉ báo Phát hiện Sự cố

Các chỉ báo	Ví dụ
Báo cáo về hành vi bất thường hoặc đáng ngờ của nhân viên hoặc các bên liên quan bên ngoài.	Một nhân viên nhận được email yêu cầu xác nhận thông tin đăng nhập mạng của họ hoặc cung cấp thông tin cá nhân, thông tin nhạy cảm khác.
	Nhiều nhân viên báo cáo bị 'khóa' tài khoản mạng của họ.
	Một bên liên quan bên ngoài báo cáo việc nhận được các thư điện tử rác hoặc lừa đảo từ tổ chức của bạn.
	Thông báo nhận được từ các bên thứ ba tin cậy như VNCERT/CC.
Một hoặc nhiều hệ thống hoặc dịch vụ CNTT không hoạt động như mong đợi.	Một hoặc nhiều hệ thống hoặc dịch vụ CNTT có thể ngừng hoạt động hoặc có thể không hoạt động như mong đợi và không có nguyên nhân dễ nhận biết (chẳng hạn như nâng cấp hoặc ngừng hoạt động đã lên kế hoạch).
	Chứng chỉ SSL không hợp lệ; ví dụ: khách hàng phàn nàn rằng trang web có liên kết bị hỏng.
Hoạt động bất thường	Nhân viên quan sát thấy một số lượng lớn email bị trả lại có chứa nội dung đáng ngờ hoặc không mong muốn; hoặc có sự thay đổi đáng kể về lưu lượng truy cập mạng mà không có nguyên nhân rõ ràng.
	Nhật ký mạng hoặc ứng dụng cho thấy nhiều đăng nhập không thành công từ các hệ thống từ xa không quen thuộc, chẳng hạn như các địa điểm ở nước ngoài.
	Cảnh báo chống vi-rút – thông báo đã phát hiện hoạt động hoặc tệp đáng ngờ trên mạng của bạn, cần phân tích và khắc phục.
	Tài khoản dịch vụ hoặc quản trị viên sửa đổi quyền; tài khoản quản trị viên thêm người dùng tiêu chuẩn vào các nhóm; tài khoản dịch vụ đăng nhập vào một máy trạm.
	Quản trị viên hệ thống nhận thấy tên tệp có các ký tự bất thường hoặc các tệp được mong đợi không còn hiển thị trên mạng.

Bảng 23: Các Chỉ báo Phát hiện Sự cố

Phụ lục H. Tài nguyên với phần mềm tống tiền

Tài nguyên	Nội dung
No More Ransom (https://www.nomoreransom.org/en/index.html)	No More Ransom là một trang web lưu trữ các công cụ giải mã đã biết cho các biến thể ransomware phổ biến. Dự án này là một sáng kiến của Đơn vị Tội phạm Công nghệ Cao Quốc gia của Cảnh sát Hà Lan, Trung tâm Tội phạm Mạng Châu Âu của Europol, Kaspersky và McAffee.
Trung tâm ATTTM Úc (https://www.cyber.gov.au/) **Trung tâm ATTTM Quốc gia Vương Quốc Anh** (https://www.ncsc.gov.uk/) **Cơ quan ATTTM và An toàn hạ tầng Hoa Kỳ** (https://www.cisa.gov/) **Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ** (https://www.nist.gov/) **Cục An toàn thông tin** (https://ais.gov.vn/) **Viện Công nghệ SANS** (https://www.sans.org/) **CyberCX** (https://cybercx.com.au/)	Các trung tâm an toàn mạng của các quốc gia thường xuyên đăng các tư vấn và ấn phẩm chi tiết về các nhóm tấn công ransomware có thể hỗ trợ ứng cứu cho cuộc tấn công bằng mã độc tống tiền.

Bảng 24: Tài nguyên với phần mềm tống tiền

Phụ lục I. Hướng dẫn Điều tra Chuyên sâu

1. Lĩnh vực điều tra

Hành động	Nội dung
Xác định (các) hệ thống bị xâm phạm	Tổng hợp danh sách các hệ thống bị xâm phạm dựa trên điều tra của đội ứng cứu sự cố.

Xác định quy mô và phạm vi của sự cố	Xem xét và đánh giá:
	• Phương thức xâm nhập ban đầu là gì?
	  ○ Phương thức này đã được vá/bảo vệ để tránh khai thác thêm chưa?
	  ○ Liệu phương thức xâm nhập này có thể hoặc dễ được nhân rộng không?

