TCVN TIÊU CHUẨN QUỐC GIA

TCVN 11239:2015
ISO/IEC 27035:2011

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN

Information technology - Security techniques - Information security incident management

HÀ NỘI - 2015

Mục lục

Lời nói đầu

TCVN 11239:2015 hoàn toàn tương đương với ISO/IEC 27035:2011.

TCVN 11239:2015 do Viện Khoa học Kỹ thuật Bưu điện biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin

Information technology - Security techniques - Information security incident management

1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra một phương pháp tiếp cận có cấu trúc và có kế hoạch để:

a) phát hiện, báo cáo và đánh giá các sự cố an toàn thông tin;

b) ứng phó và quản lý các sự cố an toàn thông tin;

c) phát hiện, đánh giá và quản lý các điểm yếu an toàn thông tin; và

d) liên tục cải tiến việc quản lý sự cố và an toàn thông tin sau khi thực hiện quản lý các sự cố và điểm yếu an toàn thông tin.

Tiêu chuẩn này đưa ra hướng dẫn quản lý sự cố an toàn thông tin cho các tổ chức quy mô lớn và trung bình. Tùy theo quy mô và loại hình nghiệp vụ liên quan đến tình trạng rủi ro an toàn thông tin, các tổ chức có quy mô nhỏ hơn vẫn có thể sử dụng bộ các tài liệu, quy trình và thủ tục cơ bản được mô tả trong tiêu chuẩn này. Tiêu chuẩn này cũng đưa ra hướng dẫn cho các tổ chức bên ngoài cung cấp các dịch vụ quản lý sự cố an toàn thông tin.

2 Tài liệu viện dẫn

Tài liệu viện dẫn sau đây là cần thiết để áp dụng tiêu chuẩn này. Đối với tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả các sửa đổi, bổ sung).

- TCVN 11238 (ISO/IEC 27000), Information technology – Security techniques – Information security management systems – Overview and vocabulary *(Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Tổng quan và từ vựng)*.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa nêu trong TCVN 11238 và các thuật ngữ, định nghĩa sau:

3.1

Điều tra an toàn thông tin (information security forensics)

Áp dụng các kỹ thuật điều tra và phân tích để nắm bắt, báo cáo và phân tích các sự cố an toàn thông tin.

3.2

Nhóm ứng cứu sự cố an toàn thông tin (information security incident response team)

ISIRT

Nhóm gồm các thành viên có kỹ năng phù hợp và được tin cậy của tổ chức làm nhiệm vụ xử lý các sự cố an toàn thông tin trong suốt vòng đời của chúng.

CHÚ THÍCH: ISIRT được mô tả trong tiêu chuẩn này là một bộ phận chức năng có tổ chức thực hiện xử lý các sự cố an toàn thông tin và tập trung chủ yếu vào các sự cố liên quan đến IT. Các bộ phận chức năng thông thường khác (có chữ viết tắt tương tự) trong việc xử lý sự cố có thể có mục đích và phạm vi hơi khác một chút. Các chữ viết tắt sau được sử dụng rộng rãi có nghĩa tương tự như ISIRT, tuy nhiên không hoàn toàn giống:

- CERT (Computer Emergency Response Team): Nhóm Ứng cứu Máy tính Khẩn cấp chủ yếu tập trung vào xử lý các sự cố công nghệ thông tin và truyền thông (ICT). Tùy theo quốc gia thì CERT có thể có các định nghĩa khác.
- CSIRT (Computer Security Incident Response Team): Nhóm Ứng cứu Sự cố An toàn Máy tính là một tổ chức dịch vụ chịu trách nhiệm tiếp nhận, xem xét, và ứng phó với các báo cáo và hoạt động về sự cố an toàn máy tính. Các dịch vụ này thường được thực hiện cho một phạm vi xác định, đó có thể là một công ty mẹ ví dụ như một tập đoàn, tổ chức chính phủ, hoặc tổ chức giáo dục; một vùng hoặc một quốc gia; một mạng lưới nghiên cứu; hoặc một khách hàng đã chi trả.

3.3

Sự kiện an toàn thông tin (information security event)

Sự kiện xác định của một hệ thống, dịch vụ hoặc trạng thái mạng cho thấy có khả năng vi phạm chính sách an toàn thông tin hay sự thất bại của các biện pháp kiểm soát hoặc một tình huống chưa biết có thể liên quan đến an toàn thông tin.

[TCVN 11238:2015]

3.4

Sự cố an toàn thông tin (information security incident)

Một hoặc một loạt các sự kiện an toàn thông tin không mong muốn hoặc không dự tính có khả năng ảnh hưởng đáng kể các đến hoạt động nghiệp vụ và đe dọa an toàn thông tin.

[TCVN 11238:2015]

4 Tổng quan

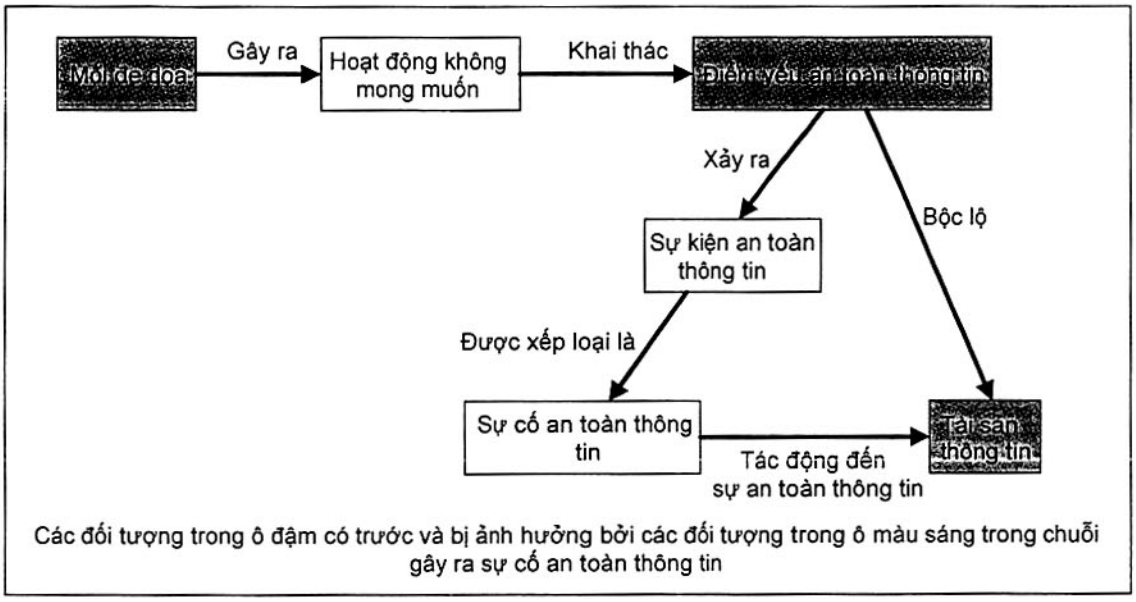
4.1 Các khái niệm cơ bản

Sự kiện an toàn thông tin là một sự kiện xác định của một hệ thống, dịch vụ hay trạng thái mạng cho thấy khả năng vi phạm an toàn thông tin, sự thất bại của các biện pháp kiểm soát, hoặc một tình huống chưa biết có thể liên quan đến an toàn thông tin. Một sự cố an toàn thông tin là một hoặc một chuỗi các

sự kiện an toàn thông tin không mong muốn hoặc không trông đợi có nhiều khả năng làm tổn hại các hoạt động nghiệp vụ và đe dọa an toàn thông tin.

Việc xảy ra một sự kiện an toàn thông tin không phải lúc nào cũng có nghĩa là một cố gắng đã thành công hoặc có hệ quả nào đó đến tính bí mật, tính vẹn toàn và/hoặc tính sẵn sàng, tức là không phải mọi sự kiện an toàn thông tin đều được xếp loại là sự cố an toàn thông tin.

Mối đe dọa khai thác các điểm yếu (nhược điểm) của các hệ thống, dịch vụ và mạng thông tin theo các cách không mong muốn, đó chính là sự xảy ra các sự kiện an toàn thông tin và tiềm ẩn gây ra các sự cố không mong muốn đối với các tài sản thông tin có điểm yếu. Hình 1 mô tả mối quan hệ giữa các đối tượng trong chuỗi gây ra sự cố an toàn thông tin. Các đối tượng trong ô màu đậm là các đối tượng có trước và bị ảnh hưởng bởi các đối tượng trong ô màu sáng trong chuỗi gây ra sự cố an toàn thông tin.



Hình 1 – Mối quan hệ giữa các đối tượng trong chuỗi gây ra sự cố an toàn thông tin

4.2 Các mục đích

Là một phần chính trong chiến lược an toàn thông tin tổng thể của tổ chức, tổ chức cần triển khai các biện pháp kiểm soát và các thủ tục để có được một phương pháp tiếp cận có cấu trúc và có kế hoạch chặt chẽ để quản lý các sự cố an toàn thông tin. Theo quan điểm nghiệp vụ thì mục đích quan trọng nhất là tránh hoặc kìm hãm tác động của các sự cố an toàn thông tin nhằm làm giảm chi phí trực tiếp và gián tiếp phát sinh từ các sự cố đó.

Các bước cơ bản để giảm thiểu tác động tiêu cực trực tiếp của các sự cố an toàn thông tin gồm:

- ngăn chặn và kìm hãm,
- loại trừ,

- phân tích và báo cáo,
- theo dõi.

Các mục đích của một phương pháp tiếp cận có cấu trúc và có kế hoạch chặt chẽ cần đảm bảo các vấn đề sau:

a) Các sự kiện an toàn thông tin được phát hiện và giải quyết một cách hiệu quả, đặc biệt trong việc xác định xem liệu chúng có cần được phân loại và phân cấp như các sự cố an toàn thông tin hay không.

b) Các sự cố an toàn thông tin xác định được đánh giá và ứng phó theo cách thức phù hợp và hiệu quả nhất.

c) Các ảnh hưởng bất lợi của các sự cố an toàn thông tin lên tổ chức và các hoạt động nghiệp vụ của tổ chức được giảm thiểu bằng các biện pháp kiểm soát phù hợp, đây chính là một phần của việc ứng phó với sự cố, việc này có thể được kết hợp với các phần liên quan của một hoặc nhiều kế hoạch quản lý khủng hoảng.

d) Các điểm yếu an toàn thông tin được báo cáo sẽ được đánh giá và giải quyết một cách hợp lý.

e) Các bài học kinh nghiệm được nhanh chóng rút ra từ các sự cố, điểm yếu an toàn thông tin và việc quản lý liên quan. Điều này nhằm làm tăng các cơ hội ngăn chặn xảy ra các sự cố an toàn thông tin trong tương lai, cải tiến việc triển khai và sử dụng các biện pháp kiểm soát an toàn thông tin, và cải tiến lược đồ quản lý sự cố an toàn thông tin tổng thể.

Để đạt được các mục đích trên, các tổ chức cần đảm bảo rằng các sự cố an toàn thông tin đều được ghi vào tài liệu theo cách thích hợp, có sử dụng các tiêu chuẩn phù hợp cho phân loại, phân cấp sự cố và chia sẻ về sự cố sao cho các số đo đều được thiết lập từ dữ liệu tập hợp được trong một khoảng thời gian. Đây sẽ là nguồn cung cấp thông tin có giá trị để hỗ trợ quy trình đưa ra quyết định chiến lược khi tập trung vào các biện pháp kiểm soát an toàn thông tin.

Cần nhắc lại rằng tiêu chuẩn này còn có một mục đích khác là đưa ra hướng dẫn cho các tổ chức mong muốn thỏa mãn các yêu cầu của TCVN ISO/IEC 27001:2009 (và do vậy cũng được hỗ trợ từ các hướng dẫn của TCVN ISO/IEC 27002:2011). TCVN ISO/IEC 27001:2009 cũng đưa ra các yêu cầu liên quan đến quản lý sự cố an toàn thông tin. Phụ lục A đưa ra bảng tham chiếu chéo giữa các điều liên quan đến quản lý sự cố an toàn thông tin trong TCVN ISO/IEC 27001:2009 và TCVN ISO/IEC 27002:2011 và các điều trong tiêu chuẩn này.

4.3 Các lợi ích của phương pháp tiếp cận có cấu trúc

Mỗi tổ chức sử dụng phương pháp tiếp cận có cấu trúc để quản lý sự cố an toàn thông tin sẽ nhận được các lợi ích lớn theo các nhóm sau:

a) Cải thiện an toàn thông tin tổng thể

Quy trình có cấu trúc để phát hiện, báo cáo, đánh giá và đưa ra quyết định về các sự kiện và sự cố an toàn thông tin sẽ cho phép xác định và ứng phó nhanh chóng. Điều đó sẽ cải thiện sự an toàn tổng thể nhờ giúp nhanh chóng xác định và triển khai giải pháp phù hợp, và do vậy sẽ đưa ra được cách thức phòng ngừa các sự cố an toàn thông tin tương tự trong tương lai. Hơn nữa, tổ chức cũng sẽ có thêm nhiều lợi ích trong việc chia sẻ và tập hợp thông tin. Sự tín nhiệm của tổ chức cũng sẽ được cải thiện nếu thể hiện được triển khai thực hành tốt nhất về quản lý sự cố an toàn thông tin.

b) Giảm các tác động nghiệp vụ bất lợi

Phương pháp tiếp cận có cấu trúc để quản lý sự cố an toàn thông tin có thể hỗ trợ làm giảm mức tác động nghiệp vụ bất lợi tiềm ẩn liên quan đến các sự cố an toàn thông tin. Các tác động này có thể là sự thiệt hại tài chính tức thì và thiệt hại lâu dài phát sinh từ sự suy giảm danh tiếng và tín nhiệm (xem hướng dẫn về phân tích tác động nghiệp vụ trong ISO/IEC 27005:2014).

c) Tăng cường sự tập trung ngăn chặn sự cố an toàn thông tin

Sử dụng phương pháp tiếp cận có cấu trúc để quản lý sự cố an toàn thông tin sẽ giúp thiết lập sự tập trung tốt hơn vào việc ngăn chặn sự cố trong mỗi tổ chức, bao gồm cả các phương pháp xác định các mối đe dọa và các điểm yếu mới. Phân tích dữ liệu về sự cố có thể cho phép xác định các kiểu và các xu hướng, do đó dễ dàng tập trung chính xác hơn vào việc ngăn chặn sự cố và do vậy sẽ xác định được các hành động phù hợp để ngăn chặn xảy ra sự cố.

d) Tăng cường phân cấp ưu tiên

Phương pháp tiếp cận có cấu trúc để quản lý sự cố an toàn thông tin sẽ cung cấp một cơ sở vững chắc để phân cấp ưu tiên khi tiến hành các điều tra sự cố an toàn thông tin, khi đó có sử dụng các thang phân loại và phân cấp hiệu quả. Nếu không có các thủ tục rõ ràng thì nguy cơ là các hoạt động điều tra có thể đã được tiến hành theo phương thức phản ứng, tức là ứng phó với các sự cố khi chúng xảy ra và bỏ qua các hoạt động cần thiết. Điều này có thể ngăn cản các hoạt động điều tra tập trung trực tiếp các khu vực nơi chúng có thể có độ ưu tiên cao hơn, nơi chúng thực sự cần thiết và có độ ưu tiên lý tưởng.

e) Tăng cường chứng cứ

Các thủ tục điều tra sự cố rõ ràng có thể giúp đảm bảo rằng việc thu thập và xử lý dữ liệu là có cơ sở rõ ràng và được chấp nhận về mặt pháp lý. Đây là những vấn đề quan trọng nếu sau này có thể xảy ra hành động kỷ luật hoặc khởi tố. Tuy nhiên, cũng cần thấy rằng các hành động cần thiết để khôi phục sau mỗi sự cố an toàn thông tin có thể lại vô tình hủy hoại sự toàn vẹn của mọi chứng cứ được thu thập đó.

f) Đóng góp vào việc cân đối nguồn lực và ngân quỹ

Phương pháp tiếp cận có cấu trúc và có kế hoạch chặt chẽ để quản lý sự cố an toàn thông tin sẽ giúp cân đối và đơn giản hóa việc phân bổ các nguồn lực và ngân quỹ trong các đơn vị tổ chức tham gia. Hơn nữa, lợi ích sẽ gia tăng với lược đồ quản lý sự cố an toàn thông tin có đặc điểm:

- sử dụng số lượng nhỏ những người có kỹ năng để xác định và lọc ra các cảnh báo về sự bất thường hoặc khác lạ,
- cung cấp định hướng tốt hơn cho các hoạt động của đội ngũ có kỹ năng,
- chỉ cần sự tham gia của người có kỹ năng trong các quy trình cần các kỹ năng của họ và chỉ tại giai đoạn của quy trình cần sự đóng góp của họ.

Một phương pháp tiếp cận tốt khác để kiểm soát và tối ưu các nguồn lực và ngân quỹ là bổ sung truy vết thời gian vào việc quản lý sự cố an toàn thông tin để hỗ trợ các đánh giá định lượng về việc xử lý các sự cố an toàn thông tin của tổ chức. Ví dụ, phương pháp này phải có thể cung cấp thông tin về thời gian cần để giải quyết các sự cố an toàn thông tin với thứ tự ưu tiên khác nhau và trên các nền tảng khác nhau. Nếu có các tắc nghẽn trong quy trình quản lý sự cố an toàn thông tin thì chúng cũng phải dễ xác định.

g) Cải tiến các cập nhật đối với các kết quả đánh giá và quản lý rủi ro an toàn thông tin

Việc sử dụng phương pháp tiếp cận có cấu trúc để quản lý sự cố an toàn thông tin sẽ tạo điều kiện

- thu thập tốt hơn các dữ liệu để hỗ trợ xác định và quyết định đặc điểm của các loại đe dọa khác nhau và các điểm yếu liên quan,
- cung cấp dữ liệu về tần suất xảy ra các loại đe dọa xác định

Dữ liệu được thu thập về các tác động bất lợi đến hoạt động nghiệp vụ của các sự cố an toàn thông tin sẽ giúp ích cho việc phân tích tác động nghiệp vụ. Dữ liệu được thu thập để xác định tần suất xảy ra của các loại đe dọa khác nhau sẽ hỗ trợ rất nhiều cho chất lượng của việc đánh giá mối đe dọa. Tương tự như vậy, dữ liệu được thu thập về các điểm yếu sẽ hỗ trợ rất nhiều cho chất lượng của các đánh giá điểm yếu sau này (xem hướng dẫn đánh giá và quản lý rủi ro an toàn thông tin trong ISO/IEC 27005:2011).

h) Cung cấp tài liệu tiên tiến cho chương trình đào tạo và nâng cao nhận thức về an toàn thông tin

Phương pháp tiếp cận có cấu trúc để quản lý sự cố an toàn thông tin sẽ cung cấp thông tin trọng tâm cho các chương trình nâng cao nhận thức về an toàn thông tin. Thông tin trọng tâm này sẽ cung cấp các ví dụ thực tế về các sự cố an toàn thông tin sẽ xảy ra đối với các tổ chức có thực. Thông tin trọng tâm này còn có thể thể hiện các lợi ích liên quan đến việc cung cấp nhanh chóng thông tin giải pháp. Hơn nữa, sự nhận thức đó sẽ giúp con người giảm lỗi hoặc hoảng loạn/bối rối khi có sự cố an toàn thông tin xảy ra.

i) Cung cấp đầu vào cho các soát xét chính sách an toàn thông tin và hệ thống tài liệu liên quan

Dữ liệu được cung cấp bởi lược đồ quản lý sự cố an toàn thông tin có thể cung cấp đầu vào giá trị cho các soát xét về tính hiệu lực và sự cải tiến liên tục của các chính sách an toàn thông tin (và các tài liệu an toàn thông tin liên quan khác). Điều đó cũng đúng đối với mọi chính sách và tài liệu liên quan sử dụng rộng rãi trong tổ chức và cả các hệ thống, dịch vụ và mạng của cá nhân.

4.4 Khả năng ứng dụng

Hướng dẫn được đưa ra trong tiêu chuẩn này có ý nghĩa áp dụng rộng rãi và nếu được tuân thủ hoàn toàn thì có thể phải cần có các nguồn lực lớn để vận hành và quản lý. Do vậy, điều quan trọng là mỗi tổ chức áp dụng hướng dẫn này cần duy trì quan điểm và đảm bảo rằng các nguồn lực dùng cho quản lý sự cố an toàn thông tin và sự phức tạp của các cơ chế được triển khai phải luôn được giữ cân xứng với:

a) quy mô, cấu trúc và tính chất nghiệp vụ của tổ chức,

b) quy mô của mọi hệ thống quản lý an toàn thông tin dùng để xử lý các sự cố,

c) khả năng thiệt hại do sự xuất hiện của các sự cố chưa được phòng ngừa,

d) các mục tiêu nghiệp vụ.

Do đó, mỗi tổ chức sử dụng tiêu chuẩn này cần thích ứng hướng dẫn của tiêu chuẩn cân đối với quy mô và các đặc điểm nghiệp vụ của tổ chức.

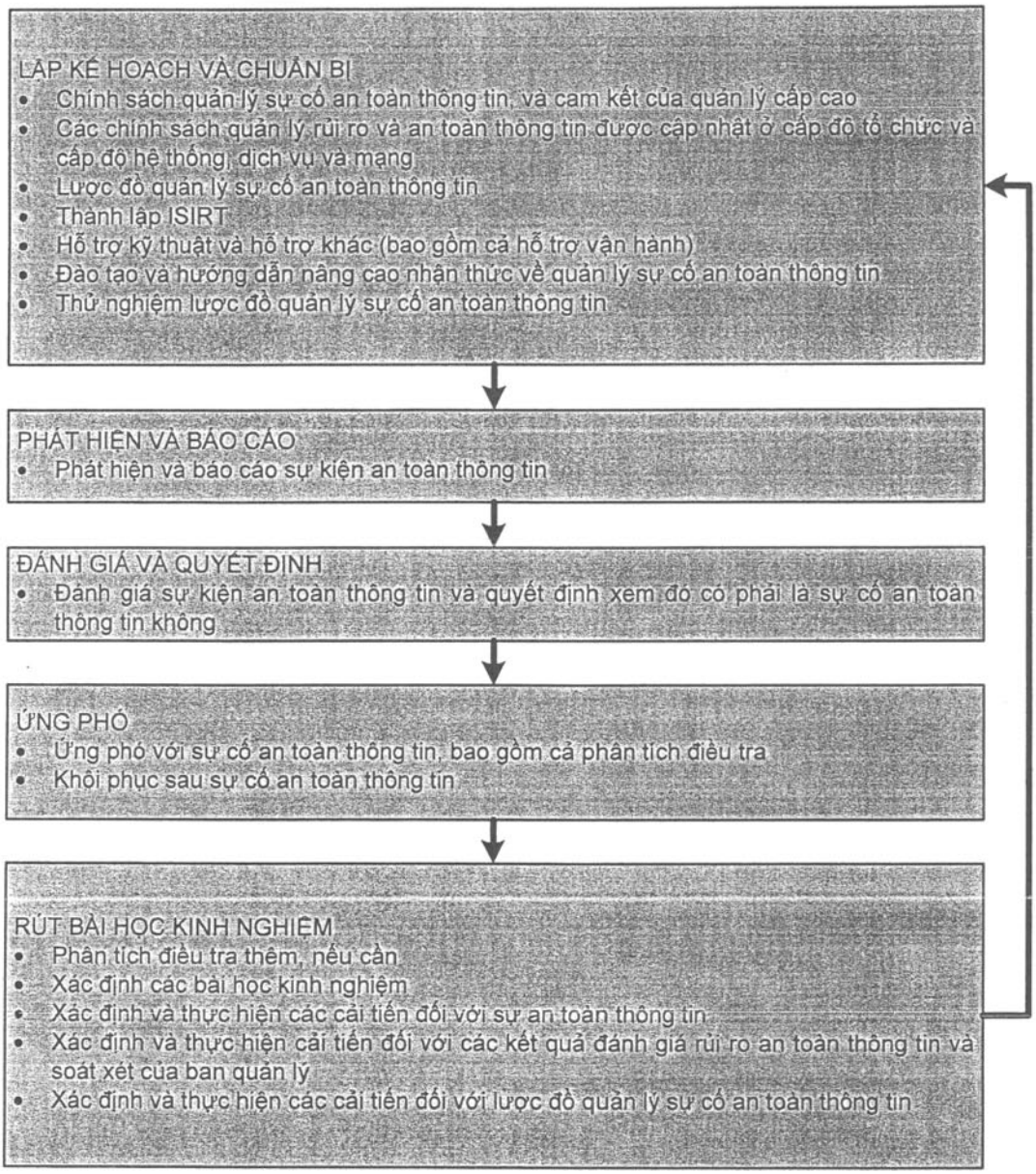
4.5 Các giai đoạn

Để đạt được các mục đích đã đề cập trong 4.2, quản lý sự cố an toàn thông tin gồm năm giai đoạn riêng biệt sau:

- Lập kế hoạch và chuẩn bị,
- Phát hiện và báo cáo,
- Đánh giá và quyết định,
- Ứng phó,
- Rút ra các bài học kinh nghiệm.

Giai đoạn đầu tiên là đạt được tất cả những gì được yêu cầu phải có để vận hành quản lý sự cố an toàn thông tin thành công. Bốn giai đoạn sau là sử dụng vận hành quản lý sự cố an toàn thông tin.

Hình 2 mô tả tổng quan nhất về các giai đoạn này.



Hình 2 – Các giai đoạn quản lý sự cố an toàn thông tin

4.6 Ví dụ về các sự cố an toàn thông tin

Các sự cố an toàn thông tin có thể do cố ý hoặc vô tình (ví dụ do lỗi hoặc thảm họa thiên nhiên) và có thể do các phương tiện vật lý hoặc kỹ thuật. Hậu quả của chúng có thể là làm tiết lộ, thay đổi, hủy hoại hoặc làm mất tính sẵn sàng của thông tin theo cách thức không được phép, làm hư hại hoặc đánh cắp các tài sản của tổ chức. Nếu các sự kiện an toàn thông tin chưa được báo cáo được xác định là các sự cố thì việc điều tra và kiểm soát các sự cố để ngăn chặn tái diễn sẽ trở nên khó khăn.

Phụ lục B mô tả các sự cố an toàn thông tin ví dụ được lựa chọn và các nguyên nhân của chúng chỉ với mục đích cung cấp thông tin. Cần lưu ý rằng các ví dụ này chưa bao hàm mọi trường hợp.

5 Giai đoạn lập kế hoạch và chuẩn bị

5.1 Tổng quan về các hoạt động chính

Quản lý an toàn thông tin hiệu quả đòi hỏi việc lập kế hoạch và chuẩn bị phù hợp. Để một lược đồ quản lý sự kiện, sự cố và điểm yếu an toàn thông tin hiệu lực và hiệu quả được đưa vào sử dụng vận hành thì sau quá trình lập kế hoạch cần thiết, mỗi tổ chức cần hoàn tất nhiều hoạt động chuẩn bị. Tổ chức cần đảm bảo rằng các hoạt động của giai đoạn lập kế hoạch và chuẩn bị bao gồm:

a) Hoạt động để xây dựng và đưa ra chính sách quản lý sự kiện/sự cố/điểm yếu an toàn thông tin và được quản lý cấp cao cam kết về chính sách đó. Trong đó, việc soát xét các điểm yếu của tổ chức, xác nhận yêu cầu cần có lược đồ quản lý an toàn thông tin và xác định các lợi ích đối với toàn bộ tổ chức và các phòng ban của tổ chức (xem 5.2) cần được thực hiện trước. Việc đảm bảo cam kết liên tục của cấp quản lý là điều quan trọng để có được sự chấp nhận đối với phương pháp tiếp cận có cấu trúc để quản lý sự cố an toàn thông tin. Đội ngũ nhân viên cần nhận biết được sự cố, biết phải làm gì và hiểu được các lợi ích của phương pháp tiếp cận đối với tổ chức. Cấp quản lý cần hỗ trợ lược đồ quản lý để đảm bảo rằng tổ chức cam kết phân bổ nguồn lực và duy trì khả năng ứng phó với sự cố.

b) Hoạt động để cập nhật các chính sách quản lý rủi ro và an toàn thông tin ở cấp độ tổ chức và tại các cấp độ hệ thống, dịch vụ và mạng cụ thể. Điều này cũng cần áp dụng cả cho quản lý sự kiện, sự cố và điểm yếu an toàn thông tin. Các chính sách cần được soát xét thường xuyên theo các đầu ra từ lược đồ quản lý sự cố an toàn thông tin (xem 5.2).

c) Hoạt động để xác định và lập tài liệu lược đồ quản lý sự cố an toàn thông tin chi tiết. Nhìn chung, hệ thống tài liệu về lược đồ quản lý cần bao gồm các mẫu, thủ tục, các thành phần tổ chức và các công cụ hỗ trợ để phát hiện, báo cáo, đánh giá, đưa ra quyết định liên quan, thực hiện các ứng phó và rút ra các bài học kinh nghiệm về các sự cố an toàn thông tin. Tóm lại, các chủ đề gồm:

   1) Thang phân cấp sự kiện/sự cố an toàn thông tin sẽ được sử dụng để xếp hạng các sự kiện/sự cố. Trong mỗi sự kiện, việc quyết định cần được dựa trên các tác động bất lợi thực tế và dự kiến lên các hoạt động nghiệp vụ của tổ chức

      CHÚ THÍCH: Phụ lục C đưa ra một ví dụ về phương pháp tiếp cận trong việc phân loại và phân cấp các sự kiện và sự cố an toàn thông tin.

   2) Các mẫu báo cáo sự kiện/sự cố/điểm yếu an toàn thông tin:

      i. được hoàn thành bởi người báo cáo sự kiện an toàn thông tin (tức là không phải thành viên của nhóm quản lý sự cố an toàn thông tin), trong đó thông tin đã được ghi trong cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin.

ii. được sử dụng bởi người quản lý sự cố an toàn thông tin dựa trên thông tin sự kiện an toàn thông tin đã được báo cáo lúc đầu và để có được hồ sơ cập nhật của các đánh giá sự cố theo thời gian cho đến khi sự cố được giải quyết hoàn toàn. Ở mỗi giai đoạn, thông tin cập nhật được ghi lại trong cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin. Hồ sơ cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin đây đủ sau đó được sử dụng trong các hoạt động phân tích sau sự cố.

iii. được hoàn thành bởi người báo cáo điểm yếu an toàn thông tin (điểm yếu này vẫn chưa bị khai thác để gây ra sự kiện an toàn thông tin, và có thể cả sự cố an toàn thông tin), trong đó thông tin đã được ghi lại trong cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin.

Các mẫu báo cáo cần có dạng điện tử (ví dụ trong web page an toàn), có liên kết trực tiếp đến cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin điện tử. Trong thế giới hiện nay, việc sử dụng văn bản cứng sẽ rất mất thời gian. Tuy nhiên, văn bản cứng có thể sẽ cần thiết trong trường hợp không thể sử dụng được dạng điện tử.

CHÚ THÍCH: Phụ lục D đưa ra ví dụ về các mẫu báo cáo.

3) Các thủ tục được lập tài liệu và các hành động liên quan đến việc sử dụng các mẫu này, tức là liên quan đến việc phát hiện sự kiện, sự cố và điểm yếu an toàn thông tin, trong đó có liên kết với các thủ tục thông thường về sử dụng dữ liệu, các dạng dự phòng của hệ thống, dịch vụ và/hoặc mạng và các kế hoạch quản lý khủng hoảng.

4) Các thủ tục vận hành dùng cho ISIRT kèm các quy trình đã được lập tài liệu và các trách nhiệm liên quan, và phân bổ vai trò cho những người đã được dự kiến sẽ thực hiện các hoạt động khác nhau (mỗi cá nhân có thể được phân cho nhiều vai trò tùy theo quy mô, cấu trúc và tính chất nghiệp vụ của tổ chức), ví dụ:

i. tắt hệ thống, dịch vụ và/hoặc mạng bị ảnh hưởng trong các tình huống nhất định đã được thỏa thuận trước đó với người quản lý IT và/hoặc nghiệp vụ liên quan,

ii. loại bỏ hệ thống, dịch vụ và/hoặc mạng đang được kết nối và hoạt động bị ảnh hưởng,

iii. giám sát dữ liệu đến, tới và trong hệ thống, dịch vụ và/hoặc mạng bị ảnh hưởng,

iv. khởi động các thủ tục và hành động quản lý khủng hoảng và dự phòng thông thường theo chính sách an toàn cho hệ thống, dịch vụ và/hoặc mạng,

v. giám sát và duy trì sự bảo quản an toàn cho chứng cứ điện tử trong trường hợp chúng được yêu cầu cho hành động khởi tố hoặc kỷ luật nội bộ,

vi. thông tin chi tiết về sự cố an toàn thông tin tới các tổ chức hoặc nhân sự trong nội bộ hoặc bên ngoài.

