Sổ tay Tham khảo nhanh Ứng phó Sự cố An toàn thông tin mạng

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

Đối tượng sử dụng: Thành viên Mạng lưới ứng cứu sự cố an toàn không gian mạng quốc gia Việt Nam

Tháng 1/2025

Nội dung

Tables

Giới thiệu

Sổ tay Tham khảo nhanh Ứng phó Sự cố An toàn thông tin mạng (Cyber Security Incident Quick Reference Playbook) này nhằm hỗ trợ các chuyên gia ứng phó nhanh và hiệu quả đối với các sự cố an toàn thông tin mạng nghiêm trọng hoặc rất nghiêm trọng, sẽ được sử dụng cùng với Quy trình ứng cứu sự cố trong dự án này, dành cho các thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia.

Tài liệu này không phải là hướng dẫn kỹ thuật.

1 Cách sử dụng Sổ tay

Các sự cố không gian mạng cần được ứng phó phù hợp tùy vào mức độ ưu tiên của sự cố. Sự cố an toàn thông tin mạng (sau đây gọi tắt là ATTTM) nghiêm trọng sẽ cần sử dụng tài liệu này. Các sự cố nhỏ sẽ được giải quyết bằng các quy trình thông thường. Lãnh đạo cấp cao nên:

1. Đặt các câu hỏi cho nhóm ứng phó sự cố trong Giai đoạn Chuẩn bị theo bảng **Các câu hỏi trước và trong sự cố an toàn thông tin mạng** để giúp hiểu rõ các nghĩa vụ và trách nhiệm của nhóm trong khi xử lý sự cố.
2. Trong khi triển khai ứng cứu sự cố, hãy làm theo **Danh sách kiểm tra ứng cứu sự cố an toàn thông tin mạng,** và bảng **Các câu hỏi trước và trong sự cố an toàn thông tin mạng".**

2 Danh sách kiểm tra (checklist) ứng cứu sự cố

Các bảng bên dưới đây là danh sách các hoạt động chính giúp theo dõi hiệu quả hiệu quả các nỗ lực ứng cứu sự cố của Đội ứng cứu sự cố.

Phát hiện & Phân tích		
Nhiệm vụ	**Người chịu trách nhiệm**	**Hoàn thành**
Phân loại và Xác định		
Theo dõi nguồn gốc của sự cố, xác minh tính hợp lệ của sự cố.	<nhập vị trí liên quan>	☐
Phân tích tất cả các tài sản có thể bị ảnh hưởng. Đánh giá tác động tiềm tàng của sự cố.	<nhập vị trí liên quan>	☐
Đánh giá tác động và mức độ nghiêm trọng, xem xét các hệ thống bị ảnh hưởng và các dữ liệu có rủi ro.	<nhập vị trí liên quan>	☐
Phân phối đến các lãnh đạo có liên quan trong nội bộ (tối đa trong 2 giờ). Tiếp tục cập nhật cho đến khi xác định được mức độ ưu tiên.	<nhập vị trí liên quan>	☐
Điểm quyết định 1: Xác định và ưu tiên sự cố ATTTM, sử dụng ma trận Phân loại **(xem Phụ lục A: Phân loại sự cố ưu tiên ATTTM)**	<nhập vị trí liên quan>	☐
Tiếp tục giám sát các nhật ký liên quan và các chỉ báo từ hệ thống Cyber Threat Intelligence (CTI) để đánh giá lại mức độ nghiêm trọng thực tế.	<nhập vị trí liên quan>	☐

<table>
<tr><th colspan="5">Tăng cấp và truyền thông</th></tr>
<tr><td colspan="3">Tuyên bố sự cố ATTT, thông báo cho nhóm lãnh đạo điều hành và các thành viên đội ứng cứu sự cố và kỹ thuật liên quan (xem Phụ lục B: Mẫu truyền thông).</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td colspan="3">Chuyển liên lạc sang kênh liên lạc dùng riêng.</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td rowspan="6">Thông báo cho các bên liên quan chính</td><td>Cơ quan điều phối quốc gia về sự cố an toàn thông tin VNCERT/CC</td><td>☐</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td>Khách hang</td><td>☐</td><td rowspan="5"><nhập vị trí liên quan></td><td rowspan="5">☐</td></tr>
<tr><td>Nhà thầu</td><td>☐</td></tr>
<tr><td>Cơ quan nhà nước</td><td>☐</td></tr>
<tr><td>Nhà cung cấp bảo hiểm mạng</td><td>☐</td></tr>
<tr><td>Phương tiện truyền thông đại chúng</td><td>☐</td></tr>
<tr><th colspan="5">Ngăn chặn, Loại bỏ & Phục hồi</th></tr>
<tr><th colspan="3">Nhiệm vụ</th><th>Người chịu trách nhiệm</th><th>Hoàn thành</th></tr>
<tr><th colspan="5">Các Ứng phó Ban đầu</th></tr>
<tr><td colspan="3">Thu thập và bảo quản bằng chứng số của các hệ thống bị ảnh hưởng. Ghi lại tất cả các hoạt động đã thực hiện.</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td colspan="3">Điều phối đội ứng cứu sự cố thực hiện ứng phó sự cố.</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td colspan="3">Điều phối và truyền thông việc xử lý sự cố. Thiết lập tiến trình cập nhật với đội ứng cứu sự cố. Nếu cần, có thể sử dụng Phụ lục C: Mẫu báo cáo tình huống.</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td colspan="3">Xác định xem có cần chuyên gia về vấn đề này hay không. Bố trí thêm những người liên quan nếu cần.</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td colspan="3">Điểm Quyết định 2: Nếu có liên quan, xác định việc có đưa ra quyết định trả tiền chuộc hay không (tham khảo Phụ lục D: Tiến trình Ra quyết định về Ransomware).</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td colspan="3">Lập kế hoạch và điều phối các hoạt động ngăn chặn sự cố, bao gồm:
<table>
<tr><th>Xác định và cô lập các hệ thống bị ảnh hưởng</th><th>Chọn</th></tr>
<tr><td>Loại bỏ quyền truy cập đã bị xâm phạm</td><td>☐</td></tr>
<tr><td>Điều tra và lập danh mục tất cả các tài sản có khả năng bị xâm phạm. Xác định mô hình lây lan.</td><td>☐</td></tr>
<tr><td>Phân tích mọi mã độc nếu có, thu thập thông tin.</td><td>☐</td></tr>
<tr><td>Kiểm tra các chỉ báo xâm nhập khác và thông tin tình báo về mối đe dọa.</td><td>☐</td></tr>
<tr><td>Xác nhận việc ngăn chặn.</td><td>☐</td></tr>
</table>
Bảng 1: Xác định và cách ly các hệ thống bị ảnh hưởng</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
</table>