2. Động cơ của kẻ tấn công

Hiểu được động cơ của kẻ tấn công đằng sau một cuộc tấn công là rất quan trọng để định hướng cho ứng phó. Trong quá trình điều tra, đội UCSC nên xem xét động cơ đằng sau cuộc tấn công, chẳng hạn như::

- Mục đích tài chính.
- Mục đích chính trị.
- Mục đích quân sự.
- Chủ nghĩa Hacktivisim.

Hiểu được động cơ hoặc ít nhất là xác định các động cơ tiềm ẩn đằng sau các cuộc tấn công ATTTM có thể hỗ trợ đội UCSC hiểu được các rủi ro liên quan và quyết định các bước tiếp theo.

3. Điều tra liên kết độc hại:

Việc điều tra các liên kết độc hại trong email lừa đảo là một bước điều tra quan trọng giúp cung cấp thông tin rõ ràng về tác động tiềm ẩn, từ đó đưa ra các bước xóa bỏ và phục hồi thích hợp.

Nếu liên kết bị nghi ngờ là độc hại, đội UCSC nên xem xét các câu hỏi dưới đây:

- Phân tích động liên kết độc hại có nên diễn ra trong môi trường sandbox không?
- Có thể sử dụng các công cụ điều tra của bên thứ ba để hỗ trợ quá trình phân tích không?
- Đội UCSC có môi trường phù hợp để xem xét các liên kết độc hại không?

Nếu đội UCSC không có đủ khả năng, hãy tham khảo **Phụ lục H - Đánh giá năng lực** và cân nhắc việc yêu cầu hỗ trợ của bên thứ ba.

Sao chép liên kết:

Để điều tra một liên kết độc hại, trước tiên liên kết đó cần phải được sao chép. Xem lời khuyên dưới đây về cách thực hiện bước này:

(Nếu có thể) Sử dụng độc hại của việc tách URL/Siêu liên kết

Kẻ tấn công có thể chia nhỏ một liên kết thành hai phần để đánh lừa người dùng. Khi bạn cố gắng sao chép và dán liên kết, chỉ có một phần (thường là phần không gây hại) được hiển thị. Để phát hiện điều này, bạn cần kiểm tra mã nguồn của email, từ đó có thể xem xét và chọn được toàn bộ liên kết.

(Nếu có thể) Liên kết độc hại trong hình ảnh

Các liên kết độc hại có thể được nhúng trong hình ảnh để lừa người dùng tương tác và thực thi liên kết đó. Trong khi việc xem xét metadata là cách thức tốt nhất để thu thập liên kết đã được nhúng đó, liên kết cũng có thể được chọn khi di chuột qua hoặc nhấp chuột phải vào hình ảnh. Nếu nghi ngờ nó điều hướng đến một trang web độc hại, đội UCSC nên thận trọng khi sao chép liên kết.

Phân tích liên kết

Khi sao chép xong liên kết độc hại, có thể dùng các nền tảng mã nguồn mở khác nhau để phân tích thêm. Mục tiêu chính của bước điều tra này là xác định mục đích và phạm vi của liên kết độc hại.

Liên kết nên được xem xét trong môi trường sandbox và/hoặc ứng dụng web proxy..

Ứng dụng web proxy:

Sau khi sao chép xong liên kết, đội UCSC nên sử dụng một ứng dụng web proxy để xem xét liên kết đó, ví dụ Urlscan hoặc các ứng dụng web proxy ưa thích khác. Đội UCSC nên xem xét và chọn các công cụ liên quan phù hợp nhất với môi trường làm việc, ngưỡng rủi ro và ngân sách của đội.

Các ứng dụng web như Urlscan sẽ cung cấp một môi trường sandbox chụp màn hình trực tiếp.

Nếu Urlscan được chọn cho mục đích này, hãy truy cập vào trang trang web và dán liên kết độc hại vào thanh tìm kiếm (chọn Private Scan – quét riêng tư).

Sử dụng ứng dụng web proxy này, đội UCSC có thể phát hiện:

- Địa chỉ IP của trang web
- Trạng thái HTTP
- Các chuyển hướng
- Các liên kết và hành vi
- Các chỉ báo
- Các liên kết tương tự
- Cấu trúc của trang web (DOM)
- Nội dung và API
- Ảnh chụp màn hình của trang tại thời điểm quét
- Xác định của Urlscan về trang web cụ thể
- Kết quả từ Google Safe Browsing và Bản ghi DNS
- Các công nghệ được sử dụng trên trang web

Tất cả thông tin trên sẽ được tổng hợp với điều tra địa chỉ IP, hoạt động của kẻ tấn công đã biết và các thực hành điều tra khác để xác định mục đích thực sự của trang web độc hại.