Trong một số tổ chức, lược đồ này có thể được coi là kế hoạch ứng phó sự cố an toàn thông tin (xem 5.4).

d) Hoạt động để thành lập ISIRT, trong đó một chương trình đào tạo phù hợp được thiết kế, phát triển và cung cấp cho nhóm này. Tùy theo quy mô, cấu trúc và tính chất nghiệp vụ của tổ chức, ISIRT có thể là nhóm riêng, nhóm ảo, hoặc nhóm pha trộn giữa hai hình thức này. Nhóm ISIRT riêng có thể gồm cả các thành viên ảo lấy từ các đơn vị/bộ phận chức năng nhất định, các thành viên này cần phối hợp chặt chẽ với ISIRT trong suốt quá trình giải quyết sự cố an toàn thông tin (các bộ phận ICT, pháp lý, quan hệ công chúng, các công ty thuê ngoài...). Nhóm ISIRT ảo có thể có một người quản lý cấp cao để lãnh đạo nhóm, nhóm này được hỗ trợ bởi các nhóm gồm những người có chuyên môn về các chủ đề nhất định, ví dụ trong việc xử lý các tấn công của mã độc, những người này sẽ được gọi tùy theo loại sự cố (xem 5.5).

e) Hoạt động để thiết lập và duy trì các mối quan hệ và kết nối phù hợp với các tổ chức nội bộ và bên ngoài có tham gia trực tiếp vào việc quản lý sự kiện, sự cố và điểm yếu an toàn thông tin.

f) Hoạt động để thiết lập, triển khai và vận hành các cơ chế hỗ trợ kỹ thuật và hỗ trợ khác (bao gồm cả về mặt tổ chức) để hỗ trợ lược đồ quản lý sự cố an toàn thông tin (và do vậy cả công việc của ISIRT), và phòng ngừa xảy ra sự cố an toàn thông tin hoặc giảm nhẹ xu hướng xảy ra các sự cố an toàn thông tin (xem 5.6). Các cơ chế này có thể gồm:

   1) Các cơ chế đánh giá an toàn thông tin nội bộ để đánh giá mức độ an toàn và theo dõi các hệ thống dễ bị tổn hại,

   2) Quản lý điểm yếu (bao gồm cả các cập nhật an toàn và việc vá an toàn cho các hệ thống dễ bị tổn hại),

   3) Theo dõi về công nghệ để phát hiện các dạng đe dọa và tấn công mới,

   4) Các hệ thống phát hiện xâm nhập (xem chi tiết trong ISO/IEC 18043),

   5) Các thiết bị, phương tiện bảo vệ và công cụ giám sát an toàn mạng (xem chi tiết trong ISO/IEC 27033 (TCVN 9801)),

   6) Phần mềm chống mã độc,

   7) Các hồ sơ nhật ký đánh giá, và phần mềm giám sát nhật ký,

   8) Các trách nhiệm và các thủ tục vận hành đã được lập tài liệu của nhóm hỗ trợ vận hành.

g) Hoạt động để thiết kế và phát triển chương trình đào tạo và nâng cao nhận thức về quản lý sự kiện, sự cố và điểm yếu an toàn thông tin. Mọi nhân sự thuộc tổ chức đều cần được lưu ý về sự tồn tại, lợi ích của lược đồ quản lý sự kiện, sự cố và điểm yếu an toàn thông tin và cách để báo cáo các sự kiện, sự cố (và điểm yếu) an toàn thông tin thông qua các chỉ dẫn ngắn gọn và/hoặc các cơ chế khác. Đồng thời, chương trình đào tạo phù hợp cũng cần được cung cấp cho những người chịu trách nhiệm quản lý lược đồ quản lý sự kiện, sự cố và điểm yếu an toàn thông tin, những người ra quyết định có tham gia vào việc quyết định xem liệu các sự kiện an toàn thông tin có phải là các sự cố không, và những người tham gia vào việc điều tra các sự cố. Các chỉ dẫn

nâng cao nhận thức và các khóa đào tạo cần được lặp lại sau đó để thích ứng với những thay đổi về nhân sự (xem 5.7).

h) Hoạt động để thử nghiệm sử dụng lược đồ quản lý sự cố an toàn thông tin, các quy trình và thủ tục của lược đồ. Các thử nghiệm cần được tổ chức định kỳ không chỉ để thử nghiệm lược đồ theo tình huống thực tế mà còn để kiểm chứng cách mà ISIRT ứng phó khi có áp lực về một sự cố nguy hiểm, phức tạp. Cần đặc biệt chú ý đến việc thiết lập các bài thử nghiệm tập trung vào các kịch bản điểm yếu, mối đe dọa và rủi ro đang bùng nổ (xem 5.8). Lược đồ cần gồm cả các tiêu chuẩn hỗ trợ chia sẻ thông tin, cả trong tổ chức và ra bên ngoài (nếu tổ chức yêu cầu). Một trong những lợi ích của việc chia sẻ là tập hợp được dữ liệu thành các thông tin hữu dụng nhằm hỗ trợ các quyết định nghiệp vụ chiến lược. Các thành viên của mỗi cộng đồng chia sẻ thông tin tin cậy còn cung cấp các cảnh báo sớm về các tấn công và họ cần được khuyến khích trong mọi chính sách của lược đồ quản lý sự cố an toàn thông tin và các chính sách liên quan.

Khi giai đoạn này hoàn tất, các tổ chức cần được chuẩn bị đầy đủ để quản lý các sự cố an toàn thông tin một cách phù hợp. Các điều sau sẽ mô tả từng hoạt động được liệt kê ở trên, bao gồm cả các nội dung của từng tài liệu được yêu cầu.

5.2 Chính sách quản lý sự cố an toàn thông tin

5.2.1 Giới thiệu

Mỗi tổ chức cần lập tài liệu chính sách để quản lý các sự kiện, sự cố, và điểm yếu an toàn thông tin thành một tài liệu riêng với vai trò là bộ phận của chính sách hệ thống quản lý an toàn thông tin tổng thể của tổ chức (xem 4.2.1 b của TCVN ISO/IEC 27001:2009), hoặc bộ phận của Chính sách an toàn thông tin của tổ chức (xem 5.1.1 của TCVN ISO/IEC 27002:2011). Quy mô, cấu trúc và tính chất nghiệp vụ của tổ chức và phạm vi của chương trình quản lý sự cố an toàn thông tin chính là các yếu tố quyết định trong việc xác định sẽ thực hiện theo lựa chọn nào ở trên. Mỗi tổ chức cần cung cấp trực tiếp chính sách quản lý an toàn thông tin tới tất cả mọi người có truy cập hợp pháp đến các hệ thống thông tin và các địa điểm liên quan của tổ chức.

Trước khi chính sách được xây dựng, tổ chức cần tiến hành soát xét an toàn thông tin tập trung vào các điểm yếu của tổ chức, xác nhận nhu cầu quản lý sự cố an toàn thông tin, và xác định các lợi ích đối với toàn bộ tổ chức cũng như các phòng ban.

5.2.2 Các bên liên quan

Mỗi tổ chức cần đảm bảo rằng chính sách quản lý sự cố an toàn thông tin được người quản lý cấp cao của tổ chức phê chuẩn, có sự xác nhận bằng văn bản của tất cả ban quản lý cấp cao. Chính sách quản lý sự cố an toàn thông tin này cần được cung cấp tới mọi nhân viên và nhà thầu, và cũng cần được đề cập trong các chỉ dẫn và chương trình đào tạo nâng cao nhận thức về an toàn thông tin (xem 5.7).

5.2.3 Nội dung

Mỗi tổ chức cần đảm bảo rằng nội dung chính sách quản lý an toàn thông tin đề cập đến các chủ đề sau:

a) Tầm quan trọng của quản lý sự cố an toàn thông tin đối với tổ chức và cam kết của ban quản lý cấp cao về quản lý sự cố và lược đồ liên quan.

b) Tổng quan về phát hiện, báo cáo sự kiện an toàn thông tin và thu thập các thông tin liên quan, và cách thức sử dụng thông tin này để xác định các sự cố an toàn thông tin.

Thông tin tổng quan này phải gồm thông tin tóm tắt về các loại sự kiện an toàn thông tin có thể, cách thức báo cáo, những vấn đề cần báo cáo, nơi và người cần được báo cáo, và cách thức xử lý toàn bộ các loại sự kiện an toàn thông tin mới. Thông tin tổng quan cũng phải gồm cả thông tin tóm tắt về việc báo cáo và xử lý điểm yếu an toàn thông tin.

c) Tổng quan về đánh giá sự cố an toàn thông tin, bao gồm cả tóm tắt về người chịu trách nhiệm đánh giá, các việc cần thực hiện, việc thông báo và việc tăng cấp xử lý.

d) Tóm tắt về các hoạt động cần thực hiện sau khi có xác nhận rằng sự kiện an toàn thông tin là sự cố an toàn thông tin.

e) Nhắc đến yêu cầu cần đảm bảo rằng mọi hoạt động quản lý an toàn thông tin đều được ghi nhật ký một cách phù hợp để dùng cho các phân tích về sau, và việc giám sát liên tục được tiến hành để đảm bảo sự bảo quản an toàn cho các chứng cứ điện tử trong trường hợp chúng cần cho hành động khởi tố hoặc kỷ luật nội bộ.

f) Các hoạt động giải quyết sau sự cố an toàn thông tin, bao gồm cả việc rút bài học kinh nghiệm và cải tiến quy trình sau các sự cố an toàn thông tin.

g) Tổng quan về việc báo cáo và xử lý điểm yếu an toàn thông tin.

h) Thông tin chi tiết về nơi giữ hệ thống tài liệu lược đồ, bao gồm cả các thủ tục.

i) Tổng quan về ISIRT, bao gồm các chủ đề sau:

1) Cơ cấu tổ chức của ISIRT và thông tin định danh về người quản lý ISIRT và những người có vai trò quan trọng khác, bao gồm cả người chịu trách nhiệm:

i. chỉ dẫn cho ban quản lý cấp cao về các sự cố,

ii. xử lý các cuộc thẩm vấn, điều tra sau này...,

iii. kết nối với các tổ chức bên ngoài (khi cần).

2) Tuyên bố về quản lý sự cố an toàn thông tin, trong đó chỉ rõ những điều ISIRT phải làm và thẩm quyền để ISIRT thực hiện những điều đó. Ít nhất, tuyên bố cũng cần gồm tuyên bố về nhiệm vụ, định nghĩa phạm vi của ISIRT, và thông tin chi tiết về người bảo trợ và thẩm quyền ở mức cao nhất của ISIRT.

3) Tuyên bố nhiệm vụ của ISIRT, trong đó tập trung vào các hoạt động chính của nhóm. Để được là một ISIRT thì nhóm cần hỗ trợ việc đánh giá, ứng phó và quản lý các sự cố an toàn thông tin đến khi có được kết luận là thành công. Các mục tiêu và mục đích của nhóm là đặc biệt quan trọng và đòi hỏi được định nghĩa rõ ràng, tránh mập mờ.

4) Định nghĩa phạm vi các hoạt động của ISIRT. Thông thường, phạm vi của ISIRT của một tổ chức phải bao hàm tất cả các hệ thống, dịch vụ và mạng thông tin của tổ chức. Trong các trường hợp khác, tổ chức có thể, dù bất cứ lý do gì, yêu cầu phạm vi nhỏ hơn, thì khi đó cần ghi rõ vào tài liệu những gì thuộc và không thuộc phạm vi.

5) Thông tin định danh của người quản lý cấp cao nhất, thành viên hội đồng quản trị hoặc người quản lý cấp cao có thẩm quyền ra quyết định về ISIRT và thiết lập các mức quyền đối với ISIRT. Việc biết điều này sẽ giúp tất cả các thành viên trong tổ chức hiểu được nền tảng và cơ cấu của ISIRT, và đó là thông tin sống còn cho việc xây dựng niềm tin về ISIRT. Cũng cần lưu ý rằng trước khi thông tin chi tiết này được công bố thì chúng cũng cần được kiểm tra về phương diện pháp lý. Trong một số tình huống, việc tiết lộ thẩm quyền của nhóm có thể khiến nhóm bị đặt vào tình thế đối mặt với trách nhiệm pháp lý.

6) Các kết nối với các tổ chức cung cấp các hỗ trợ cụ thể bên ngoài, ví dụ các nhóm điều tra (xem 5.5.4).

j) Tổng quan về các cơ chế kỹ thuật và hỗ trợ khác.

k) Tổng quan về chương trình đào tạo và nâng cao nhận thức về quản lý sự cố an toàn thông tin.

l) Tóm tắt về các khía cạnh pháp lý và quy định phải được đề cập (xem chi tiết trong Phụ lục E).

5.3 Tích hợp quản lý sự cố an toàn thông tin trong các chính sách khác

5.3.1 Giới thiệu

Các tổ chức cần đưa nội dung quản lý sự cố an toàn thông tin vào các chính sách quản lý rủi ro và an toàn thông tin ở cấp độ tổ chức cũng như ở các cấp độ hệ thống, dịch vụ và mạng cụ thể và liên kết nội dung này với chính sách quản lý sự cố. Việc tích hợp này cần hướng đến các mục đích sau:

a) Mô tả lý do vì sao quản lý sự cố an toàn thông tin, đặc biệt là lược đồ báo cáo và xử lý sự cố an toàn thông tin, lại quan trọng.

b) Chỉ ra cam kết của quản lý cấp cao về nhu cầu cần chuẩn bị và ứng phó phù hợp với các sự cố an toàn thông tin, tức là cam kết đối với lược đồ quản lý sự cố an toàn thông tin.

c) Đảm bảo tính nhất quán giữa các chính sách.

d) Đảm bảo có các ứng phó theo kế hoạch, có hệ thống và bình tĩnh đối với các sự cố an toàn thông tin, do đó tối giảm các tác động bất lợi của các sự cố.

Xem hướng dẫn về đánh giá và quản lý rủi ro an toàn thông tin trong ISO/IEC 27005:2011.

5.3.2 Nội dung

Mỗi tổ chức cần cập nhật và duy trì các chính sách quản lý sự cố và an toàn thông tin ở cấp độ tổ chức, và các chính sách an toàn thông tin cho hệ thống, dịch vụ và mạng cụ thể. Các chính sách này cần hướng theo chính sách quản lý sự cố an toàn thông tin ở cấp độ tổ chức và lược đồ liên quan.

a) Các phần liên quan cần tham chiếu đến cam kết của quản lý cấp cao.

b) Các phần liên quan cần phác thảo chính sách.

c) Các phần liên quan cần phác thảo các quy trình của lược đồ, và cơ sở hạ tầng liên quan.

d) Các phần liên quan cần phác thảo các yêu cầu đối với việc phát hiện, báo cáo, đánh giá và quản lý các sự kiện, sự cố và điểm yếu an toàn thông tin.

e) Các phần liên quan cần chỉ định rõ những người có trách nhiệm về phân quyền và/hoặc thực hiện các hành động quan trọng nhất định (ví dụ, ngắt ra khỏi mạng hoặc thậm chí là tắt một hệ thống thông tin).

Các chính sách cần đưa ra yêu cầu cần thiết lập các cơ chế soát xét phù hợp. Các cơ chế này cần đảm bảo rằng thông tin từ việc phát hiện, giám sát và giải quyết các sự cố an toàn thông tin và từ việc xử lý các điểm yếu an toàn thông tin được báo cáo sẽ được sử dụng như là đầu vào để đảm bảo tính hiệu lực luôn hiện hữu với các chính sách quản lý rủi ro và an toàn thông tin ở cấp độ tổ chức, và các chính sách an toàn thông tin cho hệ thống, dịch vụ và mạng cụ thể.

5.4 Lược đồ quản lý sự cố an toàn thông tin

5.4.1 Giới thiệu

Mục đích của lược đồ quản lý sự cố an toàn thông tin là cung cấp hệ thống tài liệu chi tiết mô tả các hoạt động và thủ tục để xử lý các sự kiện và sự cố an toàn thông tin, và truyền thông về các sự kiện, sự cố và điểm yếu đó. Lược đồ quản lý sự cố an toàn thông tin sẽ phát huy hiệu lực bất cứ khi nào mỗi sự kiện an toàn thông được phát hiện hoặc mỗi điểm yếu an toàn thông tin được báo cáo. Mỗi tổ chức cần sử dụng lược đồ này như là hướng dẫn để:

a) ứng phó với các sự kiện an toàn thông tin,

b) xác định xem liệu các sự kiện an toàn thông tin có trở thành các sự cố an toàn thông tin không,

c) quản lý các sự cố an toàn thông tin đến khi kết thúc,

d) ứng phó với các điểm yếu an toàn thông tin,

e) xác định các bài học kinh nghiệm và các cải tiến đối với lược đồ và/hoặc sự an toàn nói chung theo yêu cầu,

f) thực hiện các cải tiến đã xác định.

5.4.2 Các bên liên quan

Mỗi tổ chức cần đảm bảo rằng lược đồ quản lý sự cố an toàn thông tin được đề cập với mọi nhân viên và các nhà thầu liên quan, các nhà cung cấp dịch vụ ICT, các nhà cung cấp viễn thông và các công ty thuê ngoài, do vậy sẽ bao hàm các trách nhiệm sau:

a) phát hiện và báo cáo các sự kiện an toàn thông tin (đây là trách nhiệm của mọi nhân viên hợp đồng hoặc biên chế trong tổ chức và các đối tác của tổ chức),

b) đánh giá và ứng phó với các sự kiện và sự cố an toàn thông tin, việc này có liên quan đến các hoạt động giải quyết sau sự cố gồm rút ra bài học kinh nghiệm và tự cải tiến lược đồ quản lý sự cố an toàn thông tin và an toàn thông tin (đây là trách nhiệm của các thành viên của PoC (đầu mối liên lạc – Point of Contact), ISIRT, ban quản lý, nhân viên quan hệ công chúng và các đại diện pháp lý), và

c) báo cáo các điểm yếu an toàn thông tin (đây là trách nhiệm của mọi nhân viên hợp đồng hoặc biên chế trong tổ chức và các đối tác của tổ chức) và xử lý chúng.

Lược đồ này cũng cần xem xét mọi người dùng của bên thứ ba, các sự cố an toàn thông tin và các điểm yếu liên quan được báo cáo từ các tổ chức thứ ba và các tổ chức cung cấp thông tin về các sự cố, điểm yếu an toàn thông tin thương mại và chính phủ.

5.4.3 Nội dung

Mỗi tổ chức cần đảm bảo rằng nội dung của hệ thống tài liệu lược đồ quản lý sự cố an toàn thông tin bao gồm các thông tin sau:

a) Tổng quan về chính sách quản lý sự cố an toàn thông tin.

b) Tổng quan về toàn bộ lược đồ quản lý sự cố an toàn thông tin.

c) Các hoạt động, thủ tục và thông tin chi tiết liên quan đến các vấn đề sau:

1) Lập kế hoạch và chuẩn bị

i. Phương pháp tiếp cận chuẩn để phân loại và phân cấp sự kiện/sự cố an toàn thông tin để cho phép đưa ra các kết quả nhất quán. Trong mọi sự kiện, việc quyết định cần được dựa trên các tác động bất lợi thực tế hoặc dự kiến lên các hoạt động nghiệp vụ của tổ chức, và hướng dẫn liên quan.

CHÚ THÍCH: Phụ lục C đưa ra một ví dụ về phương pháp tiếp cận để phân loại và phân cấp các sự kiện và sự cố an toàn thông tin.

ii. Cấu trúc cơ sở dữ liệu chuẩn về sự kiện/sự cố/điểm yếu an toàn thông tin, các thông tin này có thể cung cấp khả năng so sánh các kết quả, cải tiến thông tin cảnh báo và cho phép có sự nhìn nhận chính xác hơn về các mối đe dọa và các điểm yếu của các hệ thống thông tin.

iii. Hướng dẫn để quyết định xem liệu có cần tăng cấp xử lý trong từng quy trình liên quan không, người được chuyển xử lý, và các thủ tục liên quan. Dựa trên hướng dẫn trong hệ thống tài liệu về lược đồ quản lý sự cố an toàn thông tin thì người đánh giá sự kiện, sự cố hoặc điểm yếu an toàn thông tin phải biết trong các tình huống nào thì cần tăng cấp xử lý, và người cần được chuyển xử lý. Hơn nữa, vẫn có những tình huống chưa biết trước có thể cần tăng cấp xử lý. Ví dụ, một sự cố an toàn thông tin nhỏ có thể phát triển thành một tình huống nghiêm trọng hoặc khủng hoảng nếu không được xử lý một cách phù hợp hoặc một sự cố an toàn thông tin nhỏ không được theo dõi trong vòng một tuần cũng có thể trở thành một sự cố an toàn thông tin lớn. Hướng dẫn cần xác định các loại sự kiện và sự cố an toàn thông tin, các hình thức tăng cấp xử lý và người có thể bắt đầu việc tăng cấp xử lý.

iv. Các thủ tục cần tuân thủ để đảm bảo rằng mọi hoạt động quản lý an toàn thông tin đều được ghi nhật ký một cách thích hợp trong mẫu phù hợp và việc phân tích nhật ký đó được thực hiện bởi người được chỉ định.

v. Các thủ tục và cơ chế để đảm bảo rằng cách thức kiểm soát thay đổi được duy trì đối với việc truy vết sự kiện, sự cố và điểm yếu an toàn thông tin và các cập nhật của báo cáo sự kiện/sự cố/điểm yếu an toàn thông tin, và các thông tin đó được tự cập nhật vào lược đồ.

vi. Các thủ tục phân tích điều tra an toàn thông tin.

vii. Các thủ tục và hướng dẫn sử dụng các Hệ thống phát hiện xâm nhập (IDS), trong đó đảm bảo rằng các khía cạnh pháp lý và quy định liên quan đều được đề cập. Hướng dẫn cũng cần đưa cả các thuận lợi và khó khăn khi tiến hành các hoạt động giám sát tấn công. Thông tin chi tiết hơn về IDS có trong ISO/IEC 18043: 2006.

viii. Hướng dẫn và các thủ tục liên quan đến các cơ chế kỹ thuật và tổ chức đã được thiết lập, triển khai và vận hành nhằm ngăn chặn xảy ra các sự cố an toàn thông tin, làm giảm xu hướng xảy ra các sự cố an toàn thông tin và xử lý các sự kiện an toàn thông tin đã xảy ra.

ix. Tài liệu cho chương trình đào tạo và nâng cao nhận thức về quản lý sự kiện, sự cố và điểm yếu an toàn thông tin.

x. Các thủ tục và chỉ tiêu kỹ thuật để thử nghiệm lược đồ quản lý sự cố an toàn thông tin.

xi. Lược đồ về cơ cấu tổ chức cho quản lý sự cố an toàn thông tin.

xii. Các điều khoản tham chiếu và trách nhiệm của ISIRT nói chung và của các cá nhân riêng lẻ.

xiii. Thông tin liên hệ quan trọng.

2) Phát hiện và báo cáo

i. Phát hiện và báo cáo về việc xảy ra các sự kiện an toàn thông tin (bằng con người hoặc các phương tiện tự động).

ii. Thu thập thông tin về các sự kiện an toàn thông tin.

iii. Phát hiện và báo cáo về các điểm yếu an toàn thông tin.

iv. Lập hồ sơ đầy đủ mọi thông tin tập hợp được trong cơ sở dữ liệu quản lý sự cố an toàn thông tin.

3) Đánh giá và quyết định

i. PoC tiến hành các đánh giá về các sự kiện an toàn thông tin (bao gồm cả việc tăng cấp xử lý theo yêu cầu), trong đó có sử dụng thang phân cấp sự kiện/sự cố an toàn thông tin đã được chấp nhận (gồm cả việc xác định các tác động của các sự kiện dựa trên các tài sản/dịch vụ bị ảnh hưởng) và quyết định xem liệu các sự kiện có cần được xếp loại là các sự cố an toàn thông tin không.

ii. ISIRT đánh giá các sự kiện an toàn thông tin cần xác nhận xem liệu sự kiện có là một sự cố an toàn thông tin hay không, và sau đó cần thực hiện một đánh giá khác sử dụng thang phân cấp sự kiện/sự cố đã được chấp nhận để xác nhận thông tin chi tiết về loại sự kiện (sự cố tiềm ẩn) và nguồn lực bị tác động (phân loại). Sau đó, cần đưa ra các quyết định về cách thức xử lý sự cố an toàn thông tin đã được xác nhận, người xử lý và mức độ ưu tiên, cũng như các mức tăng cấp xử lý.

iii. Đánh giá các điểm yếu an toàn thông tin (các điểm yếu này chưa bị khai thác để gây ra các sự kiện an toàn thông tin và các sự cố an toàn thông tin tiềm ẩn), trong đó quyết định xem cần xử lý cái gì, người xử lý, cách thức xử lý và mức ưu tiên.

iv. Ghi đầy đủ mọi kết quả đánh giá và các quyết định liên quan vào cơ sở dữ liệu quản lý sự cố an toàn thông tin.

4) Ứng phó

i. ISIRT thực hiện soát xét để xác định xem sự cố an toàn thông tin đó có đang được kiểm soát không, và

- Nếu sự cố đó đang được kiểm soát thì cần xúc tiến ứng phó được yêu cầu ngay tức thì (theo thời gian thực hoặc gần thực) hoặc tại thời điểm sau đó.

- Nếu sự cố đó đang không được kiểm soát hoặc sắp có tác động bất lợi lên các dịch vụ quan trọng của tổ chức thì cần xúc tiến các hoạt động ứng phó khủng hoảng theo cách tăng cấp xử lý lên bộ phận chức năng xử lý khủng hoảng.

ii. Xác lập một bản đồ tất cả các bộ phận chức năng và tổ chức trong nội bộ và bên ngoài có thể liên quan trong suốt quá trình quản lý sự cố.

iii. Tiến hành phân tích điều tra an toàn thông tin như yêu cầu.

iv. Tăng cấp xử lý theo cách thức được yêu cầu.

v. Đảm bảo rằng mọi các hoạt động liên quan đều được ghi nhật ký một cách phù hợp để sử dụng cho việc phân tích sau này.

vi. Đảm bảo rằng chứng cứ điện tử được tập hợp và lưu giữ an toàn một cách phù hợp.

vii. Đảm bảo rằng cách thức kiểm soát thay đổi được duy trì, và do đó cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin luôn được cập nhật.

viii. Truyền thông tin về sự tồn tại của sự cố an toàn thông tin hoặc các thông tin chi tiết liên quan tới các nhân viên hoặc tổ chức khác trong nội bộ hoặc bên ngoài.

ix. Xử lý các điểm yếu an toàn thông tin.

x. Khi sự cố đã được xử lý thành công thì sự cố phải chính thức được đóng lại và và ghi điều này vào cơ sở dữ liệu quản lý sự cố an toàn thông tin.

Mỗi tổ chức cần đảm bảo rằng hệ thống tài liệu lược đồ quản lý sự cố an toàn thông tin phải đưa ra các ứng phó tức thì hoặc dài hạn đối với sự cố an toàn thông tin. Mọi sự cố an toàn thông tin cần được đánh giá sớm về các tác động bất lợi tiềm ẩn lên các hoạt động nghiệp vụ, cả ngắn hạn và dài hạn (ví dụ, một thảm họa lớn đôi khi có thể xảy ra sau một sự kiện an toàn thông tin ban đầu). Hơn nữa, cần có một số ứng phó cần thiết đối với các sự cố an toàn thông tin hoàn toàn chưa được dự đoán, khi đó các kiểm soát đặc biệt sẽ được yêu cầu. Thậm chí trong tình huống này, các tổ chức cần thực hiện các hướng dẫn chung trong hệ thống tài liệu lược đồ theo các bước cần thiết.

5) Rút ra các bài học kinh nghiệm

i. Tiến hành phân tích điều tra an toàn thông tin sâu hơn theo yêu cầu.

ii. Xác định các bài học kinh nghiệm từ các sự cố và điểm yếu an toàn thông tin.

iii. Soát xét, xác định và thực hiện các cải tiến trong việc triển khai các biện pháp kiểm soát an toàn thông tin (các biện pháp kiểm soát mới và/hoặc cập nhật) và chính sách quản lý sự cố an toàn thông tin sau khi đã rút ra các bài học kinh nghiệm.

iv. Soát xét, xác định và nếu có thể thì thực hiện các cải tiến đối với các kết quả đánh giá rủi ro an toàn thông tin hiện tại và soát xét của ban quản lý sau khi đã rút ra các bài học kinh nghiệm.

v. Soát xét tính hiệu lực của các quy trình, thủ tục, các mẫu báo cáo và/hoặc cơ cấu tổ chức trong việc đáp ứng với việc đánh giá và khôi phục từ mỗi sự cố an toàn thông tin và xử lý các điểm yếu an toàn thông tin, và trên cơ sở các bài học kinh nghiệm phải xác định và thực hiện các cải tiến đối với lược đồ quản lý sự cố an toàn thông tin và hệ thống tài liệu lược đồ.

vi. Cập nhật cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin.

vii. Thông tin và chia sẻ các kết quả soát xét trong một cộng đồng tin cậy (nếu tổ chức mong muốn).

5.4.4 Các thủ tục

Trước khi có thể bắt đầu vận hành lược đồ quản lý sự cố an toàn thông tin thì điều quan trọng là tổ chức đã ghi vào văn bản và kiểm tra cho thấy các thủ tục đã sẵn sàng. Mỗi thủ tục cần chỉ ra các nhóm hoặc các cá nhân chịu trách nhiệm sử dụng và quản lý thủ tục đó, mà phù hợp nhất là người của PoC và/hoặc ISIRT. Các thủ tục đó cần đảm bảo rằng chứng cứ điện tử được tập hợp và lưu giữ an toàn, và sự bảo quản an toàn chứng cứ được giám sát liên tục vì chứng cứ có thể được yêu cầu cho hành động khởi tố hoặc kỷ luật nội bộ. Hơn nữa, cần có các thủ tục được lập tài liệu không chỉ về các hoạt động của PoC và ISIRT mà cả các hoạt động liên quan trong quá trình phân tích điều tra an toàn thông tin và các hoạt động ứng phó khủng hoảng – nếu chúng chưa nằm trong tài liệu nào khác, ví dụ trong kế hoạch nghiệp vụ liên tục hoặc kế hoạch quản lý khủng hoảng. Các thủ tục được lập tài liệu cần hoàn toàn thống nhất với chính sách quản lý an toàn thông tin được lập tài liệu và hệ thống tài liệu lược đồ quản lý sự cố an toàn thông tin khác.

Điều quan trọng là phải hiểu rằng không phải mọi thủ tục đều cần được cung cấp rộng rãi. Ví dụ, không phải mọi nhân viên thuộc tổ chức đều cần phải hiểu về sự vận hành nội bộ của ISIRT khi tương tác với nhóm này. ISIRT cần đảm bảo rằng hướng dẫn được cung cấp rộng rãi, bao gồm cả thông tin có được từ phân tích sự cố an toàn thông tin, phải luôn ở dạng sẵn sàng, ví dụ trên mạng nội bộ của tổ chức. Việc giữ bí mật một vài thông tin chi tiết về lược đồ quản lý sự cố an toàn thông tin có thể cũng rất quan trọng để đề phòng người trong nội bộ can thiệp vào quá trình điều tra. Ví dụ, nếu một nhân viên ngân hàng biển thủ ngân quỹ biết được một số thông tin chi tiết về lược đồ thì họ có thể dễ dàng che dấu các hoạt động của mình trước các nhân viên điều tra hoặc gây cản trở việc cho việc phát hiện, điều tra và khôi phục sau sự cố an toàn thông tin.

Nội dung của các thủ tục vận hành phụ thuộc vào nhiều tiêu chí, đặc biệt có liên quan đến tính chất của các sự kiện, sự cố, điểm yếu an toàn thông tin tiềm ẩn đã biết và các loại tài sản hệ thống thông tin có thể liên quan và môi trường của chúng. Do vậy, mỗi thủ tục vận hành có thể liên quan đến một loại sự kiện hoặc sản phẩm cụ thể (ví dụ: tường lửa, cơ sở dữ liệu, hệ điều hành, ứng dụng) hoặc một sản phẩm cụ thể. Thủ tục vận hành cần xác định rõ các bước cần được thực hiện và người thực hiện. Thủ tục vận hành cần phản ánh kinh nghiệm từ các nguồn bên ngoài (ví dụ, các ISIRT thương mại và chính phủ hoặc tương tự như vậy, và các nhà cung cấp) cũng như từ các nguồn nội bộ.

Cần có các thủ tục vận hành để xử lý các loại sự kiện, sự cố và điểm yếu an toàn thông tin đã biết. Cũng cần có các thủ tục vận hành để xử lý các sự kiện, sự cố và điểm yếu an toàn thông tin không thuộc các loại đã biết. Trong trường hợp này, các vấn đề sau cần được đề cập:

a) quy trình báo cáo về việc xử lý các ngoại lệ,

b) hướng dẫn về thời gian có được sự chấp thuận của cấp quản lý nhằm tránh mọi chậm trễ trong việc đối phó,

c) việc ủy quyền trước trong việc đưa ra quyết định mà không cần theo quy trình phê chuẩn thông thường.

5.4.5 Sự tin cậy

ISIRT đóng vai trò quyết định đối với sự an toàn thông tin tổng thể của mỗi tổ chức. ISIRT đòi hỏi có sự cộng tác của mọi cá nhân thuộc tổ chức trong việc phát hiện, giải quyết và điều tra các sự cố an toàn thông tin. Về cơ bản, ISIRT được tất cả mọi người cả trong và ngoài tổ chức tin tưởng. Sự chấp nhận việc báo cáo các điểm yếu, sự kiện và sự cố an toàn thông tin từ nguồn ẩn danh cũng có thể có lợi trong việc xây dựng sự tin cậy.

Các tổ chức cần đảm bảo rằng lược đồ quản lý sự cố an toàn thông tin có đề cập đến các tình huống mà trong đó điều quan trọng là phải đảm bảo sự ẩn danh của người hoặc tổ chức báo cáo về các sự cố hoặc điểm yếu an toàn thông tin tiềm ẩn trong các hoàn cảnh cụ thể. Tổ chức cũng cần có các điều khoản thể hiện rõ mong muốn được những người hoặc các bên ẩn danh báo cáo về sự kiện hoặc điểm yếu an toàn thông tin tiềm ẩn. ISIRT có thể cần nhận được các thông tin bổ sung mà lúc đầu chưa được người hoặc bên báo cáo sự cố cung cấp. Hơn nữa, các thông tin quan trọng về sự cố hoặc điểm yếu an toàn thông tin có thể lại được lấy từ người phát hiện đầu tiên.

Một phương pháp tiếp cận khác có thể được ISIRT chấp nhận là có được sự tin cậy của người dùng nhờ các quy trình hoàn thiện và minh bạch. ISIRT cần đào tạo người dùng, giải thích cách ISIRT làm việc, cách ISIRT bảo vệ tính bí mật của thông tin được thu thập và cách ISIRT quản lý các báo cáo của người dùng về các sự kiện, sự cố và điểm yếu.

ISIRT cần có thể đáp ứng một cách hiệu quả các nhu cầu về chức năng, tài chính, pháp lý và chính trị của tổ chức và có thể tự quyết định về tổ chức khi quản lý các sự kiện và điểm yếu an toàn thông tin. Chức năng của ISIRT cũng cần được kiểm tra một cách độc lập để xác nhận rằng mọi yêu cầu về nghiệp vụ đều đang được thỏa mãn một cách hiệu quả.

Thêm nữa, có một cách phù hợp để có được sự kiểm tra độc lập là tách chuỗi công việc báo cáo sự cố và điểm yếu an toàn thông tin khỏi ban quản lý điều hành và trao trách nhiệm trực tiếp quản lý các ứng phó với sự cố và điểm yếu an toàn thông tin cho một người quản lý cấp cao. Năng lực về tài chính cũng cần được tách bạch để tránh các tác động không đáng có.

5.4.6 Tính bí mật

Lược đồ quản lý sự cố an toàn thông tin có thể chứa thông tin nhạy cảm, và những người tham gia vào việc giải quyết các sự cố và điểm yếu có thể được yêu cầu xử lý các thông tin nhạy cảm. Mỗi tổ chức cần đảm bảo có các thủ tục cần thiết được thiết lập để ẩn danh thông tin nhạy cảm và yêu cầu những người truy cập tới thông tin nhạy cảm phải ký vào các thỏa thuận về sự bí mật. Nếu các sự kiện/sự cố/điểm yếu an toàn thông tin được ghi nhật ký qua một hệ thống quản lý lỗi tập trung thì các thông tin nhạy cảm chi tiết có thể phải bị bỏ qua. Hơn nữa, mỗi tổ chức cần đảm bảo rằng lược đồ quản lý sự cố an toàn thông tin có chuẩn bị để kiểm soát việc truyền thông về các sự cố và điểm yếu tới các bên bên

ngoài, bao gồm giới truyền thông, các đối tác nghiệp vụ, các khách hàng, các tổ chức hành pháp và công chúng nói chung.

5.5 Thành lập ISIRT

5.5.1 Giới thiệu

Mục đích thành lập ISIRT là cung cấp cho tổ chức năng lực phù hợp để đánh giá, ứng phó và học hỏi từ các sự cố an toàn thông tin, và cung cấp sự phối hợp, quản lý, phản hồi và truyền thông cần thiết. ISIRT góp phần trong việc giảm nhẹ các thiệt hại vật chất và kinh tế, cũng như giảm nhẹ sự tổn hại danh tiếng của tổ chức mà đôi khi có liên quan đến các sự cố an toàn thông tin.