<table>
<tr><td>Đánh giá tất cả thông tin đã thu thập, nắm bắt các việc sau:
<table>
<tr><th>Phương thức lây nhiễm ban đầu</th><th>Chọn</th></tr>
<tr><td>Khai thác điểm yếu hoặc lỗ hổng bảo mật</td><td>☐</td></tr>
<tr><td>Các tài sản được nhắm đến</td><td>☐</td></tr>
<tr><td>Các tài sản bị xâm phạm.</td><td>☐</td></tr>
<tr><td>Loại và khả năng của phần mềm độc hại.</td><td>☐</td></tr>
<tr><td>Thông tin bổ sung hoặc các tài sản có khả năng bị xâm phạm.</td><td>☐</td></tr>
<tr><td>Các lệnh thay thế hoặc cửa hậu có sẵn cho kẻ tấn công.</td><td>☐</td></tr>
</table>
Bảng 2: Các phương thức lây nhiễm ban đầu</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td>Lập kế hoạch và điều phối các hoạt động loại bỏ sự cố:
<table>
<tr><th>Xác định các kỹ thuật và tiến trình của kẻ tấn công</th><th>Chọn</th></tr>
<tr><td>Quét các bản sao lưu trước đó để tìm mã độc/các tiến trình không hoạt động</td><td>☐</td></tr>
<tr><td>Điều phối kế hoạch loại bỏ sự cố bằng cách sử dụng thông tin thu thập được.</td><td>☐</td></tr>
<tr><td>Xác nhận việc loại bỏ thành công.</td><td>☐</td></tr>
</table>
Bảng 3: Kỹ thuật và tiến trình của kẻ tấn công</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td>Lập kế hoạch và điều phối các hoạt động khôi phục sự cố:
<table>
<tr><th>Khôi phục tài sản/hệ thống từ các bản sao lưu tin cậy</th><th>Chọn</th></tr>
<tr><td>Kết nối lại có tính hệ thống các tài sản/hệ thống đã khôi phục vào mạng</td><td>☐</td></tr>
<tr><td>Cài đặt lại các máy bị xâm nhập.</td><td>☐</td></tr>
<tr><td>Xem xét và loại bỏ các thay đổi cấu hình tạm thời</td><td>☐</td></tr>
</table>
Bảng 4: Khôi phục tài sản và hệ thống</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td colspan="3">Họp rút kinh nghiệm ngay</td></tr>
<tr><td>Chính thức dừng quy trình ứng cứu sự cố an toàn thông tin mạng.</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td>Tổ chức ngay một cuộc họp với các thành viên đội ứng cứu kỹ thuật tham gia trực tiếp ngay sau khi khôi phục, tham khảo Phụ lục E: Mẫu Phân tích Đánh giá Sau Sự cố.</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td>Thiết lập, ban hành và duy trì các hành động cần thiết hoặc đã thực hiện.</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
<tr><td>Thực hiện tất cả các việc còn tồn đọng nêu ra trong cuộc họp.</td><td><nhập vị trí liên quan></td><td>☐</td></tr>
</table>

Bảng 5: Danh sách kiểm tra ứng cứu sự cố ATTTM

3 Các câu hỏi trước và trong sự cố ATTTM

Bảng bên dưới hỗ trợ tiến trình ra quyết định với các câu hỏi hướng dẫn cho tiến trình thu thập thông tin.