Thông thường, các trang web độc hại có mục đích thu thập thông tin đăng nhập hoặc tải xuống các phần mềm độc hại.

Đối với các cuộc tấn công phức tạp, đội UCSC có thể cần sử dụng các công cụ và nền tảng chuyên sâu hơn để phân tích chi tiết.

Nếu có thể, đội UCSC nên xem xét việc xem lại các Nhật ký của Proxy để tìm bằng chứng về việc truy cập vào URL lừa đảo. Sau khi xác định người dùng đã truy cập vào URL, tiếp cận để khắc phục tiềm năng bị xâm phạm.

Xem bảng dưới đây để biết những hướng dẫn điều tra hữu ích:

Tổ chức	URL
Hướng dẫn thực hành từng bước của Trung tâm ACSC Úc	Hướng dẫn từng bước (https://www.cyber.gov.au/acsc/small-and-medium-businesses/step-by-step-guides)

Tư vấn và hướng dẫn của Trung tâm NCSC Anh	Tất cả các chủ đề (https://www.ncsc.gov.uk/section/advice-guidance/all-topics)
Các ấn phẩm của CISA	Thư viện Công cộng (https://www.cisa.gov/publications-library/cybersecurity?page=0)
Các ấn phẩm của NIST	Thư viện (https://csrc.nist.gov/publications)
Mô hình tấn công MITRE ATT&CK®	MITER ATT&CK® (https://attack.mitre.org/)

Bảng 25: Đề xuất các hướng dẫn điều tra

4. Điều tra tấn công từ chối dịch vụ phân tán (DDoS)

DDoS là một loại tấn công mạng thường sử dụng mạng lưới các hệ thống bị xâm phạm để làm quá tải các trang web với các yêu cầu kết nối, khiến trang web hoặc máy chủ bị chậm lại và/hoặc ngừng hoạt động. Cuộc tấn công DDoS hạn chế tính khả dụng của tài nguyên, ngăn cản người dùng hoạt động như bình thường.

Các cuộc tấn công DDoS có thể được phân loại thành các cuộc tấn công logic hoặc các cuộc tấn công làm cạn kiệt tài nguyên

- Các cuộc tấn công logic lợi dụng các lỗ hổng bảo mật để làm máy chủ hoặc dịch vụ bị sập hoặc chậm lại, giảm đáng kể hoạt động và hiệu suất bình thường.
- Các cuộc tấn công làm cạn kiệt tài nguyên khiến tài nguyên của máy chủ hoặc mạng bị tiêu thụ quá mức, không thể phản hồi hoặc phản hồi bị giảm đáng kể.

Các cuộc tấn công DDoS có thể xảy ra như các cuộc tấn công mạng đơn lẻ do các kẻ tấn công tận dụng cơ hội hoặc các cuộc tấn công được lên kế hoạch kỹ càng. Tuy nhiên, các cuộc tấn công này cũng có thể được sử dụng cùng với các kiểu tấn công mạng khác, chẳng hạn như lan truyền các chủng phần mềm độc hại khác nhau.

Thu thập thông tin tấn công mạng DDoS:

Trong việc thực hiện phản ứng sự cố hiệu quả đối với một cuộc tấn công DDoS được báo cáo, nhóm phản ứng sự cố nên xem xét các thông tin có sẵn và đảm bảo có tầm nhìn và hiểu biết về các điểm dưới đây:

Để thực hiện ứng cứu sự cố hiệu quả với một cuộc tấn công DDoS được báo cáo, đội UCSC nên xem xét thông tin có sẵn và đảm bảo góc nhìn, hiểu biết về các điểm dưới đây:

- Kiến trúc mạng của hệ thống liên quan.
- Loại tấn công đã được báo cáo.
- Các bước giảm thiểu hiện tại đã được thực hiện.