5.5.2 Các thành viên và cấu trúc

Quy mô, cấu trúc và thành phần của ISIRT cần phù hợp với quy mô, cấu trúc và tính chất nghiệp vụ của tổ chức. Mặc dù ISIRT có thể là một nhóm hoặc phòng ban riêng nhưng các thành viên cũng có thể có thêm các nhiệm vụ khác, tức là khuyến khích sử dụng các thành viên từ nhiều khu vực thuộc tổ chức. Mỗi tổ chức cần đánh giá xem tổ chức cần ISIRT là nhóm riêng, nhóm ảo hay dưới dạng pha trộn của cả hai hình thức này. Để lựa chọn, tổ chức cần dựa vào số lượng sự cố và các hoạt động do ISIRT thực hiện.

ISIRT trải qua các giai đoạn hoàn thiện khác nhau và thường các điều chỉnh về mô hình tổ chức sẽ được chấp nhận dựa trên kịch bản cụ thể mà tổ chức phải đối mặt. Mọi minh chứng đều đưa đến một khuyến nghị rằng đó nên là một nhóm cố định dưới sự chỉ đạo của một người quản lý cấp cao. Các nhóm ISIRT ảo có thể cũng được chỉ đạo bởi một người quản lý cấp cao. Người quản lý cấp cao cần được những người có chuyên môn trong các lĩnh vực cụ thể hỗ trợ, ví dụ trong việc xử lý các tấn công của mã độc, họ sẽ được gọi đến tùy theo loại sự cố an toàn thông tin cần quan tâm. Tùy thuộc vào quy mô, cấu trúc và tính chất nghiệp vụ của tổ chức mà mỗi thành viên có thể còn phải đảm nhiệm nhiều vai trò trong ISIRT. ISIRT có thể gồm những người từ các bộ phận khác nhau của tổ chức (ví dụ, các bộ phận điều hành nghiệp vụ, ICT, kiểm tra, nhân sự và tiếp thị). Điều này cũng áp dụng đối với các ISIRT cố định; thậm chí trong trường hợp có nhân sự chuyên nghiệp thì ISIRT cũng luôn đòi hỏi có sự hỗ trợ từ các phòng ban khác.

Các thành viên của nhóm phải dễ liên lạc, do vậy tên và các thông tin liên lạc của họ và của các thành viên dự phòng phải luôn sẵn sàng trong tổ chức. Các thông tin chi tiết cần thiết cần được chỉ rõ trong hệ thống tài liệu lược đồ quản lý sự cố an toàn thông tin, bao gồm mọi tài liệu về thủ tục, và các mẫu báo cáo, nhưng không có trong các tuyên bố về chính sách.

Người quản lý ISIRT phải luôn có kênh báo cáo riêng đến ban quản lý cấp cao, tách bạch khỏi các vận hành nghiệp vụ thông thường. Người quản lý ISIRT cần được ủy quyền đưa ra các quyết định tức thì về cách xử lý sự cố, và cần đảm bảo rằng mọi thành viên của ISIRT đều có mức độ kiến thức và kỹ năng như yêu cầu, và điều đó phải luôn được duy trì. Người quản lý ISIRT cần phân trách nhiệm điều tra về từng sự cố cho thành viên phù hợp nhất trong nhóm, mỗi sự cố được phân cho một người quản lý.

5.5.3 Mối quan hệ với các bộ phận khác của tổ chức

ISIRT cần chịu trách nhiệm đảm bảo rằng các sự cố đều được giải quyết, và về vấn đề này thì người quản lý ISIRT và các thành viên trong nhóm cần có một mức quyền để thực hiện các hành động cần thiết được cho là phù hợp để ứng phó với các sự cố an toàn thông tin. Tuy nhiên, các hành động mà có thể có các tác động bất lợi lên toàn bộ tổ chức, cả về mặt tài chính và danh tiếng, thì cần được thỏa thuận với ban quản lý cấp cao. Vì lý do này mà lược đồ và chính sách quản lý sự cố an toàn thông tin cần phải đưa chi tiết về mức quyền phù hợp để người quản lý ISIRT báo cáo về các sự cố an toàn thông tin nghiêm trọng.

Các thủ tục và trách nhiệm trong việc xử lý về truyền thông cũng cần được thỏa thuận với ban quản lý cấp cao và được lập thành tài liệu. Các thủ tục này cần chỉ rõ ai trong tổ chức sẽ xử lý với các yêu cầu của truyền thông, và cách để bộ phận đó của tổ chức tương tác với ISIRT.

5.5.4 Mối quan hệ với các bên có lợi ích bên ngoài

Các tổ chức cần thiết lập các mối quan hệ giữa ISIRT các bên có lợi ích bên ngoài phù hợp . Các bên có lợi ích bên ngoài có thể gồm:

a) nhân viên hỗ trợ bên ngoài theo hợp đồng,

b) các ISIRT của các tổ chức bên ngoài,

c) các nhà cung cấp dịch vụ được quản lý, bao gồm các nhà cung cấp dịch vụ viễn thông, các ISP và các nhà cung cấp dịch vụ khác,

d) các tổ chức hành luật,

e) các cơ quan tình trạng khẩn cấp,

f) các tổ chức chính phủ thích hợp,

g) nhân viên pháp lý,

h) các nhân viên quan hệ công chúng và/hoặc các thành viên truyền thông,

i) các đối tác nghiệp vụ,

j) các khách hàng,

k) công chúng nói chung.

5.6 Hỗ trợ kỹ thuật và các hỗ trợ khác (bao gồm cả hỗ trợ vận hành)

Để đảm bảo có thể có được các ứng phó nhanh chóng và hiệu lực đối với các sự cố an toàn thông tin thì mỗi tổ chức cần có, chuẩn bị và kiểm tra mọi phương tiện hỗ trợ kỹ thuật và hỗ trợ khác cần thiết. Các phương tiện hỗ trợ bao gồm:

a) truy cập đến các thông tin chi tiết về các tài sản của tổ chức cùng với đăng ký tài sản cập nhật và thông tin về các liên hệ của chúng với các bộ phận chức năng nghiệp vụ,

b) truy cập đến các thủ tục được lập tài liệu liên quan đến quản lý khủng hoảng,

c) các quy trình truyền thông được lập tài liệu và được công bố chính thức,

d) việc sử dụng cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin và các phương tiện kỹ thuật để ghi và cập nhật cơ sở dữ liệu một cách nhanh chóng, phân tích thông tin cơ sở dữ liệu và hỗ trợ các ứng phó (trong một số trường hợp, tổ chức có thể cần đến các hồ sơ viết tay), khi đó cơ sở dữ liệu vẫn được giữ an toàn một cách phù hợp,

e) các phương tiện hỗ trợ cho thu thập và phân tích chứng cứ điều tra an toàn thông tin,

f) các chuẩn bị quản lý khủng hoảng phù hợp dành cho cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin (xem hướng dẫn quản lý sự liên tục về nghiệp vụ trong ISO/IEC 27031).

Mỗi tổ chức cần đảm bảo rằng các phương tiện kỹ thuật được sử dụng để ghi và cập nhật cơ sở dữ liệu một cách nhanh chóng, phân tích thông tin trong đó và hỗ trợ các ứng phó với các sự cố an toàn thông tin phải hỗ trợ các việc sau:

g) nhanh chóng có được các báo cáo sự kiện/sự cố/điểm yếu an toàn thông tin,

h) thông báo của người bên ngoài được lựa chọn trước bằng các phương tiện phù hợp (ví dụ thư điện tử, fax hoặc điện thoại), do vậy đòi hỏi duy trì một cơ sở dữ liệu liên hệ tin cậy, sẵn sàng cho truy cập (gồm cả cơ sở dữ liệu dự phòng trên giấy và các hình thức dự phòng khác), và phương tiện hỗ trợ để truyền thông tin tới các cá nhân theo hình thức an toàn phù hợp,

i) có những đề phòng tương xứng với các rủi ro đã được đánh giá để đảm bảo rằng sự truyền thông tin điện tử, dù là internet hay không phải internet, không thể bị nghe lén và vẫn luôn sẵn sàng trong hệ thống, dịch vụ và/hoặc mạng đang bị tấn công (điều này có thể đòi hỏi các cơ chế truyền thông khác được chuẩn bị từ trước phải được triển khai),

j) đảm bảo thu thập mọi dữ liệu về hệ thống, dịch vụ và/hoặc mạng thông tin, và mọi dữ liệu đã được xử lý,

k) sử dụng biện pháp kiểm soát sự toàn vẹn bằng mật mã để giúp xác định xem liệu và các bộ phận nào của hệ thống, dịch vụ và/hoặc mạng , và dữ liệu nào đã bị thay đổi, những thay đổi đó có tương xứng với các rủi ro đã được đánh giá không,

l) hỗ trợ để có được và đảm bảo an toàn cho thông tin thu thập được (ví dụ, bằng cách sử dụng chữ ký số cho nhật ký và các chứng cứ khác trước khi được lưu giữ trong các phương tiện chỉ cho phép đọc như CD hoặc DVD ROM),

m) cho phép chuẩn bị các bản in (ví dụ của các nhật ký), bao gồm cả các bản in thể hiện tiến trình của sự cố, quy trình giải quyết và chứng nhận chuỗi hành trình sản phẩm,

n) khôi phục hệ thống, dịch vụ và/hoặc mạng thông tin trở về trạng thái hoạt động bình thường bằng các thủ tục sau đồng bộ với việc quản lý khủng hoảng liên quan:

   1) kiểm tra dự phòng,

2) kiểm soát mã độc,

3) phương tiện truyền thông gốc có phần mềm hệ thống và ứng dụng,

4) phương tiện truyền thông có khả năng khởi động,

5) các bản vá hệ thống và ứng dụng sạch, tin cậy và cập nhật.

Thông thường, các tổ chức thiết lập một hình ảnh chuẩn từ phương tiện cài đặt và sử dụng hình ảnh chuẩn đó như nền tảng sạch để thiết lập các hệ thống. Việc sử dụng hình ảnh như vậy thay cho phương tiện lưu trữ ban đầu thường phổ biến vì hình ảnh đã được vá, làm ổn định và đã được kiểm tra...

Hệ thống, dịch vụ hoặc mạng bị tấn công có thể không hoạt động đúng. Do vậy, không nên tin tưởng hoàn toàn vào các vận hành của mọi phương tiện kỹ thuật (phần cứng và phần mềm) cần để ứng phó với mỗi sự kiện an toàn thông tin trên các hệ thống , dịch vụ và/hoặc mạng chủ đạo của tổ chức, tùy theo các rủi ro đã được đánh giá. Tất cả các phương tiện kỹ thuật đều cần được lựa chọn cẩn thận, được triển khai đúng cách thức và được kiểm tra thường xuyên (các phương tiện dự phòng cũng phải được kiểm tra). Nếu có thể thì các phương tiện kỹ thuật cần hoàn toàn độc lập với nhau.

CHÚ THÍCH: Các phương tiện kỹ thuật được mô tả trong điều này không bao gồm các phương tiện kỹ thuật được sử dụng để phát hiện các sự cố an toàn thông tin và các xâm nhập trực tiếp, và tự động thông báo cho những người phù hợp. Các phương tiện kỹ thuật như vậy được mô tả trong ISO/IEC 18043.

Mặc dù PoC của tổ chức có vai trò đang ngày càng lớn trong việc cung cấp các hỗ trợ trên mọi khía cạnh xử lý IT và thông tin liên quan nhưng nhóm này cũng có vai trò chính trong việc quản lý sự cố an toàn thông tin. Khi các sự kiện an toàn thông tin được báo cáo lần đầu, PoC sẽ giải quyết chúng trong giai đoạn phát hiện và báo cáo. PoC cần xem xét thông tin được tập hợp và thực hiện đánh giá ban đầu xem liệu các sự kiện có cần được xếp loại là sự cố hay không. Nếu sự kiện không được xếp loại là sự cố thì PoC cần xử lý chúng sao cho phù hợp. Nếu một sự kiện được xếp loại là sự cố thì có thể PoC sẽ xử lý chúng, mặc dù vậy đa số trường hợp đều mong rằng trách nhiệm xử lý sự cố cần được chuyển cho ISIRT. Người của PoC không cần phải là các chuyên gia an toàn.

5.7 Đào tạo và nâng cao nhận thức

Quản lý sự cố an toàn thông tin là một quy trình không chỉ liên quan đến các phương tiện kỹ thuật mà còn cả con người. Do vậy, quy trình này cần được hỗ trợ bởi những người đào tạo và có nhận thức phù hợp về an toàn thông tin trong tổ chức.

Sự nhận thức và tham gia của mọi cá nhân trong tổ chức có ý nghĩa quyết định cho sự thành công của phương pháp tiếp cận quản lý sự cố an toàn thông tin có cấu trúc. Mặc dù người dùng cần được yêu cầu tham gia nhưng họ ít có xu hướng tham gia hiệu quả vào việc vận hành quy trình nếu họ chưa nhận thấy lợi ích mà họ và phòng ban của họ có thể có được từ việc tham gia vào phương pháp tiếp cận có cấu trúc để quản lý sự cố an toàn thông tin. Hơn nữa, tính hiệu lực trong điều hành và chất lượng của một phương pháp tiếp cận có cấu trúc để quản lý sự cố an toàn thông tin tùy thuộc vào nhiều yếu tố, bao gồm nghĩa vụ thông báo sự cố, chất lượng của thông báo, tính dễ sử dụng, sự nhanh

chóng và quá trình đào tạo. Một vài trong số các yếu tố này liên quan đến việc đảm bảo chắc chắn rằng người dùng nhận thức được giá trị của việc quản lý sự cố an toàn thông tin và được khuyến khích báo cáo các sự cố.

Tổ chức cần đảm bảo rằng vai trò của quản lý sự cố an toàn thông tin được nâng cao một cách tích cực trong chương trình đào tạo và nâng cao nhận thức về an toàn thông tin ở cấp độ tổ chức. Tài liệu về chương trình nâng cao nhận thức và các tài liệu liên quan cần sẵn sàng được cung cấp cho mọi nhân viên, kể cả các nhân viên mới, người dùng thuộc bên thứ ba và các nhà thầu, nếu thích hợp. Nếu cần thì phải có một chương trình đào tạo riêng cho các thành viên PoC, ISIRT, nhân viên an toàn thông tin và các nhà quản trị cụ thể. Mỗi nhóm người liên quan trực tiếp đến việc quản lý sự cố có thể cần các cấp độ đào tạo khác nhau tùy theo loại hình, tần suất và tầm quan trọng của tương tác của họ với lược đồ quản lý sự cố an toàn thông tin.

Các chỉ dẫn nâng cao nhận thức của tổ chức cần gồm các vấn đề sau:

a) các lợi ích cần có từ phương pháp tiếp cận quản lý sự cố an toàn thông tin có cấu trúc đối với tổ chức và nhân viên của tổ chức,

b) cách thức hoạt động của lược đồ quản lý sự cố an toàn thông tin, gồm cả phạm vi và luồng công việc quản lý sự kiện, sự cố và điểm yếu an toàn,

c) cách báo cáo các sự kiện, sự cố và điểm yếu an toàn thông tin,

d) thông tin sự cố và các đầu ra từ cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin,

e) các biện pháp kiểm soát tính bí mật của các nguồn tin liên quan,

f) các thỏa thuận mức dịch vụ của lược đồ,

g) thông báo về các kết quả - ở những tình huống nào thì các nguồn cấp tin sẽ được hỏi đến,

h) các hạn chế được áp bởi các thỏa thuận bảo mật,

i) thẩm quyền của tổ chức quản lý sự cố an toàn thông tin và luồng báo cáo,

j) người nhận các báo cáo từ lược đồ quản lý sự cố an toàn thông tin, và cách thức các báo cáo được chuyển đi.

Trong một số trường hợp, tổ chức có thể mong muốn đưa thông tin chi tiết về việc nâng cao nhận thức, đặc biệt là về quản lý sự cố an toàn thông tin, vào các chương trình đào tạo khác (ví dụ, các chương trình định hướng về nhân sự hoặc các chương trình nâng cao nhận thức về an toàn ở cấp độ tổ chức nói chung). Cách tiếp cận theo nhận thức này có thể cung cấp nội dung giá trị cho các nhóm người cụ thể và cải thiện tính hiệu quả và hiệu lực của chương trình đào tạo.

Trước khi lược đồ quản lý sự cố an toàn thông tin trở nên khả dụng thì tổ chức cần đảm bảo rằng mọi cá nhân liên quan đều đã quen với các thủ tục trong việc việc phát hiện và báo cáo các sự kiện an toàn thông tin, và những người được lựa chọn đều có kiến thức rất tốt về các hoạt động tiếp theo. Việc này cần được thực hiện bằng các chỉ dẫn nâng cao nhận thức và các khóa đào tạo thường xuyên. Việc

đào tạo cần được hỗ trợ bằng các bài tập cụ thể và việc sát hạch các thành viên của PoC và ISIRT, nhân viên an toàn thông tin và các cán bộ quản trị cụ thể.

Hơn nữa, các chương trình đào tạo và nâng cao nhận thức cần được bổ trợ bằng việc thiết lập và vận hành hỗ trợ "đường dây nóng" của các nhân viên quản lý sự cố an toàn thông tin nhằm tối giảm sự chậm trễ trong việc báo cáo và xử lý các sự kiện, sự cố và điểm yếu an toàn thông tin.

5.8 Thử nghiệm lược đồ

Tổ chức cần lập lịch kiểm tra và thử nghiệm các quy trình và thủ tục quản lý sự cố an toàn thông tin thường xuyên để chỉ ra các thiếu sót và lỗi tiềm ẩn có thể xuất hiện trong khi quản lý các sự kiện, sự cố và điểm yếu an toàn thông tin. Các thử nghiệm định kỳ cần được tổ chức để kiểm tra các quy trình/thủ tục và xác nhận lại cách thức mà ISIRT ứng phó với các sự cố cực kỳ phức tạp thông qua việc mô phỏng các tấn công, thất bại hoặc lỗi thực tế. Cần đặc biệt lưu ý đến việc thiết lập các kịch bản mô phỏng, các kịch bản này cần dựa trên những mối đe dọa an toàn thông tin mới và thực tế. Các thử nghiệm cần có sự tham gia không chỉ của ISIRT mà tất cả các tổ chức nội bộ và bên ngoài tham gia vào việc quản lý các sự kiện an toàn thông tin. Các tổ chức cần đảm bảo rằng mọi thay đổi có được sau khi thực hiện các soát xét sau thử nghiệm đều phải được kiểm tra một cách thấu đáo, kể cả được thử nghiệm tiếp, trước khi lược đồ đã thay đổi được đưa vào vận hành.

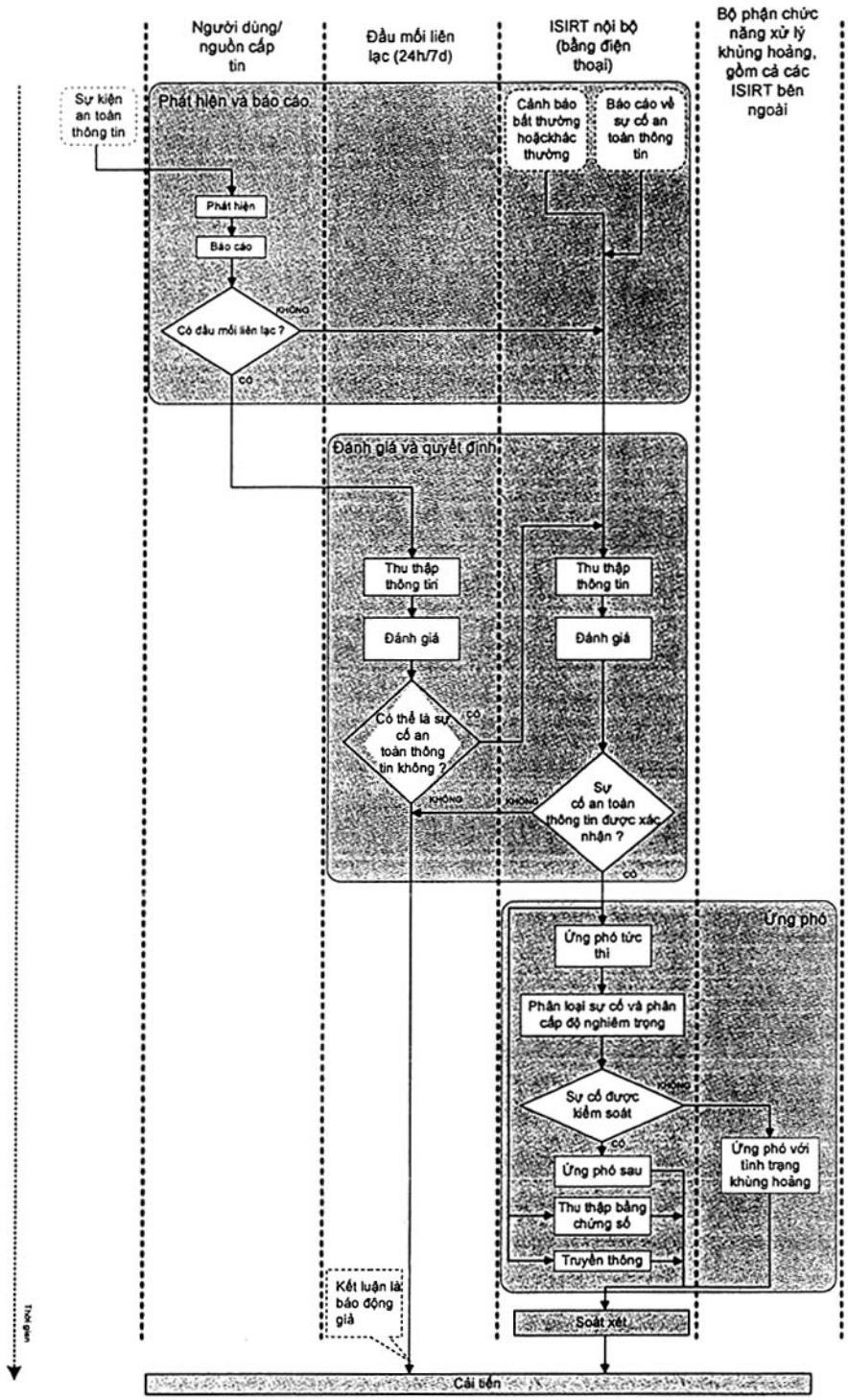
6 Giai đoạn phát hiện và báo cáo

6.1 Tổng quan về các hoạt động chính

Giai đoạn đầu tiên trong việc sử dụng vận hành lược đồ quản lý sự cố an toàn thông tin gồm phát hiện, thu thập thông tin liên quan, và báo cáo về việc xảy ra các sự kiện an toàn thông tin và sự tồn tại của các điểm yếu an toàn thông tin bằng con người hoặc các phương tiện tự động. Việc vận hành quản lý sự cố an toàn thông tin gồm ba giai đoạn chính: Phát hiện và báo cáo, Đánh giá và quyết định (xem điều 7) và Ứng phó (xem điều 8). Giai đoạn Rút bài học kinh nghiệm được thực hiện tiếp theo các giai đoạn này khi các cải tiến đã được xác định và thực hiện. Các giai đoạn này và các hoạt động liên quan đã được giới thiệu trong 4.5.

Các điều tiếp theo chủ yếu đề cập đến việc xử lý các sự kiện và sự cố an toàn thông tin. Tổ chức cần đảm bảo rằng người phù hợp sẽ xử lý các điểm yếu an toàn thông tin đã được báo cáo theo cách tương tự với cách mà các lỗi không phải là an toàn thông tin được xử lý, trong đó có thể việc đánh giá và giải quyết có sử dụng nhân viên kỹ thuật (người này có thể hoặc không phải là thành viên của ISIRT). Thông tin về các điểm yếu và các giải pháp cho chúng cần được đưa vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin do ISIRT quản lý. Phụ lục D đưa ra một ví dụ về mẫu báo cáo điểm yếu an toàn thông tin.

Hình 3 mô tả tất cả các giai đoạn vận hành và các hoạt động liên quan.



Hình 3 – Sơ đồ luồng sự kiện và sự cố an toàn thông tin

CHÚ THÍCH: Báo động giả là một chỉ thị về một sự kiện không mong muốn nhưng đã được thấy rằng không có thật hoặc không gây bất cứ hậu quả nào.

Giai đoạn đầu tiên của sử dụng vận hành lược đồ quản lý sự cố an toàn thông tin gồm phát hiện, thu thập thông tin liên quan và báo cáo về việc xảy ra các sự kiện an toàn thông tin bằng con người hoặc các phương tiện tự động. Tổ chức cần đảm bảo rằng giai đoạn này bao gồm cả việc phát hiện các điểm yếu an toàn thông tin chưa bị khai thác để gây nên các sự kiện an toàn thông tin, và có thể cả các sự cố an toàn thông tin, và báo cáo về chúng.

Đối với giai đoạn Phát hiện và báo cáo, tổ chức cần đảm bảo các hoạt động chính gồm:

a) Hoạt động để phát hiện và báo cáo về việc xảy ra sự kiện an toàn thông tin hoặc sự tồn tại của điểm yếu an toàn thông tin, cho dù do một trong các nhân viên/khách hàng của tổ chức thực hiện hoặc thực hiện tự động, được hỗ trợ bởi:

   1) các cảnh báo từ các hệ thống giám sát an ninh như IDS/IPS, chương trình chống virút, honeypot (thuật ngữ chung dùng cho hệ thống bẫy được sử dụng để đánh lừa, làm sao nhãng, làm chuyển hướng và khuyến khích những kẻ tấn công tiêu tốn thời gian vào các thông tin có vẻ rất giá trị nhưng thực tế lại bị giả mạo và là mối quan tâm của người dùng hợp pháp [ISO/IEC 27039:2015])/tarpit (các hệ thống bị đặt vào nguy hiểm một cách có chủ ý và được thiết kế để làm chậm các cuộc tấn công), các hệ thống giám sát nhật ký, các hệ thống quản lý thông tin an ninh, các công cụ tương quan và các phương tiện khác,

   2) các cảnh báo từ các hệ thống giám sát mạng như tường lửa, phân tích luồng thông tin trong mạng, lọc web và các hệ thống khác,

   3) phân tích thông tin nhật ký từ các thiết bị, dịch vụ, máy chủ, và nhiều các hệ thống khác,

   4) sự tăng cấp xử lý với các sự kiện bất thường được ICT phát hiện,

   5) sự tăng cấp xử lý với các sự kiện bất thường được hệ thống hỗ trợ phát hiện,

   6) các báo cáo của người dùng,

   7) các thông báo từ bên ngoài đến từ bên thứ ba như các ISIRT khác, các dịch vụ an toàn thông tin, các ISP, các nhà cung cấp dịch vụ viễn thông, các công ty thuê ngoài hoặc các ISIRT của quốc gia.

b) Hoạt động để thu thập thông tin về sự kiện hoặc điểm yếu an toàn thông tin.

c) Hoạt động để đảm bảo rằng mọi thành viên tham gia vào PoC đều ghi nhật ký một cách phù hợp mọi hoạt động, kết quả và quyết định liên quan để dùng cho việc phân tích sau này.

d) Hoạt động để đảm bảo rằng chứng cứ điện tử được tập hợp và lưu giữ an toàn, và sự bảo quản an toàn chứng cứ được giám sát liên tục trong trường hợp chúng được yêu cầu cho hoạt động khởi tố hoặc kỷ luật nội bộ.

CHÚ THÍCH: Tiêu chuẩn quốc tế sau này (ISO/IEC 27037) sẽ cung cấp thông tin chi tiết hơn về việc xác định, thu thập, tiếp nhận và bảo quản chứng cứ số.

e) Hoạt động để đảm bảo rằng cách thức kiểm soát thay đổi được duy trì đối với việc truy vết sự kiện và điểm yếu an toàn thông tin và các cập nhật trong báo cáo sự kiện và điểm yếu, và do đó cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin sẽ luôn được cập nhật.

f) Hoạt động để tăng cấp xử lý, trên cơ sở theo yêu cầu cho toàn giai đoạn, đối với việc soát xét và/hoặc quyết định thêm.

g) Hoạt động để đăng ký vào một Hệ thống truy vết sự cố.

Mọi thông tin được thu thập liên quan đến mỗi sự kiện hoặc điểm yếu an toàn thông tin cần được lưu giữ trong cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin do ISIRT quản lý. Thông tin được báo cáo trong mỗi hoạt động cần đầy đủ nhất có thể để đảm bảo rằng đó sẽ là cơ sở tốt sẵn sàng cho các đánh giá và quyết định sẽ được đưa ra, và cho cả các hành động phải được thực hiện.

6.2 Phát hiện sự kiện an toàn thông tin

Các sự kiện an toàn thông tin có thể được phát hiện trực tiếp bởi một hoặc nhiều người để ý thấy có điều gì đó đáng quan tâm, dù là có liên quan đến vấn đề kỹ thuật, vật lý hoặc thủ tục. Việc phát hiện có thể, ví dụ, từ các thiết bị báo cháy/báo khói hoặc các chuông báo đột nhập (trộm) có các cảnh báo thông báo tại các vị trí định trước về hành động của con người. Các sự kiện an toàn thông tin kỹ thuật có thể được phát hiện bằng các phương tiện tự động, ví dụ các cảnh báo thực hiện bởi các thiết bị phân tích truy vết kiểm tra, tường lửa, hệ thống phát hiện xâm nhập, và các công cụ chống mã độc (bao gồm cả virus), trong mọi trường hợp đều được mô phỏng bởi các tham số thiết lập trước.

Các nguồn phát hiện sự kiện an toàn thông tin có thể gồm:

a) người dùng,

b) người quản lý chuyên môn và người quản lý an toàn,

c) khách hàng,

d) phòng IT, bao gồm cả Trung tâm điều hành mạng và Trung tâm điều hành an toàn (trên hỗ trợ mức thứ 2),

e) bộ phận hỗ trợ IT (trên hỗ trợ mức thứ nhất),

f) những nhà cung cấp dịch vụ được quản lý (gồm các ISP, các nhà cung cấp dịch vụ viễn thông, và các nhà cung cấp dịch vụ khác),

g) các ISIRT,

h) các đơn vị và nhân viên khác có thể phát hiện ra các bất thường trong công việc hàng ngày của họ,

i) phương tiện truyền thông đại chúng (báo đài, truyền hình...),

j) các website (các website về an toàn cho công chúng, các website của các chuyên gia nghiên cứu về an toàn, các website lưu trữ...).

6.3 Báo cáo sự kiện an toàn thông tin

Cho dù nguồn phát hiện sự kiện an toàn thông tin là thế nào thì người được thông báo bằng các phương tiện tự động, hoặc trực tiếp để ý thấy có điều bất thường, cũng phải có trách nhiệm khởi động quy trình phát hiện và báo cáo. Người này có thể là thành viên bất kỳ trong nhân sự của tổ chức, cho dù là lao động biên chế hay theo hợp đồng.

Người đó cần tuân theo các thủ tục và sử dụng mẫu báo cáo sự kiện an toàn thông tin đã được quy định bởi lược đồ quản lý sự cố an toàn thông tin để sự kiện an toàn thông tin đó được PoC và ban quản lý lưu ý. Do vậy, điều quan trọng là mọi nhân viên đều có ý thức tốt và được truy cập đến các hướng dẫn báo cáo các loại khác nhau của các sự kiện an toàn thông tin có thể. Hướng dẫn này phải có cả định dạng của mẫu báo cáo sự kiện an toàn thông tin và các thông tin chi tiết về người cần được thông báo khi có sự kiện (tối thiểu thì mọi nhân viên đều phải biết về định dạng của mẫu báo cáo sự kiện an toàn thông tin để giúp họ hiểu về lược đồ). Cần lưu ý rằng điện thoại cố định, điện thoại không dây và điện thoại di động không có biện pháp an toàn cho bàn phím đều được coi là không an toàn. Khi xử lý thông tin bí mật hoặc tuyệt mật, cần sử dụng thêm các biện pháp an toàn hỗ trợ.

Các thông tin sau có thể được dùng như là thông tin cơ bản của mẫu báo cáo theo dõi sự cố:

a) thời gian/ngày tháng phát hiện,

b) những điều quan sát thấy,

c) thông tin liên hệ (tùy chọn).

Mẫu đầy đủ (trình dưới dạng văn bản giấy, qua thư điện tử hoặc dạng web) chỉ cần được sử dụng bởi nhân viên ISIRT khi đăng ký các sự cố an toàn thông tin vào Hệ thống truy vết sự cố. Điều quan trọng là phải thu nhận được kiến thức/các báo cáo về sự kiện an toàn thông tin khả nghi/đã xảy ra/được phát hiện chứ không phải là điền đầy đủ mọi thông tin.

Bất cứ khi nào có thể thì việc truy vết sự kiện an toàn thông tin (có thể là sự cố) cũng cần được hỗ trợ bởi một ứng dụng tự động. Việc sử dụng một hệ thống thông tin là cần thiết để bắt buộc nhân viên phải tuân thủ các thủ tục và các danh mục đã được tạo lập. Việc giữ truy vết về "ai đã làm điều gì và khi nào", các thông tin chi tiết có thể bị đã bỏ quên do nhầm lẫn trong suốt mỗi sự kiện an toàn thông tin (có thể là sự cố) cũng cực kỳ có lợi.

Cách thức mỗi sự kiện an toàn thông tin được xử lý tùy thuộc vào việc sự kiện đó là gì, và các vấn đề liên quan và các hậu quả có thể. Đối với nhiều người thì đây sẽ là một quyết định được đưa ra trên cơ sở năng lực của họ. Do đó, người báo cáo sự kiện an toàn thông tin cần hoàn tất mẫu báo cáo sự kiện an toàn thông tin theo cách tường thuật tối đa những gì đã xảy ra và các thông tin khác có được tại thời điểm đó, liên lạc với người quản lý nội bộ của họ nếu cần. Mẫu báo cáo này cần được thông tin một cách an toàn đến PoC được chỉ định, và bản sao được gửi cho ISIRT chịu trách nhiệm. Tốt nhất là PoC cần cung cấp dịch vụ 24 giờ trong 7 ngày mỗi tuần. Phụ lục D đưa ra một ví dụ về mẫu báo cáo sự kiện an toàn thông tin.

ISIRT cần chỉ định một thành viên trong nhóm hoặc ủy quyền luân phiên về trách nhiệm đối với các báo cáo nhận được qua thư điện tử, điện thoại, fax, các báo cáo trên giấy và bằng miệng. Trách nhiệm này có thể quay vòng giữa các thành viên của nhóm theo tuần. Thành viên được chỉ định của nhóm phải tiến hành đánh giá và thực hiện các hành động phù hợp để báo cho các bên chịu trách nhiệm và liên quan cũng như giải quyết sự kiện an toàn thông tin đó.

