TCVN **T I Ê U C H U Ẩ N Q U Ố C G I A**

TCVN 10543:2014

ISO/IEC 27010 : 2012

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – QUẢN LÝ AN TOÀN TRAO ĐỔI THÔNG TIN LIÊN TỔ CHỨC, LIÊN NGÀNH

Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications

HÀ NỘI – 2014

Mục lục

Lời nói đầu

TCVN 10543:2014 hoàn toàn tương đương với ISO/IEC 27010:2012

TCVN ISO/IEC 10543:2014 do Viện Khoa học Kỹ thuật Bưu điện biên soạn, Bộ Thông tin và truyền thông tổ chức xây dựng và 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 an toàn trao đổi thông tin liên tổ chức, liên ngành

Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications

1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp thêm các hướng dẫn đã được đưa ra trong bộ tiêu chuẩn ISO/IEC 27000 để triển khai quản lý an toàn thông tin trong các cộng đồng chia sẻ thông tin.

Tiêu chuẩn này cung cấp các biện pháp quản lý và hướng dẫn cụ thể liên quan đến việc khởi tạo, triển khai, duy trì và cải tiến an toàn thông tin trong trao đổi thông tin liên tổ chức và liên ngành.

Tiêu chuẩn này áp dụng cho tất cả các hình thức trao đổi và chia sẻ thông tin nhạy cảm, cả công khai lẫn riêng tư, ở phạm vi quốc gia lẫn quốc tế, trong cùng lĩnh vực ngành nghề hoặc thị trường hoặc giữa các ngành nghề. Đặc biệt, tiêu chuẩn này có thể áp dụng để trao đổi và chia sẻ thông tin liên quan đến việc hỗ trợ, duy trì vào bảo vệ cơ sở hạ tầng quan trọng của một tổ chức hoặc một quốc gia.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

ISO/IEC 27000:2009, Information technology - Security techniques - Information security manegerment 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)*

TCVN ISO/IEC 27001:2009, Công nghệ thông tin - Hệ thống quản lý an toàn thông tin - Các yêu cầu

TCVN ISO/IEC 27002:2011, Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành quản lý an toàn thông tin.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong ISO/IEC 27000 và các thuật ngữ và định nghĩa sau:

3.1

Cộng đồng chia sẻ thông tin (information sharing community)

Nhóm các tổ chức đồng ý chia sẻ thông tin

CHÚ THÍCH: Tổ chức có thể là cá nhân.

3.2

Thực thể truyền thông thông tin tin cậy (trusted information communication entity)

Tổ chức độc lập hỗ trợ trao đổi thông tin trong một cộng đồng chia sẻ thông tin

4 Các khái niệm và giải thích

4.1 Giới thiệu

Hướng dẫn cụ thể hệ thống quản lý an toàn thông tin cho trao đổi thông tin liên tổ chức và liên ngành được đề cập trong các điều từ điều 5 đến điều 15 của tiêu chuẩn này.

TCVN ISO/IEC 27002:2011 đưa ra các biện pháp quản lý bao gồm cả việc trao đổi thông tin song phương giữa các tổ chức, cũng như các biện pháp quản lý việc phát tán thông tin sẵn có công khai nói chung. Tuy nhiên, trong một số trường hợp vẫn cần chia sẻ thông tin trong cộng đồng các tổ chức, nơi thông tin này là nhạy cảm và không thể được cung cấp công khai ngoại trừ cho các thành viên trong cộng đồng. Thông thường, thông tin chỉ sẵn sàng sử dụng cho các cá nhân nhất định trong mỗi tổ chức thành viên, hoặc có thể có các yêu cầu an toàn thông tin khác như ẩn danh thông tin. Tiêu chuẩn này bổ sung một số biện pháp quản lý tiềm năng, cung cấp các hướng dẫn bổ sung và giải thích tiêu chuẩn TCVN ISO/IEC 27001:2009 và TCVN ISO/IEC 27002:2011 để đáp ứng các yêu cầu này.

4.2 Cộng đồng chia sẻ thông tin

Để đạt hiệu quả, cộng đồng chia sẻ thông tin phải có lợi ích chung hoặc mối quan hệ khác để xác định phạm vi thông tin nhạy cảm được chia sẻ. Ví dụ, các cộng đồng có thể là các thị trường cụ thể và giới hạn thành viên trong các tổ chức trong một ngành. Ngoài ra, còn có thể dựa vào các lợi ích chung khác như vị trí địa lý hoặc quyền sở hữu chung.

4.3 Quản lý cộng đồng

Cộng đồng chia sẻ thông tin được tạo ra từ các tổ chức độc lập hoặc các bộ phận của các tổ chức. Do vậy có thể không có các cơ cấu tổ chức và các chức năng quản lý rõ ràng và đồng bộ áp dụng cho tất cả các thành viên. Để quản lý an toàn thông tin đạt hiệu lực thì cần có sự cam kết của ban quản lý. Do đó, các cơ cấu tổ chức và các chức năng quản lý áp dụng cho quản lý an toàn thông tin cộng đồng phải được xác định rõ ràng.

Sự khác nhau giữa các tổ chức thành viên của cộng đồng chia sẻ thông tin phải được xem xét. Sự khác nhau này có thể bao gồm:

- Các tổ chức thành viên đã vận hành hệ thống quản lý an toàn thông tin riêng hay chưa, và
- Các quy tắc của các tổ chức thành viên về việc bảo vệ tài sản và tiết lộ thông tin.

4.4 Các thực thể hỗ trợ

Các cộng đồng chia sẻ thông tin sẽ lựa chọn thiết lập hoặc chỉ định một thực thể hỗ trợ tập trung để tổ chức hoặc hỗ trợ chia sẻ thông tin. Thực thể đó có thể cung cấp nhiều biện pháp quản lý hỗ trợ như ẩn danh nguồn gốc và bên nhận dễ dàng và hiệu lực hơn so với các thành viên trao đổi thông tin trực tiếp. Có một số mô hình tổ chức khác nhau được sử dụng để tạo ra thực thể hỗ trợ. Phụ lục D trong tiêu chuẩn này mô tả hai mô hình phổ biến là Thực thể truyền thông thông tin tin cậy (TICE) và Điểm báo cáo, tư vấn và cảnh báo (WARP).

4.5 Trao đổi thông tin liên ngành

Nhiều cộng đồng chia sẻ thông tin là các ngành, do đó nó đương nhiên có một phạm vi lợi ích chung. Tuy nhiên, thông tin được chia sẻ bởi cộng đồng đó có thể sẽ có lợi cho các cộng đồng chia sẻ thông tin khác được thiết lập trong các ngành khác. Trong trường hợp như vậy, có thể thiết lập cộng đồng chia sẻ thông tin của các cộng đồng chia sẻ thông tin dựa trên một vài lợi ích chung như là bản chất của thông tin được chia sẻ. Đó chính là trao đổi thông tin liên ngành.

Trao đổi thông tin liên ngành có được thuận lợi lớn khi các thực thể hỗ trợ tồn tại trong mỗi cộng đồng chia sẻ thông tin, vì sau đó các biện pháp quản lý và thỏa thuận trao đổi thông tin cần thiết có thể được thiết lập giữa các thực thể hỗ trợ chứ không phải giữa mọi thành viên của tất cả các cộng đồng. Một số trao đổi thông tin liên ngành yêu cầu ẩn danh các tổ chức nguồn hoặc các tổ chức nhận, điều này cũng có thể đạt được bằng cách sử dụng các thực thể hỗ trợ.

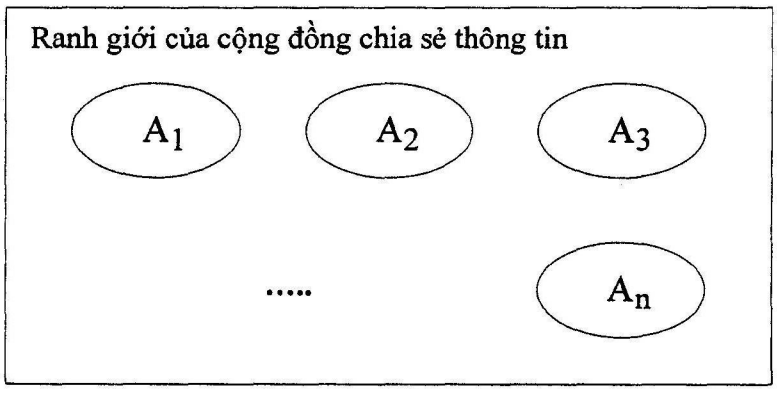
4.6 Tính phù hợp

Bất kỳ hệ thống quản lý an toàn thông tin (ISMS) nào được thiết lập, vận hành tuân theo TCVN ISO/IEC 27001:2009 và sử dụng các biện pháp quản lý của TCVN ISO/IEC 27002:2011, tiêu chuẩn này và các nguồn khác đều có thể được đánh giá phù hợp với TCVN ISO/IEC 27001:2009 mà không cần sửa đổi hoặc bổ sung thêm.