Đội UCSC có thể nhận được báo cáo về các nghi ngờ là tấn công DDoS., có thể khgo6ng phải là tấn công mà gây ra do tải năng (ví dụ sử dụng nhiều) hoặc lỗi hệ thống chưa biết. Trong khi thu thập thông tin phù hợp về sự cố đã báo cáo, cần xác định trước tiên là một cuộc tấn công hay điều gì khác. Để làm như vậy, đội UCSC sẽ tìm cách trả lời các câu hỏi dưới đây:

- Hệ thống có đang chịu tải nặng chưa từng có trước đây không?
- Hệ thống trước đây đã từng được chuẩn hoá để thiết lập tại hoạt động bình thường chưa?
    - Nếu có tải hệ thống bình thường, thì cần so sánh với lưu lượng quan sát được ở thời điểm hiện tại.

- Cuộc tấn công được báo cáo có được cô lập với một hệ thống cụ thể hay cuộc tấn công đang lan sang các hệ thống/ứng dụng khác?
- Người báo cáo có gặp bất kỳ hoạt động đáng ngờ nào khác trên hệ thống không?
- Người báo cáo có nhận được bất kỳ yêu cầu hoặc liên lạc nào liên quan đến DDoS được báo cáo không?
  - Nếu có, những yêu cầu hoặc liên lạc này là gì?
  - Chúng đến từ ai? Đó là một tác nhân đe dọa đã biết hay chưa biết?
  - Những yêu cầu pháp lý và quy định nào có thể cần được xem xét khi liên lạc với các tác nhân đe dọa tiềm ẩn?
- Cuộc tấn công được báo cáo xảy ra vào thời gian nào?
  - Thời gian này có phản ánh thời gian thường gia tăng tải hay không?
- Có bất kỳ trường hợp nào, chẳng hạn như một sự kiện chính trị có liên quan có thể giải thích việc tăng tải không?
- Có bất kỳ sửa chữa hoặc gián đoạn dịch vụ nào đã biết có thể giải thích hoạt động bất thường không?
- Hệ thống bị ảnh hưởng có mất kết nối hoặc hoạt động với hiệu suất giảm không?

Các cân nhắc phân loại DDoS:

Sau các bước điều tra trên, đội UCSC nên xác định mức độ nghiêm trọng hiện tại của sự cố và phân loại sự cố là một trong các loại dưới đây:

- Từ chối dịch vụ hoàn toàn: dịch vụ ảnh hưởng không thể hoạt động theo mọi cách, ngăn mọi hoạt động kinh doanh thông thường.
- Từ chối dịch vụ ở mức trung bình: dịch vụ bị chậm hoặc gián đoạn.
  - Có thể duy trì hoạt động kinh doanh với dịch vụ bị gián đoạn.
- Tác động từ chối dịch vụ tối thiểu: dịch vụ bị chậm hoặc dừng.
  - Dịch vụ chậm gián đoạn
  - Ít hoặc không có tác động đến các hoạt động kinh doanh.

Điều tra địa chỉ IP:

Tùy thuộc vào mức độ phức tạp của cuộc tấn công, đội UCSC có thể xác định địa chỉ IP gây ra cuộc tấn công, sẽ cần trong giai đoạn loại bỏ. Việc sử dụng bot trên diện rộng, kết hợp với việc giả mạo địa chỉ IP trên quy mô lớn là một chiến thuật phổ biến trong các cuộc tấn công phức tạp. Thường thì điều này được thực hiện bằng cách làm giả nội dung trong tiêu đề IP với các số ngẫu nhiên để che giấu địa chỉ IP của người gửi (hoặc để khởi động một cuộc tấn công DDoS phản xạ).

Trong các trường hợp tấn công botnet, giả mạo địa chỉ IP có thể được sử dụng trên các thiết bị chủ bị xâm phạm để tránh bị phát hiện, ngăn chặn thông báo về các máy chủ bị xâm phạm và vượt qua các kịch bản lập danh sách đen các địa chỉ IP tấn công. Đội UCSC nên cố gắng theo dõi các kẻ tấn công này, thu thập:

- Địa chỉ IP.
- Định vị địa lý.
- Các nhà cung cấp mạng.

Các kẻ tấn công có thể nhanh chóng thay đổi cơ sở hạ tầng, cho phép chúng tránh các biện pháp chặn trong một số trường hợp.

Trong trường hợp các cuộc tấn công botnet phức tạp với quy mô lớn, việc theo dõi tất cả các địa chỉ IP vi phạm có thể không thực tế hoặc không hiệu quả.