Cần nhấn mạnh rằng, không chỉ tính chính xác mà cả sự kịp thời đều rất quan trọng trong nội dung được điền vào mẫu báo cáo sự kiện an toàn thông tin. Sự chậm trễ trong việc trình mẫu báo cáo nhằm cải thiện tính chính xác của nội dung báo cáo là việc không được khuyến khích. Nếu người báo cáo không chắc chắn về dữ liệu trong một trường nào đó của mẫu báo cáo thì mẫu báo cáo sẽ vẫn được trình nhưng có thêm phần lưu ý phù hợp, và các bản sửa đổi sẽ được cung cấp sau. Cũng cần thừa nhận rằng bản thân một số cơ chế báo cáo (ví dụ thư điện tử) cũng đã là mục tiêu tấn công dễ thấy.

Khi có các vấn đề xảy ra hoặc được coi là đã xảy ra với các cơ chế báo cáo điện tử (ví dụ thư điện tử) thì cần sử dụng các phương tiện truyền thông thay thế khác. Đó là khi hệ thống được cho là đang bị tấn công và người không có thẩm quyền có thể đọc các mẫu báo cáo điện tử. Các phương tiện thay thế có thể là con người, điện thoại hoặc tin nhắn văn bản. Các phương tiện thay thế này cần được sử dụng nhiều nếu đã sớm có chứng cứ trong việc điều tra rằng sự kiện an toàn thông tin có vẻ sẽ được xếp loại là sự cố an toàn thông tin không, đặc biệt là các sự kiện lớn.

Mặc dù trong nhiều trường hợp sự kiện an toàn thông tin phải được báo cáo cho PoC để hành động thì đôi khi sự kiện an toàn thông tin vẫn được xử lý nội bộ, có thể với sự giúp đỡ của ban quản lý nội bộ. Ban quản lý nội bộ cần được huấn luyện để có thể tiến hành đánh giá giống như ISIRT và thực hiện các biện pháp ứng phó tương tự/giống, cũng như sử dụng cùng một hệ thống truy vết sự cố, nhằm sử dụng hiệu quả các nguồn lực nội bộ. Việc này sẽ tránh cho ISIRT lại thực hiện các công việc trùng lặp.

Sự kiện an toàn thông tin có thể nhanh chóng được xác định là báo động giả, hoặc chúng có thể được giải quyết thỏa đáng. Trong các trường hợp đó, mẫu báo cáo cần được hoàn tất và được gửi đến ban quản lý nội bộ, PoC và ISIRT để báo cáo, tức là được đưa vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin. Trong các tình huống như vậy, người báo cáo về sự khép lại sự kiện an toàn thông tin có thể có khả năng hoàn tất một số thông tin được yêu cầu cho mẫu báo cáo sự cố an toàn thông tin – nếu đây là trường hợp mà sau đó mẫu báo cáo sự cố an toàn thông tin còn được hoàn thiện tiếp và chuyển đi. Việc sử dụng các công cụ tự động có thể hỗ trợ hoàn thiện một số trường, ví dụ trường thời gian. Việc sử dụng các công cụ tự động còn hỗ trợ chia sẻ/chuyển giao các thông tin cần thiết.

7 Giai đoạn đánh giá và quyết định

7.1 Tổng quan về các hoạt động chính

Giai đoạn thứ hai trong việc sử dụng vận hành lược đồ quản lý sự cố an toàn thông tin gồm đánh giá thông tin liên quan đến sự xảy ra các sự kiện an toàn thông tin và quyết định xem đó có phải là sự cố an toàn thông tin không.

Với giai đoạn đánh giá và quyết định, tổ chức cần đảm bảo các hoạt động chính gồm:

a) Hoạt động để PoC tiến hành đánh giá để quyết định xem liệu sự kiện có phải là một sự cố an toàn thông tin có thể hoặc đã chấm dứt hay chỉ là báo động giả, và nếu đó không phải là báo động giả thì liệu có cần tăng cấp xử lý không. Các đánh giá cần sử dụng thang phân cấp sự kiện/sự cố/điểm yếu an toàn thông tin đã được chấp nhận (bao gồm cả việc xác định tác động của các sự kiện trên cơ sở các tài sản/dịch vụ bị ảnh hưởng) và cần quyết định xem liệu các sự kiện có cần được xếp loại là các sự cố an toàn thông tin không (xem ví dụ về các hướng dẫn trong Phụ lục C). Trong khi xác định tác động của các sự kiện an toàn thông tin (và do đó có thể là sự cố an toàn thông tin) trên khía cạnh ảnh hưởng của các vi phạm về tính bí mật, tính toàn vẹn và tính sẵn sàng, tổ chức cũng cần đảm bảo rằng các vấn đề sau sẽ được xác định:

   1) vùng ảnh hưởng (vật lý hoặc logic),

   2) các tài sản, cơ sở hạ tầng, thông tin, quy trình, dịch vụ và ứng dụng bị ảnh hưởng, hoặc sẽ bị ảnh hưởng,

   3) các tác động có thể lên các dịch vụ quan trọng của tổ chức.

b) Hoạt động để ISIRT tiến hành đánh giá để xác nhận các kết quả từ đánh giá của PoC xem sự kiện có phải là sự cố an toàn thông tin hay không, nếu phù hợp. Nếu cần thì tiến hành một đánh giá khác sử dụng thang phân cấp sự kiện/sự cố/điểm yếu an toàn thông tin đã được chấp thuận, với các thông tin chi tiết về loại sự kiện (có thể là sự cố) và nguồn lực bị ảnh hưởng (phân loại) (xem hướng dẫn ví dụ trong Phụ lục C). Sau đó, cần đưa ra các quyết định về cách thức xử lý, người xử lý và độ ưu tiên khi xử lý sự kiện an toàn thông tin. Việc này cần có sự tham gia của quy trình phân mức ưu tiên đã định để phân bổ từng sự cố an toàn thông tin cho những người phù hợp và xác định tính cấp bách của việc xử lý và các ứng phó với sự cố an toàn thông tin, gồm cả việc xác định xem có cần ứng phó tức thì, các hoạt động phân tích điều tra an toàn thông tin và truyền thông không, trong giai đoạn tiếp theo (Ứng phó – xem điều 8).

c) Hoạt động để nâng dần cấp xử lý, trên cơ sở theo yêu cầu cho toàn giai đoạn, đối với các đánh giá và/hoặc quyết định thêm.

d) Hoạt động để đảm bảo rằng tất cả những người tham gia, đặc biệt là ISIRT, đều ghi nhật ký mọi hoạt động theo cách phù hợp để dùng cho các phân tích sau này.

e) Hoạt động để đảm bảo rằng chứng cứ điện tử được tập hợp và lưu giữ an toàn, và sự bảo quản an toàn chứng cứ được giám sát liên tục, nếu chúng được yêu cầu cho hoạt động khởi tố hoặc kỷ luật nội bộ.

f) Hoạt động để đảm bảo rằng cách thức kiểm soát thay đổi được duy trì đối với việc truy vết sự cố an toàn thông tin và các cập nhật báo cáo sự cố, và do vậy cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin luôn được cập nhật.

Mọi thông tin được thu thập liên quan đến sự kiện, sự cố, điểm yếu an toàn thông tin cần được lưu giữ trong cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin do ISIRT quản lý. Thông tin được báo cáo

trong mỗi hoạt động phải đầy đủ nhất có thể để đảm bảo rằng đó sẽ là cơ sở tốt sẵn sàng cho các đánh giá và quyết định sẽ được đưa ra, và cho cả các hành động phải được thực hiện.

Khi sự kiện đã được phát hiện và báo cáo thì các hoạt động tiếp theo sẽ gồm:

g) Hoạt động để phân bổ trách nhiệm đối với các hoạt động quản lý sự cố an toàn thông tin theo một phân cấp nhân sự phù hợp, trong đó việc đánh giá, đưa ra quyết định và các hành động đều có sự tham gia của cả nhân viên an toàn và nhân viên không làm về an toàn.

h) Hoạt động để cung cấp các thủ tục chính thức cho từng người đã được thông báo để thực hiện, bao gồm việc soát xét và bổ sung báo cáo cũ, đánh giá thiệt hại, và thông báo cho những người liên quan (trong đó các hành động của cá nhân phụ thuộc vào loại và mức độ nghiêm trọng của sự cố).

i) Hoạt động để sử dụng các hướng dẫn để lập tài liệu kỹ lưỡng về sự kiện an toàn thông tin.

j) Hoạt động để sử dụng các hướng dẫn để lập tài liệu kỹ lưỡng về các hành động tiếp theo cho sự kiện an toàn thông tin nếu sự kiện an toàn thông tin đó được xếp loại là sự cố an toàn thông tin.

k) Hoạt động để cập nhật cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin.

Tổ chức cần đảm bảo rằng giai đoạn này gồm cả việc đánh giá thông tin được tập hợp về các điểm yếu an toàn thông tin đã được báo cáo (các điểm yếu này chưa bị khai thác để gây nên các sự kiện an toàn thông tin, và có thể là các sự cố an toàn thông tin), trong đó các quyết định được đưa ra dựa trên vấn đề cần xử lý, người xử lý, cách thức xử lý và mức độ ưu tiên xử lý.

7.2 Đánh giá và quyết định ban đầu từ PoC

Người nhận báo cáo thuộc PoC cần báo là đã nhận được mẫu báo cáo sự kiện an toàn thông tin hoàn tất, đưa mẫu này vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin, và xem xét. Người này cần yêu cầu sự giải thích rõ ràng từ người báo cáo sự kiện an toàn thông tin, và thu thập mọi thông tin bổ sung được yêu cầu và được biết là có từ người báo cáo hoặc từ những người khác. Sau đó, PoC cần tiến hành đánh giá để xác định xem liệu sự kiện an toàn thông tin đó có cần được xếp loại là sự cố an toàn thông tin không hay thực tế đó chỉ là một báo động giả (trong đó, có sử dụng thang phân cấp sự cố đã được chấp thuận của tổ chức). Nếu sự kiện an toàn thông tin được xác định là một báo động giả thì mẫu báo cáo sự kiện an toàn thông tin cần được hoàn tất và được gửi đến ISIRT để bổ sung vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin và xem xét, và đợc sao gửi đến người báo cáo và người quản lý nội bộ của người báo cáo.

Các thông tin và chứng cứ được thu thập khác tại giai đoạn này có thể cần được sử dụng trong tương lai cho các hành động khởi tố hoặc kỷ luật. Người hoặc những người thực hiện các nhiệm vụ thu thập thông tin và đánh giá cần được đào tạo về các yêu cầu trong việc thu thập và bảo quản chứng cứ.

Bên cạnh việc ghi lại ngày tháng và thời điểm của các hành động thì cũng cần lập tài liệu đầy đủ các thông tin sau:

a) những điều đã được trông thấy và thực hiện (gồm cả các công cụ được sử dụng) và lý do,

b) vị trí của chứng cứ tiềm ẩn,

c) cách thức chứng cứ được lấy(nếu thích hợp),

d) cách xác minh chứng cứ được thực hiện (nếu thích hợp),

e) các thông tin chi tiết về nơi lưu giữ/nơi cất giữ an toàn của tài liệu và việc truy cập về sau đến đó.

Nếu sự kiện an toàn thông tin được xác định một sự cố an toàn thông tin có thể, và nếu người của PoC có đủ khả năng thì có thể tiến hành đánh giá thêm. Việc đánh giá thêm có thể yêu cầu các hành động khắc phục, ví dụ xác định các biện pháp kiểm soát khẩn cấp bổ sung đang có và các biện pháp kiểm soát được đề nghị phải thực hiện đối với người phù hợp. Trong trường hợp có chứng cứ xác định rằng sự kiện an toàn thông tin sẽ là một sự cố an toàn thông tin lớn (sử dụng thang mức độ nghiêm trọng đã được xác định trước của tổ chức) thì người quản lý ISIRT cần được thông báo trực tiếp. Trong trường hợp có chứng cứ xác định rằng một tình huống khủng hoảng cần phải được công bố thì người quản lý quản lý khủng hoảng phải được thông báo về sự khởi động có thể của một kế hoạch quản lý khủng hoảng, và người quản lý ISIRT và ban quản lý cấp cao cũng cần được thông báo về điều này. Tuy nhiên, tình huống hay xảy ra nhất là sự cố an toàn thông tin cần được chuyển trực tiếp cho ISIRT để có đánh giá thêm và hành động.

Cho dù bước tiếp theo được xác định là gì thì PoC cũng cần hoàn tất mẫu báo cáo sự cố an toàn thông tin đầy đủ nhất có thể. Mẫu báo cáo sự cố an toàn thông tin cần chứa thông tin tường thuật, và nếu có thể thì cần xác nhận và mô tả các vấn đề sau:

a) sự kiện an toàn thông tin đó là gì,

b) chúng xảy ra như thế nào, do cái gì hoặc do ai,

c) chúng ảnh hưởng hoặc có thể ảnh hưởng đến cái gì,

d) tác động hoặc tác động tiềm ẩn của sự cố an toàn thông tin đến hoạt động nghiệp vụ của tổ chức,

e) dấu hiệu cho thấy sự cố an toàn thông tin đó có vẻ nghiêm trọng hoặc không nghiêm trọng (sự dụng thang phân cấp đã xác định trước của tổ chức),

f) cách sự kiện được xử lý cho đến nay.

Dưới đây là một số ví dụ về ảnh hưởng bất lợi tiềm ẩn hoặc thực tế của một sự cố an toàn thông tin lên hoạt động nghiệp vụ của tổ chức:

a) sự tiết lộ thông tin trái phép,

b) sự thay đổi thông tin trái phép,

c) sự bác bỏ thông tin,

d) sự không sẵn sàng của thông tin và/hoặc dịch vụ,

e) sự phá hoại thông tin và/hoặc dịch vụ,

f) chất lượng dịch vụ suy giảm.

Bước đầu tiên là cân nhắc xem hậu quả nào liên quan. Đối với các hậu quả được xem là liên quan thì hướng dẫn cho dạng liên quan cần được sử dụng để thiết lập các tác động tiềm ẩn hoặc thực tế để đưa vào báo cáo sự cố an toàn thông tin. Phụ lục C đưa ra các hướng dẫn ví dụ. Dưới đây là các dạng hậu quả ví dụ:

a) thiệt hại về tài chính/phá vỡ các điều hành nghiệp vụ,

b) các lợi ích thương mại và kinh tế,

c) thông tin cá nhân,

d) các nghĩa vụ pháp lý và quy định,

e) các điều hành nghiệp vụ và quản lý,

f) mất tín nhiệm,

g) tổn thương hoặc tổn thất về người,

h) phá vỡ xã hội.

Nếu một sự cố đã được giải quyết thì báo cáo cần đưa cả thông tin chi tiết về các biện pháp kiểm soát đã được thực hiện và mọi bài học kinh nghiệm đã được rút ra (ví dụ, các biện pháp kiểm soát sẽ được chấp nhận để ngăn chặn tái diễn hoặc xảy ra các sự cố tương tự). Khi đã được hoàn tất tối đa thì mẫu báo cáo sau đó cần được chuyển cho ISIRT để đưa vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin và xem xét.

Nếu cuộc điều tra có khả năng phải kéo dài hơn khoảng thời gian đã định trong chính sách quản lý sự cố an toàn thông tin thì báo cáo tạm thời cần được đưa ra trong khoảng thời gian theo quy định của chính sách.

Cần nhấn mạnh rằng PoC thực hiện đánh giá sự cố an toàn thông tin cần được biết về các vấn đề như đã được hướng dẫn trong hệ thống tài liệu lược đồ quản lý sự cố an toàn thông tin, ví dụ:

a) thời điểm cần tăng cấp xử lý các vấn đề và người được chuyển xử lý,

b) các thủ tục kiểm soát thay đổi cần được tuân thủ trong mọi hoạt động do PoC tiến hành.

Theo cách thức tương tự như đã đề cập trong 6.2 và 6.3 ở trên về phát hiện và báo cáo sự cố, các phương tiện truyền thông thay thế khác cho các mẫu báo cáo sự kiện cập nhật cũng cần được sử dụng khi lỗi xảy ra hoặc được coi là đã xảy ra, bằng các cơ chế báo cáo điện tử (ví dụ, thư điện tử).

7.3 Đánh giá và xác nhận sự cố từ ISIRT

Việc đánh giá và xác nhận về quyết định một sự kiện an toàn thông có được xếp loại là sự cố an toàn thông tin hay không phải là trách nhiệm của ISIRT. Người nhận báo cáo sự cố của ISIRT cần thực hiện các công việc sau:

a) Xác nhận đã nhận được mẫu báo cáo sự cố an toàn thông tin hoàn thiện nhất có thể từ PoC.

b) Đưa mẫu báo cáo này vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin nếu việc này chưa được PoC làm và cập nhật cơ sở dữ liệu nếu cần.

c) Yêu cầu làm rõ từ PoC, nếu cần.

d) Xem xét nội dung của mẫu báo cáo.

e) Thu thập mọi thông tin bổ sung được yêu cầu và được biết là có từ PoC, người hoàn tất mẫu báo cáo sự cố an toàn thông tin hoặc từ các nguồn khác.

Nếu vẫn còn có sự không chắc chắn về tính xác thực của sự cố an toàn thông tin hoặc tính đầy đủ của thông tin được báo cáo thì thành viên ISIRT cần tiến hành đánh giá để xác định xem sự kiện an toàn thông tin đó là có thực hay thực tế chỉ là báo động giả (thông qua việc sử dụng thang phân cấp sự cố được chấp nhận của tổ chức). Nếu sự cố an toàn thông tin được xác định là báo động giả thì báo cáo sự kiện an toàn thông tin cần được hoàn tất, được bổ sung vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin và được thông tin đến người quản lý ISIRT. Các bản sao của báo cáo cần được gửi đến PoC, người báo cáo và người quản lý nội bộ của người báo cáo.

Mỗi sự cố an toàn thông tin cần được tương liên với các sự kiện/sự cố khác được báo cáo đến ISIRT. Hoạt động quan trọng này là để xác nhận xem sự cố đó có mối liên hệ nào với các sự kiện/sự cố khác không hay đó đơn giản chỉ là ảnh hưởng của sự cố khác, ví dụ trong các tấn công Từ chối dịch vụ (DoS) hoặc Từ chối dịch vụ phân tán (DDoS). Sự tương liên của các sự cố còn rất quan trọng trong việc phân cấp ưu tiên các cố gắng của ISIRT.

Nếu sự cố an toàn thông tin được xác định là có thật thì thành viên ISIRT và các những người được yêu cầu cần tiến hành đánh giá thêm. Mục đích của việc này là để xác nhận các vấn đề sau sớm nhất có thể:

a) Sự cố an toàn thông tin đó là gì, xảy ra như thế nào, do cái gì hoặc do ai, ảnh hưởng hoặc có thể ảnh hưởng đến cái gì, tác động hoặc tác động tiềm ẩn của sự cố an toàn thông tin đến hoạt động nghiệp vụ của tổ chức, dấu hiệu cho thấy sự cố an toàn thông tin có vẻ lớn hoặc không lớn (sử dụng thang mức độ nghiêm trọng đã quyết định của tổ chức). Nếu sự cố gây ra tác động bất lợi nghiêm trọng lên hoạt động nghiệp vụ thì cần xúc tiến các hoạt động ứng phó khủng hoảng (xem 8.2.4).

b) Các khía cạnh sau đối với tấn công kỹ thuật có chủ ý của con người lên hệ thống, dịch vụ và/hoặc mạng thông tin, ví dụ:

   1) độ sâu mà hệ thống, dịch vụ và/hoặc mạng bị xâm nhập, và mức độ kiểm soát của kẻ tấn công,

   2) dữ liệu nào đã bị kẻ tấn công truy cập, có thể đã bị sao chép, thay đổi hoặc phá hủy,

   3) phần mềm nào đã bị kẻ tấn công sao chép, thay đổi hoặc phá hủy,

c) các ảnh hưởng trực tiếp hoặc gián tiếp (ví dụ, là sự mở truy cập vật lý do hỏa hoạn, là hệ thống thông tin dễ bị tổn hại do lỗi phần mềm hoặc trục trặc đường truyền, hoặc do lỗi của con người), và

d) cách sự cố an toàn thông tin đó được xử lý cho đến nay và người thực hiện.

Khi xem xét các ảnh hưởng bất lợi thực tế hoặc tiềm ẩn của một sự cố an toàn thông tin lên hoạt động nghiệp vụ của tổ chức, từ một số thông tin và/hoặc dịch vụ đã đề cập trong 7.2, cần xác nhận xem có các hậu quả nào liên quan. Các dạng hậu quả ví dụ đã được đề cập trong 7.2 và Phụ lục C.

Quy trình phân cấp ưu tiên cần được sử dụng để phân bổ sự kiện an toàn thông tin cho người hoặc nhóm người phù hợp nhất trong ISIRT để có được ứng phó phù hợp đối với sự cố an toàn thông tin. Cụ thể là, nếu các sự cố an toàn thông tin nghiêm trọng đang được xử lý đồng thời thì các mức ưu tiên phải được thiết lập để sắp xếp thứ tự các ứng phó sẽ được thực hiện đối với các sự cố an toàn thông tin.

Các mức ưu tiên cần thiết lập phù hợp với các tác động nghiệp vụ bất lợi đã xác định có liên quan đến sự cố an toàn thông tin và nỗ lực theo ước đoán cần để ứng phó với sự cố an toàn thông tin. Đối với các sự cố có cùng mức ưu tiên thì nỗ lực được yêu cầu là một tham số để xác định thứ tự mà chúng cần được ứng phó. Ví dụ, một sự cố được giải quyết dễ dàng có thể được xử lý trước một sự cố đòi hỏi nhiều nỗ lực hơn.

Đối với các sự cố được coi là liên quan thì cần sử dụng hướng dẫn cho loại liên quan để thiết lập các tác động thực tế hoặc tiềm ẩn để đưa vào báo cáo sự cố an toàn thông tin. Các Phụ lục C và D đưa ra các hướng dẫn ví dụ.

8 Giai đoạn ứng phó

8.1 Tổng quan về các hoạt động chính

Giai đoạn thứ ba của sử dụng vận hành lược đồ quản lý sự cố an toàn thông tin gồm tiến hành các ứng phó với các sự cố an toàn thông tin theo các hành động đã được chấp thuận trong giai đoạn đánh giá và quyết định. Tùy thuộc vào các quyết định mà các ứng phó có thể được tiến hành tức thì, theo thời gian thực hay gần thời gian thực, và một số ứng phó có thể gồm cả phân tích điều tra an toàn thông tin.

Với giai đoạn Ứng phó, tổ chức cần đảm bảo các hoạt chính gồm:

a) Hoạt động để ISIRT xem xét để xác định xem sự kiện an toàn thông tin đã được kiểm soát chưa, và hoạt động dưới đây:

1) Hoạt động để xúc tiến ứng phó được yêu cầu nếu sự cố đang được kiểm soát. Đó có thể là một ứng phó tức thì, gồm việc khởi động các thủ tục khôi phục, và/hoặc tiến hành truyền thông tới những người liên quan, hoặc là một ứng phó chậm hơn về sau (ví dụ, trong việc hỗ trợ khôi phục hoàn toàn sau thảm họa), trong khi đó vẫn đảm bảo rằng mọi thông tin đều sẵn sàng cho các hoạt động soát xét sau sự cố.

2) Hoạt động để xúc tiến các hoạt động ứng phó khủng hoảng thông qua việc tăng dần mức xử lý lên bộ phận chức năng xử lý khủng hoảng nếu sự cố chưa được kiểm soát hoặc sắp có tác động nghiêm trọng đến các dịch vụ quan trọng của tổ chức (xem 8.2.4). Bộ phận chức năng xử lý khủng hoảng sau đó sẽ chịu trách nhiệm với sự cố với sự hỗ trợ hoàn toàn của ISIRT (đó có thể là việc khởi động kế hoạch quản lý khủng hoảng), và với sự tham gia của những người liên quan, ví dụ người quản lý và nhóm quản lý khủng hoảng của tổ chức (hướng dẫn về quản lý sự liên tục của hoạt động nghiệp vụ trong ISO/IEC 27031 và ISO/PAS 22399:2007).

b) Hoạt động để phân bổ các nguồn lực nội bộ và xác định các nguồn lực bên ngoài để ứng phó với mỗi sự cố.

c) Hoạt động để tiến hành phân tích điều tra an toàn thông tin, theo yêu cầu và cân xứng với xếp hạng theo thang phân cấp sự cố an toàn thông tin, và thay đổi xếp hạng theo thang phân cấp nếu cần.

d) Hoạt động để tăng cấp xử lý, trên cơ sở được yêu cầu trong toàn giai đoạn, đối với các đánh giá thêm và/hoặc các quyết định.

e) Hoạt động để đảm bảo rằng tất cả những người tham gia, đặc biệt là ISIRT, đều ghi nhật ký một cách phù hợp mọi hoạt động để dùng cho việc phân tích sau này.

f) Hoạt động để đảm bảo rằng chứng cứ điện tử được tập hợp và lưu giữ an toàn theo cách phù hợp, và sự bảo quản an toàn chứng cứ được giám sát liên tục, nếu chúng được yêu cầu cho hành động khởi tố hoặc kỷ luật nội bộ.

g) Hoạt động để đảm bảo rằng cách thức kiểm soát thay đổi được duy trì đối với việc truy vết sự cố an toàn thông tin và các cập nhật báo cáo sự cố, và do vậy cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin cũng luôn được cập nhật.

h) Hoạt động để thông tin về sự tồn tại của sự cố an toàn thông tin hoặc mọi thông tin chi tiết liên quan đến người hoặc các tổ chức trong nội bộ hoặc bên ngoài, cụ thể là những người sở hữu tài sản/thông tin/dịch vụ (đã được xác định trong quá trình phân tích tác động) và các tổ chức nội bộ/bên ngoài cần được tham gia vào việc quản lý và giải quyết sự cố.

Mọi thông tin thu thập được liên quan đến mỗi sự kiện, sự cố hoặc điểm yếu an toàn thông tin cần được lưu giữ trong cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin do ISIRT quản lý, để dùng cho việc phân tích thêm. Thông tin được báo cáo trong mỗi hoạt động cần đầy đủ nhất có thể để đảm bảo đó sẽ là cơ sở tốt sẵn sàng cho các đánh giá và các quyết định sẽ được đưa ra, và tất nhiên cả các hành động cần được thực hiện.

Khi sự cố đã được xác định và các ứng phó được chấp thuận thì các hoạt động tiếp theo sẽ là:

a) Hoạt động để phân bổ trách nhiệm đối với các hoạt động quản lý sự cố theo một phân cấp nhân sự phù hợp, trong đó việc đưa ra quyết định và các hành động nếu cần thì cần có sự tham gia của cả nhân viên an toàn và không làm về an toàn.

b) Hoạt động để cung cấp các thủ tục chính thức cho từng người liên quan để thực hiện, bao gồm việc xem xét và bổ sung các báo cáo đã có, đánh giá lại thiệt hại, và thông báo cho những người liên quan (trong đó các hành động của cá nhân sẽ phụ thuộc vào loại và mức độ nghiêm trọng của sự cố).

c) Hoạt động để sử dụng các hướng dẫn để lập tài liệu kỹ lưỡng về mỗi sự cố an toàn thông tin, về các hành động tiếp theo, và cập nhật cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin.

d) Hoạt động để sử dụng các hướng dẫn để lập tài liệu kỹ lưỡng về các hành động tiếp theo.

e) Hoạt động để cập nhật cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin.

Khi một sự cố an toàn thông tin đã được xử lý thành công thì sự cố cần được chính thức khép lại và điều này được ghi vào trong cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin. Tổ chức cần đảm bảo rằng giai đoạn này còn có cả việc tiến hành các ứng phó đối với các điểm yếu an toàn thông tin được báo cáo theo các hành động đã được chấp thuận trong giai đoạn đánh giá và quyết định. Khi điểm yếu nào đó đã được xử lý thì thông tin chi tiết cần được ghi vào trong cơ sở dữ liệu quản lý sự cố an toàn thông tin.

Hướng dẫn về các ứng phó với các sự cố an toàn thông tin được cung cấp trong 8.2.

8.2 Ứng phó

8.2.1 Ứng phó tức thì

8.2.1.1 Tổng quan

Trong phần lớn các trường hợp, các hoạt động tiếp theo của thành viên ISIRT là xác định các hành động ứng phó tức thì để xử lý sự cố an toàn thông tin, ghi các thông tin chi tiết vào mẫu báo cáo sự cố an toàn thông tin và cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin, và thông báo các hành động được yêu cầu tới những người hoặc nhóm người phù hợp. Việc này có thể dẫn đến các biện pháp kiểm soát khẩn cấp (ví dụ, cắt/ngắt hệ thống, dịch vụ và/hoặc mạng thông tin bị ảnh hưởng, có sự chấp thuận trước của ban quản lý IT và/hoặc nghiệp vụ liên quan) và/hoặc các biện pháp kiểm soát thường xuyên bổ sung sẽ được xác định, và được báo cho người hoặc nhóm người phù hợp để thực hiện. Nếu việc này chưa được hoàn tất thì mức độ của sự cố an toàn thông tin cần được xác định nhờ thang phân cấp đã xác định trước của tổ chức, và nếu sự cố được xác định là đủ lớn thì cần thông báo điều này trực tiếp cho người quản lý cao cấp phù hợp. Nếu đã có chứng cứ xác định rằng cần công bố về một tình trạng khủng hoảng thì người quản lý quản lý khủng hoảng cần được thông báo về việc khởi động có thể của một kế hoạch quản lý khủng hoảng, khi đó người quản lý ISIRT và ban quản lý cấp cao cũng được báo như vậy.

Dưới đây là các mục đích chung trong việc ứng phó với các sự cố an toàn thông tin:

a) hạn chế các tác động bất lợi tiềm ẩn (của các sự cố an toàn thông tin),

b) cải thiện sự an toàn thông tin.

Mục tiêu chủ yếu của lược đồ quản lý sự cố an toàn thông tin và các hoạt động liên quan phải là tối giảm các tác động bất lợi lên hoạt động nghiệp vụ, trong khi đó việc xác định kẻ tấn công nên được coi là mục tiêu thứ yếu.

8.2.1.2 Ví dụ về các hành động

Một ví dụ của các hành động ứng phó tức thì liên quan là khi xảy ra tấn công có chủ ý lên một hệ thống, dịch vụ và/hoặc mạng thông tin làm cho hệ thống, dịch vụ và/hoặc mạng đó có thể bị kết nối vào internet hoặc mạng khác. Ứng phó tức thì sẽ cho phép các ứng dụng nghiệp vụ quan trọng làm việc đúng, và thu thập nhiều thông tin nhất có thể về kẻ tấn công với giả thiết rằng kẻ tấn công không biết rằng họ đang bị giám sát.

Điều đặc biệt quan trọng là phải tuân thủ các thủ tục đã được lên kế hoạch và lập hồ sơ về hành động. Cần lưu ý đến các mô hình tấn công dạng Trojan, rootkit và kernel vì chúng có thể gây thiệt hại nghiêm trọng cho hệ thống. Chứng cứ có thể được bảo vệ bằng mật mã, khóa và các hồ sơ truy cập.

a) Trong thực hiện một quyết định như vậy thì cần nghĩ rằng kẻ tấn công có thể nhận ra họ đang bị quan sát và có thể thực hiện các hành động gây thiệt hại hơn nữa cho hệ thống thông tin, dịch vụ và/hoặc mạng bị ảnh hưởng và các dữ liệu liên quan, và kẻ tấn công có thể đã phá hủy các thông tin hữu ích cho việc truy vết họ.

b) Việc cắt và/hoặc ngắt, bằng phương tiện kỹ thuật, các hệ thống, dịch vụ và/hoặc mạng bị tấn công một cách nhanh chóng và tin cậy ngay khi quyết định được đưa ra là điều cần thiết. Điều này cũng cần được áp dụng khi có sự cố.

Có một điều cần quan tâm thêm là sự ngăn chặn tái diễn thường có độ ưu tiên cao, và người ta có thể kết luận rằng kẻ tấn công đã khai thác một điểm yếu cần được khắc phục, và những điều có được từ việc truy vết kẻ tấn công không lý giải được những nỗ lực để làm việc đó. Điều này đặc biệt đúng nếu kẻ tấn công không phải là mã độc và chỉ gây thiệt hại rất nhỏ hoặc không gây thiệt hại.

Cũng cần xác định nguồn gốc tấn công của các sự cố an toàn thông tin do các nguồn khác ngoài tấn công có chú ý. Mặc dù các biện pháp kiểm soát đã được triển khai nhưng có thể vẫn cần tắt hệ thống, dịch vụ và/hoặc mạng thông tin, hoặc cách ly phần liên quan và tắt chúng (có sự chấp nhận trước của ban quản lý IT và/hoặc nghiệp vụ liên quan. Việc này có thể mất nhiều thời gian nếu điểm yếu là vấn đề cơ bản của thiết kế hệ thống, dịch vụ và/hoặc mạng thông tin, hoặc nếu đó là một điểm yếu nghiêm trọng.

Một hoạt động ứng phó khác có thể là khởi động các kỹ thuật giám sát (ví dụ, honeypot – xem ISO/IEC 18043). Đây có thể là cơ sở cho các thủ tục đã được lập tài liệu đối với lược đồ quản lý sự cố an toàn thông tin.

Thông tin có thể bị sửa đổi do sự cố an toàn thông tin cần được thành viên ISIRT kiểm tra so với các hồ sơ dự phòng để tìm những phần thông tin đã bị thay đổi, xóa bỏ, hoặc chèn thêm. Có thể cũng cần phải kiểm tra tính toàn vẹn của các nhật ký vì kẻ tấn công có thể đã ngụy tạo các nhật ký này để che dấu các dấu vết của họ.

8.2.1.3 Cập nhật thông tin sự cố

Cho dù bước tiếp theo được xác định là gì thì thành viên ISIRT cũng cần cập nhật báo cáo sự cố an toàn thông tin nhiều nhất có thể, bổ sung cập nhật đó vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin và thông báo cho người quản lý ISIRT và những người khác nếu cần. Cập nhật có thể gồm thông tin bổ sung về các vấn đề sau:

a) sự cố an toàn thông tin đó là gì,

b) sự cố xảy ra như thế nào, do cái gì hoặc do ai,

c) ảnh hưởng hoặc có thể ảnh hưởng đến điều gì,

d) tác động hoặc tác động tiềm ẩn của sự cố an toàn thông tin đến hoạt động nghiệp vụ của tổ chức,

e) những thay đổi về dấu hiệu cho thấy sự cố an toàn thông tin có vẻ lớn hoặc không lớn (sử dụng thang mức độ nghiêm trọng được xác định trước của tổ chức),

f) cách sự cố đã được xử lý cho đến nay.

Nếu sự cố an toàn thông tin đã được giải quyết thì báo cáo phải gồm thông tin chi tiết về các biện pháp kiểm soát đã được thực hiện và các bài học kinh nghiệm đã được rút ra (ví dụ, các biện pháp kiểm soát bổ sung sẽ được chấp thuận để ngăn chặn tái diễn hoặc xảy ra tương tự). Báo cáo cập nhật cần được bổ sung vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin, và được thông báo đến người quản lý ISIRT và những người khác nếu cần.