Tuy nhiên, có một số điểm trong TCVN ISO/IEC 27001:2009 cần được giải thích khi áp dụng cho một cộng đồng chia sẻ thông tin (hoặc cho trao đổi thông tin liên ngành, một cộng đồng của các cộng đồng).

Điểm đầu tiên cần giải thích là định nghĩa tổ chức liên quan.

TCVN ISO/IEC 27001:2009 yêu cầu ISMS được thiết lập bởi một tổ chức và vận hành trong bối cảnh hoạt động nghiệp vụ của tổ chức đó nói chung và các rủi ro mà tổ chức phải đối mặt (4.1 của TCVN ISO/IEC 27001:2009). Trong bối cảnh này, tổ chức liên quan là cộng đồng chia sẻ thông tin. Tuy nhiên, các thành viên của cộng đồng chia sẻ thông tin sẽ tự tổ chức – xem Hình 1.

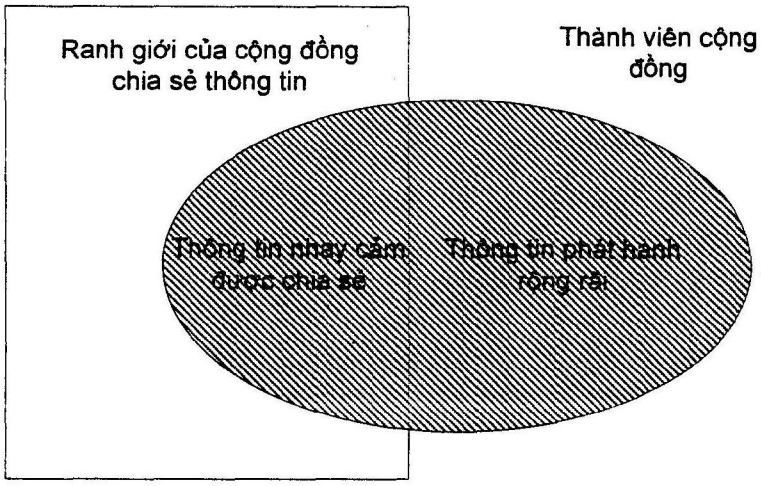


A_k là tổ chức thành viên k của cộng đồng (k= 1...n), bao gồm cả thực thể hỗ trợ

Hình 1 – Các cộng đồng và các tổ chức

Thứ hai, trong nhiều cộng đồng chia sẻ thông tin, không phải tất cả mọi người trong tổ chức thành viên đều được phép truy nhập vào thông tin nhạy cảm được chia sẻ giữa các thành viên. Trong trường hợp này, một phần thành viên của tổ chức nằm trong phạm vi của hệ thống quản lý an toàn thông tin cộng

đồng và một phần nằm ngoài. Phần nằm ngoài phạm vi cộng đồng chỉ được truy nhập vào thông tin cộng đồng nếu thông tin đó được đánh dấu để phát hành trên diện rộng – xem Hình 2.



Hình 2 – Thành viên có một phần nằm trong phạm vi chia sẻ thông tin.

Các thành viên của cộng đồng chia sẻ thông tin có thể có hệ thống quản lý an toàn thông tin riêng, do đó một số quy trình có thể nằm trong phạm vi của hệ thống quản lý của cả thành viên lẫn cộng đồng. Trong trường hợp này, xảy ra ít nhất một khả năng lý thuyết là các yêu cầu không tương thích và mâu thuẫn trong các quy trình đó. Đây là trường hợp bị loại bỏ khỏi phạm vi của hệ thống quản lý an toàn thông tin thành viên– xem 4.2.1 a) của TCVN ISO/IEC 27001:2009.

Khi xác định phương pháp đánh giá rủi ro (4.2.1 c của TCVN ISO/IEC 27001:2009), cộng đồng chia sẻ thông tin cần thấy rằng tác động của rủi ro có thể khác nhau đối với các thành viên khác nhau của cộng đồng. Do đó, cộng đồng cần lựa chọn một phương pháp đánh giá rủi ro để có thể xử lý các tác động không đồng nhất, như các tiêu chí đánh giá rủi ro.

Việc đo hiệu lực của các biện pháp quản lý được lựa chọn (4.2.3 c của TCVN ISO/IEC 27001:2009) cần sự tham gia của tất cả các thành viên của cộng đồng chia sẻ thông tin. Tất cả các thành viên cần cung cấp phản hồi thường xuyên cho nhà cung cấp thông tin và cộng đồng về tất cả những gì liên quan đến hiệu lực của biện pháp quản lý trong môi trường riêng của họ.

4.7 Mô hình trao đổi thông tin

Trao đổi thông tin nhạy cảm được nêu trong tiêu chuẩn này có thể ở bất kỳ hình thức nào – văn bản, bằng lời nói hoặc điện tử - miễn là đáp ứng các yêu cầu quản lý được lựa chọn.

Trong phần còn lại của tiêu chuẩn này, trao đổi thông tin nhạy cảm cá nhân được mô tả theo các dạng bên tham gia như sau:

- Nguồn gốc của một danh mục thông tin là cá nhân hoặc tổ chức tạo ra danh mục thông tin đó; nguồn gốc không nhất thiết là một thành viên của cộng đồng.
- Bên khởi tạo là thành viên của một cộng đồng chia sẻ thông tin thực hiện khởi đầu phổ biến thông tin của mình trong cộng đồng. Bên khởi tạo có thể phổ biến thông tin trực tiếp, hoặc gửi thông tin tới một thực thể hỗ trợ để phổ biến. Bên khởi tạo và nguồn gốc thông tin không nhất thiết phải là một; bên khởi tạo có thể che giấu định danh nguồn gốc. Các cộng đồng có thể cung

cấp phương tiện để cho phép một thành viên che giấu định danh riêng của họ như bên khởi tạo.

- Bên nhận là bên nhận thông tin được phổ biến trong cộng đồng. Bên nhận không nhất thiết là các thành viên trong cộng đồng nếu thông tin được định danh sẵn sàng để phổ biến trên diện rộng. Các cộng đồng có thể cung cấp phương tiện để cho phép bên nhận che giấu định danh của họ từ thông tin bên khởi tạo.

5 Chính sách an toàn thông tin

5.1 Chính sách an toàn thông tin

5.1.1 Tài liệu chính sách an toàn thông tin

Xem 4.1.1 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Tài liệu chính sách an toàn thông tin phải xác định cách các thành viên của cộng đồng làm việc cùng nhau để thiết lập các chính sách quản lý an toàn thông tin và định hướng cho cộng đồng chia sẻ thông tin. Tài liệu này phải sẵn sàng cho tất cả các nhân viên tham gia vào việc chia sẻ thông tin trong cộng đồng. Chính sách có thể hạn chế phổ biến tài liệu tới các nhân viên khác của các thành viên trong cộng đồng.

Tài liệu chính sách an toàn thông tin phải xác định chính sách phổ biến và đánh dấu thông tin được sử dụng trong cộng đồng.

5.1.2 Soát xét chính sách an toàn thông tin

Xem 4.1.2 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Đầu vào quy trình soát xét của ban quản lý phải bao gồm các thông tin về những thay đổi đáng kể đối với toàn bộ thành viên của cộng đồng chia sẻ thông tin.

6 Tổ chức đảm bảo an toàn thông tin

6.1 Tổ chức nội bộ

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

6.2 Các bên tham gia bên ngoài

6.2.1 Xác định các rủi ro liên quan đến các bên tham gia bên ngoài

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

6.2.2 Giải quyết an toàn khi làm việc với khách hàng

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

6.2.3 Giải quyết an toàn trong các thỏa thuận với bên thứ ba

Xem 5.2.3 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Tất cả các thành viên của cộng đồng phải nhận biết được các định danh của các bên thứ ba liên quan đến việc cung cấp dịch vụ cộng đồng trong trường hợp họ có kháng nghị đối với các bên cụ thể liên quan đến xử lý thông tin mà họ cung cấp.

Các thỏa thuận với các nhà sản xuất và nhà cung cấp dịch vụ liên quan tới việc cung cấp dịch vụ cộng đồng phải cho phép thực hiện đánh giá và soát xét an toàn các dịch vụ của họ một cách thường xuyên.

7 Quản lý tài sản

7.1 Trách nhiệm đối với tài sản

7.1.1 Kiểm kê tài sản

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

7.1.2 Quyền sở hữu tài sản

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

7.1.3 Sử dụng hợp lý tài sản

Xem 6.1.3 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Thông tin được cung cấp bởi các thành viên khác của một cộng đồng chia sẻ thông tin cũng là tài sản, cần được bảo vệ và phổ biến theo mọi quy tắc được thiết lập bởi cộng đồng chia sẻ thông tin hoặc bởi bên khởi tạo.