3.1 Chuẩn bị

	Lĩnh vực	Tuyên bố /Câu hỏi	Chọn
Chuẩn bị	Pháp lý/Đạo đức	1. Cục An toàn thông tin không khuyến khích thanh toán tiền chuộc cho những kẻ tấn công ransomware vì những lý do sau: • Khuyến khích hoạt động tội phạm: Trả tiền chuộc khuyến khích những kẻ tấn công tiếp tục thực hiện các cuộc tấn công tương tự, vì họ coi đó là một cách dễ dàng để kiếm tiền. • Không đảm bảo phục hồi dữ liệu: Ngay cả khi tiền chuộc được chuyển, không có gì đảm bảo rằng những kẻ tấn công sẽ cung cấp khóa giải mã và trả lại dữ liệu cho nạn nhân. • Hỗ trợ các hoạt động bất hợp pháp: Trả tiền chuộc cho phép những kẻ tấn công tiếp tục các hoạt động bất hợp pháp của họ, gây hại cho nhiều cá nhân và tổ chức khác. Thay vì chuyển tiền chuộc, Cục An toàn thông tin khuyến nghị thực hiện: • Phòng ngừa các cuộc tấn công ransomware • Báo cáo khi bị tấn công ransomware • Khôi phục dữ liệu từ bản sao lưu	☐
	Quản lý	2. Các quyết định cho nhân viên trong sự cố sẽ được ghi lại như thế nào?	☐
		3. Chúng ta đã tập hợp và thực hiện các nghĩa vụ phải thực hiện theo hợp đồng cho bên thứ ba để báo cáo sự cố tiềm ẩn chưa?	☐
	Khả năng kỹ thuật	4. Khả năng phát hiện cuộc tấn công trước khi nó xảy ra là gì và khả năng đó có nguồn lực không?	☐
		5. Chúng ta có hiểu rõ về tính thường xuyên trong các lần kiểm tra sao lưu toàn đầy đủ và Kế hoạch Khôi phục Thảm họa (DRP)/Kế hoạch Hoạt động Liên tục (BCP) được thực hiện không? Xác nhận các chức năng của tổ chức khi dựa vào BCP.	☐
		6. Chúng ta có nhận thức và quyền truy cập vào danh sách các tài sản quan trọng không? Chúng ta có thể đánh giá mức độ quan trọng của hệ thống dựa trên phân loại hệ thống thông tin không?	☐
	Yêu cầu Quy định	7. Chiến lược và kế hoạch ATTTM có mạch lạc và đủ nguồn lực không? Chúng ta có thể so sánh với các bên tương đồng với mình không?	☐
		8. Chúng ta có đang xây dựng năng lực và ngày càng trưởng thành hơn trong vị thế an toàn mạng của mình không? Chúng ta có đang giảm thiểu các rủi ro của chính mình qua việc đầu tư hợp lý và mô hình đảm bảo an toàn thông tin bền vững không?	☐
		9. Kế hoạch ứng cứu sự cố của chúng ta có đủ chi tiết, dễ sử dụng và được diễn tập trước hay không?	☐
	Phạm vi Bảo hiểm (nếu có liên quan)	10. Chúng ta có đáp ứng được các yêu cầu của hợp đồng bảo hiểm liên quan đến năng lực và đầu tư an toàn mạng hay không? Chúng ta có đang thực hiện các biện pháp hợp lý để ngăn chặn tấn công hoặc tác động có thể xảy ra để đảm bảo chúng ta không bị xem là không tuân thủ hay không?	☐

	Điều phối các bên liên quan	11. Chúng ta có mô hình RACI rõ ràng và được thống nhất cho từng khía cạnh ứng cứu sự cố trong trường hợp ransomware không?	☐
		12. Mỗi giai đoạn của kế hoạch ứng cứu sự cố có được sắp xếp hợp lý để đảm bảo đã thu thập đủ thông tin và cân nhắc đến việc giao tiếp với các bên liên quan không?	☐
		13. Chúng ta sẽ liên lạc như thế nào trong trường hợp hệ thống chính của chúng ta không khả dụng hoặc bị kẻ tấn công thấy được?	☐
		14. Chúng ta có danh sách những người cần thông báo về sự cố cụ thể hay không và theo thứ tự nào? (Ví dụ: Cơ quan quản lý, Khách hàng, bên thứ ba, công ty bảo hiểm, công chúng).	☐
		15. Nhóm truyền thông của chúng ta có đủ hiểu biết về kỹ thuật để truyền thông hiệu quả không? Chúng ta có hiểu cần hỗ trợ bên ngoài nào không và có thể tạo trước các bản truyền thông nào với thông tin đầu vào từ nhóm kỹ thuật trong quá trình xảy ra sự cố khi cần không? Nhóm có khả năng bị quá tải do khối lượng thông tin liên lạc cần thiết cho một sự cố ransomware nghiêm trọng hay không?	☐

Bảng 6: Preparation checklist/ Danh sách kiểm tra chuẩn bị

3.2 Phát hiện và phân tích

	Lĩnh vực	Câu hỏi	Chọn
Phát hiện	Tác động ban đầu đến hoạt động	16. Chúng tà có thể tiếp tục cung cấp những dịch vụ nào trong hoàn cảnh hiện tại?	☐
		17. Tình hình sắp tới có thể tệ hơn hay cải thiện hơn? Ước tính thời gian phục hồi một phần hay toàn bộ?	☐
		18. Các nỗ lực khắc phục và khôi phục sẽ tốn bao nhiêu tiền và mất bao lâu?	☐
	Điều tra Sự cố	19. Phương pháp xâm nhập vào mạng có do lỗi hoặc sơ suất của chúng ta hay không?	☐
		20. Kẻ tấn công đã có được quyền truy cập vào đâu, có vào các hệ thống và dữ liệu quan trọng nhất của chúng ta hay không?	☐
Phân tích	Phản ứng kỹ thuật	21. Chúng ta có đủ nguồn lực để nhanh chóng ngăn chặn tấn công và khôi phục các hệ thống quan trọng không? Đội ngũ nội bộ của chúng ta có cần hỗ trợ từ bên ngoài để ứng phó với sự cố này hay không?	☐
		22. Rủi ro của các hành động cụ thể nhằm khôi phục các chức năng hoạt động là gì, vì chúng liên quan đến sức khỏe và an toàn, bảo đảm an toàn rộng hơn và có thể mất thêm dữ liệu?	☐
	Giao tiếp với các bên liên quan	23. Chúng ta có biết các bên liên quan yêu cầu cập nhật thường xuyên như thế nào và chúng ta đã cập nhật phù hợp chưa?	☐
		24. Truyền thông của chúng ta có phù hợp với những nỗ lực đang thực hiện để quản lý cuộc tấn công và thể thu hút kẻ tấn công hay không?	☐