Phụ lục J. Khung phân loại sự cố

Ưu tiên xử lý một sự cố là điểm quyết định quan trọng trong tiến trình ứng phó sự cố. Thay vì xử lý theo thứ tự nhận được, các sự cố cần được ưu tiên dựa trên mức độ ảnh hưởng đến doanh nghiệp, phù hợp với chính sách quản lý rủi ro tổng thể. Việc phân loại các sự cố cũng cung cấp cho các bên liên quan bên trong và bên ngoài hiểu rõ hơn về mức độ nghiêm trọng của sự cố được nhận diện.

KIẾN NGHỊ

Khung dưới đây là một ví dụ, khung này cần được sửa đổi để phản ánh quy mô của tổ chức/doanh nghiệp, cơ sở hạ tầng của nó, mức độ trưởng thành về ATTTM và khẩu vị rủi ro.

Cách sử dụng:

Khung Phân loại Sự cố được thiết kế để tạo ra một số sự cố cuối, dao động từ P4 - Sự cố Nhỏ đến P1 - Sự cố Thảm khốc. Khung ví dụ tìm cách xem xét sự cố được xác định trên 6 lĩnh vực chính:

- Pháp lý
- Hoạt động
- Tài chính
- Sức khỏe & An toàn
- Danh tiếng
- CNTT & Mạng

Bước 1: Bắt đầu với pháp lý, đội UCSC nên xem xét các tuyên bố tác động từ P4 – P1, chọn xếp hạng sự cố phù hợp nhất dựa trên mô tả. Nếu có ít thông tin, đội UCSC nên xem xét kích bản có khả năng xảy ra nhất bằng cách sử dụng thông tin có sẵn. Sau tiến trình này, đội UCSC sẽ có xếp hạng sự cố cho hạng mục Pháp lý.

Bước 2: Tiến trình tương tự nên được lặp lại trên các lĩnh vực Hoạt động, Tài chính, Sức khỏe & An toàn, Danh tiếng và CNTT & Mạng. Sau khi hoàn thành, đội UCSC sẽ có sự phân loại cho từng lĩnh vực trong 6 lĩnh vực.

Bước 3: Phân loại sự cố cao nhất hoặc phân loại có tỷ lệ xếp hạng cao nhất trong một lĩnh vực sẽ xác định xếp hạng tổng thể.

Xếp hạng sự cố phải được xem xét liên tục trong suốt quá trình ứng phó sự cố và khi phát hiện ra thông tin bổ sung có thể làm tăng hoặc giảm xếp hạng của sự cố.

Dưới đây là ví dụ về khung phân loại và ưu tiên sự cố.

Ưu tiên	*P4 – Sự cố nhỏ*	*P3 – Sự cố vừa phải*	*P2 – Sự cố lớn*	*P1 – Sự cố thảm khốc*
Ví dụ	Nhiều lần đăng nhập không thành công. Chia sẻ mật khẩu. Đã mở liên kết trang web độc hại.	Truy cập mạng trái phép. Máy tính xách tay của nhân viên bị mất/bị đánh cắp. Một thiết bị bị nhiễm phần mềm độc hại.	Truy cập mạng trong đó bất kỳ lượng thông tin cá nhân hoặc khách hàng nào cũng bị lấy cắp. Sự xâm phạm email doanh nghiệp, theo đó một tài khoản được sử dụng để phân phối các liên kết hoặc tệp đính kèm độc hại.	Tấn công ransomware trên diện rộng. Tấn công từ chối dịch vụ làm hạn chế các hoạt động kinh doanh.
Pháp lý	Các khiếu nại/sự cố riêng lẻ có thể được ban quản lý giải quyết hoặc khi có mối đe dọa về hành động pháp lý có thể được ban quản lý giải quyết. Không tuân thủ tối thiểu hoặc nhỏ với quy định. Không có tác động riêng tư.	Các khiếu nại/sự cố quan trọng có nguy cơ dẫn đến hành động pháp lý mà ban quản lý có thể giải quyết. Việc không tuân thủ dẫn đến việc bị cơ quan quản lý kiểm duyệt hoặc cảnh báo. Không có tác động riêng tư.	Vụ kiện dân sự và/hoặc cáo buộc hình sự được đưa ra chống lại tổ chức hoặc (các) nhân viên. Tiền phạt và/hoặc hình phạt từ các cơ quan quản lý. Bất kỳ thông tin cá nhân nhạy cảm nào của nhân viên, khách hàng, công chúng, v.v. đã bị truy cập hoặc lấy cắp.	Vụ kiện dân sự lớn và/hoặc cáo buộc hình sự chống lại tổ chức hoặc (các) nhân viên. Hạn chế việc ngừng hoạt động kinh doanh của cơ quan quản lý. Thông tin cá nhân nhạy cảm của nhân viên, khách hàng, công chúng, v.v. đã bị truy cập hoặc rò rỉ trên quy mô lớn.
Hoạt động	Không có tác động đáng kể đến doanh nghiệp hoặc các phản ứng hoạt động thường lệ có thể hấp thụ tác động với sự hỗ trợ của ban quản lý.	Tác động đáng kể đến doanh nghiệp yêu cầu phản hồi không thường xuyên để tiếp tục/sửa chữa các hoạt động. Tác động của sự kiện có thể được hấp thụ nhưng cần có nỗ lực quản lý đáng kể.	Các mục tiêu quan trọng của doanh nghiệp chưa đạt được nhưng tình hình hoạt động có thể phục hồi được. Mất chức năng/khả năng của doanh nghiệp.	Thất bại/gián đoạn kinh doanh nghiêm trọng có khả năng gây ra tổn thất hoặc phá sản vĩnh viễn cho toàn bộ doanh nghiệp. Sự kiện quan trọng đòi hỏi nỗ lực quản lý chuyên biệt để tránh sự sụp đổ của doanh nghiệp.