Cần nhấn mạnh rằng ISIRT chịu trách nhiệm đảm bảo sự duy trì an toàn của mọi thông tin liên quan đến tất cả các sự cố an toàn thông tin để dùng cho việc phân tích thêm, và sử dụng làm bằng chứng pháp lý tiềm năng. Ví dụ, đối với mỗi sự cố an toàn thông tin hướng IT thì cần thực hiện các hành động sau.

Sau phát hiện ban đầu về sự cố, mọi dữ liệu dễ thay đổi cần được thu thập trước khi hệ thống, dịch vụ và/hoặc mạng bị ảnh hưởng bị tắt để phục vụ cho một cuộc điều tra an toàn thông tin toàn diện. Thông tin cần được thu thập gồm các nội dung của bộ nhớ, thẻ nhớ và các đăng ký, các thông tin chi tiết về mọi hoạt động đang diễn ra, và các việc sau:

a) Bản sao đầy đủ về an toàn thông tin của hệ thống bị ảnh hưởng hoặc bản sao mức thấp của các nhật ký và các tệp quan trọng cần được xây dựng tùy theo tính chất của sự cố an toàn thông tin.

b) Các nhật ký từ các hệ thống, dịch vụ và/hoặc mạng xung quanh, ví dụ từ các bộ định tuyến và tường lửa, cần được thu thập và xem xét.

c) Mọi thông tin được thu thập cần được lưu giữ an toàn trong phương tiện lưu giữ chỉ cho phép đọc.

d) Từ hai người trở lên phải có mặt khi thực hiện việc sao chép điều tra an toàn thông tin được thực hiện để xác nhận và chứng thực rằng mọi hoạt động đều đã được tiến hành theo các quy định và điều luật liên quan.

e) Các yêu cầu kỹ thuật và mô tả về các công cụ và câu lệnh được sử dụng để thực hiện sao chép điều tra an toàn thông tin cần được lập tài liệu và được giữ cùng với phương tiện lưu trữ ban đầu.

Nếu có thể thì tại giai đoạn này, một thành viên ISIRT sẽ chịu trách nhiệm hỗ trợ trong việc đưa thiết bị bị ảnh hưởng (IT hoặc khác) về trạng thái vận hành an toàn không dễ bị tổn thương bởi các tấn công tương tự.

8.2.1.4 Các hoạt động tiếp theo

Nếu một thành viên ISIRT xác định rằng một sự cố an toàn thông tin là có thật thì sau đó các hoạt động quan trọng khác phải gồm:

a) hoạt động để bắt đầu phân tích điều tra an toàn thông tin, và

b) hoạt động để thông báo cho những người chịu trách nhiệm về việc truyền thông trong nội bộ và ra bên ngoài về những vấn đề đã xảy ra và các đề xuất về những điều cần được thông tin, hình thức thông tin và người được thông tin.

Khi báo cáo sự cố an toàn thông tin được hoàn thiện đầy đủ nhất có thể thì cần được đưa vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin và được thông tin tới người quản lý ISIRT.

Nếu điều tra có thể phải kéo dài hơn khoảng thời gian đã được chấp nhận trước trong tổ chức thì cần đưa ra báo cáo tạm thời.

Thành viên ISIRT đánh giá sự cố an toàn thông tin cần được biết, dựa trên hướng dẫn được cung cấp trong tài liệu lược đồ quản lý sự cố an toàn thông tin, về những điều sau:

a) thời điểm cần tăng dần mức xử lý các vấn đề và người được chuyển xử lý,

b) các thủ tục kiểm soát thay đổi cần được tuân thủ trong mọi hoạt động được ISIRT tiến hành.

Khi có lỗi xảy ra hoặc được coi là đã xảy ra với các phương tiện truyền thông điện tử (ví dụ, thư điện tử hoặc web), kể cả nếu chỉ nghĩ có thể hệ thống đang bị tấn công, thì cũng cần báo cáo đến người liên quan bằng điện thoại hoặc tin nhắn văn bản.

Nếu một sự kiện an toàn thông tin được kết luận là lớn hoặc một tình trạng khủng hoảng được xác định thì khi đó người quản lý ISIRT, có quan hệ với người quản lý an toàn thông tin của tổ chức và thành viên hội đồng quản trị/người quản lý cấp cao liên quan, cần liên lạc với tất cả các bên liên quan, kể cả trong nội bộ và bên ngoài của tổ chức.

Để đảm bảo rằng các liên lạc được tổ chức nhanh chóng và hiệu quả thì cần phải thiết lập trước một phương pháp truyền thông an toàn, phương pháp này phải không hoàn toàn phụ thuộc vào các hệ thống, dịch vụ và/hoặc mạng có thể bị ảnh hưởng bởi sự cố an toàn thông tin. Ngoài ra, có thể chỉ định những người cố vấn dự phòng hoặc những người đại diện để sử dụng trong trường hợp vắng mặt.

8.2.2 Đánh giá sự kiểm soát các sự cố an toàn thông tin

Sau khi thành viên ISIRT đã xúc tiến các ứng phó tức thì, các hoạt động phân tích điều tra sự cố an toàn thông tin và truyền thông liên quan thì cần nhanh chóng xác định chắc chắn xem sự cố an toàn thông tin đã được kiểm soát chưa. Nếu cần thì thành viên ISIRT có thể bàn với các đồng nghiệp, người quản lý ISIRT và/hoặc những người hoặc nhóm người khác.

Nếu sự cố an toàn thông tin được xác nhận là đang được kiểm soát thì thành viên ISIRT cần xúc tiến mọi ứng phó được yêu cầu tiếp sau, các hoạt động phân tích điều tra an toàn thông tin và truyền thông để kết thúc sự cố an toàn thông tin và khôi phục hệ thống thông tin bị ảnh hưởng về trạng thái vận hành bình thường.

Nếu sự cố an toàn thông tin được xác nhận là chưa được kiểm soát thì sau đó thành viên ISIRT cần xúc tiến các hoạt động ứng phó khủng hoảng.

Nếu sự cố an toàn thông tin có liên quan đến việc mất tính sẵn sàng thì thang đo để đánh giá xem sự cố an toàn thông tin đã được kiểm soát chưa có thể là thời gian cần để khôi phục về trạng thái bình thường chứ không phải là sự xảy ra của một sự cố an toàn thông tin. Đối với từng tài sản, tổ chức cần xác định, trên cơ sở các kết quả của việc đánh giá rủi ro an toàn thông tin, cửa sổ gián đoạn được chấp nhận trước khi có thể khởi động lại dịch vụ hoặc truy cập thông tin. Ngay khi ứng phó kéo dài hơn cửa sổ gián đoạn được chấp nhận của tài sản cụ thể thì sự cố an toàn thông tin có thể đã không được kiểm soát nữa và khi đó cần đưa ra quyết định phải nâng dần cấp xử lý sự cố an toàn thông tin.

Các sự cố an toàn thông tin liên quan đến việc mất tính bí mật, tính toàn vẹn... lại cần cách đánh giá khác để xác định xem tình huống đã được kiểm soát chưa và các thang đo liên quan có thể theo các kế hoạch quản lý rủi ro của tổ chức.

8.2.3 Các ứng phó về sau

Khi đã xác định được rằng sự cố an toàn thông tin đã được kiểm soát và không cần các hoạt động ứng phó khủng hoảng thì thành viên ISIRT cần xác định xem có cần và cần các ứng phó tiếp theo nào để xử lý sự cố an toàn thông tin. Các ứng phó này có thể gồm cả việc khôi phục (các) hệ thống, dịch vụ và/hoặc mạng bị ảnh hưởng trở về trạng thái hoạt động bình thường. Sau đó, họ cần ghi lại các thông tin chi tiết vào mẫu báo cáo sự cố an toàn thông tin, cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin và thông báo cho những người có trách nhiệm để hoàn tất các hành động liên quan. Khi các hành động này đã được hoàn tất thành công thì các thông tin chi tiết cần được ghi vào mẫu báo cáo sự cố an toàn thông tin và cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin, và sau đó sự cố an toàn thông tin cần được khép lại và được thông báo cho người phù hợp.

Một số ứng phó hướng đến việc ngăn chặn sự tái diễn hoặc xảy ra sự cố an toàn thông tin tương tự. Ví dụ, nếu đã xác định được rằng nguyên nhân của sự cố an toàn thông tin là do lỗi phần cứng hoặc phần mềm IT mà hiện tại tổ chức lại không có bản vá thì cần liên hệ ngay tức khắc với nhà cung cấp. Nếu một điểm yếu IT đã biết có liên quan đến một sự cố an toàn thông tin thì điểm yếu đó cần được vá bằng bản cập nhật an toàn thông tin liên quan. Mọi lỗi liên quan đến cấu hình IT bị làm rõ bởi sự cố an

toàn thông tin đều cần được xử lý sau đó. Các biện pháp khác nhằm làm giảm khả năng tái diễn hoặc xảy ra sự cố an toàn thông tin IT tương tự có thể là thay đổi mật khẩu hệ thống và vô hiệu hóa các dịch vụ chưa sử dụng.

Một hình thức ứng phó khác có thể là giám sát hệ thống, dịch vụ và/hoặc mạng IT. Tiếp theo việc đánh giá sự cố an toàn thông tin, có thể sẽ phù hợp nếu tiến hành các biện pháp kiểm soát giám sát bổ sung nhằm hỗ trợ phát hiện các sự kiện bất thường và khả nghi có dấu hiệu của các sự cố an toàn thông tin sau này. Việc giám sát như vậy có thể còn phát hiện được thông tin sâu hơn về sự cố an toàn thông tin và xác định được các hệ thống IT khác đã bị tổn thương.

Có thể cũng cần khởi động các ứng phó nhất định đã được ghi trong kế hoạch quản lý khủng hoảng liên quan. Điều này có thể áp dụng với cả các sự cố an toàn thông tin liên quan và không liên quan đến IT. Các ứng phó như vậy cần có sự tham gia của các phương tiện dùng cho mọi khía cạnh hoạt động nghiệp vụ, không chỉ trực tiếp liên quan đến IT mà còn liên quan đến việc duy trì các bộ phận chức năng nghiệp vụ chính và việc khôi phục về sau - nếu phù hợp thì gồm các phương tiện truyền giọng nói, các phương tiện cá nhân và các phương tiện vật lý.

Hình thức ứng phó cuối cùng là khôi phục (các) hệ thống, dịch vụ và/hoặc mạng bị ảnh hưởng về trạng thái hoạt động bình thường. Việc khôi phục (các) hệ thống, dịch vụ và/hoặc mạng bị ảnh hưởng về trạng thái hoạt động an toàn có thể đạt được thông qua việc sử dụng các bản vá cho các điểm yếu đã biết hoặc bằng cách vô hiệu hóa thành phần đã bị tổn hại. Nếu toàn bộ phạm vi của sự cố an toàn thông tin đều chưa được rõ do sự phá hủy của các nhật ký trong thời gian sự cố thì có thể cần phải xây dựng lại toàn bộ hệ thống, dịch vụ và/hoặc mạng. Có thể cũng cần phải khởi động các bộ phận của kế hoạch quản lý khủng hoảng liên quan.

Nếu một sự cố an toàn thông tin không có liên quan đến IT, ví dụ có nguyên nhân từ hỏa hoạn, lũ lụt hoặc bom mìn, thì khi đó các hoạt động khôi phục cần thực hiện là các hoạt động đã được ghi trong kế hoạch quản lý khủng hoảng liên quan.

8.2.4 Ứng phó với tình huống khủng hoảng

Như đã đề cập trong 8.2.2, có thể ISIRT lại xác định rằng sự cố an toàn thông tin vẫn chưa được kiểm soát và cần tăng cấp xử lý thành tình trạng khủng hoảng sử dụng kế hoạch đã định trước.

Các lựa chọn tốt nhất để xử lý mọi loại có thể của các sự cố an toàn thông tin mà có thể ảnh hưởng đến tính sẵn sàng và một mức độ toàn vẹn nào đó của hệ thống thông tin, có thể đã được xác định trong kế hoạch quản lý khủng hoảng của tổ chức. Các lựa chọn này phải có liên quan trực tiếp đến các ưu tiên nghiệp vụ và các thời gian biểu liên quan đến việc khôi phục của tổ chức, và do đó liên quan đến cả các khoảng thời gian ngừng hoạt động lớn nhất chấp nhận được đối với IT, thoại, con người và các tiện nghi. Chiến lược ứng phó cần định rõ các vấn đề sau:

a) các biện pháp quản lý phòng ngừa, khôi phục và khủng hoảng được yêu cầu,

b) cơ cấu tổ chức được yêu cầu và các trách nhiệm ứng phó với khủng hoảng,

c) cấu trúc và nội dung sơ lược được yêu cầu của kế hoạch hoặc các kế hoạch quản lý khủng hoảng.

(Các) kế hoạch quản lý khủng hoảng và các biện pháp kiểm soát được triển khai để hỗ trợ khởi động (các) kế hoạch này, khi đã được kiểm tra một cách thỏa đáng, sẽ là cơ sở để xử lý hầu hết các sự cố được tăng cấp xử lý khi chúng được xác định như vậy.

Tùy thuộc vào loại sự cố và việc chúng đã được kiểm soát hay chưa mà sự tăng cấp xử lý có thể dẫn đến các hoạt động nghiêm trọng để xử lý sự cố và khởi động kế hoạch quản lý khủng hoảng nếu có. Các hoạt động như vậy có thể gồm, nhưng không giới hạn, việc khởi động:

a) các phương tiện ngăn chặn hỏa hoạn và các thủ tục sơ tán,

b) các phương tiện ngăn chặn lũ lụt và các thủ tục sơ tán,

c) các thủ tục xử lý bom mìn và sơ tán liên quan,

d) các điều tra viên chuyên về lỗi hệ thống thông tin,

e) các điều tra viên chuyên về tấn công kỹ thuật.

8.2.5 Phân tích điều tra an toàn thông tin

Nếu được xác định bởi đánh giá trước kia theo yêu cầu cho các mục đích chứng minh và nếu đó là sự cố an toàn thông tin lớn thì việc phân tích điều tra an toàn thông tin cần được ISIRT tiến hành. Khi đó, cần sử dụng các kỹ thuật và công cụ điều tra trên cơ sở IT, với sự hỗ trợ của các thủ tục đã được lập tài liệu, để xem xét (các) sự cố an toàn thông tin đã định một cách chi tiết hơn những gì đã được thực hiện cho đến nay trong quy trình quản lý sự cố an toàn thông tin. Việc này cần được tiến hành theo một phương thức có cấu trúc, và nếu phù hợp thì cần xác định rõ những gì sẽ được sử dụng làm chứng cứ, cho đó là các thủ tục kỷ luật nội bộ hay hành động pháp lý.

Các phương tiện cần cho phân tích điều tra an toàn thông tin cần được phân loại thành phương tiện kỹ thuật (ví dụ, các công cụ kiểm tra, các phương tiện khôi phục chứng cứ), phương tiện thủ tục, phương tiện nhân sự và phương tiện văn phòng an toàn. Mỗi hoạt động phân tích điều tra an toàn thông tin cần được lập tài liệu đầy đủ, gồm cả các ảnh chụp liên quan, các báo cáo phân tích nhật ký đánh giá và các nhật ký khôi phục dữ liệu. Trình độ của người hoặc những người thực hiện phân tích điều tra an toàn thông tin cần được ghi vào tài liệu kèm các hồ sơ kiểm tra trình độ. Mọi thông tin khác thể hiện mục tiêu và tính logic của việc phân tích cũng cần được ghi vào tài liệu. Mọi hồ sơ của chính các sự cố an toàn thông tin, các hoạt động phân tích điều tra an toàn thông tin..., và phương tiện lưu trữ liên quan, đều cần được lưu giữ trong một môi trường vật lý an toàn và được kiểm soát bằng các thủ tục nhằm ngăn chặn những người không có thẩm quyền truy cập, thay đổi hoặc làm chúng trở nên không sẵn sàng. Các công cụ dựa trên IT dùng cho phân tích điều tra an toàn thông tin cần tuân thủ các tiêu chuẩn sao cho độ chính xác của chúng không bị nghi ngờ về mặt pháp lý, và luôn được cập nhật theo các thay đổi về công nghệ. Môi trường vật lý của ISIRT cần cung cấp các điều kiện rõ ràng để đảm bảo chứng cứ được xử lý theo cách thức để không bị nghi ngờ. Đủ nhân sự sẵn sàng, nếu cần thì bằng điện thoại, để có thể ứng phó tại mọi thời điểm.

Theo thời gian, có thể xuất hiện thêm các yêu cầu phải xem xét chứng cứ của nhiều sự cố an toàn thông tin, bao gồm gian lận, trộm cắp và phá hoại. Do đó, để hỗ trợ ISIRT thì cần rất nhiều các phương tiện dựa trên IT và thủ tục hỗ trợ để giúp làm sáng tỏ các thông tin đã bị che dấu trong các hệ thống, dịch vụ hoặc mạng thông tin, bao gồm cả thông tin mà điều tra ban đầu cho là đã bị xóa, bị mã hóa hoặc bị tổn hại. Các phương tiện này cần giải quyết mọi khía cạnh đã biết liên quan đến các loại sự cố an toàn thông tin đã biết và đã được lập tài liệu trong các thủ tục của ISIRT.

Trong môi trường hiện nay, phân tích điều tra an toàn thông tin thường cần phải thực hiện trên cả các môi trường nối mạng phức tạp, ở đó việc điều tra cần thực hiện trên toàn bộ môi trường vận hành bao gồm nhiều các máy chủ (ví dụ cho tệp tin, máy in, truyền thông và thư điện tử), cũng như các phương tiện truy cập từ xa. Hiện trên thị trường đã có rất nhiều công cụ, gồm các công cụ tìm kiếm văn bản, các bộ phần mềm phân vùng ổ đĩa và điều tra an toàn thông tin. Mục đích chính của các thủ tục phân tích điều tra an toàn thông tin là đảm bảo rằng chứng cứ được giữ nguyên vẹn và được kiểm tra để đảm bảo đứng vững trước mọi thử thách pháp lý.

Cần nhấn mạnh rằng phân tích điều tra an toàn thông tin cần được thực hiện trên bản sao chính xác của dữ liệu ban đầu nhằm đề phòng việc phân tích làm tổn hại đến tính nguyên vẹn của phương tiện lưu trữ ban đầu. Nếu có thể thì quy trình phân tích điều tra an toàn thông tin tổng thể phải gồm các hoạt động sau:

a) Hoạt động để đảm bảo rằng hệ thống, dịch vụ và/hoặc mạng mục tiêu được bảo vệ trong suốt quá trình phân tích điều tra an toàn thông tin để không bị mất tính sẵn sàng, bị thay đổi hoặc bị tổn hại, bao gồm cả do mã độc (cả virus), và không gây ảnh hưởng hoặc không có ảnh hưởng nhỏ nào đến các vận hành thông thường.

b) Hoạt động để phân cấp ưu tiên trong việc thu nhận và thu thập chứng cứ, mà cụ thể là phải bắt đầu từ những chứng cứ chắc chắn nhất đến những chứng cứ kém chắc chắn nhất (phụ thuộc chủ yếu vào tính chất của sự cố an toàn thông tin).

c) Hoạt động để xác định mọi tệp tin liên quan trong hệ thống, dịch vụ và/hoặc mạng mục tiêu, bao gồm các tệp tin thông thường, mật khẩu hoặc các tệp được bảo vệ khác, và các tệp được mã hóa.

d) Hoạt động để khôi phục tối đa các tệp tin bị xóa được phát hiện và các dữ liệu khác.

e) Hoạt động để khám phá các địa chỉ IP, tên máy, tuyến mạng và thông tin website.

f) Hoạt động để lấy nội dung của các tệp tin bị che giấu, tạm thời và hoán đổi được sử dụng bởi phần mềm ứng dụng và hệ điều hành.

g) Hoạt động để truy cập nội dung của các tệp được bảo vệ và được mã hóa (trừ các tệp bị hạn chế bởi luật).

h) Hoạt động để phân tích mọi dữ liệu liên quan có thể được tìm thấy trong các khu vực ổ đĩa lưu trữ đặc biệt (và điển hình là không thể truy cập).

i) Hoạt động để phân tích thời gian truy cập, thay đổi và tạo tệp tin.

j) Hoạt động để phân tích các nhật ký hệ thống/dịch vụ/mạng và ứng dụng.

k) Hoạt động để xác định hoạt động của người dùng và/hoặc ứng dụng trên hệ thống/dịch vụ/mạng.

l) Hoạt động để phân tích các thư điện tử về thông tin nguồn và nội dung.

m) Hoạt động để thực hiện các kiểm tra tính toàn vẹn của tệp tin nhằm phát hiện các tệp ngựa Trojan và các tệp không có nguồn gốc trên hệ thống.

n) Hoạt động để phân tích, nếu thích hợp, chứng cứ vật lý, ví dụ dấu vân tay, sự hư hại tài sản, giám sát video, các nhật ký của hệ thống cảnh báo, các nhật ký truy cập mã thẻ, và phỏng vấn các nhân chứng.

o) Hoạt động để đảm bảo rằng chứng cứ tiềm ẩn thu được sẽ được xử lý và lưu giữ theo cách thức sao cho chúng không thể bị hư hại hoặc trở thành không có giá trị sử dụng, và các tài liệu nhạy cảm không thể bị những người không có thẩm quyền trông thấy. Cần nhấn mạnh rằng việc tập hợp chứng cứ phải luôn theo đúng luật của tòa án hoặc phiên tòa mà trong đó chứng cứ có thể được trình bày.

p) Hoạt động để kết luận về các lý do của sự cố an toàn thông tin, các hành động được yêu cầu và khung thời gian, trong đó chứng cứ sẽ gồm các danh sách của các tệp liên quan có trong thông tin đính kèm của báo cáo chính.

q) Hoạt động để cung cấp hỗ trợ chuyên gia cho mọi hành động kỷ luật hoặc pháp lý được yêu cầu.

(Các) phương pháp phải tuân thủ cần được lập tài liệu trong các thủ tục của ISIRT.

ISIRT cần có đủ các tập hợp kỹ năng thích hợp để bao quát phạm vi kiến thức kỹ thuật rộng (bao gồm cả các công cụ và kỹ thuật có xu hướng được các kẻ tấn công có chủ ý sử dụng), kinh nghiệm phân tích/điều tra (bao gồm cả kinh nghiệm liên quan đến việc giữ gìn chứng cứ), kiến thức về khía cạnh luật pháp và quy định liên quan, và kiến thức hiện hành về các xu hướng sự cố.

Cần được thừa nhận các vấn đề sau:

a) một số tổ chức có thể không có tất cả các nguồn lực này sẵn sàng và có thể cần phải thuê các chuyên gia làm công việc phân tích điều tra an toàn thông tin,

b) việc thu thập tài liệu điều tra an toàn thông tin có thể chỉ là một phương kế (tức là nỗ lực và chi phí là cân đối) trong đó sự tổn thất nghiêm trọng đã xảy ra và/hoặc các hành động phạm tội có xu hướng sẽ xảy ra,

c) việc không sử dụng các nguồn lực chuyên gia để thu thập các tài liệu điều tra an toàn thông tin có thể làm cho các phát hiện trở nên không được chấp nhận khi có hành động pháp lý được yêu cầu.

8.2.6 Truyền thông

Trong nhiều trường hợp nếu sự cố an toàn thông tin được ISIRT xác nhận là có thật thì những người nhất định nào đó sẽ cần được thông báo, kể cả trong nội bộ (bên ngoài các kênh truyền thông

ISIRT/quản lý thông thường) và bên ngoài tổ chức, gồm cả báo giới. Điều này có thể cần được thực hiện ở nhiều giai đoạn, ví dụ khi một sự cố an toàn thông tin được xác nhận là có thật, khi chúng được xác nhận là đã được kiểm soát, khi chúng được chỉ định cho các hoạt động ứng phó khủng hoảng, khi chúng được khép lại và khi việc soát xét sau sự cố đã được hoàn tất và các kết luận đã được đưa ra.

Nếu việc truyền thông được yêu cầu thì cần đảm bảo rằng người cần biết sẽ biết được những điều cần thiết và thời gian xảy ra. Các bên liên quan bị ảnh hưởng cũng cần được xác định và thường được chia thành các nhóm, ví dụ:

a) các bên trong nội bộ có liên quan (đội ngũ quản lý nhân viên, quản lý khủng hoảng...),

b) các bên bên ngoài có liên quan trực tiếp (những người sở hữu, các khách hàng, các đối tác, các nhà cung cấp...),

c) các đầu mối liên hệ bên ngoài như báo chí và/hoặc các đối tác truyền thông khác.

Mỗi nhóm có thể cần các thông tin đặc biệt mà có thể đến từ các kênh phù hợp của tổ chức. Nhiệm vụ quan trọng nhất về truyền thông sau mỗi sự cố an toàn thông tin là đảm bảo rằng các bên liên quan trực tiếp trong nội bộ và bên ngoài sẽ có thông tin trước khi các thông tin này đến qua các đầu mối liên hệ bên ngoài khác như báo chí.

Để hỗ trợ hoạt động này khi có yêu cầu thì có một cách phù hợp là chuẩn bị trước các thông tin nhất định sao cho chúng sẽ được điều chỉnh nhanh chóng theo các tình huống của mỗi sự cố an toàn thông tin cụ thể và chúng sẽ được cung cấp cho từng nhóm liên quan và cụ thể là báo chí và/hoặc các đối tác truyền thông khác. Nếu thông tin nào đó có liên quan đến các sự cố an toàn thông tin được cung cấp cho báo chí thì việc đó cần được thực hiện theo chính sách phổ biến thông tin của tổ chức. Thông tin sẽ được cung cấp cần được các bên liên quan soát xét, trong đó có thể gồm ban quản lý cấp cao, nhân viên điều phối quan hệ công chúng và nhân viên an toàn thông tin.

CHÚ THÍCH: Việc truyền thông về sự cố an toàn thông tin có thể thay đổi tùy theo sự cố và các tác động của chúng cùng với các mối quan hệ của tổ chức và loại hình nghiệp vụ. Loại hình nghiệp vụ có thể còn thiết lập các quy tắc cụ thể về cách thức truyền thông, ví dụ nếu tổ chức đã được định danh trên thị trường chứng khoán.

8.2.7 Tăng cấp xử lý

Trong những tình huống nghiêm trọng, các vấn đề có thể phải được tăng cấp xử lý để thích ứng với các sự cố đang bị mất kiểm soát và mối nguy hiểm tiềm ẩn đối với tác động nghiệp vụ không thể chấp nhận. Các sự cố này cần được tăng cấp xử lý để khởi động kế hoạch liên tục nghiệp vụ thay vì phải báo cáo đến ban quản lý cấp cao, nhóm khác trong tổ chức hoặc những người hoặc các nhóm bên ngoài tổ chức. Việc này có thể là để đưa ra quyết định về các hành động được đề xuất để xử lý sự kiện an toàn thông tin, hoặc để đánh giá thêm để xác định các hành động được yêu cầu. Việc này có thể được thực hiện sau các hoạt động đánh giá đã được mô tả trong 7.2 và 7.3 ở trên, hoặc trong các hoạt động này nếu vấn đề chính nào đó đã trở nên sớm rõ ràng. Hướng dẫn cần có trong hệ thống tài liệu lược đồ quản lý sự cố an toàn thông tin dành cho những người cần phải nâng dần cấp xử lý các vấn đề, tức là các thành viên PoC và ISIRT.

8.2.8 Ghi nhật ký hoạt động và kiểm soát thay đổi

Cần nhấn mạnh rằng tất cả những người tham gia vào việc báo cáo và quản lý sự cố an toàn thông tin đều cần ghi nhật ký mọi hoạt động theo cách thích hợp để dùng cho việc phân tích sau này. Nhật ký này cần được đưa vào mẫu báo cáo sự cố an toàn thông tin và cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin,và liên tục được cập nhật trong suốt chu trình của mỗi sự cố an toàn thông tin từ khi báo cáo lần đầu đến lúc hoàn tất việc soát xét sau sự cố.

Thông tin này cần được giữ an toàn một cách phù hợp và có chế độ sao lưu phù hợp. Hơn nữa, mọi thay đổi đã có trong nội dung truy vết mỗi sự cố an toàn thông tin và cập nhật mẫu báo cáo sự cố an toàn thông tin và cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin đều cần được kiểm soát bởi lược đồ kiểm soát thay đổi chính thức đã được chấp nhận.

9 Giai đoạn rút bài học kinh nghiệm

9.1 Tổng quan về các hoạt động chính

Giai đoạn thứ tư của sử dụng vận hành lược đồ quản lý sự cố an toàn thông tin bắt đầu khi các sự cố an toàn thông tin đã được giải quyết/khép lại, và bao gồm việc rút ra các bài học kinh nghiệm từ cách giải quyết và xử lý các sự cố (và điểm yếu). Với giai đoạn rút bài học kinh nghiệm, mỗi tổ chức cần đảm bảo các hoạt động chính gồm:

a) Hoạt động để tiến hành phân tích điều tra an toàn thông tin thêm theo yêu cầu.

b) Hoạt động để xác định các bài học kinh nghiệm từ các sự cố và điểm yếu an toàn thông tin.

c) Hoạt động để soát xét, xác định và thực hiện các cải tiến đối với việc triển khai các biện pháp kiểm soát an toàn thông tin (các biện pháp kiểm soát mới và/hoặc cập nhật), cũng như chính sách quản lý sự cố an toàn thông tin sau khi đã rút ra các bài học kinh nghiệm từ một hoặc nhiều sự cố an toàn thông tin (hoặc từ các điểm yếu an toàn được báo cáo). Việc này được hỗ trợ bởi tiêu chí được đưa vào chiến lược của tổ chức về nơi cần đầu tư các biện pháp kiểm soát an toàn thông tin.

d) Hoạt động để soát xét, xác định và thực hiện các cải tiến đối với các kết quả đánh giá rủi ro an toàn thông tin hiện tại và soát xét của ban quản lý của tổ chức sau khi đã rút ra các bài học kinh nghiệm.

e) Hoạt động để soát xét sự hiệu lực của các quy trình, thủ tục, các định dạng báo cáo và/hoặc cơ cấu tổ chức trong việc ứng phó, đánh giá và khôi phục từ mỗi sự cố an toàn thông tin và xử lý các điểm yếu an toàn thông tin, và trên cơ sở các bài học kinh nghiệm đã được rút ra để xác định và thực hiện các cải tiến đối với lược đồ quản lý sự cố an toàn thông tin và hệ thống tài liệu của lược đồ.

f) Hoạt động để cập nhật cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin.

g) Hoạt động để truyền thông và chia sẻ kết quả soát xét trong một cộng đồng tin cậy (nếu tổ chức mong muốn).

Cần nhấn mạnh rằng các hoạt động quản lý sự cố an toàn thông có tính lặp, và do vậy mỗi tổ chức cần thực hiện các cải tiến thường xuyên đối với nhiều thành phần an toàn thông tin. Các cải tiến này cần được đề xuất trên cơ sở các soát xét dữ liệu về các sự cố toàn thông tin, các ứng phó đối với chúng và các điểm yếu an toàn thông tin được báo cáo, cũng như các xu hướng theo thời gian.

9.2 Phân tích điều tra thêm về an toàn thông tin

Có thể có trường hợp một sự cố đã được giải quyết nhưng vẫn yêu cầu phải phân tích điều tra an toàn thông tin để xác định chứng cứ. Việc này cần được ISIRT tiến hành sử dụng cùng bộ công cụ và các thủ tục như đã đề xuất trong 8.2.5.

9.3 Xác định các bài học kinh nghiệm

Khi mỗi sự cố an toàn thông tin được khép lại thì điều quan trọng là tổ chức cần nhanh chóng xác định và rút ra các bài học kinh nghiệm từ việc xử lý sự cố an toàn thông tin và đảm bảo rằng các kết luận đã được đưa ra. Hơn nữa, có thể có cả các bài học kinh nghiệm cần được rút ra từ việc đánh giá và và giải quyết các điểm yếu an toàn thông tin đã được báo cáo. Các bài học kinh nghiệm có thể liên quan đến các vấn đề sau:

a) Các yêu cầu mới hoặc thay đổi về các biện pháp kiểm soát an toàn thông tin. Đó có thể là các biện pháp kỹ thuật hoặc phi kỹ thuật (bao gồm cả vật lý). Tùy thuộc vào các bài học kinh nghiệm được rút ra thì các biện pháp này có thể gồm nhu cầu cần các cập nhật tài liệu nhanh chóng và cung cấp các chỉ dẫn nâng cao nhận thức về an toàn thông tin (cho người dùng cũng như các nhân viên khác) và bản sửa nhanh, và ban hành các hướng dẫn và/hoặc tiêu chuẩn an toàn.

b) Thông tin về mối đe dọa và điểm yếu mới hoặc thay đổi và do đó cả các thay đổi đối với việc đánh giá rủi ro an toàn thông tin hiện tại và các kết quả soát xét của ban quản lý.

c) Các thay đổi đối với lược đồ quản lý sự cố an toàn thông tin, các quy trình, thủ tục của lược đồ, các định dạng và/hoặc cơ cấu tổ chức trong việc báo cáo, và cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin.

Các tổ chức cần nghiên cứu sâu hơn là mỗi sự cố hoặc điểm yếu an toàn thông tin đơn lẻ và tìm kiếm các xu hướng/mô hình có thể giúp xác định nhu cầu đối với các biện pháp kiểm soát hoặc những thay đổi về phương pháp tiếp cận. Thông thường sau mỗi sự cố an toàn thông tin hướng IT thì cần tiến hành kiểm tra an toàn thông tin, cụ thể là đánh giá điểm yếu. Do vậy, mỗi tổ chức cần thường xuyên phân tích dữ liệu trong cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin nhằm thực hiện các việc sau:

a) xác định các xu hướng/mô hình,

b) xác định các phạm vi cần quan tâm,

c) phân tích những nơi cần tiến hành hành động phòng ngừa để giảm xu hướng xảy ra các sự cố trong tương lai.

Thông tin liên quan có được trong suốt tiến trình của mỗi sự cố an toàn thông tin cần được đưa vào phân tích xu hướng/mô hình (tương tự như cách thức mà các điểm yếu an toàn thông tin được báo cáo đã được xử lý). Điều đó sẽ góp phần đáng kể vào việc sớm xác định được các sự cố an toàn thông tin và cung cấp cảnh báo về các sự cố an toàn thông tin tiếp theo có thể xuất hiện, trên cơ sở kinh nghiệm trước đó và kiến thức đã được lập tài liệu.

Cũng cần sử dụng thông tin sự cố an toàn thông tin và điểm yếu liên quan có được từ chính phủ, các ISIRT thương mại và các nhà cung cấp.

Việc đánh giá điểm yếu/kiểm tra an toàn cho hệ thống, dịch vụ và/hoặc mạng thông tin sau mỗi sự cố an toàn thông tin không được bị giới hạn chỉ với các hệ thống, dịch vụ và/hoặc mạng thông tin bị ảnh hưởng bởi sự cố an toàn thông tin. Việc này cần được mở rộng với mọi hệ thống, dịch vụ và/hoặc mạng thông tin liên quan. Cuộc đánh giá điểm yếu đầy đủ được sử dụng để phát hiện sự tồn tại của các điểm yếu đã bị khai thác trong sự cố an toàn thông tin trên các hệ thống, dịch vụ và/hoặc mạng thông tin khác và đảm bảo không có thêm các điểm yếu mới.