Bảng 7: Danh sách kiểm tra phát hiện & phân tích

3.3 Ngăn chặn, Loại bỏ & Khôi phục

	Lĩnh vực	Câu hỏi	Chọn
Ngăn chặn	Hồ sơ kẻ tấn công, Tác động duy trì hoạt động và/hoặc tống tiền	25. Chúng ta biết gì về kẻ tấn công?	☐
		26. Họ có hồ sơ ghi nhận về khả năng sẵn sàng và có thể khôi phục các hệ thống hoặc dữ liệu hay không?	☐
		27. Ví dụ nếu như có yêu cầu liên hệ với kẻ tấn công để thu thập thêm thông tin về động cơ của họ, thì người đàm phán của chúng ta đã chuẩn bị những nội dung gì để chia sẻ?	☐
	Phạm vi bảo hiểm (nếu có liên quan)	28. Công ty bảo hiểm của chúng ta đã phản hồi liên lạc của chúng ta và đưa ra thông tin rõ ràng về những chi phí họ sẵn sàng chi trả trong trường hợp này chưa?	☐
	Yêu cầu quy định	29. Chúng ta đã cập nhật các cơ quan quản lý theo yêu cầu chưa và họ phản hồi như thế nào?	☐
Khôi phục	Cập nhật cho pháp lý	30. Chúng ta đã cập nhật cho tư vấn pháp lý của mình về bản chất của cuộc tấn công này và thủ phạm của nó chưa?	☐
		31. Phương pháp/nền tảng của chúng ta để ghi lại các quyết định được đưa ra trong sự cố này là gì và cần có các chi tiết nào? Nhân viên của chúng ta có được bảo vệ bởi bồi thường nghề nghiệp đối với những quyết định họ đưa ra hay không?	☐
	Thiệt hại về danh tiếng	32. Phản ứng của các bên liên quan chính đối với vụ việc là gì?	☐

Bảng 8: Danh sách kiểm tra ngăn chặn, loại bỏ & khôi phục

3.4 Hoạt động Sau Sự cố

	Lĩnh vực	Câu hỏi	Chọn
Hoạt động Sau Sự cố	Dòng thời gian và Tài liệu	33. Việc gì xảy ra và vào thời gian nào?	☐
		34. Mọi quyết định của nhân viên đội ứng cứu sự cố có được ghi chép đầy đủ không?	☐
	Truyền thông và Ra quyết định	35. Tất cả các tiến trình được tuân theo ở đâu và chúng phù hợp để quản lý sự cố ở đâu?	☐
		36. Thông tin có được truyền đạt có kịp thời và giúp đưa ra quyết định hiệu quả hay không?	☐
	Cải tiến Ứng cứu sự cố Tương lai	37. Kế hoạch hành động nhằm cải thiện khả năng ứng phó sự cố đã được xây dựng chưa?	☐
		38. Những hành động nào đã được thực hiện để ngăn chặn sự cố tương tự xảy ra trong tương lai? (Bao gồm các quy trình và công nghệ)	☐

Bảng 9: Danh sách kiểm tra hoạt động sau sự cố

Phụ lục A: Phân loại Sự cố Ưu tiên về ATTTM

Ma trận phân loại sự cố ưu tiên về ATTTM sẽ phân loại các sự cố ATTTM như bên dưới, trong đó có các định nghĩa hỗ trợ về tác động đến hoạt động, khả năng khôi phục và hậu quả của sự cố.

		Tác động đến Hoạt động			
		Cao	**Trung bình**	**Thấp**	**Khôngkhôi**
Khả năng khôi phục	**Không thể khôi phục**	***SP1*** Hậu quả cực kỳ nghiêm trọng	***SP1*** Hậu quả nghiêm trọng	***SP2*** Hậu quả trung bình	***SP3*** Hậu quả nhỏ
	Kéo dài	***SP1*** Hậu quả cực kỳ nghiêm trọng	***SP1*** Hậu quả nghiêm trọng	***SP2*** Hậu quả trung bình	***SP3*** Hậu quả nhỏ
	Cần bổ sung	***SP1*** Hậu quả nghiêm trọng	***SP2*** Hậu quả trung bình	***SP3*** Hậu quả nhỏ	***SP4*** Hậu quả không đáng kể
	Thông thường	***SP2*** Hậu quả trung bình	***SP3*** Hậu quả nhỏ	***SP3*** Hậu quả nhỏ	***SP4*** Hậu quả không đáng kể

Bảng 10: Ma trận phân loại sự cố ưu tiên về an toàn thông tin mạng

Các Hành động của ma trận ưu tiên về ATTTM	
SP1-SP2	Cần phải hành động ngay lập tức để ngăn chặn và giảm thiểu. Cần kích hoạt Quy trình ứng phó sự cố ATTTM.
SP3-SP4	Sự cố ATTTM có thể được quản lý và khắc phục thông qua các quy trình hoạt động/kinh doanh thông thường.

Bảng 11: Các hành động theo ma trận ưu tiên an toàn thông tin mạng

Các định nghĩa ma trận ưu tiên về ATTTM	
Tính Bảo mật	Hạn chế quyền truy cập và tiết lộ thông tin, bao gồm các biện pháp bảo vệ quyền riêng tư cá nhân và thông tin độc quyền.
Tính Toàn vẹn	Các kiểm soát an toàn bảo vệ thông tin tránh bị tạo lập, sửa đổi hoặc xóa bởi các bên trái phép.
Tính Khả dụng	Các quy trình đảm bảo người dùng được ủy quyền có thể truy cập mạng, hệ thống và ứng dụng một cách đáng tin cậy khi được yêu cầu.