	Hoạt động kinh doanh như thường lệ (BAU – Business As Usual) bị ảnh hưởng tới 2 ngày.	BAU tác động lên tới 1 tuần.	BAU tác động 1-2 tuần.	BAU bị ảnh hưởng > 2 tuần.
Tài chính	Tác động đến chi phí hoạt động <5%.	Tác động đến chi phí hoạt động từ 5 – 15%.	Tác động đến chi phí hoạt động từ 15 – 30%.	Tác động đến chi phí hoạt động >30%.
Sức khỏe & An toàn	Cần sơ cứu.	Bất kỳ thương tích hoặc tai nạn nào dẫn đến mất hơn một ngày làm việc.	Chấn thương hoặc sự cố gây tàn tật, ví dụ như cắt cụt chi, mất vĩnh viễn chức năng cơ thể hoặc bất kỳ ảnh hưởng sức khỏe vĩnh viễn nào khác.	Tử vong một hoặc nhiều người.
Danh tiếng	Không có tác động bên ngoài hoặc sự chú ý nhỏ từ khách hàng/nhân viên.	Sự chú ý hoặc khiếu nại từ các bên liên quan chính trong nội bộ hoặc bên ngoài.	Mối quan tâm rộng rãi từ các bên liên quan chính trong nội bộ hoặc bên ngoài. Khó khăn trong việc thu hút các đối tác kinh doanh, khách hàng hoặc nhân viên mới hoặc tiềm năng do bị tổn hại về danh tiếng.	Sự phẫn nộ từ các bên liên quan chính trong nội bộ hoặc bên ngoài. Mất các đối tác kinh doanh, khách hàng hoặc nhân viên hiện tại do tổn hại về danh tiếng.
CNTT & Mạng	Không ảnh hưởng đến các ứng dụng hoặc hệ thống quan trọng. Tính khả dụng của ứng dụng hoặc hệ thống không quan trọng chỉ ảnh hưởng đến một nhân viên. Không ảnh hưởng đến tính bảo mật hoặc tính toàn vẹn của thông tin.	Tác động đến các ứng dụng hoặc hệ thống quan trọng được bản địa hóa cho một trang hoặc nhóm cụ thể. Tính khả dụng của ứng dụng hoặc hệ thống quan trọng bị ảnh hưởng cho dưới 50 nhân viên và/hoặc ít hơn 4 giờ. Tính bảo mật hoặc tính toàn vẹn của thông tin không nhạy cảm bị ảnh hưởng.	Tác động đến các ứng dụng hoặc hệ thống quan trọng liên quan đến nhiều địa điểm hoặc nhóm nhưng không phải là toàn bộ doanh nghiệp. Tính khả dụng của ứng dụng hoặc hệ thống quan trọng ảnh hưởng đến 50-500 nhân viên và/hoặc trong 4-24 giờ. Tính bảo mật hoặc tính toàn vẹn của thông tin nhạy cảm bị ảnh hưởng ở mọi quy mô.	Các ứng dụng hoặc hệ thống quan trọng đã ảnh hưởng đến toàn bộ doanh nghiệp/tổ chức. Tính khả dụng của ứng dụng hoặc hệ thống quan trọng ảnh hưởng trên 500 nhân viên và/hoặc trên 24 giờ. Tính bảo mật hoặc tính toàn vẹn của thông tin nhạy cảm bị ảnh hưởng trên quy mô lớn.