7.2 Phân loại thông tin

7.2.1 Hướng dẫn phân loại

Xem 6.2.1 của TCVN ISO/IEC 27002:2011 và bổ sung:

Biện pháp quản lý

Thông tin phải được phân loại theo giá trị, yêu cầu pháp lý, độ nhạy cảm, độ tin cậy và độ quan trọng của chúng đối với tổ chức.

Hướng dẫn triển khai

Cũng như tiêu chí đưa ra trong TCVN ISO/IEC 27002:2011, thông tin phải được phân loại theo độ tin cậy của chúng. Điều này phải được đánh giá theo uy tín của nguồn tin, nội dung kỹ thuật và chất lượng của miêu tả.

Tương tự như vậy, độ nhạy cảm có thể phụ thuộc vào nhiều khía cạnh của thông tin ngoài nhu cầu duy trì tính bảo mật của thông tin như tác động của việc tiết lộ, sự khẩn cấp khi phát tán hay nguy cơ tổn thương tính ẩn danh của nguồn thông tin.

Phải giải thích rõ ràng các cách đánh dấu phân loại được ấn định bởi các thành viên khác của cộng đồng chia sẻ thông tin.

VÍ DỤ: Một Email khách hiển thị thông điệp "Vui lòng xem điều này như thông tin mật" khi đang hiển thị email trong đó trường tiêu đề nhạy cảm được thiết lập là "thông tin mật công ty" (RFC 4021 [2]). Trường hợp này, dụng ý của bên khởi tạo không rõ ràng là "thông tin mật công ty" (và thông điệp gửi đi bị lỗi) hay "thông tin mật cho bên nhận".

7.2.2 Gắn nhãn và xử lý thông tin

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

7.3 Bảo vệ trao đổi thông tin

Bổ sung thêm một mục tiêu quản lý sau vào điều 7 của TCVN ISO/IEC 27002:2011, quản lý tài sản:

Mục tiêu: Đảm bảo bảo vệ đầy đủ việc trao đổi thông tin trong cộng đồng chia sẻ thông tin. Thông tin trao đổi giữa các thành viên của cộng đồng chia sẻ thông tin phải được bảo vệ một cách phù hợp, ngay cả khi các thành viên là các thực thể độc lập hoặc các phần của thực thể có thể đánh dấu, phổ biến và bảo vệ thông tin của mình theo các cách khác nhau. Khi có yêu cầu ẩn danh, mọi thông tin định danh nguồn gốc trao đổi thông tin phải được loại bỏ. Cũng như vậy, yêu cầu phải có khả năng nhận thông tin chia sẻ mà không tiết lộ định danh bên nhận. Việc phát hành thông tin chia sẻ ra ngoài cộng đồng phải được quản lý.

7.3.1 Phổ biến thông tin

Biện pháp quản lý

Việc phổ biến thông tin bên trong thành viên nhận phải được giới hạn trên cơ sở việc đánh dấu phổ biến xác định trước bởi cộng đồng.

Hướng dẫn triển khai

Thông tin không được ấn định đánh dấu phổ biến phải được phổ biến theo mặc định xác định bởi cộng đồng chia sẻ thông tin. Nếu có nghi ngờ, hoặc không có thỏa thuận chung về phổ biến mặc định thì thông tin phải được xử lý thận trọng. Nếu có thể, bên nhận phải yêu cầu bên khởi tạo gửi lại thông tin với đánh dấu phổ biến rõ ràng.

Việc hạn chế phổ biến có thể bao gồm các hạn chế sử dụng như kiểm soát sao chép điện tử, ngăn chặn chụp ảnh màn hình, hoặc ngặn chặn in ấn và xuất dữ liệu.

Thông tin khác

Các thành phần hoặc thuộc tính khác nhau của thông tin được chia sẻ có thể có độ nhạy cảm khác nhau. Cụ thể, việc biết đến sự tồn tại của một thông điệp hoặc thông tin được chia sẻ khác có thể có độ nhạy cảm khác nhau so với nội dung của nó.

Chức năng quản lý bản quyền của thông tin thường được sử dụng để ràng buộc các giới hạn sử dụng. Do đó, một mô hình hoặc chính sách bản quyền người sử dụng rõ ràng rất cần thiết để người sử dụng biết những gì hệ thống của họ cho phép họ làm và nơi họ sẽ bị chặn.

7.3.2 Lưu ý sử dụng thông tin

Biện pháp quản lý

Mỗi một quy trình trao đổi thông tin phải bắt đầu với một lưu ý sử dụng, liệt kê các yêu cầu đặc biệt mà bên nhận phải thực hiện bên cạnh các đánh dấu thông tin thông thường.

Hướng dẫn triển khai

Bên nhận phải yêu cầu bên khởi tạo làm sáng tỏ nếu lưu ý sử dụng không được hiểu đầy đủ hoặc không được triển khai.

7.3.3 Độ tin cậy của thông tin

Biện pháp quản lý

Mỗi quy trình trao đổi thông tin phải chỉ ra mức độ tin tưởng của bên khởi tạo về độ chính xác và độ tin cậy của thông tin được truyền.

Hướng dẫn triển khai

Dựa vào ràng buộc kỹ thuật và hậu quả tiềm ẩn và tính khẩn cấp thì có thể không kiểm tra được tính hợp lệ của toàn bộ thông tin trước khi truyền. Nếu có các giới hạn thì giới hạn đó phải được chỉ ra như một phần của thông điệp.

Việc chỉ ra các hạn chế về độ tin cậy của thông tin đặc biệt quan trọng khi nguồn là ẩn danh hoặc không được biết. Việc chỉ ra nơi bên khởi tạo có thể kiểm tra tính hợp lệ của thông tin đã cho trực tiếp và có thể đảm bảo tính xác thực của nó là rất quan trọng.

7.3.4 Giảm tính nhạy cảm của thông tin

Biện pháp quản lý

Bên khởi tạo quy trình trao đổi thông tin phải chỉ báo nếu độ nhạy cảm của thông tin được cung cấp sẽ suy giảm sau một số sự kiện bên ngoài hoặc theo thời gian.

Hướng dẫn triển khai

Ngay cả khi độ nhạy cảm của thông tin được cung cấp giảm theo thời gian thì nó vẫn cần bảo vệ. Hướng dẫn phân loại (xem 6.4.2) cần bao gồm các mặc định cho sự suy giảm độ nhạy cảm.

7.3.5 Bảo vệ nguồn ẩn danh

Biện pháp quản lý

Thành viên cộng đồng phải loại bỏ mọi thông tin định danh nguồn gốc trong mọi trao đổi thông tin mà họ khởi tạo hoặc nhận nếu việc ẩn danh được yêu cầu.

Hướng dẫn triển khai

Bên khởi tạo thông tin chịu trách nhiệm đạt được sự chấp thuận từ nguồn gốc (nếu khác nhau) trước khi trao đổi thông tin đó đến các thành viên khác của cộng đồng chia sẻ thông tin. Bên khởi tạo cũng phải hỏi nguồn gốc nếu nó được xác định là nhà cung cấp đầu tiên của thông tin.

Điều quan trọng là quy trình bảo vệ nguồn gốc xem xét nội dung thông điệp cũng như nguồn gốc thông điệp, bởi vì phân tích nội dung có thể phát hiện định danh nguồn gốc. Nếu có thể, bên khởi tạo thông điệp nên yêu cầu nguồn gốc soát xét thông tin được ẩn danh và danh sách bên nhận mong đợi trước khi nó được phổ biến.

VÍ DỤ: Một thông điệp như "Các ATM của chúng tôi đã bị mất khả năng hoạt động do một loại virus mới mà tường lửa không phát hiện ra nhưng máy chủ chính sách phát hiện ra" có thể tiết lộ nguồn gốc thông điệp nếu chỉ có một ngân hàng bị ngắt dịch vụ công cộng vào ngày thông điệp được phát ra.

Có một số cơ chế kỹ thuật có thể được sử dụng để cung cấp xác thực mà không ảnh hưởng đến ẩn danh. Ví dụ, các bí mật mã hóa được chia sẻ có thể được sử dụng để xác nhận trao đổi thông tin được khởi nguồn từ một thành viên của cộng đồng mà không tiết lộ định danh thực của bên khởi tạo.

7.3.6 Bảo vệ bên nhận ẩn danh

Biện pháp quản lý

Với sự chấp thuận của bên khởi tạo, các thành viên cộng đồng phải có khả năng nhận các trao đổi thông tin mà không tiết lộ định danh của họ.

Hướng dẫn triển khai

Tiếp nhận ẩn danh được triển khai bằng cả biện pháp kỹ thuật (ví dụ, mã hóa) và biện pháp mang tính thủ tục (ví dụ, định tuyến thông qua một thực thể hỗ trợ). Phải chú ý đảm bảo ẩn danh không vi phạm những ràng buộc theo pháp luật hoặc giảm mức độ tin cậy tổng thể trong cộng đồng.

Thông tin khác

Tiếp nhận ẩn danh thường cần thiết để trao đổi thông tin liên ngành có hiệu quả vì các cộng đồng ngành mong muốn giữ các chi tiết về thành viên của họ một cách riêng tư.