Tác động đến Hoạt động	Các loại Tác động đến Hoạt động được đề cập trong Ma trận Ưu tiên về ATTTM như sau: • **Không**: Không ảnh hưởng đến khả năng của nạn nhân trong việc cung cấp tất cả các dịch vụ hoặc thực hiện các nhiệm vụ quan trọng đối với /với tất cả người dùng. • **Thấp**: Ảnh hưởng tối thiểu. Nạn nhân vẫn có thể cung cấp tất cả các dịch vụ quan trọng hoặc thực hiện các nhiệm vụ quan trọng cho/với tất cả người dùng nhưng đã mất hiệu quả. • **Trung bình**: Nạn nhân đã mất khả năng cung cấp dịch vụ quan trọng hoặc thực hiện các nhiệm vụ quan trọng cho/với một nhóm nhỏ người dùng hệ thống. • **Cao**: Nạn nhân không còn có thể cung cấp một số dịch vụ quan trọng hoặc thực hiện các nhiệm vụ quan trọng cho/với bất kỳ người dùng hoặc khách hàng nào của mình.
Khả năng Phục hồi	Khả năng Phục hồi đề cập đến khả năng nạn nhân quay lại hoặc tiếp tục hoạt động kinh doanh của mình. Các loại khả năng phục hồi được đề cập trong Ma trận Ưu tiên như sau: • **Thông thường**: Thời gian phục hồi có thể dự đoán được với các nguồn lực hiện có. • **Được bổ sung**: Thời gian phục hồi có thể dự đoán được với các nguồn lực bổ sung. • **Kéo dài**: Thời gian phục hồi không thể dự đoán được; cần có thêm nguồn lực và hỗ trợ chuyên gia bên ngoài. • **Không thể phục hồi**: Việc phục hồi từ sự cố là không thể hoặc tốn kém quá mức (ví dụ: dữ liệu nhạy cảm bị đánh cắp và đăng công khai); tiến hành điều tra.
Incident Consequence Hậu quả của Sự cố	Hậu quả của sự cố là mức độ tiềm ẩn mà sự cố an toàn thông tin mạng có thể gây ra. Các loại hậu quả gồm: • Tài chính • Con người • Năng suất • Uy tín • Pháp lý và Tuân thủ

Bảng 12: Định nghĩa ma trận ưu tiên an toàn thông tin mạng

Phụ lục B: Các mẫu thông báo

Các mẫu thông báo bên dưới có thể điều chỉnh để sử dụng khi cần để giao tiếp với các bên liên quan bên trong và bên ngoài trong sự cố ATTTM. Tất cả các thông tin liên lạc phải được thực hiện bởi đại diện ủy quyền của tổ chức, người quản lý sự cố hoặc nhân viên truyền thông khủng hoảng. Danh sách các đại diện được ủy quyền của tổ chức để gửi thông tin liên lạc đến các nhóm / các bên liên quan cụ thể nên được hoàn thiện theo bên dưới:

Nhóm liên quan	Đại diện Uỷ quyền
Nhân viên của Tổ chức bị ảnh hưởng	<nhập đại diện ủy quyền>
Các Bộ khác	<nhập đại diện ủy quyền>
Truyền thông/Công chúng	<nhập đại diện ủy quyền>

Bảng 13: Mẫu truyền thông cho các bên liên quan

Các mẫu dưới đây được thiết kế để sử dụng thực tế trong quá trình ứng phó, từ thông tin ban đầu đến các cập nhật thường xuyên. Các mẫu dưới đây chỉ là hướng dẫn - email nên được soạn thảo mới.

Email 1: Sự cố an toàn thông tin thảm khốc

Từ: <Đầu mối UCSC>
Đến: Các nhân viên có liên quan
Chủ đề: QUAN TRỌNG: Sự cố an toàn thông tin mạng

Các đồng nghiệp thân mến,

Đội ứng cứu sự cố được cảnh báo một sự cố an toàn thông tin mạng đã xác nhận.
Tất cả thông tin mà chúng tôi biết được trình bày dưới đây.
Chúng tôi sẽ cập nhật thông tin về sự cố hàng ngày vào lúc <**nhập thời gian**> cho <n**hập khoảng thời gian**> kế tiếp.

Điều gì đang xảy ra?
Vào ngày <**nhập ngày**>, đội UCSC đã nhận được thông tin về sự cố bảo mật ảnh hưởng đến <**nạn nhân và các dịch vụ/hệ thống**>.
Chúng tôi đã xác định rằng < các tác động đã biết được đồng ý truyền đạt cho nhân viên, ví dụ các hệ thống chứa thông tin của người dùng đã bị xâm phạm>. Chúng tôi vẫn đang đánh giá tác động rộng hơn đối với các hệ thống và thông tin.

Chúng ta đang làm gì?
Đội ứng cứu sự cố đã bắt đầu các hoạt động ứng phó với sự hỗ trợ từ <n**hập tên đối tác, ví dụ: công ty điều tra số, cảnh sát, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam**>. Ưu tiên của chúng ta là đưa hệ thống <**nạn nhân**> quay trở lại hoạt động càng nhanh càng tốt.