Bảng 26: Ví dụ về Khung Phân loại Sự cố

Phụ lục K. Các câu hỏi Đề xuất dành cho cấp điều hành trong Sự cố ATTTM

Phần sau đây được chuẩn bị để hỗ trợ quá trình ra quyết định. Nó cung cấp một danh sách các câu hỏi nên được hỏi trước khi tuyên bố một vụ việc.

Lãnh địa	Tuyên bố/Câu hỏi	đánh dấu
Pháp lý/Đạo đức	Vị thế pháp lý của chúng ta trong việc phản ứng với một sự cố cụ thể là gì?	
	Vị thế đạo đức của chúng ta về việc phản ứng với một số sự cố cụ thể là gì?	
	Chúng ta có hiểu các yêu cầu báo cáo pháp lý/quy định của chúng ta sau khi tuyên bố một sự cố ATTTM không?	
	Vị thế pháp lý của chúng ta trong việc tương tác với kẻ tấn công là gì?	
Truyền thông	Liên quan đến sự cố này, chúng ta muốn cách tiếp cận truyền thông trong nội bộ như thế nào?	
	Chúng ta nên tiếp cận báo cáo cho các bên liên quan bên ngoài như thế nào, chẳng hạn như với cơ quan thực thi pháp luật, Bộ Thông tin và Truyền thông?	
Năng lực kỹ thuật	Chúng ta có đủ nguồn lực để nhanh chóng ngăn chặn sự cố và khôi phục các hệ thống quan trọng không? Nhóm nội bộ của chúng ta có cần sự hỗ trợ từ bên ngoài để ứng phó với sự cố này không?	
Tài chính	Có đủ ngân sách để chi trả cho các dịch vụ ứng cứu sự cố không, ví dụ chi cho dịch vụ từ bên thứ ba không?	
	Chúng ta có bảo hiểm ATTTM không?	

Bảng 27: Câu hỏi dành cho cấp điều hành

Phụ lục L. Hướng dẫn đánh giá bên thứ ba

Cân nhắc	Câu hỏi

Phạm vi hỗ trợ	• Bản chất chính xác của sự hỗ trợ cần thiết là gì?
	  ○ Hỗ trợ từ đầu đến cuối?
	  ○ Hỗ trợ tư vấn?
	  ○ Ngăn chặn, khôi phục, tái xây dựng?

Rủi ro	• Rủi ro hoặc kết quả tiềm ẩn nếu có sự hỗ trợ từ bên thứ ba là gì?
Kết quả mong muốn	• Kết quả mong muốn từ các tiến trình ứng phó sự cố là gì? ○ Bên thứ ba có giúp đạt được kết quả mong muốn này không?
Ngân sách	• Chi phí phát sinh từ bên thứ ba có ít hơn chi phí tiềm ẩn của sự cố ATTTM nếu không được giải quyết? • Có ngân sách hiện tại cho việc ký hợp đồng với các dịch vụ của bên thứ ba không? • Những cân nhắc ngân sách nào cần được thảo luận trước khi tìm kiếm sự hỗ trợ của bên thứ ba?
Hỗ trợ và phê duyệt của lãnh đạo	• Những quy trình và thông tin nào cần được thực hiện trước khi có được sự hỗ trợ và phê duyệt của lãnh đạo? • Cấp lãnh đạo có hỗ trợ và phê duyệt việc sử dụng bên thứ ba không?
Khung thời gian	• Bên thứ ba có thể được đưa vào hỗ trợ các tiến trình ứng phó sự cố nhanh như thế nào? ○ Khung thời gian này có chập nhận được không?
Các vấn đề nhạy cảm	• Có bất kỳ mối quan ngại hoặc sự nhạy cảm nào biện minh cho quyết định không sử dụng bên thứ ba không?