7.3.7 Quyền phát hành tiếp

Biện pháp quản lý

Nếu không được đánh dấu phổ biến rộng hơn thì thông tin không được phổ biến trên cộng đồng chia sẻ thông tin khi không có sự chấp thuận chính thức từ bên khởi tạo.

Hướng dẫn triển khai

Mỗi bên nhận phải có trách nhiệm nhận được sự cho phép cần thiết để phát hành rộng rãi từ bên khởi tạo trước khi phổ biến tiếp.

Trong trao đổi thông tin liên ngành, bên khởi tạo không thể biết tất cả các tổ chức sẽ nhận thông tin. Trong trường hợp đó, chấp thuận phát hành chung hoặc cho ngành cụ thể cần thiết được ban hành.

Thông tin khác

Giao thức đèn giao thông (xem Phụ lục C) được sử dụng để chỉ ra cách thông tin có thể phổ biến hơn nữa mà không cần thêm sự chấp thuận.

8 Đảm bảo an toàn thông tin từ nguồn nhân lực

8.1 Trước khi tuyển dụng

8.1.1 Các vai trò và trách nhiệm

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

8.1.2 Thẩm tra

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

8.1.3 Điều khoản và điều kiện tuyển dụng

Xem 7.1.3 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Các quy định thẩm tra chưa chắc đã nhất quán trong tất cả các thành viên của cộng đồng chia sẻ thông tin. Cộng đồng phải xem xét xác định mức độ kiểm tra xác minh tối thiểu để áp dụng cho tất cả nhân viên hoặc nhà thầu của các thành viên được truy nhập vào thông tin được chia sẻ của cộng đồng.

8.2 Trong thời gian làm việc

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

8.3 Chấm dứt hoặc thay đổi công việc

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

9 Đảm bảo an toàn vật lý và môi trường

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10 Quản lý trao đổi thông tin và vận hành

10.1 Các trách nhiệm và thủ tục vận hành

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.2 Quản lý chuyển giao dịch vụ của bên thứ ba

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.3 Lập kế hoạch và chấp nhận hệ thống

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.4 Bảo vệ chống lại mã độc và mã di động

10.4.1 Quản lý chống lại mã độc hại

Xem 9.4.1 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Thông tin nhận từ các thành viên khác của một cộng đồng chia sẻ thông tin phải được quét các mã độc hiện tại, bất chấp dịch vụ trao đổi thông tin giữa các thành viên của cộng đồng có cung cấp quét bản tin bị nhiễm virus hay không.

10.4.2 Kiểm soát các mã di động

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.5 Sao lưu

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.6 Quản lý an toàn mạng

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.7 Xử lý phương tiện

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.8 Trao đổi thông tin

10.8.1 Các chính sách và thủ tục trao đổi thông tin

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.8.2 Các thỏa thuận trao đổi

Xem 9.8.2 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Tất cả các cộng đồng chia sẻ thông tin phải xác định các thỏa thuận trao đổi thông tin và chỉ cho phép các thành viên tham gia cộng đồng nếu các thỏa thuận đó được ký kết và chấp nhận.

10.8.3 Vận chuyển phương tiện vật lý

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.8.4 Thông điệp điện tử

Xem 9.8.4 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Tất cả các cộng đồng chia sẻ thông tin phải xác định các quy tắc bảo vệ thông tin đang truyền tải và chỉ cho phép các thành viên tham gia cộng đồng nếu các quy tắc như vậy được chấp nhận và được triển khai bởi thành viên đó. Mọi thực thể hỗ trợ phải triển khai các quy tắc đó.

Các cộng đồng chia sẻ thông tin phải xem xét việc triển khai các cơ chế thay thế đối với chia sẻ thông tin không dựa vào thông điệp điện tử và cho phép thành viên xác định các thông điệp cụ thể được phổ biến bằng các con đường khác đó.

10.8.5 Các hệ thống thông tin nghiệp vụ

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.9 Các dịch vụ thương mại điện tử

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.10 Giám sát

10.10.1 Ghi nhật ký đánh giá

Xem 9.10.1 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Khi cộng đồng chia sẻ thông tin yêu cầu, các thành viên phải ghi lại việc phổ biến nội bộ của thông tin được chia sẻ.

10.10.2 Giám sát sử dụng hệ thống

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.10.3 Bảo vệ các thông tin nhật ký

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.10.4 Nhật ký của người điều hành và người quản trị

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.10.5 Ghi nhật ký lỗi

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

10.10.6 Đồng bộ thời gian

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

11 Quản lý truy nhập

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

12 Tiếp nhận, phát triển và duy trì các hệ thống thông tin

12.1 Yêu cầu đảm bảo an toàn cho các hệ thống thông tin

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

12.2 Xử lý đúng trong các ứng dụng

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

12.3 Quản lý mã hóa

12.3.1 Chính sách sử dụng các biện pháp quản lý mã hóa

Xem 11.3.1 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Các kỹ thuật mã hóa được sử dụng để triển khai các quy tắc phân tán chia sẻ thông tin, ví dụ thông qua quản lý bản quyền của thông tin.

12.3.2 Quản lý khóa

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

12.4 An toàn cho các tệp tin hệ thống

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

12.5 Bảo đảm an toàn trong các quy trình hỗ trợ và phát triển

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

12.6 Quản lý các điểm yếu kỹ thuật

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

13 Quản lý các sự cố an toàn thông tin

13.1 Báo cáo về các sự kiện an toàn thông tin và các điểm yếu

13.1.1 Báo cáo các sự kiện an toàn thông tin

Xem 12.1.1 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Các thành viên của một cộng đồng chia sẻ thông tin phải xem xét các sự kiện được phát hiện nên được báo cáo cho các thành viên khác trong cộng đồng hay không. Cộng đồng phải đồng ý và phát hành hướng dẫn về các loại sự cố mà các thành viên khác quan tâm. Các thành viên cần phải cân nhắc để đảm bảo rằng chỉ có các sự kiện mà các thành viên khác quan tâm mới được báo cáo.

Xu hướng chung là các sự cố được giữ bí mật và các thành viên cộng đồng không tiết lộ thông tin sự cố để bảo vệ uy tín của tổ chức. Tuy nhiên, việc trao đổi thông tin sự cố đến các thành viên khác sẽ khuyến khích hợp tác và phối hợp trong việc ngăn ngừa sự cố, phản ứng nhanh trước các sự cố và cải tiến an toàn thông tin tổng thể trong cộng đồng. Các sự kiện và sự cố có thể được báo cáo mà không cần tiết lộ tất cả các hậu quả của chúng.

Các thành viên phải nhanh chóng kiểm tra tất cả các sự kiện được báo cáo để xem xét nếu chúng ảnh hưởng tới hoạt động riêng của họ. Ví dụ, một thông báo thường lệ của một thành viên cung cấp dịch vụ bảo trì theo kế hoạch có thể yêu cầu các thành viên khác soát xét độ tin cậy của các nhà cung cấp thay thế trước khi bắt đầu hoạt động bảo trì.

13.1.2 Báo cáo các điểm yếu về an toàn thông tin

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

13.1.3 Hệ thống cảnh báo sớm

Bổ sung biện pháp quản lý sau vào 12.1 của TCVN ISO/IEC 27002:2011, báo cáo về các sự kiện an toàn thông tin và các điểm yếu.

Biện pháp quản lý

Một hệ thống cảnh báo sớm phải được triển khai trong cộng đồng chia sẻ thông tin để trao đổi thông tin ưu tiên một cách hiệu quả ngay khi nó xuất hiện.

Hướng dẫn triển khai

Thông tin ưu tiên là thông tin làm cho các thành viên cộng đồng khác tránh hoặc giảm thiểu được các sự kiện không mong muốn tương tự. Điều này rất quan trọng nên thông tin như vậy được chia sẻ khẩn cấp thậm chí ngay cả khi nó chưa được phân tích hoặc xác nhận đầy đủ.

13.2 Quản lý các sự cố an toàn thông tin và cải tiến

13.2.1 Các trách nhiệm và thủ tục

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

13.2.2 Rút bài học kinh nghiệm từ các sự cố an toàn thông tin

Xem 12.2.2 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Các điều tra dựa trên thông tin được phổ biến bởi một cộng đồng chia sẻ thông tin phải được thực hiện để giảm thiểu rủi ro của các sự cố tương tự và phát triển sự hiểu biết tốt hơn về các rủi ro mà cộng đồng và cấu trúc thông tin quan trọng liên quan phải đối mặt. Các điều tra như vậy được thực hiện bởi các thành viên tham gia, hoặc một thực thể hỗ trợ nếu nó tồn tại.