Những gì chúng tôi cần từ bạn
Đội UCSC yêu cầu bạn không thảo luận về sự cố an toàn thông tin với bất kỳ bên ngoài nào. Mọi thông tin liên lạc nào với các bên liên quan bên ngoài, bao gồm cả công chúng, sẽ được điều phối bởi <đầu mối truyền thông khủng hoảng>.

Nếu bạn có bất kỳ câu hỏi hoặc thông tin nào giúp ích cho việc ứng phó sự cố, vui lòng liên hệ <**nhập tên đội trưởng đội UCSC**>.

Nếu bạn đang đảm nhận vai trò với công chúng, bạn sẽ nhận được hướng dẫn riêng.

Trân trọng.
<nhập chức danh hoặc tên>

Bảng 14: Mẫu email về sự cố thảm khốc

Email 2: Thông báo của Bộ đến Khách hàng hoặc Công dân bị ảnh hưởng

Từ: <Đầu mối liên lạc/xử lý khủng hoảng truyền thông>
Đến: Các liên hệ chính
Chủ đề: Thông báo Sự cố an toàn thông tin mạng

Kính gửi <**nhập liên hệ khách hàng/công dân**>,

<**Tên tổ chức**> thông báo về sự cố an toàn thông tin đang ảnh hưởng đến khả năng cung cấp dịch vụ của <**nạn nhân**>.
Thông tin của chúng tôi đang có như bên dưới đây:

Điều gì đang xảy ra?
Vào ngày <nhập ngày>, chúng tôi đã biết được sự cố an toàn thông tin đang ảnh hưởng đến <dịch vụ/hệ thống> của mình.

Chúng tôi đã xác định rằng <**nêu các tác động đã đồng ý thông báo, ví dụ các hệ thống chứa thông tin cá nhân đã bị xâm phạm**>. Chúng tôi vẫn đang đánh giá tác động rộng hơn đối với các hệ thống và thông tin công dân của mình.

Chúng tôi đang làm gì?

Chúng tôi đã thông báo cho các cơ quan có thẩm quyền về sự cố đang xảy ra này.

Đồng thời, chúng tôi cũng đã triển khai ứng phó với sự hỗ trợ của các cơ quan chuyên môn và chuyên gia. Ưu tiên của chúng tôi bảo vệ dữ liệu của công dân/khách hàng và các bên liên quan, đưa các dịch vụ và hệ thống trở lại hoạt động bình thường sớm nhất có thể.

Nếu có bất kỳ câu hỏi hoặc cần cập nhật tình hình sự cố, vui lòng liên hệ <**Đầu mối liên lạc/xử lý khủng hoảng truyền thông**> của chúng tôi.

Trân trọng,
<nhập chức danh hoặc tên>

Bảng 15: Mẫu email thông báo của Bộ

Email 3: Cập nhật về sự cố an toàn thông tin

Từ: <đại diện ủy quyền>
Đến: Các Liên hệ Chính
Chủ đề: Cập nhật về Sự cố An Toàn Thông tin <nhập Số Sự cố ATTTM >

Kính gửi các đồng nghiệp,

Vui lòng xem thông tin cập nhật về sự cố an toàn thông tin đang diễn ra dưới đây:

- **Mô tả Sự cố:** <nhập mô tả ngắn gọn về sự cố>.
- **Mức độ nghiêm trọng:** <SP1 hoặc SP2>.
- **Tác động đến hoạt động:** <nhập tác động đến hoạt động và lý do xảy ra sự cố, nếu biết. Ví dụ: chi tiết về hệ thống, tài khoản, v.v. đã bị vi phạm an ninh>.
- **Tóm tắt các hành động cho đến nay:** <nhập tóm tắt về ai đang làm việc để khắc phục sự cố>.
- **Trạng thái:** <đã giải quyết hoặc chưa giải quyết và lý do>.

<**Nếu sự cố đang diễn ra**>
>>
Các cập nhật sẽ tiếp tục được thông báo thường xuyên trong thời gian xử lý sự cố. Tuy nhiên, nếu bạn có bất kỳ câu hỏi hoặc thắc mắc cụ thể nào, vui lòng liên hệ với tôi hoặc Bộ phận Hỗ trợ.
>>

<**Nếu sự cố đã được giải quyết**>
>>
Chúng tôi cảm ơn sự hỗ trợ và kiên nhẫn của bạn trong việc giải quyết sự cố này.
Đội của tôi sẽ tiếp tục làm việc để khắc phục bất kỳ vấn đề tồn đọng nào và kinh nghiệm thu được từ sự cố này để chuẩn bị tốt hơn cho <**nạn nhân**> và đơn vị chúng tôi trong tương lai.
>>

Trân trọng,
<nhập chức danh hoặc tên>

Bảng 16: Mẫu email cập nhật sự cố

Email 4: Thông báo bị vi phạm dữ liệu cho khách hàng

Từ: <Đầu mối liên lạc/xử lý khủng hoảng truyền thông>
Đến: Liên hệ của khách hàng/người dân
Chủ đề: Thông báo sự cố ATTT của <tổ chức>

Kính gửi <**nhập tên khách hàng/người liên hệ**>,

<**Tên tổ chức**> viết email này để thông báo rằng <**nhập chi tiết về hệ thống, tài khoản đã bị lộ hoặc xâm phạm**> của <**khách hàng**> đã bị ảnh hưởng bởi một sự cố xâm phạm dữ liệu và các dữ liệu của <khách hàng> đã bị truy cập bởi kẻ tấn công chưa rõ.