Điều quan trọng cần nhấn mạnh là các đánh giá điểm yếu cần được tiến hành thường xuyên, và việc đánh giá lại các điểm yếu sau khi một sự cố an toàn thông tin xảy ra cần được coi là một phần của quy trình đánh giá liên tục, chứ không có tính chất thay thế.

Các phân tích tổng kết của các sự cố và điểm yếu an toàn thông tin cần được đưa ra thảo luận tại mỗi cuộc họp của diễn đàn an toàn thông tin của ban quản lý của tổ chức và các diễn đàn khác đã được xác định trong chính sách an toàn thông tin tổng thể của tổ chức.

9.4 Xác định và thực hiện các cải tiến trong việc triển khai các biện pháp kiểm soát an toàn thông tin

Trong quá trình soát xét sau khi một hoặc nhiều sự cố hoặc điểm yếu an toàn thông tin đã được giải quyết, các biện pháp kiểm soát mới hoặc thay đổi có thể được xác định theo yêu cầu. Các khuyến nghị và các yêu cầu liên quan về biện pháp kiểm soát có thể được đưa ra sao cho nếu xét về phương diện tài chính và vận hành thì không thể triển khai các biện pháp này ngay lập tức, mà điều đó chỉ chỉ thể hiện các mục tiêu dài hạn của tổ chức. Ví dụ, việc chuyển sang sử dụng tường lửa mạnh và an toàn hơn xét về ngắn hạn có thể không khả thi về mặt tài chính nhưng lại vẫn được yêu cầu cho các mục tiêu an toàn thông tin dài hạn của tổ chức.

Theo các khuyến nghị đã được chấp thuận, tổ chức cần triển khai các biện pháp kiểm soát được cập nhật và/hoặc mới. Đây có thể là các biện pháp kỹ thuật (gồm cả biện pháp vật lý), và có thể là cả yêu cầu cần có các cập nhật tài liệu nhanh chóng và cung cấp các chỉ dẫn nâng cao nhận thức về an toàn (cho người dùng cũng như những nhân viên khác) và bản sửa đổi bổ sung nhanh, và ban hành các hướng dẫn và/hoặc các tiêu chuẩn an toàn. Hơn nữa, các hệ thống, dịch vụ và/hoặc mạng thông tin

của tổ chức cần được đánh giá điểm yếu thường xuyên nhằm hỗ trợ việc xác định các điểm yếu và cung cấp một quy trình làm mạnh liên tục cho hệ thống/dịch vụ/mạng.

Hơn nữa, mặc dù các soát xét đối với các thủ tục và hệ thống tài liệu liên quan đến an toàn thông tin có thể được tiến hành theo hậu quả tức thì của mỗi sự cố an toàn thông tin hoặc mỗi điểm yếu đã được giải quyết, nhưng thường thì việc này được yêu cầu như một ứng phó sau này. Sau mỗi sự cố an toàn thông tin hoặc mỗi điểm yếu đã được giải quyết, nếu được thì tổ chức cần cập nhật các chính sách và thủ tục an toàn thông tin để xem xét thông tin có được và các vấn đề đã xác định trong suốt tiến trình của quy trình quản lý sự cố. Cần có sự hỗ trợ lâu dài của ISIRT cùng với người quản lý an toàn thông tin của tổ chức để đảm bảo rằng các cập nhật về thủ tục và chính sách an toàn thông tin này được phổ biến rộng rãi trong tổ chức.

9.5 Xác định và thực hiện các cải tiến đối với các kết quả đánh giá rủi ro an toàn thông tin và soát xét của ban quản lý

Tùy thuộc vào mức độ nghiêm trọng và tác động của mỗi sự cố an toàn thông tin (hoặc mức độ nghiêm trọng và tác động tiềm ẩn liên quan đến mỗi điểm yếu an toàn thông tin được báo cáo) thì tổ chức có thể cần một cuộc đánh giá các kết quả soát xét của ban quản lý và đánh giá rủi ro an toàn thông tin nhằm xem xét các mối đe dọa và các điểm yếu mới. Sau khi đã hoàn tất việc đánh giá rủi ro an toàn thông tin đã cập nhật và soát xét của ban quản lý, tổ chức có thể cần đưa ra các biện pháp kiểm soát đã thay đổi hoặc mới (xem 9.4).

9.6 Xác định và thực hiện các cải tiến đối với lược đồ quản lý sự cố an toàn thông tin

Sau khi đã giải quyết sự cố thì người quản lý ISIRT hoặc một người được chỉ định cần soát xét tất cả những việc đã xảy ra nhằm đánh giá và do đó định lượng hiệu lực của toàn bộ ứng phó đối với mỗi sự cố an toàn thông tin. Mỗi phân tích như vậy là để xác định các bộ phận đã hoạt động thành công của lược đồ quản lý sự cố an toàn thông tin và xác định các cải tiến cần thiết.

Một khía cạnh quan trọng của việc phân tích sau ứng phó là đưa thông tin và kiến thức trở lại lược đồ quản lý sự cố an toàn thông tin. Nếu sự cố đủ nghiêm trọng thì tổ chức cần đảm bảo rằng phải lên kế hoạch cho một cuộc họp có tất cả các bên liên quan ngay sau khi giải quyết xong sự cố, tức là khi thông tin vẫn còn mới mẻ. Các vấn đề cần quan tâm trong cuộc họp đó gồm:

a) Liệu các thủ tục nằm trong lược đồ quản lý sự cố an toàn thông tin đã hoạt động như mong muốn không?

b) Các thủ tục hoặc phương pháp nào có thể đã hỗ trợ trong việc phát hiện sự cố?

c) Các thủ tục hoặc công cụ nào đã được xác định là có thể đã hỗ trợ quy trình ứng phó?

d) Các thủ tục nào có thể đã hỗ trợ trong việc khôi phục các hệ thống thông tin sau khi sự cố được xác định?

e) Việc truyền thông về sự cố đến tất cả các bên liên quan đảm bảo liệu lực trong suốt quy trình phát hiện, báo cáo và ứng phó không?

Các kết quả của cuộc họp cần được ghi thành văn bản. Tổ chức cần đảm bảo rằng các phạm vi đã xác định về việc cải tiến lược đồ quản lý sự cố an toàn thông tin là những thay đổi đã được soát xét và điều chỉnh đã được đưa vào bản cập nhật của hệ thống tài liệu lược đồ. Các thay đổi đối với các quy trình, thủ tục và mẫu báo cáo quản lý sự cố an toàn thông tin cũng cần được kiểm tra và thử nghiệm kỹ lưỡng trước khi được công bố.

9.7 Các cải tiến khác

Các cải tiến khác có thể đã được xác định trong giai đoạn rút bài học kinh nghiệm, ví dụ các thay đổi về chính sách, tiêu chuẩn và thủ tục an toàn thông tin, và các thay đổi về các cấu hình phần cứng và phần mềm IT. Tổ chức cần đảm bảo rằng các cải tiến này đều được thực hiện.

Phụ lục A

(tham khảo)

Bảng tham chiếu chéo giữa TCVN 11239 và TCVN ISO/IEC 27001

Điều của TCVN ISO/IEC 27001:2005	Điều của TCVN 11239
4.2.2 Triển khai và vận hành ISMS Tổ chức phải thực hiện hành động sau: h) Triển khai các thủ tục và các biện pháp quản lý khác có khả năng nhanh chóng phát hiện các sự kiện an toàn thông tin và ứng phó với các sự cố an toàn thông tin.	4 (Tổng quan) tổng quan về triển khai quản lý sự cố an toàn thông tin. 5 (Lập kế hoạch và chuẩn bị) - nội dung có thể trợ giúp việc triển khai quản lý sự cố an toàn thông tin. 6 (Phát hiện và báo cáo), 7 (Đánh giá và quyết định), 8 (Ứng phó) và 9 (Rút bài học kinh nghiệm) – nội dung có thể trợ giúp việc vận hành quản lý sự cố an toàn thông tin.
4.2.3 Giám sát và soát xét ISMS Tổ chức phải thực hiện các hành động sau: a) Tiến hành giám sát, soát xét các thủ tục và các biện pháp quản lý khác nhằm: 2) nhanh chóng xác định các lỗ hổng và sự cố an toàn thông tin; 4) hỗ trợ phát hiện các sự kiện an toàn thông tin và do đó ngăn chặn sớm các sự cố an toàn thông tin bằng cách sử dụng các dấu hiệu cần thiết; b) Thường xuyên soát xét hiệu lực của ISMS (bao gồm việc đáp ứng các chính sách và mục tiêu quản lý của ISMS, và soát xét các biện pháp quản lý an toàn thông tin), trong đó xem xét đến các kết quả kiểm toán an toàn thông tin, các sự cố đã xảy ra, các kết quả đánh giá hiệu lực, các đề xuất và thông tin phản hồi thu thập được từ các bên liên quan.	9 (Rút bài học kinh nghiệm) - nội dung có thể trợ giúp việc giám sát và soát xét việc quản lý sự cố an toàn thông tin.

Điều của TCVN ISO/IEC 27001:2005	Điều của TCVN 11239
4.3.3 Biện pháp quản lý hồ sơ Các hồ sơ phải được lưu trữ khi thực hiện quy trình nêu tại 4.2 và trong các sự cố an toàn thông tin quan trọng liên quan đến hệ thống ISMS	5.1 (Tổng quan về các hoạt động chính), 6 (Phát hiện và báo cáo) và Phụ lục D (Ví dụ về các hồ sơ và mẫu báo cáo về sự kiện, sự cố và điểm yếu an toàn thông tin) – nội dung có thể trợ giúp việc xác định phạm vi của các hồ sơ.
A.13 Quản lý các sự cố an toàn thông tin	4 (Tổng quan) tổng quan về việc triển khai quản lý sự kiện an toàn thông tin. 5 (Lập kế hoạch và chuẩn bị) - nội dung có thể trợ giúp việc triển khai quản lý sự cố an toàn thông tin.
A.13.1 Báo cáo về các sự kiện an toàn thông tin và các nhược điểm *Mục tiêu:* Nhằm đảm bảo các sự kiện an toàn thông tin và các nhược điểm liên quan tới các hệ thống thông tin được trao đổi để các hành động khắc phục được tiến hành kịp thời Nên có các thủ tục báo cáo sự kiện và nâng dần cấp xử lý chính thức. Mọi nhân viên, nhà thầu và người dùng bên thứ ba nên được biết về các thủ tục để báo cáo các loại sự kiện và điểm yếu khác nhau có thể có tác động đến sự an toàn của các tài sản tổ chức. Họ nên được yêu cầu phải báo cáo về mọi sự kiện và điểm yếu an toàn thông tin đến PoC chỉ định nhanh nhất có thể.	5 (Lập kế hoạch và chuẩn bị) (cụ thể là 5.4 Lược đồ quản lý sự cố an toàn thông tin, 5.5 Thành lập ISIRT, 5.6 Hỗ trợ kỹ thuật và các hỗ trợ khác, 5.7 Đào tạo và nâng cao nhận thức, 5.8 Thử nghiệm lược đồ), 6 (Phát hiện và báo cáo), Phụ lục C (Ví dụ về cách phân loại và phân cấp các sự kiện và sự cố an toàn thông tin) và Phụ lục D (Ví dụ về các hồ sơ và mẫu báo cáo về sự kiện, sự cố và điểm yếu an toàn thông tin) - nội dung có thể trợ giúp việc báo cáo điểm yếu và sự kiện an toàn thông tin.
A.13.1.1 Báo cáo các sự kiện an toàn thông tin *Biện pháp quản lý:* Các sự kiện an toàn thông tin cần được báo cáo thông qua các kênh quản lý thích hợp theo cách nhanh nhất có thể.	Phụ lục D.2.1 (Ví dụ về các mục của hồ sơ sự kiện an toàn thông tin) và Phụ lục D.4.1 (Ví dụ về mẫu báo cáo sự kiện an toàn thông tin) đưa ra ví dụ về mẫu báo cáo.
A.13.1.2 Báo cáo nhược điểm về an toàn thông tin *Biện pháp quản lý:* Mọi nhân viên, nhà thầu và	Phụ lục D.2.3 (Ví dụ về các mục của hồ sơ điểm yếu an toàn thông tin) và Phụ lục D.4.3 (ví dụ về mẫu báo cáo điểm yếu an toàn thông tin) đưa ra

Điều của TCVN ISO/IEC 27001:2005	Điều của TCVN 11239
bên thứ ba của các hệ thống và dịch vụ thông tin cần được yêu cầu ghi lại và báo cáo bất kỳ nhược điểm nào về an toàn đã thấy được hoặc cảm thấy nghi ngờ trong các hệ thống dịch vụ.	ví dụ về mẫu báo cáo.
A.13.2 Quản lý các sự cố an toàn thông tin và cải tiến *Mục tiêu:* Nhằm đảm bảo một cách tiếp cận hiệu quả nhất và nhất quán được áp dụng trong việc quản lý các sự cố an toàn thông tin. Nên đưa ra các trách nhiệm và thủ tục xử lý các sự kiện và điểm yếu an toàn thông tin hiệu quả ngay khi chúng được báo cáo. Quy trình cải tiến liên tục nên được áp dụng để ứng phó, giám sát, đánh giá và quản lý tổng thể các sự kiện an toàn thông tin. Khi chứng cứ được yêu cầu thì chúng nên được thu thập để đảm bảo tuân thủ theo các yêu cầu pháp lý.	7 (Đánh giá và quyết định), 8 (Ứng phó) và 9 (Rút bài học kinh nghiệm) và Phụ lục B (Ví dụ về các sự cố an toàn thông tin và nguyên nhân), Phụ lục C (Ví dụ về phương pháp tiếp cận để phân loại và phân cấp các sự kiện và sự cố an toàn thông tin), Phụ lục E (Các khía cạnh quy định và pháp lý).
A.13.2.1 Các trách nhiệm và thủ tục *Biện pháp quản lý:* Các trách nhiệm và thủ tục quản lý cần được thiết lập nhằm đảm bảo sự phản ứng nhanh chóng, hiệu quả, đúng trình tự khi xảy ra các sự cố an toàn thông tin.	7 (Đánh giá và quyết định), 8 (Ứng phó) và Phụ lục D.2.2 (Ví dụ về các mục của hồ sơ sự cố an toàn thông tin) và Phụ lục D.4.2 (Ví dụ về mẫu báo cáo sự cố an toàn thông tin) - nội dung có thể trợ giúp xác định các trách nhiệm và thủ tục.
A.13.2.2 Rút bài học kinh nghiệm từ các sự cố an toàn thông tin *Biện pháp quản lý:* Cần có các cơ chế sẵn sàng để định lượng và giám sát các kiểu, các mức độ và chi phí của các sự cố an toàn thông tin.	9 (Rút bài học kinh nghiệm) và Phụ lục B (Ví dụ về các sự cố an toàn thông tin và nguyên nhân) và Phụ lục C (Ví dụ về các phương pháp tiếp cận phân loại và phân cấp các sự kiện và sự cố an toàn thông tin) - nội dung có thể trợ giúp việc xác định các bài học kinh nghiệm từ các sự cố an toàn thông tin.
A.13.2.3 Thu thập chứng cứ *Biện pháp quản lý:* Khi một hành động nhằm	7 (Đánh giá và quyết định), 8 (Ứng phó) (cụ thể

Điều của TCVN ISO/IEC 27001:2005	Điều của TCVN 11239
chống lại một người hay một tổ chức sau khi có một số sự cố an toàn thông tin xảy ra, liên quan đến pháp luật (có thể là dân sự hay hình sự), chứng cứ cần được thu thập, giữ lại và được trình bày sao cho phù hợp với quy định pháp lý.	là 8.2.5 Phân tích điều tra an toàn thông tin) và Phụ lục E (Các khía cạnh quy định và pháp lý) - nội dung có thể trợ giúp việc xác định các thủ tục thu thập chứng cứ.

Phụ lục B

(tham khảo)

Ví dụ về các sự cố an toàn thông tin và nguyên nhân

B.1. Các cuộc tấn công

B.1.1. Từ chối dịch vụ

Từ chối dịch vụ (DoS) và Từ chối dịch vụ phân tán (DDos) là một loại sự cố chiếm tỷ lệ lớn chiếm tỷ lệ lớn trong các sự cố an toàn thông tin nói chung. Các sự cố này làm cho hệ thống, dịch vụ hoặc mạng không thể tiếp tục hoạt động với năng lực dự kiến, phần lớn đều dẫn đến từ chối hoàn toàn truy cập của người dùng hợp pháp. Có hai loại sự cố DoS/DDoS chính do các phương tiện kỹ thuật gây ra: loại bỏ nguồn lực và làm cạn kiệt nguồn lực.

Dưới đây là một số ví dụ điển hình về các sự cố DoS/DDoS kỹ thuật cố ý:

- ping các địa chỉ mạng quảng bá nhằm làm tràn băng thông mạng bằng lưu lượng ứng phó,
- gửi dữ liệu với định dạng không mong muốn đến một hệ thống, dịch vụ, hoặc mạng nhằm đánh sập hoặc làm gián đoạn hoạt động bình thường,
- mở nhiều phiên hợp lệ với một hệ thống, dịch vụ hoặc mạng nhất định nhằm làm cạn kiệt nguồn lực (ví dụ làm chậm, khóa hoặc đánh sập).

Các cuộc tấn công như vậy thường được thực hiện thông qua các Botnet, đây là tập hợp của các rô bốt phần mềm (mã độc) chạy độc lập và tự động. Các Botnet có thể bao gồm hàng trăm đến hàng triệu máy tính bị ảnh hưởng.

Một số sự cố DoS kỹ thuật có thể là do vô tình, ví dụ do người quản trị cấu hình sai hoặc phần mềm ứng dụng không tương thích, nhưng hầu hết sự cố DoS xảy ra là do có chủ ý. Một số sự cố DoS kỹ thuật được cố ý tạo ra nhằm đánh sập hệ thống hoặc dịch vụ hoặc làm chậm mạng, một số khác đôi khi lại là kết quả của các hoạt động nguy hiểm khác. Ví dụ, một số kỹ thuật định danh và quét lén có thể làm cho các hệ thống hoặc dịch vụ cấu hình sai hoặc cũ bị phá vỡ khi chúng bị quét. Cần lưu ý rằng, nhiều sự cố DoS kỹ thuật cố ý lại thường được thực hiện nặc danh (tức là nguồn gốc của cuộc tấn công là "giả"), bởi vì chúng thường không phụ thuộc vào việc kẻ tấn công có nhận được thông tin phản hồi từ mạng hoặc hệ thống bị tấn công hay không.

Các nguyên nhân dẫn đến sự cố DoS gây ra do các phương tiện phi kỹ thuật, làm tổn thất thông tin, dịch vụ và/hoặc thiết bị, có thể là:

- các lỗ hổng trong các hệ thống an toàn vật lý dẫn đến việc đánh cắp hoặc cố ý gây hư hại và thiệt hại cho thiết bị,

- thiệt hại vô tình tới thiết bị phần cứng (và/hoặc vị trí của thiết bị) do hỏa hoạn hoặc lũ lụt,
- các điều kiện môi trường khắc nghiệt, ví dụ như nhiệt độ hoạt động cao (ví dụ do hỏng điều hòa không khí),
- trục trặc hoặc quá tải hệ thống,
- các thay đổi không được kiểm soát của hệ thống,
- trục trặc của phần mềm hoặc phần cứng.

B.1.2. Truy cập trái phép

Nói chung, sự cố loại này gồm các hành động cố gắng thực sự để truy cập hoặc lợi dụng trái phép hệ thống, dịch vụ hoặc mạng. Dưới đây là một số ví dụ về sự cố truy cập kỹ thuật trái phép bằng phương tiện kỹ thuật:

- các cố gắng lấy các tệp tin mật khẩu,
- các tấn công làm tràn bộ đệm để có dành quyền (ví dụ, quản trị hệ thống) truy cập vào một mục tiêu,
- sự khai thác các điểm yếu của giao thức để chiếm hoặc làm sai hướng của các kết nối hợp pháp,
- các cố gắng nâng cao đặc quyền đối với các nguồn lực hoặc thông tin vượt quá quyền của người dùng hoặc quản trị viên.

Dưới đây là một số ví dụ về nguyên nhân dẫn đến các sự cố truy cập trái phép do các phương tiện phi kỹ thuật, gây ra sự tiết lộ trực tiếp hoặc gián tiếp hoặc sửa đổi thông tin, các lỗ hổng về giải trình trách nhiệm hoặc sử sụng sai mục đích các hệ thống thông tin:

- các lỗ hổng trong các hệ thống an toàn vật lý dẫn đến sự truy cập trái phép thông tin,
- các hệ điều hành kém và/hoặc sai cấu hình do các thay đổi hệ thống không được kiểm soát hoặc các trục trặc trong phần mềm hoặc phần cứng.

B.1.3. Mã độc

Mã độc là một chương trình hoặc một phần của một chương trình được đưa vào một chương trình khác với mục đích làm thay đổi tính năng ban đầu của chương trình đó nhằm thực hiện các hoạt động nguy hiểm như trộm cắp thông tin và định danh, phá hủy thông tin và nguồn lực, từ chối dịch vụ, thư rác... Các tấn công do mã độc có thể chia thành năm loại: virus, sâu, ngựa trojan, mã di động và loại kết hợp. Mặc dù trong vài năm trước đây, virus được tạo ra để nhằm vào các hệ thống bị lây nhiễm dễ bị tổn hại, nhưng hiện tại, các mã độc được sử dụng cho các cuộc tấn công có mục tiêu. Đôi khi chỉ cần thực hiện một thay đổi trong mã độc có sẵn là có thể tạo ra một biến thể mã độc có khả năng tránh khỏi sự phát hiện của các công nghệ truy quét mã độc.

B.1.4. Sử dụng không phù hợp

Sự cố loại này xảy ra khi người dùng vi phạm các chính sách an toàn hệ thống thông tin của một tổ chức. Các sự cố này không phải là cuộc tấn công theo đúng nghĩa, nhưng chúng thường được thông báo là sự cố và cũng cần được ISIRT quản lý. Sử dụng không phù hợp có thể là:

- tải và cài đặt các công cụ xâm nhập,
- sử dụng thư điện tử chung của tổ chức để phát tán thư rác hoặc quảng cáo cho việc cá nhân,
- sử dụng các nguồn lực của tổ chức để lập một website trái phép,
- sử dụng các hoạt động ngang hàng để lấy hoặc phát tán các tệp tin vi phạm bản quyền (âm nhạc, hình ảnh, phần mềm).

B.2. Thu thập thông tin

Nói chung, loại sự cố thu thập thông tin bao gồm các hoạt động liên quan đến việc xác định các mục tiêu tiềm ẩn và tìm hiểu các dịch vụ hoạt động trên các mục tiêu đó. Đây là loại sự cố liên quan đến do thám, với mục đích là để xác định:

- sự tồn tại của một mục tiêu, tìm hiểu cấu trúc mạng quanh mục tiêu, và đối tượng mà mục tiêu thường xuyên liên lạc, và
- các điểm yếu tiềm ẩn có thể khai thác được của mục tiêu hoặc môi trường mạng của mục tiêu.

Dưới đây là các ví dụ về tấn công thu thập thông tin gây ra bởi các phương tiện kỹ thuật:

- việc kết xuất các hồ sơ Hệ thống tên miền (DNS) để lấy tên miền internet của mục tiêu (chuyển giao DNS giữa các vùng),
- việc ping các địa chỉ mạng để tìm những những hệ thống còn "sống",
- việc thăm dò hệ thống nhằm xác định (ví dụ, dấu vân tay) hệ điều hành máy chủ,
- việc quét các cổng mạng hiện có trên hệ thống nhằm xác định các dịch vụ liên quan (ví dụ, thư điện tử, FTP, web...) và xác định phiên bản phần mềm của những dịch vụ này,
- việc quét để tìm một hoặc nhiều dịch vụ dễ bị tổn hại trên một dải địa chỉ mạng (quét theo chiều ngang).

Tong một số trường hợp, sự cố thu thập thông tin cũng có thể là truy cập trái phép nếu, ví dụ, khi tìm kiếm các điểm yếu, kẻ tấn công cũng cố gắng truy cập trái phép. Điều này thường xảy ra với các công cụ xâm nhập tự động, các công cụ này không chỉ tìm kiếm các lỗ hổng mà còn tự động cố gắng khai thác các hệ thống, dịch vụ hoặc/và mạng dễ bị tổn hại được tìm thấy.

Các sự cố tập hợp thông tin gây ra bởi các phương tiện phi kỹ thuật, dẫn đến:

- sự tiết lộ thông tin trực tiếp hoặc gián tiếp, hoặc sự thay đổi thông tin,
- sự đánh cắp tài sản sở hữu trí tuệ được lưu trữ điện tử,

- các lỗ hổng về tính giải trình trách nhiệm, ví dụ trong việc ghi nhật ký tài khoản,
- sự lạm dụng hệ thống thông tin (ví dụ, làm trái luật hoặc chính sách của tổ chức)

có thể gây ra bởi các nguyên nhân sau:

- các lỗ hổng của các hệ thống an toàn vật lý dẫn đến sự truy cập trái phép thông tin, và đánh cắp các thiết bị lưu trữ dữ liệu có chứa thông tin quan trọng, vi dụ như mã khóa,
- các hệ điều hành kém và/hoặc sai cấu hình do các thay đổi không thể kiểm soát được của hệ thống hoặc các trục trặc trong phần mềm hoặc phần cứng, kết quả là người trong nội bộ hoặc bên ngoài truy cập được các thông tin mà họ không được phép.

Phụ lục C

(Tham khảo)

Ví dụ về các phương pháp tiếp cận để phân loại và phân cấp các sự kiện và sự cố an toàn thông tin

C.1. Giới thiệu

Phụ lục này đưa ra ví dụ về các phương pháp tiếp cận để phân loại và phân cấp các sự cố an toàn thông tin. Các phương pháp này cho phép nhân viên và tổ chức lập tài liệu các sự cố an toàn thông tin theo cách phù hợp để đạt được các lợi ích sau:

- thúc đẩy việc trao đổi và chia sẻ các thông tin về sự cố an toàn thông tin,
- hỗ trợ việc tự động báo cáo và ứng phó với sự cố an toàn thông tin,
- nâng cao hiệu lực và hiệu quả trong việc xử lý và quản lý sự cố an toàn thông tin,
- hỗ trợ thu thập và phân tích dữ liệu về các sự cố an toàn thông tin,
- xác định mức độ nghiêm trọng của các sự cố an toàn thông tin theo tiêu chí phù hợp.

Các ví dụ về phương pháp tiếp cận để phân loại và phân cấp này cũng có thể được áp dụng cho các sự kiện an toàn thông tin, nhưng không áp dụng cho các điểm yếu an toàn thông tin

C.2. Phân loại sự cố an toàn thông tin

Các sự cố an toàn thông tin có thể có nguyên nhân từ các hành động vô tình hoặc cố ý của con người, và có thể do các phương tiện kỹ thuật hoặc vật lý gây ra. Phương pháp tiếp cận sau đây sẽ phân loại sự cố an toàn thông tin dựa trên các mối đe dọa. (Xem thông tin về các mối đe dọa trong Phụ lục C Ví dụ về các mối đe dọa, của ISO/IEC 27005:2011). Bảng C.1 đưa ra danh sách phân loại sự cố an toàn thông tin.

Bảng C.1 – Phân loại sự cố an toàn thông tin theo các mối đe dọa

Loại	Mô tả	Ví dụ
Sự cố do thiên tai	Mất an toàn thông tin do các thảm họa tự nhiên ngoài tầm kiểm soát của con người.	Động đất, núi lửa, lũ lụt, gió lớn, sét, sóng thần, sụt lún...
Sự cố do bất ổn xã hội	Mất an toàn thông tin do sự bất ổn xã hội.	Bedin, khủng bố, chiến tranh...
Sự cố do thiệt hại vật chất	Mất an toàn thông tin do các hành động vật lý vô tình hoặc cố ý.	Hỏa hoạn, nguồn nước, tĩnh điện, môi trường xấu (ô nhiễm, bụi, ăn mòn, đóng băng), sự phá hoại thiết bị, sự phá hoại phương tiện lưu trữ, trộm cắp thiết bị, trộm cắp phương tiện lưu trữ, mất

Loại	Mô tả	Ví dụ
		thiết bị, mất phương tiện thông tin, sự giả mạo thiết bị, sự giả mạo phương tiện lưu trữ...
Sự cố do lỗi cơ sở hạ tầng	Mất an toàn thông tin do lỗi của các hệ thống, dịch vụ cơ bản hỗ trợ vận hành các hệ thống thông tin.	Lỗi nguồn điện, lỗi mạng, sự cố điều hòa không khí, sự cố nguồn nước...
Sự cố do nhiễu phát xạ	Mất an toàn thông tin do nhiễu phát xạ.	Phát xạ điện từ, xung điện từ, nhiễu điện từ, dao động điện áp, bức xạ nhiệt...
Sự cố do lỗi kỹ thuật	Mất an toàn thông tin do lỗi trong các hệ thống thông tin hoặc các phương tiện phi kỹ thuật liên quan, các vấn đề do con người vô ý gây ra, dẫn đến sự không sẵn sàng hoặc bị phá hủy của các hệ thống thông tin.	Lỗi phần cứng, sự cố phần mềm, quá tải (làm bão hòa năng lực của hệ thống thông tin), lỗ hổng về khả năng duy trì...
Sự cố do phần mềm độc hại	Mất an toàn thông tin do các chương trình độc hại được tạo và phát tán một cách cố ý. Chương trình độc hại được đưa vào các hệ thống thông tin nhằm gây tổn hại đến tính bí mật, toàn vẹn hoặc sẵn sàng của dữ liệu, ứng dụng hoặc hệ điều hành, và/hoặc gây ảnh hưởng đến hoạt động bình thường của hệ thống thông tin.	Virus máy tính, sâu mạng, ngựa trojan, botnet, tấn công kết hợp, mã độc được nhúng vào trong web page, trang lưu trữ mã độc... Virus máy tính là một tập hợp lệnh hoặc mã máy tính được đưa vào các chương trình máy tính. Không giống như các chương trình thông thường, virus máy tính có khả năng tự sao chép, và thường mang một tải tin có thể gây gián đoạn hoạt động của máy tính hoặc phá hủy dữ liệu. Khác với virus máy tính, sâu mạng lại là một loại chương trình độc hại tự lây lan và tự sao chép qua mạng bằng cách khai thác các điểm yếu của hệ thống thông tin trên mạng. Ngựa trojan là một loại chương trình độc hại giả dạng chức năng tốt của hệ thống thông tin, và có khả năng cho phép tác giả chương trình kiểm soát hệ thống thông tin, bao gồm cả trộm cắp hoặc ngăn chặn thông tin từ hệ thống.

Loại	Mô tả	Ví dụ
		Botnet là một nhóm các máy tính bị tổn hại (máy tính ma) trong các mạng bị kiểm soát tập trung bởi tác giả của botnet, tác giả của botnet được coi là kẻ điều khiển hoặc dẫn dắt botnet. Botnet được hình thành một cách cố ý thông qua lây nhiễm hàng loạt các máy tính trong mạng bằng các chương trình tự động. Botnet có thể được sử dụng trong các tấn công cơ hội vào mạng, trộm cắp thông tin, và phát tán ngựa trojan, sâu mạng và các chương trình độc hại khác. Tấn công kết hợp có thể có đặc điểm kết hợp của các virus máy tính, sâu mạng, ngựa trojan hoặc botnet... Tấn công kết hợp cũng có thể là kết quả của các hoạt động kết hợp của nhiều phần mềm độc hại khác nhau. Ví dụ, virus máy tính hoặc sâu mạng xâm nhập vào một hệ thống máy tính, sau đó cài đặt một chương trình ngựa trojan vào hệ thống. Web page nhúng mã độc hủy hoại các website bằng cách đưa mã độc cài đặt phần mềm độc hại vào hệ thống máy tính truy cập vào trang đó. Địa chỉ lưu trữ mã độc sẽ dụ website lưu trữ mã độc đã được những người dùng mục tiêu tải về.
Sự cố do tấn công kỹ thuật	Mất an toàn thông tin do sự tấn công các hệ thống thông tin thông qua mạng hoặc các phương tiện kỹ thuật khác, bằng cách khai thác các điểm yếu trong cấu hình, giao thức hoặc chương trình của các hệ thống thông tin, gây ra tình trạng bất thường của hệ thống thông tin, hoặc gây tổn hại tiềm ẩn đến các hệ điều hành đang chạy.	Quét mạng, khai thác điểm yếu, khai thác cổng sau, cố gắng đăng nhập, nhiễu, DoS... Quét mạng là sử dụng phần mềm quét mạng để lấy các thông tin về cấu hình, các cổng, dịch vụ và điểm yếu của mạng. Khai thác điểm yếu là khai thác và sử dụng các nhược điểm của hệ thống thông tin, ví dụ nhược điểm về cấu hình, giao thức, hoặc chương trình. Khai thác cổng sau là sử dụng các cổng sau hoặc các chương tình độc hại được để lại trong quá trình thiết kế hệ thống phần mềm và phần cứng.

Loại	Mô tả	Ví dụ
		Cố gắng đăng nhập là cố gắng đoán, bẻ gãy mật khẩu. Nhiễu gây cản trở các mạng máy tính, các mạng truyền dẫn vô tuyến và truyền hình không dây hoặc có dây, hoặc các tín hiệu vô tuyến hoặc truyền hình vệ tinh, bằng các phương tiện kỹ thuật. DoS gây ra do việc sử dụng hệ thống thông tin và các tài nguyên mạng như CPU, bộ nhớ, dung lượng ổ cứng hoặc băng thông mạng, và gây ảnh hưởng đến hoạt động bình thường của các hệ thống thông tin, ví dụ SYS-a, làm tràn bằng lệnh PING, bom thư điện tử.
Sự cố do vi phạm quy định	Mất an toàn thông tin do cố tình hoặc vô ý vi phạm các quy định	Sử dụng trái phép nguồn lực, vi phạm bản quyền... Sử dụng trái phép nguồn lực là truy cập vào các nguồn lực để dùng cho các mục đích không được phép, bao gồm các công việc sinh lợi nhuận, ví dụ sử dụng thư điện tử để tham gia vào việc gửi thư theo dây chuyền bất hợp pháp để kiếm lời hoặc các mô hình đa cấp. Vi phạm bản quyền gây ra do mua bán hoặc cài đặt các bản sao phần mềm thương mại không có giấy phép hoặc các tài liệu có bản quyền được bảo vệ, ví dụ, warez.
Sự cố do tổn hại chức năng	Mất an toàn thông tin do cố tình hoặc vô ý làm tổn hại chức năng của hệ thống thông tin về phương diện an toàn .	Lạm dụng quyền, giả mạo quyền, phủ nhận hành động, vận hành sai, vi phạm biên chế nhân sự... Lạm dụng quyền là sử dụng quyền vượt quá điều khoản quy định. Giả mạo quyền hạn là tạo nên các quyền giả mạo với mục đích lừa gạt. Phủ nhận hoạt động là khi một một người nào đó phủ nhận những điều mà họ đã làm.