Sau khi các sự cố được báo cáo, việc soát xét sự cố phải được thực hiện bởi các thành viên của cộng đồng chia sẻ thông tin để cho phép cập nhật các kế hoạch ứng phó sự cố an toàn thông tin, các thủ tục liên quan và hồ sơ rủi ro nghiệp vụ, ngay cả khi thành viên không bị ảnh hưởng bởi sự cố. Mỗi thành viên phải đảm bảo rằng những ứng phó sự cố đã báo cáo được đánh giá và bất kỳ bài học hoặc sự cải tiến cho các quy trình được xác định và tác động đến cải tiến liên tục quy trình ứng phó của thành viên.

13.2.3 Thu thập chứng cứ

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

14 Quản lý sự liên tục của hoạt động nghiệp vụ

14.1 Các khía cạnh an toàn thông tin trong quản lý sự liên tục của hoạt động nghiệp vụ

14.1.1 Tính đến an toàn thông tin trong các quy trình quản lý sự liên tục của hoạt động nghiệp vụ

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

14.1.2 Đánh giá rủi ro và sự liên tục trong hoạt động của tổ chức

Xem 13.1.2 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Đánh giá rủi ro về sự liên tục trong hoạt động của tổ chức bởi các thành viên của cộng đồng chia sẻ thông tin phải xem xét phụ thuộc vào sự cung cấp thông tin nhạy cảm từ các thành viên khác.

14.1.3 Xây dựng và triển khai các kế hoạch về tính liên tục, trong đó bao gồm vấn đề đảm bảo an toàn thông tin

Xem 13.1.3 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Các kế hoạch về tính liên tục trong hoạt động của tổ chức được phát triển bởi các thành viên của cộng đồng chia sẻ thông tin phải đề cập đến nhu cầu trao đổi thông tin nhạy cảm với các thành viên khác như một phần của quy trình khôi phục.

14.1.4 Khung hoạch định sự liên tục trong hoạt động nghiệp vụ

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

14.1.5 Kiểm tra, duy trì và đánh giá lại các kế hoạch đảm bảo sự liên tục trong hoạt động nghiệp vụ

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

15 Sự tuân thủ

15.1 Sự tuân thủ các quy định pháp lý

15.1.1 Xác định các điều luật hiện hành

Xem 14.1.1 của TCVN ISO/IEC 27002:2011 và bổ sung thêm hướng dẫn sau:

Hướng dẫn triển khai

Cộng đồng chia sẻ thông tin phải xem xét mọi điều luật, thỏa thuận thích hợp và các quy định liên quan đến chia sẻ thông tin, như các quy định hoặc điều luật về chống độc quyền. Điều này có thể ngăn chặn những tổ chức nhất định tham gia vào cộng đồng, hoặc đặt ra các hạn chế đối với việc đại diện của họ.

15.1.2 Quyền sở hữu trí tuệ (IPR)

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

15.1.3 Bảo vệ các hồ sơ của tổ chức

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

15.1.4 Bảo vệ dữ liệu và sự riêng tư của thông tin cá nhân

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

15.1.5 Ngăn ngừa việc lạm dụng phương tiện xử lý thông tin

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

15.1.6 Quy định về quản lý mã hóa

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

15.1.7 Trách nhiệm với cộng đồng chia sẻ thông tin

Bổ sung thêm vào 14.1 của TCVN ISO/IEC 27002:2011, sự tuân thủ các quy định pháp lý, như sau:

Biện pháp quản lý

Các vấn đề về trách nhiệm pháp lý và khắc phục hậu quả phải được làm rõ, được hiểu và chấp thuận bởi tất cả thành viên của cộng đồng chia sẻ thông tin, để giải quyết các tình huống mà thông tin cố tình hoặc vô tình bị tiết lộ.

Hướng dẫn triển khai

Khắc phục hậu quả tối thiểu phải bao gồm thông báo về mọi tiết lộ trái phép cho bên khởi tạo một cách đầy đủ và chi tiết để định danh thông tin bị tiết lộ.

Nếu có thể, thông báo phải cung cấp ngược lại cho nguồn gốc, ngay cả khi thông tin được làm sạch và không tiết lộ nguồn gốc của nó. Điều này có thể đạt được thông qua một bên thứ ba tin cậy như Thực thể truyền thông thông tin tin cậy (TICE).

Hậu quả của việc tiết lộ thông tin trái phép có thể ảnh hưởng trực tiếp đến các bên chịu trách nhiệm và có thể liên quan đến việc loại bỏ hoặc hạn chế truy nhập tới một số thành viên trong một khoảng thời gian để thiết lập lại sự tin cậy của cộng đồng.

15.2 Sự tuân thủ các chính sách và tiêu chuẩn an toàn, và tương thích kỹ thuật

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

15.3 Xem xét việc đánh giá các hệ thống thông tin

15.3.1 Các biện pháp quản lý đánh giá các hệ thống thông tin

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

15.3.2 Bảo vệ các công cụ đánh giá hệ thống thông tin

Không có thêm thông tin cụ thể nào cho trao đổi thông tin liên tổ chức, liên ngành.

15.3.3 Các chức năng đánh giá cộng đồng

Bổ sung thêm vào 14.3 của TCVN ISO/IEC 27002:2005, xem xét việc đánh giá các hệ thống thông tin, như sau:

Biện pháp quản lý

Mọi cộng đồng chia sẻ thông tin nên định rõ quyền của các thành viên trong việc đánh giá các hệ thống của các thành viên khác và của bất kỳ nhà cung cấp dịch vụ tin cậy nào.

Hướng dẫn triển khai

Tổ chức có thẩm quyền đánh giá các hệ thống thành viên có thể được giới hạn trong một bên thứ ba tin cậy, như TICE hoặc WARP.

Phụ lục A

(Tham khảo)

Chia sẻ thông tin nhạy cảm

A.1 Giới thiệu

Thông tin nhạy cảm là một tài sản có giá trị quan trọng cần được quản lý an toàn khi chia sẻ giữa các tổ chức. Nó phải được phổ biến đúng lúc để giải quyết các vấn đề về nghiệp vụ và đưa ra quyết định tốt hơn, thậm chí hơn thế nữa nếu nó là thiết yếu đối với tổ chức.

Các cộng đồng chia sẻ thông tin có thể đại diện nhiều loại tổ chức, thậm chí là cá nhân. Các cộng đồng có thể đa dạng về thành viên, hoặc được liên kết rất gần gũi dưới một hình thức hoạt động nghiệp vụ như là một ngành nghề hoặc thị trường cụ thể. Các cộng đồng có thể nằm trong các ngành công cộng và tư nhân, hoặc có thể chứa các thành viên của cả hai loại. Yêu cầu ở đây là một mong muốn chung về chia sẻ một số loại thông tin nhạy cảm và chấp nhận các biện pháp quản lý đã thỏa thuận và các quy trình quản trị việc sử dụng thông tin đó.

Để trao đổi an toàn các thông tin nhạy cảm trong một cộng đồng chia sẻ thông tin, cần phải thiết kế, triển khai và giám sát các quy trình cung cấp luồng thông tin an toàn một cách kịp thời. Các quy trình phải đảm bảo rằng thông tin được phổ biến đến các cá nhân thích hợp, trong khi cũng cung cấp sự đảm bảo tương đối rằng thông tin không bị sử dụng cho các mục đích có hại và không bị phổ biến lại một cách bừa bãi để trở thành thông tin công khai.

Hiệu lực của việc phổ biến được quyết định bởi mức độ tin cậy mà các thành viên nắm giữ trong mối quan hệ được thiết lập bởi cộng đồng chia sẻ thông tin. Đồng thời, các cơ chế an toàn thông tin liên quan đến trao đổi thông tin phải ngăn chặn phổ biến thông tin đến các cá nhân hoặc tổ chức:

- sử dụng hoặc thu thập dữ liệu để thực hiện các hành động xâm hại;
- phổ biến công khai thông tin mà không được sự cho phép của bên khởi tạo thông tin;
- cung cấp thông tin chưa được phân tích đầy đủ và do đó gây ra các hành động không thích hợp, có thể gây lãng phí hoặc sai lệch các tài nguyên và ảnh hưởng đến các tổ chức.

Để các cộng đồng chia sẻ thông tin hoạt động hiệu quả, bên nhận thông tin phải được các tổ chức thành viên của họ trao quyền hành động dựa trên thông tin nhận được, và không được khuyến khích sử dụng sai các thông tin này, ví dụ cho lợi ích thương mại.

A.2 Các thách thức

Việc quản lý an toàn thông tin phù hợp cho trao đổi thông tin liên tổ chức và liên ngành được khuyến nghị nhằm đối phó với các thách thức sau; nếu làm không đúng có thể ảnh hưởng đến các điều kiện nghiệp vụ thông thường và gây gián đoạn khi xảy ra các sự cố:

- Các nguy cơ và điểm yếu an toàn mới.
- Tăng sự phụ thuộc giữa hệ thống và mạng.
- Hợp đồng, pháp luật, nghĩa vụ và các giới hạn và phát triển hoạt động nghiệp vụ.
- Thiết lập các mô hình trao đổi thông tin phù hợp.
- Phối hợp quy trình tấn công và phản ứng.
- Quản trị liên tục.