Trong sự cố xâm phạm dữ liệu này, <**nhập tóm tắt thông tin cụ thể đã truy cập do vi phạm, cũng như các chi tiết khác trong danh sách bên dưới**> đã bị một bên không được phép truy cập. Trường hợp của bạn, các thông tin sau đã hoặc có khả năng có thể bị truy cập:

- <**nhập danh sách dữ liệu bị xâm phạm / lộ lọt**>

Khi <nạn nhân> biết về vi phạm này, chúng tôi đã thực hiện ngay một số hành động để hạn chế tác động của sự cố và tiếp tục khôi phục dịch vụ nhanh nhất có thể.

Sự cố cũng đã được báo cáo lên Bộ Thông tin và Truyền thông. Cơ quan điều phối quốc gia và Trung tâm Ứng cứu khẩn cấp không gian mạng VNCERT/CC đang làm việc với <nạn nhân> để ưu tiên điều tra thêm về sự cố này.

Chúng tôi thành thật xin lỗi vì bất kỳ sự bất tiện nào mà sự cố này đã gây ra.

Để biết thêm thông tin, xin vui lòng tham khảo các câu hỏi thường gặp của Chúng tôi tại <nhập trang liên kết> mà Chúng tôi sẽ cập nhật khi có thông tin mới.

Nếu có bất kỳ câu hỏi nào, xin vui lòng liên hệ với Chúng tôi qua số điện thoại <**nhập số điện thoại của Đầu mối liên lạc/xử lý khủng hoảng truyền thông**> hoặc email <**nhập địa chỉ email**>.

Trân trọng.
<nhập chức danh hoặc tên>

Bảng 17: Mẫu email thông báo vi phạm dữ liệu cho khách hang

Email 5: Yêu cầu từ giới truyền thông

Từ: < Đầu mối liên lạc/xử lý khủng hoảng truyền thông>>
Đến: Thành viên Truyền thông Liên quan
Chủ đề: Yêu cầu Truyền thông

Kính gửi <**nhập Tên Thành viên Truyền thông**>,

Tội phạm mạng đã trở thành một thực tế trong kỷ nguyên kỹ thuật số và là một mối đe dọa rất thực tế đối với tất cả các ngành. Chính phủ Việt Nam cũng không ngoại lệ.

Chúng tôi rất coi trọng trách nhiệm của mình trong việc quản lý dữ liệu công dân/khách hàng một cách an toàn và bảo mật theo quy định pháp luật của Việt Nam. Tại <**nhập Tên tổ chức**>, chúng tôi có các quy trình và thủ tục để xây dựng khả năng phục hồi và giảm thiểu rủi ro thiệt hại cho hoạt động của Chính phủ và các bên liên quan.

Vào ngày <**nhập ngày**>, <**Tên tổ chức**> đã gặp một sự cố an toàn thông tin có mức độ <**mô tả mức độ nghiêm trọng của tác động**> đã ảnh hưởng đến <**nhập các dịch vụ/hệ thống liên quan**> và dẫn đến <**nhập tóm tắt tác động**>.

Đội ngũ chuyên chuyên môn và chuyên gia ATTT của chúng tôi đã hành động ngay lập tức để bảo vệ dữ liệu và hệ thống và tăng cường các biện pháp đảm bảo an toàn hiện có. Chúng tôi đang ưu tiên điều tra sự cố mất an toàn và sẽ cung cấp thông tin cập nhật thường xuyên.

Bên cạnh đó, chúng tôi cũng đã khởi động các biện pháp đảm bảo dịch vụ của mình hoạt động và duy trì liên tục.

Chúng tôi cũng đã hợp tác với các chuyên gia đầu ngành và các cơ quan thực thi pháp luật để điều tra về sự cố và đảm bảo hệ thống được đưa trở lại hoạt động an toàn.

Ở giai đoạn này của cuộc điều tra, vẫn chưa thể ước tính khi nào hệ thống và thông tin liên quan của <**nạn nhân**> sẽ được khôi phục hoạt động đầy đủ

Để biết thêm thông tin, vui lòng tham khảo Câu hỏi thường gặp của chúng tôi có sẵn tại <**nhập liên kết trang hỏi đáp về sự cố**>.

Trân trọng,
<nhập chức danh hoặc tên>

Bảng 18: Mẫu email yêu cầu từ giới truyền thông

Phụ lục C: Mẫu Báo cáo Tình huống

Mẫu Báo cáo Tình huống hỗ trợ việc cập nhật báo cáo thông tin sự cố tới những cá nhân chịu trách nhiệm.

Ngày nhập:	**Thời gian nhập:**	**Tác giả:**
Tài liệu tham khảo sự cố		
Ngày và giờ phát hiện sự cố		
Trạng thái hiện tại: Mới, Đang tiến hành, Đã giải quyết		
Loại sự cố		
Phân loại Sự cố		
Phạm vi		
Tác động		
Mức độ nghiêm trọng		
Cần Hỗ trợ		
Hành động đã thực hiện để giải quyết sự cố		
Chi tiết liên hệ cho người quản lý sự cố và những người khác nếu cần		
Ghi chú Bổ sung		
Ngày và giờ lần cập nhật kế tiếp		

Bảng 19: Mẫu báo cáo tình huống

Phụ lục D: Quy trình ra quyết định về ransomware

Quy trình dưới đây thể hiện 9 cân nhắc chính cần được thực hiện khi quyết định trả tiền chuộc. Trường hợp câu trả lời trong quy trình này là 'Có', tổ chức KHÔNG nên xem xét đàm phán thanh toán tiền chuộc. Các tổ chức có thể cập nhật bảng này dựa vào thực tế của mình và các quy định hiện hành.