Bảng 28: Hướng dẫn đánh giá của bên thứ ba

Phụ lục M. Các câu hỏi Đánh giá Hỗ trợ của Bên thứ ba

Cân nhắc	Câu hỏi
Khả năng ứng cứu sự cố	• Bên thứ ba có kinh nghiệm liên quan gì trong việc ứng phó các sự cố ATTTM tương tự? • Bên thứ ba có khả năng thể hiện nào?
Tài nguyên	• Những nguồn lực nào (nhân viên, phần cứng và phần mềm) sẽ có sẵn?
Giá cả	• Mô hình định giá có sẵn là gì? • Những gì được bao gồm trong chi phí? • Công việc được thanh toán như thế nào?
Khung thời gian	• Nếu bên thứ ba được chọn, thời gian dự kiến là bao lâu?
Cách làm việc	• Phương thức triển khai của bên thứ ba là gì (Ví dụ: Ảo/trực tiếp/kết hợp) • Các dịch vụ sẽ được cung cấp bán thời gian, toàn thời gian hay theo yêu cầu không? • Giờ hoạt động sẽ có sẵn là gì?

Bảng 29: Câu hỏi đánh giá hỗ trợ của bên thứ ba

Phụ lục N. Hướng dẫn ngăn chặn

Đội UCSC nên xem xét các biện pháp ngăn chặn dưới đây nếu thích hợp:

Hoạt động	Mô tả
Cô lập tất cả các bản sao lưu	Nếu không bị ảnh hưởng, các bản sao lưu nên được cách ly khỏi mạng và/hoặc hệ thống để ngăn chặn sự di chuyển ngang của kẻ tấn công.
Thiết lập danh sách các điểm cuối bị ảnh hưởng và các tài khoản bị xâm nhập	Từ thông tin thu thập được ở các giai đoạn trước, đội UCSC nên thiết lập một danh sách toàn bộ các điểm cuối bị ảnh hưởng và các tài khoản bị xâm phạm.
Cô lập tất cả các điểm cuối bị ảnh hưởng hoặc ngắt kết nối chúng khỏi mạng	Cách ly các điểm cuối bị ảnh hưởng có thể ngăn chặn sự di chuyển ngang tăng thêm giữa các thiết bị và việc trích xuất dữ liệu trong khi xóa bỏ mối đe dọa.
Tắt thiết bị để ngăn chặn việc mã hóa thêm	Việc tắt thiết bị có thể ngăn chặn sự di chuyển ngang tăng thêm giữa các thiết bị/máy chủ.
Tạo các quy tắc tường lửa cần thiết để chặn lưu lượng độc hại được xác định	Tạo các quy tắc tường lửa sẽ đảm bảo rằng người dùng hợp pháp có thể truy cập các dịch vụ, đồng thời bảo vệ mạng khỏi các mối đe dọa.
Vô hiệu hóa các tài khoản độc hại/bị xâm phạm	Vô hiệu hóa các tài khoản độc hại/bị xâm phạm có thể từ chối quyền truy cập và các kênh điều khiển của các kẻ tấn công.
Vô hiệu hóa/cấm theo các mã băm mã độc	Cấm theo mã băm có thể ngăn chặn các tiến trình mã độc chạy trong tương lai.

Bảng 30: Hướng dẫn ngăn chặn

Phụ lục O. Mẫu bằng chứng

Ngày, giờ và địa điểm thu thập	Được thu thập bởi	Các chi tiết của vật phẩm	Vị trí	Chi tiết
*07/12/2023 - 1743 tại cơ sở KINH DOANH	*Trưởng nhóm ứng cứu sự cố KINH DOANH Điện thoại di động: Email:	*Địa chỉ IP	*Được lưu trong bộ lưu trữ trực tuyến của DOANH NGHIỆP	*Khi điều tra sự cố ATTTM, địa chỉ IP này được xác định là đáng ngờ.

Bảng 31: Mẫu bằng chứng

Phụ lục P. Hướng dẫn Xoá bỏ

Các bước Xoá bỏ được đề xuất
Xóa sạch hệ thống bị nhiễm
Khôi phục từ bản sao lưu đã được xác thực và quét
Cài đặt các bản vá bảo mật
Loại bỏ phần mềm độc hại
Vô hiệu hóa các dịch vụ/hệ thống không sử dụng để cứng hoá (harden) hệ thống.
Đặt lại (reset) các mạng đã bị ảnh hưởng
Đặt lại (reset) các thông tin xác thực đã bị ảnh hưởng
Kích hoạt xác thực đa yếu tố trên tất cả các tài khoản
Hạn chế các đặc quyền quản trị
Thực hiện việc cứng hoá ứng dụng

Bảng 32: Các bước Xoá bỏ

KẾT THÚC TÀI LIỆU