Trao đổi thông tin an toàn và dẻo dai giữa các thành viên cộng đồng phải bao gồm các yếu tố sau:

- Hiểu biết và quản lý rủi ro.
- Phổ biến và trao đổi thông tin.
- Giám sát.

Ba yếu tố này phải thực hiện với các giá trị cụ thể của chúng, chúng được liên kết chặt chẽ và bổ sung lẫn nhau.

Rất khó để phát triển sự tin cậy giữa các thành viên trong một cộng đồng chia sẻ thông tin mà không có mối quan hệ cá nhân với các đại diện của các thành viên khác. Các cá nhân cần gặp trực tiếp để xây dựng mối quan hệ và tạo ra sự tin tưởng cho các cá nhân khác. Rất khó để tạo ra sự tin cậy mà chỉ sử dụng các công nghệ trao đổi thông tin từ xa. Và cũng thật khó để thiết lập các cơ chế cung cấp sự tin tưởng về mức độ tin cậy của nguồn thông tin trong khi tiếp tục giữ ẩn danh các nguồn này. Các cá nhân sẽ thoải mái hơn nếu họ tin tưởng định danh của họ được giữ bí mật.

Một cộng đồng chia sẻ thông tin có hiệu lực ngay cả khi không phải tất cả các thành viên chia sẻ mọi thông tin cho nhau. Các cơ chế phổ biến phải đủ linh hoạt để cho phép việc phổ biến được giới hạn trong các thành viên cụ thể của cộng đồng, hoặc bị giới hạn theo chủ đề.

Cuối cùng, khi chia sẻ thông tin giữa các cộng đồng (ví dụ, trong trao đổi thông tin liên ngành) thì các bộ phận điều khiển cổng kết nối giữa các cộng đồng phải đối diện với các khó khăn đặc biệt. Các nguồn thông tin không cần thiết phải biết về thành viên của các cộng đồng khác và phải dựa vào các giao diện để bảo vệ ẩn danh và các điều kiện phát hành khác. Các bộ phận điều khiển cổng kết nối có thể thiếu kiến thức chuyên môn để nhận ra khi nào một thông tin cộng đồng không nên được truyền đi nữa. Các vấn đề này là điển hình nhất là trong trao đổi thông tin quốc tế chứ không phải trong trao đổi thông tin liên ngành.

A.3 Các lợi ích tiềm ẩn

Chia sẻ thông tin nhạy cảm với các thành viên khác chắc chắn làm tăng rủi ro tiềm ẩn của việc bị lộ thông tin. Để một cộng đồng hoạt động hiệu quả, các rủi ro này phải được quản lý và giảm thiểu, lợi ích phải lớn hơn nhiều so với rủi ro tổn đọng đã được chấp nhận.

Các lợi ích tiềm ẩn của việc chia sẻ thông tin nhạy cảm bao gồm:

- Cảnh báo sớm khi có bất kỳ sự thay đổi quan trọng nào về tình trạng rủi ro, ví dụ các nguy cơ mới, xu hướng tấn công được cập nhật, các điểm yếu mới được phát hiện...
- Cải tiến an toàn thông tin thông qua việc chia sẻ kinh nghiệm tốt nhất.
- Truy cập đến các thông tin có ích không có sẵn từ mọi nguồn công khai.
- Tiết kiệm chi phí thông qua việc loại bỏ các cố gắng bị trùng lặp.
- Đánh giá rủi ro tốt hơn thông qua các hiểu biết nhiều hơn về nguy cơ và điểm yếu.
- Tổ chức tốt hơn việc duy trì và can thiệp từ thông tin liên quan đến các hoạt động tương tự tại các tổ chức khác.
- Chuẩn bị tốt hơn cho các sự cố an toàn thông tin.
- Chấm điểm cho các biện pháp an toàn thông tin giữa các tổ chức tương tự.
- Trách nhiệm xã hội chung.

- Tuân thủ các yêu cầu pháp luật hoặc chính sách chung.

Một điều quan trọng là các quy trình giám sát và soát xét cộng đồng xác định các lợi ích cụ thể (và các nhược điểm) từ việc làm thành viên công đồng, để các thành viên sử dụng trong việc đánh giá tính liên tục của thành viên cộng đồng.

A.4 Khả năng áp dụng

Thông tin có thể được trao đổi giữa nhiều loại hình tổ chức, quy mô lớn hoặc nhỏ, nhà nước hoặc tư nhân, tương đồng hoặc đa dạng. Tuy nhiên, các lợi ích lớn nhất thường có được từ các tổ chức hoạt động trong cùng ngành nghề hoặc có cùng các mục tiêu chung, các tổ chức này cũng có cùng các dạng rủi ro an toàn thông tin đặc thù của ngành nghề.

Cũng có thể đạt được lợi ích lớn khi chia sẻ thông tin giữa các ngành nghề, qua việc xác định các cộng đồng dựa trên các đặc tính khác (như vị trí địa lý) hay qua cách chia sẻ thông tin với các cộng đồng chia sẻ thông tin thuộc ngành nghề khác trong một cấu trúc phân cấp của các cộng đồng.

A.5 Xác định và vận hành một cộng đồng chia sẻ thông tin

Cộng đồng chia sẻ thông tin phải xác định các quy tắc và điều kiện quản trị hoạt động của nó. Các quy tắc và điều kiện như vậy phải bao gồm:

- Các quy tắc và điều kiện quản trị thành viên của cộng đồng chia sẻ thông tin và tổ chức nội bộ của nó;
- Mục tiêu của cộng đồng chia sẻ thông tin và các lợi ích dự tính cho các thành viên;
- Thủ tục để các thành viên tham gia và dời khỏi cộng đồng chia sẻ thông tin;
- Các quy tắc và điều kiện quản trị các quy trình cộng đồng tập trung hoặc các thực thể như TICE hoặc WARP;
- Các quy tắc và điều kiện liên quan đến nghĩa vụ của các thành viên cộng đồng, các quy trình và quy định về trục xuất, kỷ luật;
- Các quy tắc rõ ràng về cách thức để các thành viên có thể sử dụng và truyền đưa thông tin chia sẻ;
- Các điều kiện và nghĩa vụ về tài chính, pháp luật khác của thành viên cộng đồng.

Các quy tắc và điều kiện của cộng đồng chia sẻ thông tin cũng phải:

- Đảm bảo rằng thông tin được trao đổi theo một phương pháp hiệu quả và an toàn mà vẫn đảm bảo bên nhận đích nhận được dữ liệu đúng lúc;
- Chỉ ra và phân mức ưu tiên các kênh truyền được lựa chọn và có tiềm năng, theo quan điểm sử dụng ưu tiên để truyền dữ liệu cho từng loại thông tin xác định;
- Chỉ ra các hoàn cảnh cho phép mà theo đó thông tin được truyền tới các thành viên của cộng đồng;
- Chỉ ra các thuộc tính phổ biến và bảo vệ dữ liệu tùy chọn và bắt buộc phù hợp với phương tiện trao đổi thông tin cộng đồng;
- Chỉ ra các quy tắc rõ ràng để giải thích các thuộc tính phổ biến và bảo vệ dữ liệu liên quan đến việc phổ biến thông tin;

- Yêu cầu các thành viên cung cấp thông tin phản hồi thích hợp, kịp thời và chính xác về thông tin nhận được;
- Nếu có thể, xác định hoặc thích ứng với các tiêu chuẩn thông điệp hiện có cho việc trao đổi thông tin.

Các quy tắc trao đổi thông tin phải xác định tần suất trao đổi, các yêu cầu đối với việc xác nhận bên nhận. Các quy tắc phải nhận biết việc các thành viên của cộng đồng chia sẻ thông tin có các mức độ tin cậy khác nhau đối với các thành viên khác của cộng đồng. Độ tin cậy này có thể thay đổi theo thời gian và hoàn cảnh.

Các kênh trao đổi thông tin thích hợp nên được lựa chọn bằng cách đánh giá độ mạnh, yếu của chúng khi phân phát các loại thông tin xác định được hỗ trợ bởi cộng đồng, dựa trên các tiêu chí như độc giả đích, các thuộc tính của thông tin được phân phát, kênh tiếp cận và tần suất, và chi phí. Ví dụ về các kênh trao đổi thông tin có thể là thông điệp điện tử, các site công cộng hoặc chỉ cho thành viên, các cuộc gọi điện thoại hội nghị hoặc hai chiều, thư tay qua dịch vụ bưu chính công cộng hoặc các cuộc họp trực tiếp. Ảnh hưởng của một trao đổi thông tin đến độc giả đích của nó phụ thuộc vào hiệu lực của kênh trong tiếp cận độc giả, độ tin cậy của nó với độc giả và sự thích hợp của vấn đề hoặc chủ đề thông tin.

Không phải tất cả thông tin đều được yêu cầu trao đổi trong thời gian thực; một vài thông tin có thể được chia sẻ tốt nhất thông qua cách liên lạc thường lệ.