Quy trình ra quyết định về ransomware	
Pháp lý & Đạo đức	1. Việc thanh toán có khiến Chính phủ hoặc nạn nhân gặp rủi ro pháp lý không thể chấp nhận được không? 2. Chính phủ có từ chối thanh toán vì lý do đạo đức, pháp lý hoặc chính sách không?
Kỹ thuật	3. Có thể duy trì hoạt động ở mức chấp nhận được bằng cách sử dụng bản sao lưu không? 4. Việc xây dựng lại hệ thống có hiệu quả về chi phí và thực tế không?
Quyền riêng tư & Dữ liệu	5. Mức độ nhạy cảm và số lượng mất mát có nằm trong khả năng chấp nhận rủi ro của Chính phủ hoặc nạn nhân không?
Thông tin Tình báo	6. Kẻ tấn công có khả năng không tôn trọng thỏa thuận, bao gồm cả việc không cấp quyền truy cập cho các nhóm khác không?
Tác động đến Hoạt động / Kinh doanh	7. Rủi ro về quy định hoặc rủi ro vận hành của việc thanh toán có quá lớn không? 8. Các nhà cung cấp bảo hiểm có khả năng không chi trả cho khoản thanh toán không? 9. Có bất kỳ bên liên quan chính và người ra quyết định nào không đồng ý thanh toán không?

Bảng 20: Quy trình ra quyết định về Ransomware

Phụ lục E: Bảng phân tích đánh giá sau sự cố

Phân tích Đánh giá sau sự cố (PIR - Post Incident Review) dự kiến sẽ được hoàn thành sau khi báo cáo tóm tắt và dừng kích hoạt Quy trình ứng cứu sự cố để chuẩn bị cho cuộc báo cáo kết thúc ứng phó sự cố bởi người chịu trách nhiệm quản lý ứng phó sự cố.

Tóm tắt Sự cố	
Tham chiếu sự cố	
Ngày phát hiện sự cố	
Mức độ ưu tiên của sự cố	
Thời gian phát hiện sự cố	
Thời gian sự cố được xử lý	
Loại sự cố	
Những người liên quan	
Tác động của sự cố	
Tóm tắt các quyết định theo dòng thời gian	
Dòng Thời gian Sự cố	
Thời gian và ngày tuyên bố sự cố an toàn thông tin	
Ngày và giờ ứng phó sự cố	
Ngày và giờ khôi phục sự cố	
Người(những người) phát hiện sự cố	
Phát hiện nội bộ hay bên ngoài; nếu bên ngoài, hãy nêu rõ	
Danh sách những người đã hỗ trợ giải quyết sự cố và thời điểm họ hỗ trợ	
Danh sách các hoạt động được thực hiện để giải quyết sự cố; bao gồm ngày và giờ, và tác động	
Các hành động đề xuất - nêu các hành động nào có thể được đưa vào quy trình, sổ tay ứng cứu sự cố.	
Bảo vệ	

Các biện pháp kiểm soát đã được áp dụng trước khi xảy ra sự cố và được kỳ vọng sẽ ngăn chặn các sự cố tương tự.	
Hiệu quả của các biện pháp kiểm soát	
Các biện pháp kiểm soát khác cần xem xét để ngăn chặn loại sự cố này xảy ra lần nữa.	
Các quy trình nghiệp vụ đã được áp dụng trước khi xảy ra sự cố để ngăn chặn loại sự cố này.	
Hiệu quả của các quy trình nghiệp vụ	
Các phát hiện và/hoặc đề xuất cải tiến bổ sung	
Phát hiện Sự cố	
Cách thức phát hiện sự cố	
Các biện pháp kiểm soát để phát hiện sự cố	
Hiệu quả của các biện pháp kiểm soát	
Các cách cải thiện "thời gian phát hiện"	
Các dấu hiệu để phát hiện các sự cố tương tự trong tương lai	
Các công cụ hoặc tài nguyên bổ sung cần thiết để phát hiện các sự cố tương tự trong tương la	
Các phát hiện và/hoặc đề xuất cải tiến bổ sung	
Ứng phó Sự cố	
Nguyên nhân sự cố	
Cách giải quyết sự cố	
Các chính sách và/hoặc quy trình hoạt động/kinh doanh được sử dụng để ứng phó	
Hiệu quả của các chính sách và/hoặc quy trình hoạt động/kinh doanh	
Các trở ngại và sự chậm trễ trong việc ứng phó với sự cố	
Các điểm leo thang/tăng cấp	
Hiệu quả của các điểm leo thang/tăng cấp	
Hiệu quả của việc chia sẻ và truyền thông thông tin	
Các yêu cầu từ giới truyền thông trong thời gian xảy ra sự cố	

Các thông cáo báo chí được đưa ra trong thời gian xảy ra sự cố; phản hồi của tổ chức	
Khách hàng được thông báo trong thời gian xảy ra sự cố	
Tình trạng sẵn có các nhân viên được đào tạo	
Các phát hiện và/hoặc khuyến nghị cải tiến bổ sung	
Khôi phục Sự cố	
Thời gian cần để khôi phục tất cả các hệ thống và mạng	
Các đề xuất cải tiến để giảm thời gian	
Các nghĩa vụ báo cáo bên ngoài	
Các yêu cầu từ giới truyền thông sau sự cố	
Nhân viên và/hoặc Khách hàng được thông báo về sự cố	
Các phát hiện và/hoặc đề xuất cải tiến	

Bảng 21: Mẫu phân tích đánh giá sau sự cố

KẾT THÚC TÀI LIỆU