Loại	Mô tả	Ví dụ
		Vận hành sai là thực hiện các hoạt động không chính xác hoặc không định trước. Vi phạm biên chế nhân sự là do thiếu hoặc không có nhân lực.
Sự cố do tổn hại thông tin	Mất an toàn thông tin do cố tình hoặc vô ý làm tổn hại đến sự an toàn thông tin như tính mật, tính toàn vẹn, tính sẵn sàng, ...	Ngăn chặn, theo dõi, nghe lén, tiết lộ, giả mạo, kỹ thuật xã hội, lừa đảo trên mạng, trộm cắp dữ liệu, mất dữ liệu, giả mạo dữ liệu, lỗi dữ liệu, phân tích luồng dữ liệu, phát hiện vị trí... Ngăn chặn là lấy dữ liệu trước khi chúng có thể tiếp cận người nhận định trước. Theo dõi là bí mật thu thập và báo cáo thông tin về các hoạt động của tổ chức khác. Nghe lén là nghe cuộc hội thoại của bên khác mà họ không biết. Tiết lộ thông tin là làm cho các thông tin nhạy cảm bị công khai. Giả mạo là khi một chủ thể giả làm một đối tượng khác. Kỹ thuật xã hội là để thu thập thông tin từ một người theo hình thức phi kỹ thuật, ví dụ, lừa đảo, mánh khóe, hối lộ, hoặc đe dọa. Lừa đảo mạng là sử dụng công nghệ mạng máy tính lừa đảo để lôi kéo người dùng tiết lộ những thông tin quan trọng, như lấy thông tin chi tiết về tài khoản ngân hàng và mật khẩu của người dùng bằng các thư điện tử lừa đảo. Trộm cắp dữ liệu là hành vi lấy trộm dữ liệu. Giả mạo dữ liệu là tiếp cận hoặc tạo ra các thay đổi dữ liệu một cách trái phép. Lỗi dữ liệu là tạo ra lỗi khi nhập hoặc xử lý dữ liệu. Phát hiện vị trí là phát hiện vị trí của các hệ thống

Loại	Mô tả	Ví dụ
		hoặc thông tin nhạy cảm.
Sự cố do các nội dung độc hại	Mất an toàn thông tin do lan truyền nội dung không mong muốn qua mạng thông tin gây đe dọa đến an ninh quốc gia, ổn định xã hội và/hoặc an ninh và lợi ích công cộng.	Nội dung bất hợp pháp, nội dung gây hoang mang, nội dung độc hại, nội dung lạm dụng... Nội dung bất hợp pháp là nội dung được công bố rộng rãi vi phạm hiến pháp quốc gia hoặc quốc tế, luật pháp và quy định, ví dụ, khiêu dâm trẻ em, cổ súy bạo động, giả mạo, lừa đảo. Nội dung gây hoang mang là thảo luận hoặc bình luận độc hại có khả năng gây kích động về các vấn đề nhạy cảm trên Internet, gây ra các sự kiện như bất ổn xã hội hoặc gây hoang mang dư luận. Nội dung độc hại là truyền bá các nội dung gây tác động độc hại đến xã hội hoặc con người, ví dụ, lừa đảo, quấy rối. Nội dung lạm dụng là quảng bá các nội dung chưa được chấp thuận từ người nhận, ví dụ, thư rác.
Các sự cố khác	Không thuộc các loại sự cố trên.	

C.3. Phân cấp sự cố an toàn thông tin

Phần sau giới thiệu hai ví dụ về phương pháp tiếp cận để phân cấp sự cố an toàn thông tin.

Cần nhấn mạnh rằng đây chỉ là các ví dụ. Còn có các phương pháp tiếp cận khác như FIRST/Hệ thống chấm điểm điểm yếu thông thường (CVSS) Mitre và Định dạng thông tin cảnh báo có cấu trúc (SWIF) của Vương quốc Anh.

C.3.1 Ví dụ 1

C.3.1.1 Các yếu tố phân cấp

C3.1.1.1 Giới thiệu

Phương pháp tiếp cận này phân cấp các sự cố an toàn thông tin theo ba yếu tố sau:

- tầm quan trọng của hệ thống thông tin,
- tổn thất nghiệp vụ,
- tác động xã hội.

C3.1.1.2 Tầm quan trọng của hệ thống thông tin

Tầm quan trọng của các hệ thống thông tin bị ảnh hưởng bởi các sự cố an toàn thông tin được xác định bằng cách xem xét tầm quan trọng của các hoạt động nghiệp vụ của tổ chức được hỗ trợ bởi các hệ thống thông tin đó. Tầm quan trọng có thể được thể hiện trong mối quan hệ với an ninh quốc gia, trật tự xã hội, sự phát triển kinh tế và lợi ích công cộng, và sự phụ thuộc của nghiệp vụ vào các hệ thống thông tin. Phương pháp tiếp cận này phân cấp tầm quan trọng của các hệ thống quan trọng thành ba cấp độ chính: hệ thống thông tin đặc biệt quan trọng, hệ thống thông tin quan trọng và hệ thống thông tin thông thường.

C3.1.1.3 Tổn thất nghiệp vụ

Tổn thất nghiệp vụ của tổ chức do các sự cố an toàn thông tin được xác định bằng cách xem xét mức độ nghiêm trọng của tác động gián đoạn nghiệp vụ do thiệt hại phần cứng/phần mềm, các chức năng và dữ liệu của các hệ thống thông tin. Mức độ nghiêm trọng của tác động có thể phụ thuộc vào chi phí khôi phục nghiệp vụ trở lại bình thường và các tác động tiêu cực khác của các sự cố an toàn thông tin, bao gồm tổn thất lợi nhuận và/hoặc cơ hội. Phương pháp tiếp cận này phân cấp các tổn thất nghiệp vụ thành bốn cấp độ chính: tổn thất nghiệp vụ đặc biệt nghiêm trọng, tổn thất nghiệp vụ nghiêm trọng, tổn thất nghiệp vụ lớn và tổn thất nghiệp vụ nhỏ, như mô tả dưới đây.

a) Tổn thất nghiệp vụ đặc biệt nghiêm trọng có thể là tê liệt hoạt động nghiệp vụ lớn đến mức làm mất khả năng nghiệp vụ, và/hoặc thiệt hại rất nghiêm trọng đến tính bí mật, toàn vẹn và sẵn sàng của dữ liệu nghiệp vụ quan trọng. Điều đó có thể đồng nghĩa với mức chi phí rất lớn để khôi phục nghiệp vụ trở lại hoạt động bình thường và loại bỏ các tác động tiêu cực. Các tổ chức có thể không thể chịu được mức tổn thất nghiệp vụ này.

b) Tổn thất nghiệp vụ nghiêm trọng có thể là gián đoạn hoạt động nghiệp vụ trong một thời gian dài hoặc tê liệt nghiệp vụ nội bộ dẫn đến ảnh hưởng nghiêm trọng khả năng nghiệp vụ, và/hoặc thiệt hại nghiêm trọng đến tính bí mật, toàn vẹn và sẵn sàng của dữ liệu nghiệp vụ quan trọng. Điều đó có thể đồng nghĩa với mức chi phí cao để khôi phục nghiệp vụ trở lại hoạt động bình thường và loại bỏ các tác động tiêu cực. Các tổ chức có thể chịu được mức tổn thất nghiệp vụ này.

c) Tổn thất nghiệp vụ lớn là gián đoạn hoạt động nghiệp vụ ở một mức đáng kể ảnh hưởng đến khả năng nghiệp vụ, và/hoặc thiệt hại đáng kể đến tính bí mật, toàn vẹn và sẵn sàng của dữ liệu nghiệp vụ quan trọng. Điều đó có thể đồng nghĩa với chi phí đáng kể để khôi phục nghiệp vụ trở lại hoạt động bình thường và loại bỏ các tác động tiêu cực. Các tổ chức hoàn toàn có thể chịu được mức tổn thất nghiệp vụ này.

d) Tổn thất nghiệp vụ nhỏ là gián đoạn hoạt động nghiệp vụ trong một thời gian ngắn dẫn đến một số ảnh hưởng đến khả năng nghiệp vụ và/hoặc tác động nhỏ đến tính bí mật, toàn vẹn và sẵn sàng của dữ liệu nghiệp vụ quan trọng. Điều đó có thể đồng nghĩa với chi phí nhỏ để khôi phục nghiệp vụ trở lại hoạt động bình thường và loại bỏ các tác động tiêu cực.

C.3.1.1.4 Tác động xã hội

Tác động đối với xã hội do sự cố an toàn thông tin được xác định bằng cách xem xét quy mô và mức độ tác động đến an ninh quốc gia, trật tự xã hội, sự phát triển kinh tế và lợi ích công cộng. Phương pháp tiếp cận này phân cấp tác động xã hội thành bốn cấp độ: tác động xã hội đặc biệt quan trọng, tác động xã hội quan trọng, tác động xã hội lớn và tác động xã hội nhỏ, như mô tả dưới đây.

a) Tác động xã hội đặc biệt quan trọng có thể là các ảnh hưởng bất lợi ảnh hưởng đến hầu hết các khu vực của một hoặc nhiều tỉnh, đe dọa lớn đến an ninh quốc gia, gây ra bất ổn xã hội, mang lại hậu quả vô cùng bất lợi về phát triển kinh tế và/hoặc gây thiệt hại nghiêm trọng đến lợi ích công cộng.

b) Tác động xã hội quan trọng có thể là các ảnh hưởng bất lợi ảnh hưởng đến hầu hết các khu vực của một hoặc nhiều thành phố, đe dọa đến an ninh quốc gia, gây hoang mang dư luận, mang lại hậu quả tiêu cực đáng kể về phát triển kinh tế và/hoặc gây thiệt hại đến lợi ích công cộng.

c) Tác động xã hội đáng kể có thể là các ảnh hưởng bất lợi ảnh hưởng đến các khu vực của một hoặc nhiều thành phố, đe dọa nhỏ đến an ninh quốc gia, gây ra một số xáo trộn trật tự xã hội, mang lại một số hậu quả xấu đến phát triển kinh tế và/hoặc ảnh hưởng đến lợi ích công cộng.

d) Tác động xã hội nhỏ có thể là các ảnh hưởng bất lợi một khu vực của một thành phố, ít có cơ hội đe dọa đến an ninh quốc gia, trật tự xã hội, sự phát triển kinh tế và lợi ích công cộng, nhưng có gây thiệt hại đến lợi ích của các cá nhân, doanh nghiệp và các tổ chức khác.

C.3.1.2 Các cấp độ

C.3.1.2.1 Giới thiệu

Dựa trên các yếu tố phân cấp, các sự cố an toàn thông tin cần được phân cấp theo mức độ nghiêm trọng bằng thang phân cấp. Thang phân cấp có thể chỉ đơn giản là 'lớn' và 'nhỏ' hoặc chi tiết hơn như:

- Khẩn cấp: tác động nghiêm trọng;
- Quan trọng: tác động trung bình;
- Cảnh báo: tác động thấp;
- Thông báo: không có tác động, nhưng có thể được phân tích để cải tiến các chính sách, quy trình hoặc biện pháp kiểm soát.

Theo các yếu tố phân cấp trên thì phương pháp tiếp cận này phân cấp các sự cố an toàn thông tin thành bốn cấp độ:

- Rất nghiêm trọng (cấp IV);
- Nghiêm trọng (Cấp III);
- Ít nghiêm trọng (cấp II);
- Nhỏ (cấp I).

Cần nhấn mạnh rằng các cấp độ ở trên chỉ là ví dụ. Trong một số phương pháp tiếp cận, cấp nghiêm trọng nhất được biểu diễn có chỉ số cao nhất. Trong các phương pháp khác thì cấp nghiêm trọng nhất lại được biểu diễn có chỉ số nhỏ nhất.

C.3.1.2.2 Rất nghiêm trọng (cấp IV)

Sự cố rất nghiêm trọng là những sự cố

a) hoạt động trên các hệ thống thông tin đặc biệt quan trọng, và

b) gây tổn thất nghiệp vụ đặc biệt nghiêm trọng, hoặc

c) dẫn đến tác động xã hội đặc biệt quan trọng.

C.3.1.2.3 Nghiêm trọng (cấp III)

Sự cố nghiêm trọng là những sự cố

a) hoạt động trên các hệ thống thông tin đặc biệt quan trọng hoặc các hệ thống thông tin quan trọng, và

b) gây tổn thất nghiệp vụ nghiêm trọng, hoặc

c) dẫn đến tác động xã hội quan trọng.

C.3.1.2.3 Ít nghiêm trọng (cấp II)

Sự cố ít nghiêm trọng là những sự cố

a) hoạt động trên các hệ thống thông tin quan trọng hoặc các hệ thống thông tin thông thường, và

b) gây tổn thất nghiệp vụ đáng kể, hoặc

c) dẫn đến tác động xã hội đáng kể.

C.3.1.2.3 Nhỏ (cấp I)

Sự cố nhỏ là những sự cố

a) hoạt động trên các hệ thống thông tin quan trọng thông thường,

b) gây tổn thất nghiệp vụ nhỏ hoặc không có tổn thất nghiệp vụ,

c) dẫn đến tác động xã hội nhỏ hoặc không có tác động xã hội,

d) không có yêu cầu phải hành động và không gây hậu quả.

C.3.1.3 Loại sự cố và cấp độ nghiêm trọng

Loại sự cố an toàn thông tin và cấp độ nghiêm trọng thường liên quan với nhau. Một sự cố an toàn thông tin có thể có cấp độ nghiêm trọng khác nhau phụ thuộc không chỉ vào nghiệp vụ mà còn vào tính chất của sự cố an toàn thông tin như

- cố ý,

- có chủ đích,
- thời lượng,
- độ lớn.

Bảng C.2 đưa ra một số ví dụ về các loại sự cố an toàn thông tin có thể có các cấp độ nghiêm trọng khác nhau tùy theo tính chất của sự cố.

Bảng C.2 – Các ví dụ về danh mục sự cố và cấp độ nghiêm trọng

Cấp độ nghiêm trọng / Loại sự cố	Nhỏ	Ít nghiêm trọng	Nghiêm trọng	Rất nghiêm trọng
Tấn công bằng kỹ thuật	Nỗ lực bị thất bại	Thường là tấn công đơn lẻ (tổn hại người dùng)	Nhiều cuộc tấn công (tổn hại người dùng) Tấn công đơn lẻ quan trọng (tổn hại ứng dụng, gốc)	Tấn công hàng loạt (tấn công ứng dụng, gốc)
Tấn công bằng kỹ thuật		Quấy rối	Gây nhiễu (tác động đến thông lượng)	Không sẵn sàng (ngừng dịch vụ)
Phần mềm độc hại	Đơn lẻ, bị phát hiện (bị phát hiện và chặn bởi bảo vệ chống virus)	Đơn lẻ, không bị phát hiện	Lây nhiễm Lây nhiễm ra máy chủ	Lây nhiễm hàng loạt

C.3.2 Ví dụ 2

C.3.2.1 Giới thiệu

Phương pháp tiếp cận này đưa ra các hướng dẫn ví dụ để đánh giá các hậu quả xấu của sự cố an toàn thông tin, trong đó các hướng dẫn đều sử dụng thang điểm từ 1 (thấp) đến 10 (cao) để phân cấp các sự cố an toàn thông tin. (Trong thực tế, có thể sử dụng các thang điểm khác, như từ 1 đến 5, và mỗi tổ chức cần áp dụng một thang điểm phù hợp nhất với môi trường của mình).

Trước khi đọc các hướng dẫn ở dưới, cần lưu ý các điểm sau:

- Trong một số hướng dẫn ví dụ dưới đây có một số mục được chú thích là "Không có thông tin". Đó là do các hướng dẫn đã được xây dựng sao cho các hậu quả xấu tại mỗi cấp độ tăng dần, thể hiện trên thang điểm từ 1 đến 10, nhìn chung sẽ tương tự trên cả sáu loại được đưa đề cập từ C.3.2.2 đến C.3.2.7. Tuy nhiên, tại một số cấp độ (trên thang từ 1 đến 10) của một vài loại thì các mục hậu quả trung gian thấp hơn lại không đủ khác biệt để tạo thành một mục – do vậy các mục này được

chú thích là "Không có thông tin". Tương tự như vậy, tại các cấp độ cao hơn của một vài loại cũng không có hậu quả lớn hơn so với mục cao nhất được thấy - và do đó các mục cao hơn được chú thích là "Không có thông tin". (Vì vậy, xét về logic thì có thể sẽ không đúng nếu loại bỏ các dòng "Không có thông tin" và giảm thang đo đi.)

Như vậy, cần sử dụng các hướng dẫn dưới đây như là một bộ hướng dẫn ví dụ khi xem xét các hậu quả xấu của sự cố an toàn thông tin lên hoạt động nghiệp vụ của một tổ chức do:

- sự tiết lộ trái phép thông tin,
- sự sửa đổi trái phép thông tin,
- sự bác bỏ thông tin,
- sự không sẵn sàng của thông tin và/hoặc dịch vụ,
- sự hủy bỏ thông tin và/hoặc dịch vụ.

Bước đầu tiên là cân nhắc xem loại nào trong các loại sau đây có liên quan. Với những loại được thấy là có liên quan thì cần sử dụng hướng dẫn cho loại đó để thiết lập các tác động bất lợi thực tế đến hoạt động nghiệp vụ (hoặc giá trị) để đưa vào vào mẫu báo cáo sự cố an toàn thông tin.

C.3.2.2 Tổn thất tài chính/gián đoạn hoạt động nghiệp vụ

Hậu quả của việc tiết lộ và sửa đổi trái phép, sự bác bỏ, sự không sẵn sàng và sự hủy bỏ thông tin có thể là sự tổn thất tài chính, ví dụ làm giảm giá cổ phiếu, sự gian lận hoặc vi phạm hợp đồng do không hành động hoặc hành động chậm trễ. Tương tự như vậy, hậu quả cụ thể của sự không sẵn sàng hoặc hủy bỏ thông tin có thể là sự gián đoạn hoạt động nghiệp vụ. Để khắc phục và/hoặc khôi phục sau các sự cố như vậy sẽ đòi hỏi nhiều thời gian và công sức. Điều này trong một số trường hợp là rất quan trọng và cần được xem xét. Nhìn chung, thời gian khôi phục cần được tính theo đơn vị là thời gian sử dụng nhân lực và được chuyển đổi thành chi phí tài chính. Chi phí này cần được tính trên cơ sở tham khảo các chi phí thông thường cho một người theo tháng ở bậc/cấp độ thích hợp trong tổ chức. Cần sử dụng hướng dẫn sau.

1 Gây ra chi phí/tổn thất tài chính là x_1 hoặc thấp hơn

2 Gây ra chi phí/tổn thất tài chính trong khoảng $x_1 + 1$ và x_2

3 Gây ra phí/tổn thất tài chính trong khoảng $x_2 + 1$ và x_3

4 Gây ra chi phí/tổn thất tài chính trong khoảng $x_3 + 1$ và x_4

5 Gây ra chi phí/tổn thất tài chính trong khoảng $x_4 + 1$ và x_5

6 Gây ra chi phí/tổn thất tài chính trong khoảng $x_5 + 1$ và x_6

7 Gây ra chi phí/tổn thất tài chính trong khoảng $x_6 + 1$ và x_7

8 Gây ra chi phí/tổn thất tài chính trong khoảng $x_7 + 1$ và x_8

9 Gây ra chi phí/tổn thất tài chính lớn hơn x_8

10 Tổ chức sẽ ngừng hoạt động

Với, x_i (i = 1, 2, ..., 8) là chi phí/tổn thất tài chính theo tám bậc/cấp độ được tổ chức xác định theo bối cảnh của mình.

C.3.2.3 Lợi ích thương mại và kinh tế

Thông tin thương mại và kinh tế cần được bảo vệ và được định giá khi xem xét giá trị của chúng đối với các đối thủ cạnh tranh hoặc tác động có thể của chúng lên các lợi ích thương mại. Cần sử dụng hướng dẫn sau.

1 có lợi với đối thủ cạnh tranh nhưng không có giá trị về thương mại

2 có lợi với đối thủ cạnh tranh với giá trị y_1 hoặc thấp hơn (doanh thu)

3 có giá trị với đối thủ cạnh tranh theo giá trị trong khoảng y_1+1 và y_2 (doanh thu), hoặc gây ra tổn thất tài chính hoặc mất tiềm năng thu lợi nhuận, hoặc hỗ trợ tăng lợi thế hoặc có lợi cho các cá nhân hoặc tổ chức, hoặc cấu thành sự vi phạm các cam kết phù hợp để duy trì sự tin cậy đối với thông tin được cung cấp bởi bên thứ ba

4 có giá trị với đối thủ cạnh tranh theo giá trị trong khoảng y_2 +1 và y_3 (doanh thu)

5 có giá trị với đối thủ cạnh tranh giá giá trị trong khoảng y_3 +1 và y_4 (doanh thu)

6 có giá trị với đối thủ cạnh tranh theo giá trị lớn hơn y_4+1 (doanh thu)

7 Không có thông tin[1].

8 Không có thông tin

9 về căn bản có thể làm suy giảm các lợi ích thương mại hoặc về căn bản làm suy giảm khả năng tài chính của tổ chức

10 Không có thông tin

với, y_i (i = 1, 2, ..., 4) là các giá trị đối với đối thủ cạnh tranh trên phương diện doanh thu theo bốn bậc/cấp độ đã được tổ chức xác định theo bối cảnh của mình.

C.3.2.4 Thông tin cá nhân

Trong trường hợp thông tin về cá nhân được giữ và xử lý thì nếu đúng về mặt đạo đức và đạo lý, và đôi khi cũng được yêu cầu bởi luật thì các thông tin đó cũng được bảo vệ để không bị tiết lộ trái phép mà nhẹ nhất cũng có thể dẫn đến sự lúng túng và tệ nhất là dẫn đến hành động pháp lý bất lợi, ví dụ luật bảo vệ dữ liệu. Hơn nữa, thông tin về cá nhân được yêu cầu phải luôn chính xác, vì sự sửa đổi trái phép làm thông tin sai lệch có thể có các tác động tương tự như trường hợp tiết lộ trái phép. Một điều quan trọng nữa là thông tin về các cá nhân không được bị giấu đi hoặc bị hủy hoại vì điều đó có thể

[1] Thuật ngữ "Không có thông tin"nghĩa là không có thông tin tương đương về mức tác động này.

dẫn đến những quyết định không chính xác hoặc không có hành động trong thời gian cần thiết với các tác động tương tự như trường hợp tiết lộ hoặc sửa đổi trái phép. Cần sử dụng hướng dẫn sau.

1 Sự hơi lo lắng (băn khoăn) cho một cá nhân (tức giận, thất vọng, chán nản) nhưng không xảy ra vi phạm các yêu cầu pháp lý hoặc quy định

2 Sự lo lắng (băn khoăn) cho một cá nhân (tức giận, thất vọng, chán nản) nhưng không xảy ra vi phạm các yêu cầu pháp lý hoặc quy định

3 Sự vi phạm yêu cầu của quy định, pháp lý hay đạo đức hoặc sự chủ ý công khai về việc bảo vệ thông tin, dẫn đến sự hơi lúng túng cho một cá nhân

4 Sự vi phạm yêu cầu của quy định, pháp lý hay đạo đức hoặc sự chủ ý công khai về việc bảo vệ thông tin, dẫn đến sự lúng túng lớn cho cá nhân hay một chút lúng túng cho một nhóm người

5 Sự vi phạm yêu cầu của quy định, pháp lý hay đạo đức hoặc sự chủ ý công khai về việc bảo vệ thông tin, dẫn đến sự lúng túng nghiêm trọng cho một cá nhân

6 Sự vi phạm yêu cầu của quy định, pháp lý hay đạo đức hoặc sự chủ ý công khai về việc bảo vệ thông tin, dẫn đến sự lúng túng nghiêm trọng của một nhóm người

7 Không có thông tin

8 Không có thông tin

9 Không có thông tin

10 Không có thông tin

C.3.2.5 Trách nhiệm về pháp lý và quy định

Tổ chức nắm giữ và xử lý dữ liệu có thể bị bắt buộc phải tuân thủ các nghĩa vụ pháp lý và quy định. Sự không tuân thủ các nghĩa vụ đó, dù vô tình hay cố ý, đều có thể dẫn đến các hành động pháp lý hoặc hành chính đối với các cá nhân trong tổ chức có liên quan. Các hành động này có thể dẫn đến các bản án phạt và/hoặc bị bỏ tù. Cần sử dụng hướng dẫn sau.

1 Không có thông tin

2 Không có thông tin

3 Thông báo thi hành luật, án dân sự hoặc tội hình sự gây các thiệt hại/mức phạt tài chính là z_1 hoặc thấp hơn

4 Thông báo thi hành luật, án dân sự hoặc tội hình sự gây các thiệt hại/mức phạt tài chính trong khoảng $z_1 + 1$ và z_2

5 Thông báo thi hành luật, án dân sự hoặc tội hình sự gây các thiệt hại/mức phạt tài chính trong khoảng $z_2 + 1$ và z_3 hoặc phạt tù đến hai năm

6 Thông báo thi hành luật, án dân sự hoặc tội hình sự gây các thiệt hại/mức phạt tài chính trong khoảng $z_3 + 1$ và z_4, hoặc phạt tù từ hai năm đến mười năm

7 Thông báo thi hành luật, án dân sự hoặc tội hình sự gây các thiệt hại/mức phạt tài chính không giới hạn, hoặc phạt tù trên mười năm

8 Không có thông tin

9 Không có thông tin

10 Không có thông tin

C.3.2.6 Quản lý và các hoạt động nghiệp vụ

Các thông tin có thể ở dạng mà sự tổn hại thông tin sẽ ảnh hưởng tới sự thi hành hiệu lực của một tổ chức. Ví dụ, thông tin liên quan đến sự thay đổi một chính sách có thể kích động sự phản ứng rộng rãi nếu chúng bị tiết lộ, đến mức tổ chức có thể không thực hiện được chính sách này. Sự sửa đổi, bác bỏ hoặc không sẵn sàng của thông tin liên quan đến các khía cạnh tài chính, hoặc các phần mềm máy tính cũng có thể còn gây hậu quả nghiêm trọng đến sự vận hành của một tổ chức. Hơn nữa, việc bác bỏ các cam kết có thể có những hậu quả nghiệp vụ bất lợi. Cần sử dụng hướng dẫn sau.

1 Sự vận hành không hiệu quả trong một bộ phận của tổ chức

2 Không có thông tin

3 Làm suy yếu sự quản lý đúng của các tổ chức và sự vận hành của của tổ chức

4 Không có thông tin

5 Cản trở sự mở rộng hoặc vận hành hiệu lực của các chính sách của tổ chức

6 Gây bất lợi đến tổ chức trong các cuộc đàm phán thương mại hoặc chính sách với bên khác

7 Cản trở nghiêm trọng sự mở rộng hoặc vận hành của các chính sách chính về tổ chức, hoặc phá vỡ hoặc làm gián đoạn căn bản đến các vận hành quan trọng

8 Không có thông tin

9 Không có thông tin

10 Không có thông tin

C.3.2.7 Mất tín nhiệm

Việc tiết lộ hoặc sửa đổi trái phép, việc bác bỏ, hoặc sự không sẵn sàng thực sự của thông tin có thể dẫn đến sự mất tín nhiệm đối với một tổ chức, kết quả là gây thiệt hại cho danh tiếng của tổ chức, làm mất uy tín và gây các hậu quả xấu khác. Cần sử dụng các hướng dẫn sau.

1 Không có thông tin

2 Gây ra lúng túng nội bộ trong tổ chức

3 Ảnh hưởng xấu đến mối quan hệ với các cổ đông, khách hàng, nhà cung cấp, nhân viên, người dùng bên thứ ba, cơ quan hành pháp, chính phủ, các tổ chức khác hoặc cộng đồng, dẫn đến sự công khai các bất lợi trong phạm vi nội bộ/khu vực

4 Không có thông tin

5 Ảnh hưởng xấu đến mối quan hệ với các cổ đông, khách hàng, nhà cung cấp, nhân viên, người dùng bên thứ ba, cơ quan hành pháp, chính phủ, các tổ chức khác hoặc cộng đồng, dẫn đến một số công khai bất lợi trên phạm vi quốc gia

6 Không có thông tin

7 Ảnh hưởng chủ yếu đến mối quan hệ với các cổ đông, khách hàng, nhà cung cấp, nhân viên, người dùng bên thứ ba, cơ quan hành pháp, chính phủ, các tổ chức khác hoặc cộng đồng, dẫn đến sự công khai bất lợi rộng rãi

8 Không có thông tin

9 Không có thông tin

10 Không có thông tin

Phụ lục D

(tham khảo)

Ví dụ về báo cáo và mẫu báo cáo sự kiện, sự cố và điểm yếu an toàn thông tin

D.1 Giới thiệu

Phụ lục này gồm các mục ví dụ cần được lập hồ sơ của các sự kiện, sự cố và điểm yếu an toàn thông tin và các mẫu ví dụ để báo cáo các sự kiện, sự cố và điểm yếu an toàn thông tin, kèm các phần chú thích liên quan. Cần lưu ý đây chỉ là những ví dụ tham khảo. Ngoài ra còn có những mẫu khác, chẳng hạn mẫu Giản đồ trong tiêu chuẩn Định dạng mô tả và trao đổi đối tượng sự cố (IODEF).

D.2 Các mục ví dụ của hồ sơ

D.2.1 Các mục ví dụ của hồ sơ sự kiện an toàn thông tin

Hồ sơ sự kiện an toàn thông tin gồm các thông tin cơ bản về sự kiện an toàn thông tin, như khi nào, cái gì, như thế nào và vì sao sự kiện xảy ra, cũng như các thông tin liên lạc của người báo cáo.

Thông tin cơ bản

- Ngày xảy ra sự kiện
- Số sự kiện
- Số sự cố và/hoặc sự kiện liên quan (nếu có)

Thông tin chi tiết về người báo cáo

- Họ và tên
- Thông tin liên lạc như địa chỉ, tổ chức, bộ phận, điện thoại và thư điện tử

Mô tả sự kiện

- Cái gì đã xảy ra
- Xảy ra như thế nào
- Tại sao xảy ra
- Khái quát sơ bộ về thiết bị/tài sản bị ảnh hưởng
- Các tác động nghiệp vụ bất lợi
- Các điểm yếu được xác định

Thông tin chi tiết về sự kiện

- Ngày và thời điểm xảy ra sự kiện

Ngày và thời điểm phát hiện sự kiện

Ngày và thời thời điểm báo cáo sự kiện

D.2.2 Các mục ví dụ của hồ sơ sự cố an toàn thông tin

Hồ sơ sự cố an toàn thông tin gồm các thông tin cơ bản về sự cố an toàn thông tin, như khi nào, cái gì, như thế nào và vì sao sự cố xảy ra, cũng như loại sự cố, tác động, và kết quả của việc ứng phó với sự cố.

Thông tin cơ bản

Ngày tháng xảy ra sự cố

Số sự cố

Số sự kiện/sự cố liên quan (nếu có)

Thông tin chi tiết về người báo cáo

Họ và tên

Thông tin liên lạc như địa chỉ, tổ chức, bộ phận, điện thoại và thư điện tử

Thông tin chi tiết về đầu mối liên lạc (PoC)

Họ và tên

Thông tin liên lạc như địa chỉ, tổ chức, bộ phận, điện thoại và thư điện tử

Thông tin chi tiết về thành viên ISIRT

Họ và tên

Thông tin liên lạc như địa chỉ, tổ chức, bộ phận, điện thoại và thư điện tử

Mô tả sự cố

Cái gì đã xảy ra

Xảy ra như thế nào

Tại sao xảy ra

Khái quát sơ bộ về thiết bị/tài sản bị ảnh hưởng

Các tác động nghiệp vụ bất lợi

Các điểm yếu được xác định

Thông tin chi tiết về sự cố

Ngày và thời điểm xảy ra sự cố

Ngày và thời điểm phát hiện sự cố

Ngày và thời thời điểm báo cáo sự cố

Loại sự cố

Thiết bị/tài sản bị ảnh hưởng

Tác động/ảnh hưởng nghiệp vụ bất lợi của sự cố

Tổng chi phí khôi phục sau sự cố

Cách giải quyết sự cố

Người/thủ phạm có liên quan (nếu sự cố do con người gây ra)

Mô tả về thủ phạm

Động cơ thực tế hoặc theo cảm nhận

Các hành động được thực hiện để giải quyết sự cố

Các hành động được lập kế hoạch để giải quyết sự cố

Các hành động còn tồn tại

Kết luận

Những người/đơn vị trong nội bộ được thông báo

Những người/đơn vị bên ngoài được thông báo

D.2.3 Các mục ví dụ của hồ sơ điểm yếu an toàn thông tin

Hồ sơ điểm yếu an toàn thông tin gồm các thông tin cơ bản về điểm yếu an toàn thông tin, như khi nào, cái gì, cách xác định điểm yếu, các tác động tiềm ẩn và cách giải quyết.

Thông tin cơ bản

Ngày xác định điểm yếu

Số điểm yếu

Thông tin chi tiết về người báo cáo

Họ và tên

Thông tin liên lạc như địa chỉ, tổ chức, bộ phận, điện thoại và thư điện tử

Mô tả điểm yếu

Cách giải quyết điểm yếu

D.3 Cách sử dụng các mẫu báo cáo

D.3.1 Định dạng ngày tháng và thời điểm

Ngày tháng cần được ghi theo định dạng ngày–tháng–năm (và nếu được yêu cầu thì cả là giây-phút-giờ). Nếu có thể thì cần dùng UTC (Giờ Quốc tế Phối hợp - Coordinated Universal Time) để so sánh

khi nhiều sự kiện có thể xảy ra trong các khoảng thời gian (và tối thiểu thì số bù UTC được áp dụng cho mục thời điểm).

D.3.2 Chú thích

Mục đích của mẫu báo cáo sự kiện và sự cố an toàn thông tin là cung cấp thông tin về sự kiện an toàn thông tin, và nếu chúng được xác định là sự cố an toàn thông tin thì về cả sự cố an toàn thông tin, đến những người liên quan.

Nếu nghi ngờ rằng một sự kiện an toàn thông tin đang xảy ra hoặc có thể đã xảy ra – cụ thể là một điều gì đó có thể gây tổn thất hoặc thiệt hại đáng kể về tài sản hoặc danh tiếng của tổ chức thì lập tức cần hoàn tất và nộp mẫu báo cáo sự kiện an toàn thông tin (xem phần đầu của Phụ lục này) theo các thủ tục được mô tả trong lược đồ quản lý sự cố an toàn thông tin của tổ chức.