Các ví dụ về thông tin được phân phát đến các thành viên cộng đồng là các báo cáo tức thì về sự cố được phát hiện phù hợp hồ sơ đã xác định trước, các báo cáo thường xuyên tại đúng thời điểm, các phản hồi đối với yêu cầu thông tin từ các thành viên khác. Các ví dụ về thuộc tính phổ biến và bảo vệ dữ liệu là yêu cầu che dấu nguồn gốc thông tin, độ nhạy cảm của thông tin hoặc đánh giá của bên khởi tạo về sự tin cậy của thông tin. Một ví dụ về bộ quy tắc nhằm giải thích các thuộc tính phổ biến và bảo vệ dữ liệu là Giao thức đèn giao thông (TLP) – xem Phụ lục C. Các thuộc tính có thể khác nhau tùy thuộc vào kênh trao đổi thông tin được sử dụng. Ví dụ, các thuộc tính bắt buộc dành cho phát hành bưu chính cũng có thể khác so với thư điện tử.

Với bất kỳ giải pháp kỹ thuật nào được lựa chọn và triển khai, chúng phải phù hợp với các loại thông tin được chia sẻ trong cộng đồng và thích hợp với các mục tiêu xác định của cộng đồng. Tiếp xúc trực tiếp sẽ xây dựng sự tin cậy và có thể là một cách cần thiết để phát triển cộng đồng bằng cách mời các thành viên mới. Tuy nhiên, sự tồn tại của một nền tảng tin cậy hoặc cấu trúc chia sẻ khác có thể khuyến khích thành viên của chính nó.

A.6 Các thỏa thuận về trao đổi thông tin

Cộng đồng chia sẻ thông tin nên xác định thỏa thuận trao đổi thông tin, cơ chế và quy trình quản trị các phương tiện trao đổi thông tin cộng đồng. Thông tin có thể trao đổi bằng thư tay, hoặc bằng lời nói tại các cuộc họp trực tiếp, cũng như thư điện tử. Thông tin có thể trao đổi chính thức, sử dụng các dạng cho trước và các giao thức, hoặc không chính thức qua các cách phi cấu trúc. Thông tin có thể trao đổi thường xuyên hoặc theo tình huống.Thông tin cũng có thể trao đổi bằng các phương tiện trao đổi thông tin ngang hàng, phân cấp hoặc thông qua một thực thể hỗ trợ tập trung như TICE hoặc WARP.

Thỏa thuận trao đổi thông tin có thể cho phép thông tin được chia sẻ chỉ với các thành viên được lựa chọn trong cộng đồng chia sẻ thông tin, hoặc chỉ thực hiện chia sẻ ẩn danh. Tương tự như vậy, kể cả khi có các phương tiện báo cáo tập trung, nó có thể cho phép chuyển thông tin trực tiếp giữa các thành viên một cách trực tiếp.

Thỏa thuận trao đổi thông tin nên chỉ ra các loại thông tin có thể trao đổi giữa các thành viên của cộng đồng, để đảm bảo sự hiểu biết chung của các thành viên cộng đồng đối với thông tin trao đổi và đảm bảo rằng các thành viên thiết kế và triển khai các biện pháp an ninh phù hợp với mức độ nhạy cảm của thông tin được chia sẻ.

Ví dụ về các loại thông tin có thể truyền:

- "Các thông báo", tương ứng với các sự kiện có giải thích thông tin;
- "Các cảnh báo và báo động", tương ứng với các sự kiện liên quan đến IT hoặc vật lý không giải thích thông tin, các tấn công từ chối dịch vụ, quét và giả mạo;
- "Xử lý sự cố", tương ứng với việc phân tích, hỗ trợ ứng phó và điều phối ứng phó liên quan đến các sự cố thực tế;
- "Các yêu cầu thông tin", tương ứng với việc yêu cầu thông tin từ một thành viên của cộng đồng tới tất cả hoặc một vài thành viên khác của cộng đồng.
- "Các dự đoán chất lượng dịch vụ", cung cấp thông tin về hiệu lực và độ tin cậy được dự đoán của các kênh trao đổi thông tin cộng đồng.

Chia sẻ quá nhiều hoặc quá ít thông tin cũng không tốt; trừ khi có một phương pháp lọc dữ liệu thích hợp. Nếu việc xây dựng xu hướng thông tin được xem là một lợi ích của việc chia sẻ thì phải có một phương pháp phân biệt thông tin "hành động ngay" có ưu tiên cao với thông tin "dành cho mục đích lưu trữ" có ưu tiên thấp.

A.7 Các yếu tố thành công

Các cộng đồng hiệu quả sẽ có các lợi ích được chia sẻ thực sự, mặc dù tất cả thành viên có thể quan tâm đến mọi khía cạnh. Ví dụ, các công ty viễn thông cố định không quan tâm đến các vấn đề không dây, nhưng sẽ quan tâm như các công ty di động trong việc xác định các cuộc gọi giả.

Các thành viên của cộng đồng hiệu quả sẽ sử dụng quyền đại diện để có thể xử lý các việc nội bộ.

Cộng đồng hiệu quả có thể giới hạn hoặc nếu không cũng hạn chế thành viên, ví dụ để đảm bảo sự đại diện công bằng trong việc ra quyết định.

A.8 Phạm vi của hệ thống quản lý an toàn thông tin đối với một cộng đồng chia sẻ thông tin

Phạm vi của hệ thống quản lý an toàn thông tin đối với một cộng đồng chia sẻ thông tin nên bao gồm:

- Tất cả các quy trình được sử dụng cho trao đổi thông tin giữa các thành viên cộng đồng, bao gồm cả các thành viên trung gian;
- Việc lưu trữ thông tin có liên quan trong suốt quy trình trao đổi thông tin;
- Các quy trình được triển khai bởi các thành viên có liên quan để gửi và nhận thông tin chia sẻ;
- Các quy trình được triển khai bởi các thành viên cộng đồng trong việc loại bỏ thông tin chia sẻ.

Phạm vi không nên bao gồm các quy trình quản lý an toàn thông tin được triển khai bởi các thành viên cộng đồng có liên quan để quản lý an toàn thông tin của chính họ, và có thể được bao phủ bởi các hệ

thống quản lý an toàn thông tin khác, ngoại trừ những hạn chế đặt ra cho bản chất của thông tin chia sẻ và các giao diện của hệ thống chia sẻ thông tin. Hệ thống quản lý an toàn thông tin có thể quản lý tập trung bởi các thực thể hỗ trợ như TICE hoặc WARP, hoặc nó có thể được quản lý hợp tác bởi các thành viên cộng đồng.

Phụ lục B

(Tham khảo)

Thiết lập sự tin cậy trong trao đổi thông tin

B.1 Độ tin cậy của thông báo

Độ tin cậy của bên nhận về một thông báo nhận được chủ yếu dựa trên mức độ tin cậy của nguồn gốc thông điệp, và mức độ tin cậy của chính nguồn đối với thông báo.

Điều này có thể được đóng gói trong mô mình "5-5" được sử dụng trong thực thi luật và các cộng đồng thông tin:

- {A - E} Mức giảm dần độ tin cậy của nguồn gốc;
- {1 - 5} Mức giảm dần độ tin cậy của nguồn vào thông tin.

Như vậy thông tin "A-1" được xem như sự tin cậy tuyệt đối, trong khi thông tin "E-5" thường bị loại bỏ.

Nhưng tất nhiên trong thực tế có rất ít thông tin "A-1". Có lẽ ví dụ được biết đến tốt nhất, trong đó cả nguồn và thông tin đều được xem là tin cậy tuyệt đối nhưng đôi khi có thể vẫn có lỗi, là việc sử dụng hệ thống định vị vệ tinh toàn cầu GPS, khi có trường hợp hệ thống lập kế hoạch tuyến hoặc ánh xạ bị lỗi vô tình khiến các phương tiện vận chuyển lớn bị chỉ dẫn sai đi xuống các đường hẻm nhỏ.

Vấn đề xa hơn liên quan tới độ tin cậy trong các thông báo là rủi ro về tăng cường bè ngoài. Có một khuynh hướng nội tại – hoặc giả định cơ bản – rằng nhiều trường hợp thông tin giống nhau từ các nguồn có vẻ khác nhau là sự khẳng định.

Trong một số chừng mực, điều này hiển nhiên là đúng, nhưng độ tin cậy như vậy không thể được lấy một cách quá dập khuôn, và cụ thể, bất kỳ mô hình toán học về độ tin cậy như vậy không nên gán trọng số tuyến tính cho các trường hợp bổ sung.

B.2 Hỗ trợ kỹ thuật

B.2.1 Giới thiệu

Có một vài kỹ thuật gần đây được phát triển để hỗ trợ độ tin cậy của thông tin được cung cấp bằng hình thức điện tử được tạo bởi các thực thể chưa biết hoặc không quen thuộc. Các kỹ thuật như vậy phù hợp với khái niệm "Web 2.0" [4]. Web 2.0 không phải là một tập hợp các kỹ thuật- mà nó là một khái niệm liên quan đến trao đổi thông tin xã hội và kết hợp các ý tưởng như sử dụng Web như một nền tảng, sử dụng để thu thập.