Thông tin cung cấp sẽ được sử dụng để thực hiện đánh giá sơ bộ để xác định xem liệu sự kiện này có được xếp loại là sự cố an toàn thông tin hay không, và nếu đúng thì cả các biện pháp khắc phục cần thiết để ngăn chặn hoặc hạn chế tổn thất hoặc thiệt hại. *Do tính chất quan trọng tiềm ẩn về thời gian của quy trình này nên không cần phải hoàn thành tất cả các mục trong biểu mẫu báo cáo tại thời điểm này.*

Nếu là một thành viên PoC thực hiện xem xét các mẫu đã hoàn thành/hoàn thành một phần thì sau đó bạn sẽ được yêu cầu phải quyết định xem liệu sự kiện đó có cần được xếp loại là sự cố an toàn thông tin không. Nếu sự kiện được xếp loại như vậy thì bạn cần hoàn thành mẫu sự cố an toàn thông tin với nhiều thông tin nhất trong khả năng của bạn và chuyển cả hai mẫu sự kiện và sự cố an toàn thông tin cho ISIRT. Cho dù sự kiện an toàn thông tin có được xếp loại là sự cố hay không thì dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin cũng cần được cập nhật.

Nếu là một thành viên ISIRT thực hiện xem xét các mẫu sự kiện và sự cố an toàn thông tin được thành viên PoC chuyển đến thì sau đó mẫu sự cố cần được cập nhật theo tiến trình điều tra và các thông tin cập nhật được đưa vào cơ sở dữ liệu sự kiện/sự cố/điểm yếu an toàn thông tin.

Mục đích của mẫu báo cáo điểm yếu an toàn thông tin là cung cấp thông tin về điểm yếu được ghi nhận, và có vai trò như kho lưu trữ thông tin về cách giải quyết các điểm yếu được báo cáo.

Hãy tuân theo các hướng dẫn khi hoàn thiện các mẫu báo cáo:

- Mẫu báo cáo cần được đề nghị phải hoàn thành và trình theo đường điện tử[2]. (Khi có vấn đề xảy ra, hoặc được cho là đã xảy ra, với các cơ chế báo cáo điện tử (ví dụ như thư điện tử), kể cả khi cho rằng có thể hệ thống đang bị tấn công và các mẫu báo cáo điện tử có thể đã được đọc bởi những cá nhân không được phép, thì cần sử dụng các hình thức báo cáo thay thế khác. Các hình thức thay thế có thể là con người, hay qua điện thoại hoặc tin nhắn văn bản.)

[2] Ví dụ, trong mẫu báo cáo ở web page an toàn có liên kết với cơ sở dữ liệu điện tử về sự kiện/sự cố/điểm yếu an toàn thông tin. Hiện nay, việc vận hành một lược đồ trên giấy có thể sẽ mất nhiều thời gian. Tuy nhiên, lược đồ trên giấy cũng cần được chuẩn bị cho trường hợp không thể sử dụng lược đồ điện tử.

- Chỉ cung cấp thông tin mà bạn biết là có - không suy đoán để hoàn thành các nội dung trong mẫu. Nếu cần phải cung cấp các thông tin mà bạn không thể xác nhận thì hãy ghi rõ rằng các thông tin này chưa được xác nhận, và những điều khiến bạn tin rằng đó có thể là sự thật.
- Cần cung cấp thông tin liên lạc đầy đủ của bạn. Vì có thể cần phải liên lạc với bạn - trong trường hợp khẩn cấp hoặc vào những thời điểm sau đó - để có thêm thông tin liên quan đến báo cáo của bạn.

Nếu sau này bạn phát hiện ra bất kỳ thông tin nào mà bạn cung cấp là không chính xác, không đầy đủ hoặc sai lệch, thì cần sửa và nộp lại mẫu báo cáo.

D.4 Mẫu báo cáo ví dụ

D.4.1 Mẫu ví dụ về báo cáo sự kiện an toàn thông tin

BÁO CÁO SỰ KIỆN AN TOÀN THÔNG TIN

1. Ngày xảy ra sự kiện **Trang 1/1**

2. Số sự kiện[3] **3. (Nếu có) Số sự kiện và/hoặc sự cố liên quan**

4. THÔNG TIN CHI TIẾT VỀ NGƯỜI BÁO CÁO

4.1 Họ và tên ..... **4.2 Địa chỉ** .....

4.3 Tổ chức ..... **4.4 Đơn vị** .....

4.5 Điện thoại ..... **4.6 E-mail** .....

5. MÔ TẢ SỰ KIỆN AN TOÀN THÔNG TIN

5.1 Mô tả sự kiện

- Cái gì đã xảy ra
- Xảy ra như thế nào
- Tại sao xảy ra
- Khái quát sơ bộ về thiết bị/tài sản bị ảnh hưởng
- Các tác động nghiệp vụ bất lợi
- Các điểm yếu được xác định

6. THÔNG TIN CHI TIẾT VỀ SỰ KIỆN AN TOÀN THÔNG TIN

6.1 Ngày và thời điểm xảy ra sự kiện

6.2 Ngày và thời điểm phát hiện sự kiện

6.3 Ngày và thời điểm báo cáo sự kiện

6.4 Đã chấm dứt ứng phó với sự kiện chưa? **RỒI** ☐ **CHƯA** ☐
(Tích vào ô tương ứng)

6.5 Nếu trả lời RỒI, xác định khoảng thời gian sự kiện diễn ra theo Ngày/giờ/phút

[3] Số sự kiện nên để người quản lý ISIRT của tổ chức điền

D.4.2 Mẫu ví dụ về báo cáo sự cố an toàn thông tin

BÁO CÁO SỰ CỐ AN TOÀN THÔNG TIN

1. Ngày xảy ra sự cố **Trang 1/6**

2. Số sự cố[4] **3. (Nếu có) Số sự kiện và/hoặc sự cố liên quan**

4. THÔNG TIN CHI TIẾT VỀ THÀNH VIÊN POC

4.1 Họ và tên ..... **4.2 Địa chỉ** .....

4.3 Tổ chức ..... **4.4 Đơn vị** .....

4.5 Điện thoại ..... **4.6 E-mail** .....

5. THÔNG TIN CHI TIẾT VỀ THÀNH VIÊN ISIRT

5.1 Họ và tên ..... **5.2 Địa chỉ** .....

5.3 Tổ chức ..... **5.4 Đơn vị** .....

5.5 Điện thoại ..... **5.6 E-mail** .....

6. MÔ TẢ SỰ CỐ AN TOÀN THÔNG TIN

6.1 Mô tả sự cố

- Cái gì đã xảy ra
- Xảy ra như thế nào
- Tại sao xảy ra
- Khái quát sơ bộ về thiết bị/tài sản bị ảnh hưởng
- Các tác động nghiệp vụ bất lợi
- Các điểm yếu được xác định

7. THÔNG TIN CHI TIẾT VỀ SỰ CỐ AN TOÀN THÔNG TIN

7.1 Ngày và thời điểm xảy ra sự cố

7.2 Ngày và thời điểm phát hiện sự cố

7.3 Ngày và thời điểm báo cáo sự cố

7.4 Thông tin chi tiết về nhận dạng/liên hệ của người báo cáo

7.5 Sự cố đã kết thúc chưa? **RỒI** ☐ **CHƯA** ☐
(Tích vào ô tương ứng)

7.6 Nếu trả lời RỒI, xác định khoảng thời gian sự cố diễn ra theo Ngày/giờ/phút

---

[4] Số sự cố nên để người quản lý ISIRT của tổ chức điền, và có liên kết với số sự kiện liên quan

BÁO CÁO SỰ CỐ AN TOÀN THÔNG TIN

8. LOẠI SỰ CỐ AN TOÀN THÔNG TIN

(Lựa chọn một, sau đó hoàn thành các phần dưới đây) **8.1 Đã xảy ra** (sự cố đã xảy ra) ☐ **8.2 Nghi ngờ** (Sự cố có thể đã xảy ra nhưng chưa được xác nhận) ☐

(chọn một) **8.3 Thảm họa tự nhiên** ☐ (Cho biết loại đe dọa liên quan)

Động đất ☐ **Núi lửa** ☐ **Lũ lụt** ☐ **Lốc xoáy** ☐
Sét ☐ **Sóng thần** ☐ **Sụt lún** ☐ **Loại khác** ☐

Ghi rõ:

(chọn một) **8.4 Bất ổn xã hội** ☐ (Cho biết loại đe dọa liên quan)

Bedin ☐ **Khủng bố** ☐ **Chiến tranh** ☐ **Loại khác** ☐

Ghi rõ:

(chọn một) **8.5 Thiệt hại vật chất** ☐ (Cho biết loại đe dọa liên quan)

Hỏa hoạn ☐ **Nước** ☐ **Tĩnh điện** ☐
Môi trường độc hại (như ô nhiễm, bụi, ăn mòn, đóng băng) ☐
Phá hoại thiết bị ☐ **Phá hoại phương tiện lưu trữ** ☐ **Trộm cắp thiết bị** ☐
Trộm cắp phương tiện lưu trữ ☐ **Mất mát thiết bị** ☐ **Mất mát phương tiện lưu trữ** ☐
Giả mạo thiết bị ☐ **Giả mạo phương tiện lưu trữ** ☐ **Loại khác** ☐

Ghi rõ:

(chọn một) **8.6 Lỗi hạ tầng** ☐ (Cho biết loại đe dọa liên quan)

Lỗi nguồn điện ☐ **Lỗi mạng** ☐ **Lỗi điều hòa** ☐
Lỗi nguồn Nước ☐ **Loại khác** ☐

Ghi rõ:

(chọn một) **8.7 Nhiễu phát xạ** ☐ (Cho biết loại đe dọa liên quan)

Phát xạ điện từ ☐ **Xung điện từ** ☐ **Nhiễu điện từ** ☐
Thăng giáng điện áp ☐ **Phát xạ nhiệt** ☐ **Loại khác** ☐

Ghi rõ:

(chọn một) **8.8 Lỗi kỹ thuật** ☐ (Cho biết loại đe dọa liên quan)

Lỗi phần cứng ☐ **Sự cố phần mềm** ☐ **Quá tải (năng lực của hệ thống bị bão hòa)** ☐
Sai phạm bảo trì ☐ **Loại khác** ☐

Ghi rõ:

BÁO CÁO SỰ CỐ AN TOÀN THÔNG TIN

(chọn một) **8.9 Phần mềm độc hại** ☐ (Cho biết loại đe dọa liên quan)

Sâu mạng ☐ **Ngựa Trojan** ☐ **Botnet** ☐ **Tấn công kết hợp** ☐

Web page nhúng mã độc ☐ **Trang chứa mã độc** ☐ **Loại khác** ☐

Ghi rõ:

(chọn một) **8.10 Tấn công kỹ thuật** ☐ (Cho biết loại đe dọa liên quan)

Quét mạng ☐ **Khai thác điểm yếu** ☐ **Khai thác cửa sau** ☐

Cố đăng nhập, can thiệp ☐ **Từ chối dịch vụ** ☐ **Loại khác** ☐

Ghi rõ:

(chọn một) **8.11 Vi phạm luật** ☐ (Cho biết loại đe dọa liên quan)

Sử dụng trái phép nguồn lực ☐ **Vi phạm bản quyền** ☐ **Loại khác** ☐

Ghi rõ:

(chọn một) **8.12 Vi phạm về chức năng** ☐ (Cho biết loại đe dọa liên quan)

Lạm dụng quyền ☐ **Giả mạo quyền, từ chối hoạt động** ☐ **Vận hành sai** ☐

Vi phạm sử dụng nhân lực ☐ **Loại khác** ☐

Ghi rõ:

(chọn một) **8.13 Tổn hại thông tin** ☐ (Cho biết loại đe dọa liên quan)

Ngăn chặn ☐ **Theo dõi, nghe lén** ☐ **Tiết lộ thông tin** ☐ **Lừa đảo** ☐

Lừa đảo trực tuyến ☐ **Trộm cắp dữ liệu** ☐ **Tổn thất dữ liệu** ☐ **Giả mạo dữ liệu** ☐

Phân tích luồng dữ liệu ☐ **Dò vị trí** ☐ **Loại khác** ☐

Ghi rõ:

(chọn một) **8.14 Nội dung xấu** ☐ ((Cho biết loại đe dọa liên quan)

Nội dung bất hợp pháp ☐ **Nội dung gây hoang mang** ☐ **Nội dung độc hại** ☐

Nội dung lạm dụng ☐ **Loại khác** ☐

Ghi rõ:

8.15 Loại khác ☐ (Nếu không thuộc các loại trên thì lựa chọn mục này)

Ghi rõ:

HỒ SƠ SỰ CỐ AN TOÀN THÔNG TIN

9. THIẾT BỊ/TÀI SẢN BỊ ẢNH HƯỞNG[5]

Thiết bị/tài sản bị ảnh hưởng *(Nếu có)* *(Cung cấp mô tả về thiết bị/tài sản bị ảnh hưởng do/hoặc liên quan đến sự cố, bao gồm số sê ri, giấy phép và số phiên bản nếu có))*

9.1 Thông tin/dữ liệu .....

9.2 Phần cứng .....

9.3 Phần mềm .....

9.4 Phương tiện truyền thông .....

9.5 Tài liệu .....

9.6 Quy trình .....

9.7 Loại khác .....

10. TÁC ĐỘNG/ẢNH HƯỞNG NGHIỆP VỤ BẤT LỢI CỦA SỰ CỐ

Chọn loại phù hợp, cột "giá trị" ghi mức tác động nghiệp vụ bất lợi, bao gồm tất cả các bên bị ảnh hưởng bởi sự cố, theo thang điểm từ 1 đến 10 sử dụng các hướng dẫn đối với các loại: tổn thất tài chính/Gián đoạn hoạt động nghiệp vụ, lợi ích kinh tế thương mại, thông tin cá nhân, nghĩa vụ pháp lý và quy định, hoạt động quản lý và nghiệp vụ, và tổn thất uy tín thương mại. (Xem Phụ lục C.3.2). Ghi các ký tự mã theo như hướng dẫn vào cột "Hướng dẫn", và nếu có chi phí thực tế, ghi lại chi phí vào cột "chi phí".

		GIÁ TRỊ	HƯỚNG DẪN	CHI PHÍ
10.1 Vi phạm tính bí mật *(Ví dụ: tiết lộ trái phép)*	☐			
10.2 Vi phạm tính toàn vẹn *(Ví dụ: sửa đổi trái phép)*	☐			
10.3 Vi phạm tính sẵn sàng *(Ví dụ: không sẵn sàng)*	☐			
10.4 Vi phạm tính chống từ chối	☐			
10.1 Phá hoại	☐			

11. TỔNG CHI PHÍ KHÔI PHỤC SAU SỰ CỐ

(Nếu có thể, cần khai báo tổng chi phí thực tế để khôi phục hoàn toàn sau sự cố, cột "giá trị" sử dụng thang điểm từ 1 đến 10 và cột "chi phí" là chi phí thực tế.)	GIÁ TRỊ	HƯỚNG DẪN	CHI PHÍ

[5] Báo cáo này cho thông tin chi tiết hơn về các thiết bị/tài sản bị ảnh hưởng để sẵn sàng cho việc điều tra và phân tích (trong các giai đoạn đầu khi phân tích sự kiện và sự cố, thông thường chỉ có các thông tin 'mức cao' được thu thập).

BÁO CÁO SỰ CỐ AN TOÀN THÔNG TIN

12. GIẢI QUYẾT SỰ CỐ

12.1 Ngày bắt đầu điều tra sự cố

12.2 Tên người điều tra

12.3 Ngày kết thúc sự cố

12.4 Ngày kết thúc tác động của sự cố

12.5 Ngày hoàn thành điều tra sự cố

12.6 Địa điểm và vấn đề điều tra

13. NGƯỜI/THỦ PHẠM LIÊN QUAN (NẾU SỰ CỐ DO CON NGƯỜI GÂY RA)

(chọn một)

Người ☐ **Tổ chức/Đơn vị được thành lập hợp pháp** ☐

Nhóm người có tổ chức ☐ **Vô tình** ☐

Không có thủ phạm ☐

Ví dụ: do yếu tố tự nhiên, lỗi thiết bị, lỗi của con người

14. MÔ TẢ THỦ PHẠM

15. ĐỘNG CƠ THỰC TẾ HOẶC THEO CẢM NHẬN

(chọn một)

Tội phạm/kiếm lợi nhuận ☐ **Chính trị/khủng bố** ☐

Tiêu khiển/xâm nhập ☐ **Trả thù** ☐

Loại khác ☐

Ghi rõ:

16. CÁC HÀNH ĐỘNG ĐÃ ĐƯỢC THỰC HIỆN ĐỂ GIẢI QUYẾT SỰ CỐ

(ví dụ như "không hành động", "hành động tại chỗ", "điều tra nội bộ", điều tra "bên ngoài" bởi...)

17. CÁC HÀNH ĐỘNG ĐƯỢC LẬP KẾ HOẠCH ĐỂ GIẢI QUYẾT SỰ CỐ

(xem các ví dụ bên trên)

18. CÁC HÀNH ĐỘNG CÒN TỒN TẠI

(ví dụ: vẫn đang điều tra theo yêu cầu của những người khác)

BÁO CÁO SỰ CỐ AN TOÀN THÔNG TIN

19. KẾT LUẬN

(Xác định sự cố là lớn hay nhỏ, và đưa ra mô tả ngắn gọn để minh họa kết luận)

Lớn ☐ **Nhỏ** ☐

(đưa ra kết luận khác)

.....

20. CÁC CÁ NHÂN/ĐƠN VỊ NỘI BỘ ĐƯỢC THÔNG BÁO

(Mục này dành cho người có trách nhiệm về an toàn thông tin, nêu rõ hành động cần thiết. Phần này có thể được hiệu chỉnh bởi người quản lý an toàn thông tin của tổ chức hoặc các cá nhân có trách nhiệm khác)

Người quản lý an toàn thông tin/cá nhân có trách nhiệm ☐

Người quản lý đơn vị ☐
(nói rõ đơn vị)

Người lập báo cáo ☐

Người quản lý ISIRT ☐

Người quản lý hệ thống thông tin ☐

Người quản lý của người lập báo cáo/Người quản lý đơn vị bị ảnh hưởng ☐

Khác ☐
(ví dụ: bộ phận hỗ trợ, bộ phận tổ chức cán bộ, ban quản lý, kiểm tra nội bộ)

Ghi rõ:

21. CÁC CÁ NHÂN/ĐƠN VỊ BÊN NGOÀI ĐƯỢC THÔNG BÁO

(Mục này dành cho người có trách nhiệm về an toàn thông tin, nêu rõ hành động cần thiết. Phần này có thể được hiệu chỉnh bởi người quản lý an toàn thông tin của tổ chức hoặc các cá nhân có trách nhiệm khác)

Cảnh sát ☐

Khác ☐
(ví dụ: cơ quan chức năng, ISIRT bên ngoài)

Ghi rõ:

21. CHỮ KÝ

NGƯỜI LẬP BÁO CÁO	NGƯỜI XEM	NGƯỜI XEM
Chữ ký số	**Chữ ký số**	**Chữ ký số**
.....	.....	.....
Tên	**Tên**	**Tên** .....
Chức vụ	**Chức vụ**	**Chức vụ** .....
Ngày	**Ngày**	**Ngày** .....

D.4.3 Mẫu ví dụ của hồ sơ điểm yếu an toàn thông tin

BÁO CÁO ĐIỂM YẾU AN TOÀN THÔNG TIN

1. Ngày phát hiện điểm yếu Trang 1/1

2. Số điểm yếu[6]

3. THÔNG TIN CHI TIẾT CỦA NGƯỜI BÁO CÁO

3.1 Họ tên	.....	**3.2 Địa chỉ**	.....
3.3 Tổ chức	.....	**3.4 Đơn vị**	.....
3.5 Điện thoại	.....	**3.6 E-mail**	.....

4. MÔ TẢ ĐIỂM YẾU AN TOÀN THÔNG TIN

4.1 Ngày và thời điểm báo cáo điểm yếu

4.2 Mô tả tường thuật về điểm yếu an toàn thông tin

- Điểm yếu được phát hiện như thế nào
- Tính chất của điểm yếu - vật lý, kỹ thuật, ...
- Nếu là điểm yếu kỹ thuật, các tài sản/thiết bị mạng/công nghệ thông tin có liên quan
- Thiết bị/tài sản có thể bị ảnh hưởng nếu điểm yếu bị khai thác
- Các tác động nghiệp vụ bất lợi tiềm ẩn nếu điểm yếu bị khai thác

5. GIẢI QUYẾT ĐIỂM YẾU ANTOÀN THÔNG TIN

5.1 Điểm yếu được xác nhận chưa? *(Lựa chọn ô tương ứng)* **Rồi** ☐ **Chưa** ☐

5.2 Ngày và thời điểm xác nhận điểm yếu

5.3 Tên người xác nhận **5.4 Địa chỉ**

5.5 Tổ chức

5.6 Điện thoại **5.7 Thư điện tử**

5.8 Điểm yếu được giải quyết chưa? *(Lựa chọn ô tương ứng)* **Rồi** ☐ **Chưa** ☐

5.9 Mô tả ngắn gọn về cách giải quyết điểm yếu, thời gian và tên của người giải quyết

[6] Số của điểm yếu nên để người quản lý ISIRT của tổ chức điền

Phụ lục E

(tham khảo)

Các khía cạnh quy định và pháp lý

Các khía cạnh pháp lý và quy định sau của việc quản lý sự cố an toàn thông tin cần được đề cập trong chính sách quản lý sự cố an toàn thông tin và lược đồ liên quan:

- **Sự bảo vệ dữ liệu thỏa đáng và tính riêng tư của thông tin cá nhân được cung cấp**. Ở các quốc gia có quy định pháp luật cụ thể về tính bí mật và toàn vẹn của dữ liệu thì việc kiểm soát dữ liệu cá nhân thường bị hạn chế. Do các sự cố an toàn thông tin thường cần phải được quy cho một cá nhân cụ thể nên thông tin có chất cá nhân có thể cần phải được ghi lại và được quản lý sao cho phù hợp. Do vậy, mỗi phương pháp tiếp cận có cấu trúc để quản lý sự cố an toàn thông tin cũng cần quan tâm đến việc bảo vệ quyền riêng tư thích hợp. Vấn đề này có thể bao gồm:
  - nếu có thể thì những người có truy cập vào dữ liệu cá nhân không được có quen biết với (những) người đang bị điều tra,
  - các thỏa thuận bảo mật cần có chữ ký của những người có truy cập vào dữ liệu cá nhân trước khi họ được phép truy cập,
  - thông tin chỉ được sử dụng cho các mục đích rõ ràng theo cách chúng được thu nhận, cụ thể là dùng cho điều tra sự cố an toàn thông tin.
- **Việc lưu trữ hồ sơ theo cách phù hợp được duy trì.** Một số điều luật của các quốc gia có yêu cầu các công ty duy trì hồ sơ phù hợp về các hoạt động của họ để dùng cho việc soát xét trong quy trình đánh giá hàng năm của tổ chức. Các tổ chức chính phủ cũng có các yêu cầu tương tự. Ở một số nước, các tổ chức được yêu cầu phải báo cáo hoặc có tài liệu lưu trữ để dùng cho việc thi hành luật (ví dụ trong trường hợp có liên quan đến tội phạm nghiêm trọng hoặc có sự xâm nhập vào một hệ thống nhạy cảm của chính phủ).
- **Các biện pháp kiểm soát được thực thi để đảm bảo tuân thủ các nghĩa vụ thương mại theo hợp đồng.** Trong trường hợp có yêu cầu bắt buộc trong việc cung cấp dịch vụ quản lý sự cố an toàn thông tin, ví dụ các yêu cầu về thời gian ứng phó, thì tổ chức cần đảm bảo có được sự an toàn thông tin phù hợp nhằm đảm bảo vẫn đáp ứng mọi nghĩa vụ trong mọi tình huống. (Liên quan đến điều này, nếu một tổ chức ký hợp đồng hỗ trợ với một tổ chức bên ngoài, ví dụ ISIRT bên ngoài, thì cần đảm bảo rằng mọi yêu cầu, bao gồm cả thời gian ứng phó, đều được đưa vào bản hợp đồng với bên ngoài).
- **Các vấn đề pháp lý liên quan đến chính sách và thủ tục được giải quyết.** Các chính sách và thủ tục liên quan đến lược đồ quản lý sự cố an toàn thông tin cần được kiểm tra về các khía cạnh pháp lý và quy định tiềm ẩn, ví dụ xem có tuyên bố nào về hành động kỷ luật và/hoặc pháp lý đối với những người gây ra sự cố an toàn thông tin không. Ở một số quốc gia, việc chấm dứt sử dụng lao động là điều không dễ dàng.

- **Mọi sự phủ nhận đều được kiểm tra về mặt pháp lý**. Mọi phủ nhận liên quan đến các hành động do nhóm quản lý sự cố thông tin và những người hỗ trợ bên ngoài thực hiện đều cần được kiểm tra về phương diện pháp lý.
- **Hợp đồng với nhân viên hỗ trợ bên ngoài phải bao hàm mọi khía cạnh được yêu cầu.** Hợp đồng với nhân viên hỗ trợ bên ngoài, ví dụ với nhân viên từ ISIRT bên ngoài, cần được kiểm tra kỹ lưỡng về việc miễn trừ trách nhiệm pháp lý, bảo mật, sự sẵn sàng của dịch vụ, và hệ quả của việc tư vấn không đúng.
- **Các thỏa thuận bảo mật đều khả thi.** Các thành viên của nhóm quản lý sự cố an toàn thông tin có thể được yêu cầu ký các thỏa thuận bảo mật khi bắt đầu và khi chấm dứt hợp đồng. Ở một số quốc gia, việc ký thoả thuận bảo mật có thể không có hiệu lực về pháp lý; điều này cũng cần được kiểm tra.
- **Các yêu cầu về hành luật được đề cập**. Các vấn đề liên quan đến khả năng các cơ quan hành luật có thể yêu cầu thông tin từ lược đồ quản lý sự cố an toàn thông tin cần phải rõ ràng. Đó có thể là trường hợp cần làm rõ mức độ thông tin tối thiểu khi lập tài liệu sự cố và thời gian cần lưu giữ hồ sơ mà pháp luật yêu cầu.
- **Các khía cạnh trách nhiệm pháp lý đều rõ ràng.** Các vấn đề về trách nhiệm pháp lý tiềm ẩn và các biện pháp kiểm soát cần thiết liên quan phải được triển khai cũng cần được làm rõ. Dưới đây là ví dụ về các sự kiện có thể có các vấn đề về trách nhiệm pháp lý liên quan:
  - nếu một sự cố có thể đã ảnh hưởng đến một tổ chức khác (ví dụ, tiết lộ thông tin được chia sẻ), sự cố đó đã không được thông báo đúng lúc và tổ chức kia phải chịu tác động bất lợi,
  - nếu một điểm yếu mới trong một sản phẩm được phát hiện, nhà cung cấp không được thông báo và một sự cố lớn liên quan có tác động lớn đến một hoặc nhiều tổ chức khác đã xảy ra sau đó,
  - báo cáo không được lập ra ở những nơi, trong quốc gia cụ thể, mà các tổ chức được yêu cầu phải báo cáo hoặc xây dựng các tài liệu lưu trữ để dùng cho các cơ quan hành pháp sử dụng trong các trường hợp có thể dính líu đến tội ác nghiêm trọng, hoặc có sự xâm nhập vào một hệ thống nhạy cảm của chính phủ hoặc một bộ phận của cơ sở hạ tầng quốc gia quan trọng,
  - thông tin bị tiết lộ dường như cho thấy rằng một người hoặc một tổ chức nào đó có thể dính líu đến một cuộc tấn công. Điều này có thể gây tổn hại danh tiếng và công việc của cá nhân hoặc tổ chức liên quan,
  - thông tin được tiết lộ rằng có thể đã có trục trặc với một hạng mục nhất định nào đó của phần mềm và điều này được phát hiện là không phải sự thật.
- **Các yêu cầu trong quy định cụ thể được đề cập.** Nếu được yêu cầu bởi các yêu cầu trong quy định cụ thể thì các sự cố cần được báo cáo cho một cơ quan được chỉ định, ví dụ nhiều quốc gia

có yêu cầu điều này trong ngành công nghiệp năng lượng hạt nhân, các công ty viễn thông và các nhà cung cấp dịch vụ Internet.

- **Các thủ tục khởi tố hoặc kỷ luật nội bộ có thể thành công.** Các biện pháp kiểm soát an toàn thông tin phù hợp cần được triển khai, bao gồm các biện pháp truy vết chống giả mạo phù hợp, để có thể truy tố thành công hoặc áp dụng các thủ tục kỷ luật nội bộ đối với "kẻ tấn công", cho dù đó là tấn công kỹ thuật hoặc vật lý. Để hỗ trợ việc này thì thông thường các bằng chứng cần được thu thập theo cách thức sao cho chúng dễ dàng được chấp nhận tại các tòa án quốc gia phù hợp hoặc tại diễn đàn kỷ luật khác. Cần cho thấy rằng:
  - các hồ sơ là đầy đủ và không bị giả mạo với mọi hình thức,
  - các bản sao của chứng cứ điện tử giống hệt với bản gốc,
  - mọi hệ thống IT mà từ đó chứng cứ được tập hợp đều đã hoạt động đúng tại thời điểm chứng cứ được ghi nhận.
- **Các khía cạnh pháp lý liên quan đến các kỹ thuật giám sát được đề cập.** Các hệ quả của việc sử dụng các kỹ thuật giám sát cũng cần được đề cập theo yêu cầu của luật pháp quốc gia liên quan. Tính hợp pháp của các kỹ thuật khác nhau cũng khác giữa các quốc gia. Ví dụ, ở một số quốc gia thì điều cần làm là cho mọi người biết rằng việc giám sát các hoạt động, bao gồm cả việc giám sát thông qua các kỹ thuật theo dõi, đang được thực hiện. Các yếu tố cần được xem xét gồm ai/cái gì đang bị giám sát, họ/cái đó bị giám sát như thế nào, và khi nào việc giám sát đang được thực hiện. Cũng cần lưu ý rằng việc giám sát/theo dõi bằng IDS đã được thảo luận cụ thể trong tiêu chuẩn ISO/IEC 18043.
- **Chính sách sử dụng được chấp nhận được xác định và được thông báo.** Việc thực hành/sử dụng được chấp nhận trong tổ chức cần được xác định, lập tài liệu và thông báo cho mọi người dùng đã định. (Ví dụ, người dùng cần được thông báo về chính sách sử dụng được chấp nhận và được yêu cầu cung cấp xác nhận viết tay rằng họ đã hiểu và chấp nhận chính sách đó khi họ tham gia vào một tổ chức hoặc được cấp quyền truy cập vào hệ thống thông tin).

Thư mục tài liệu tham khảo

[1] ISO/IEC 18043, Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems

[2] ISO/IEC 20000 (all parts), Information technology - Service management

[3] ISO/PAS 22399, Societal security - Guidelines for incident preparedness and operational continuity management

[4] TCVN ISO/IEC 27001, Công nghệ thông tin – Hệ thống quản lý an toàn thông tin - Các yêu cầu

[5] TCVN ISO/IEC 27002, Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành quản lý an toàn thông tin

[6] ISO/IEC 27003, Information technology - Security techniques - Information security management system implementation guidance

[7] ISO/IEC 27004, Information technology - Security techniques - Information security management - Measurement

[8] ISO/IEC 27005, Information technology - Security techniques - Information security risk management

[9] ISO/IEC 27031, Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity

[10] ISO/IEC 27033-1, Information technology - Security techniques - Network security - Part 1: Overview and concepts

[11] ISO/IEC 27033-2, Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security

[12] ISO/IEC 27033-3, Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues

[13] Internet Engineering Task Force (IETF) Site Security Handbook, http://www.ietf.org/rfc/rfc2196.txt?number=2196

[14] Internet Engineering Task Force (IETF) RFC 2350, Expectations for Computer Security Incident Response, http://www.ietf.org/rfc/rfc2350.txt?number=2350

[15] NIST Special Publication 800-61, Computer Security Incident Handling Guide (2004), http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

[16] TERENA's Incident Object Description Exchange Format Data Model and XML

Implementation (IODEF) (produced by IETF), RFC 5070

[17] Internet Engineering Task Force (IETF) RFC 3227, Guidelines for evidence collection and archiving

[18] CESG GOVCERTUK, Incident Response Guidelines (2008),

http://www.govcertuk.gov.uk/pdfs/incident_response_guidelines.pdf

[19] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Incident Management Capability Metrics Version 0.1 (2007),

http://www.cert.org/archive/pdf/07tr008.pdf

[20] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Incident Management Mission Diagnostic Method Version 1.0,

http://www.cert.org/archive/pdf/08tr007.pdf

[21] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Defining Incident Management Processes for CSIRTs: A Work in Progress,

http://www.cert.org/archive/pdf/04tr015.pdf

[22] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Handbook for Computer Security Incident Response Teams (CSIRTs),

http://www.cert.org/archive/pdf/csirt- handbook.pdf

[23] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", State of the Practice of Computer Security Incident Response Teams,

http://www.cert.org/archive/pdf/03tr001.pdf

[24] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", CSIRT Services, http://www.cert.org/csirts/services.html

[25] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Action List for Developing a Computer Security Incident Response Team (CSIRT),

http://www.cert.org/csirts/action_list.html

[26] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?

http://www.cert.org/csirts/csirt-staffing.html

[27] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Steps for Creating National CSIRTs, http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

[28] SANS Institute, An approach to the ultimate in-depth security event management framework (2008)

[29] SANS Institute, Mining gold, A primer on incident handling and response (2008)

[30] SANS Institute, Incident Handling for SMEs (Small to Medium Enterprises) (2008)

[31] SANS Institute, Breach Notification in Incident Handling (2008)

[32] SANS Institute, Baselines and Incident Handling (2008)

[33] SANS Institute, Documentation is to Incident Response as an Air Tank is to Scuba Diving (2007)

[34] SANS Institute, Creating and Managing an Incident Response Team for a Large Company (2007)

[35] SANS Institute, An Incident Handling Process for Small and Medium Businesses (2007)

[36] SANS Institute, Incident Management 101 Preparation & Initial Response (aka Identification) (2005)

[37] SANS Institute, Building an Incident Response Program To Suit Your Business (2003)

[38] ISACA, COBIT 4.1 (Section DS5.11), www.isaca.org/cobit

[39] ENISA, A step-by-step approach on how to set up a CSIRT, http://www.enisa.europa.eu/act/cert/support/guide

[40] ENISA, CERT cooperation and its further facilitation by relevant stakeholders, http://www.enisa.europa.eu/act/cert/background/coop

[41] ENISA, A basic collection of good practices for running a CSIRT, http://www.enisa.europa.eu/act/cert/support/guide2

[42] TERENA's Incident Object Description and Exchange Format Requirements (IODEF) (produced by IETF), RFC 3067

[43] CVSS - A complete Guide to the Common Vulnerability Scoring System (Version 2.0), FIRST, 20 June 2007, http://www.first.org/cvss/cvss-guide.html

[44] SWIF - Structured Warning Information Format (Version 2.3), ITsafe, 9 May 2008

[45] ITIL, ITIL framework document, http://www.itil-officialsite.com/home/home.asp