Hai khía cạnh của Web 2.0 đặc biệt liên quan đến tiêu chuẩn này:

- Giả ẩn danh;
- Các hệ thống uy tín, cũng gọi là cơ cấu uy tín.

B.2.2 Ẩn danh và giả ẩn danh

Các nguồn và bên nhận thông tin có thể mong muốn duy trì ẩn danh với nhiều lý do. Hiệu lực của ẩn danh thực sự đạt được phụ thuộc vào hiểu biết về bối cảnh ví dụ mức độ hiểu rõ về toàn bộ hệ thống thông điệp. Trong các hệ thống lớn, phân tán, một số người tham gia có thể không biết đầy đủ về hệ thống thông điệp, và trong rất nhiều trường hợp thì bối cảnh của thông điệp sẽ thay đổi theo thời gian.

Khái niệm ẩn danh gắn chặt với với khái niệm **không có khả năng liên kết**, trong đó các hạng mục quan tâm không được liên kết ít nhiều so với khi chúng được liên kết từ các hiểu biết suy diễn.

Mối quan hệ ẩn danh ngụ ý mức độ không thể truy vết để xem ai trao đổi thông tin với người nào do không có khả năng liên kết bên khởi tạo với một hoặc nhiều bên nhận.

Không có khả năng quan sát là không thể quan sát khi nào bên khởi tạo gửi và bên nhận nhận.

Không có khả năng quan sát mối quan hệ nghĩa là không thể quan sát trao đổi thông tin giữa bên khởi tạo và bên nhận.

Ký biệt hiệu liên quan đến sự thay thế tên của một cá nhân và các đặc tính định danh khác bằng một nhãn, để bảo vệ danh tính của của đối tượng dữ liệu hoặc ít nhất cũng để khó xác định. Ký biệt hiệu là một trạng thái sử dụng biệt hiệu như một nhãn định danh.

Đối với khía cạnh mức độ khả năng liên kết, có thể có một vài loại biệt hiệu sau:

a) Biệt hiệu cá nhân: Biệt hiệu cá nhân là một sự thay thế cho tên chủ sở hữu được coi như đại diện cho số định danh chủ sở hữu. Nó có thể được dùng trong tất cả các bối cảnh, ví dụ một số chứng minh thư nhân dân, số an ninh xã hội, DNA, nickname, nghệ danh của diễn viên, hoặc một số điện thoại.

b) Biệt hiệu vai trò: sử dụng biệt hiệu vai trò được giới hạn trong các vai trò cụ thể, ví dụ: một biệt hiệu của khách hoặc tài khoản Internet được sử dụng cho nhiều thuyết minh của cùng một vai trò "người dùng internet". Cùng biệt hiệu vai trò có thể được sử dụng với các đối tác trao đổi thông tin khác nhau.

c) Biệt hiệu quan hệ: ứng với mỗi đối tác trao đổi thông tin thì sử dụng một biệt hiệu khác nhau. Điều này có nghĩa là các đối tác trao đổi thông tin khác nhau không thể nói rằng họ đang trao đổi thông tin với cùng một người dùng.

d) Biệt hiệu vai trò-quan hệ: ứng với mỗi vai trò và với mỗi đối tác trao đổi thông tin thì sử dụng một biệt hiệu vai trò-quan hệ khác nhau. Điều này có nghĩa là đối tác trao đổi thông tin không cần biết có hai biệt hiệu được sử dụng cho các vai trò khác nhau thuộc về cùng một chủ sở hữu. Mặt khác, hai đối tác trao đổi thông tin khác nhau tương tác với cùng một người dùng trong cùng một vai trò cũng không biết các biệt hiệu là của cùng một người.

VÍ DỤ: Giả sử một nguồn thông tin thường sử dụng tên "Wool" khi trao đổi thông tin không trong miền công cộng tới Bernstein và "Touched" khi trao đổi cùng thông tin như vậy đến Woolward. Bernstein sau đó nhận thông tin về một chủ đề mới từ "Deep Throat" và Woolward từ "Watergate". Bernstein và Woolward không biết "Deep Throat" và "Watergate" có phải là cùng một người hay không và cũng không biết "Deep Throat" có phải là "Wool" hay "Touched", hoặc cả hai.

e) Biệt hiệu giao dịch: Đối với mỗi giao dịch, một biệt hiệu giao dịch không có khả năng liên kết đến nhiều biệt hiệu giao dịch khác và ít nhất không thể bắt đầu liên kết với bất kỳ biệt hiệu giao dịch nào đang sử dụng, ví dụ số giao dịch đã được tạo ngẫu nhiên cho ngân hàng trực tuyến. Do đó, các biệt hiệu giao dịch có thể được sử dụng để nhận ra độ mạnh của ẩn danh.

Nói chung, ẩn danh bằng cả biệt hiệu vai trò và biệt hiệu quan hệ tốt hơn ẩn danh bằng biệt hiệu cá nhân. Độ mạnh của ẩn danh tăng lên với việc áp dụng ẩn danh vai trò-quan hệ, việc sử dụng ẩn danh được hạn chế cho cả cùng vai trò và cùng mối quan hệ.

Ẩn danh sẽ mạnh hơn nếu càng ít dữ liệu cá nhân của chủ sở hữu biệt hiệu có thể được liên kết đến biệt hiệu.

B.2.3 Cơ chế đánh giá uy tín

Khái niệm về công cụ danh tiếng hình thành nên cơ sở của nhiều phương tiện truyền thông xã hội và mạng xã hội trên Web. Các công cụ danh tiếng được dùng để lọc các thông tin có liên quan nhất và chúng trở nên thích hợp hơn khi số lượng và sự đa dạng của thông tin tăng lên đáng kể.

Một công cụ danh tiếng có thể được định nghĩa như một tập chính thức các chính sách và thủ tục được sử dụng để tính điểm danh tiếng cho một cá nhân dựa trên hoạt động quá khứ của họ. Trong thế giới trực tuyến, một công cụ danh tiếng được gắn với ý tưởng về dấu chân số. Dấu chân số lần theo hoạt động của ai đó trong môi trường số.

Báo cáo tín nhiệm và các cơ chế khác luôn cung cấp công cụ để định lượng danh tiếng – nhưng một so sánh của các cơ chế Web về danh tiếng (như các hệ số đánh giá Internet) với các báo cáo tín nhiệm truyền thống là đáng quan tâm. Khi chúng ta giao dịch trên web (mua, bán, mượn, trả lại) chúng ta tạo ra các dữ liệu số. Dữ liệu này được chụp lại bởi người khác (như các cơ quan đánh giá hệ số tín nhiệm) và mặc dù nó thuộc về chúng ta - nó "được sở hữu" bởi cơ quan đánh giá hệ số tín nhiệm (và thực sự chúng ta phải trả phí để tiếp cận đến nó).

Có nhiều hình thức công cụ danh tiếng được làm tinh tế hơn như công cụ danh tiếng eBay. Công cụ eBay khác ở điểm tín nhiệm bởi vì nó minh bạch. Mọi thông tin phản hồi (bao gồm thông tin phản hồi tiêu cực) được phản hồi tới từng cá nhân về người nào đã viết bình luận – do đó đưa ra cơ hội để phản kháng.

Một công cụ danh tiếng có thể được sử dụng để tăng độ tin cậy bằng cách kết hợp các nhận thức từ nguồn gốc cộng đồng rộng lớn thông qua các nhiệm vụ như xác nhận hợp lệ nguồn thông tin mới, xác nhận nguồn nội dung, cảnh báo thời gian thực như tìm kiếm Twitter và các cảnh báo Google, củng cố độ tin cậy từ các nguồn vô danh, bổ sung tìm kiếm bằng quan niệm bên ngoài, mang các ý kiến mới/bên ngoài đến miền chia sẻ tin cậy, dự báo các cơ hội và nguy cơ từ các nguồn bên ngoài... Tuy nhiên, nhiều kỹ thuật Web 2.0 hiện tại (giống wiki) có giới hạn trong việc xây dựng độ tin cậy do chúng không có các mô hình nội bộ tin cậy đủ mạnh.

B.3 Truy nhập thông tin tin cậy

Các khái niệm làm trụ cột cho sự tin cậy về thực chất có bản chất chủ quan hơn là khách quan, và như vậy không cần thiết tuân theo một biểu diễn máy móc. Tuy nhiên, cách tiếp cận Pareto [5] có thể được dùng để giải quyết vấn đề: một giải pháp khi phần lớn kết quả mong đợi có thể đạt được với một khối lượng nỗ lực tương đối nhỏ, mặc dù bất kỳ cố gắng để hoàn thiện mô hình sẽ yêu cầu một khối lượng nỗ lực không cân xứng.

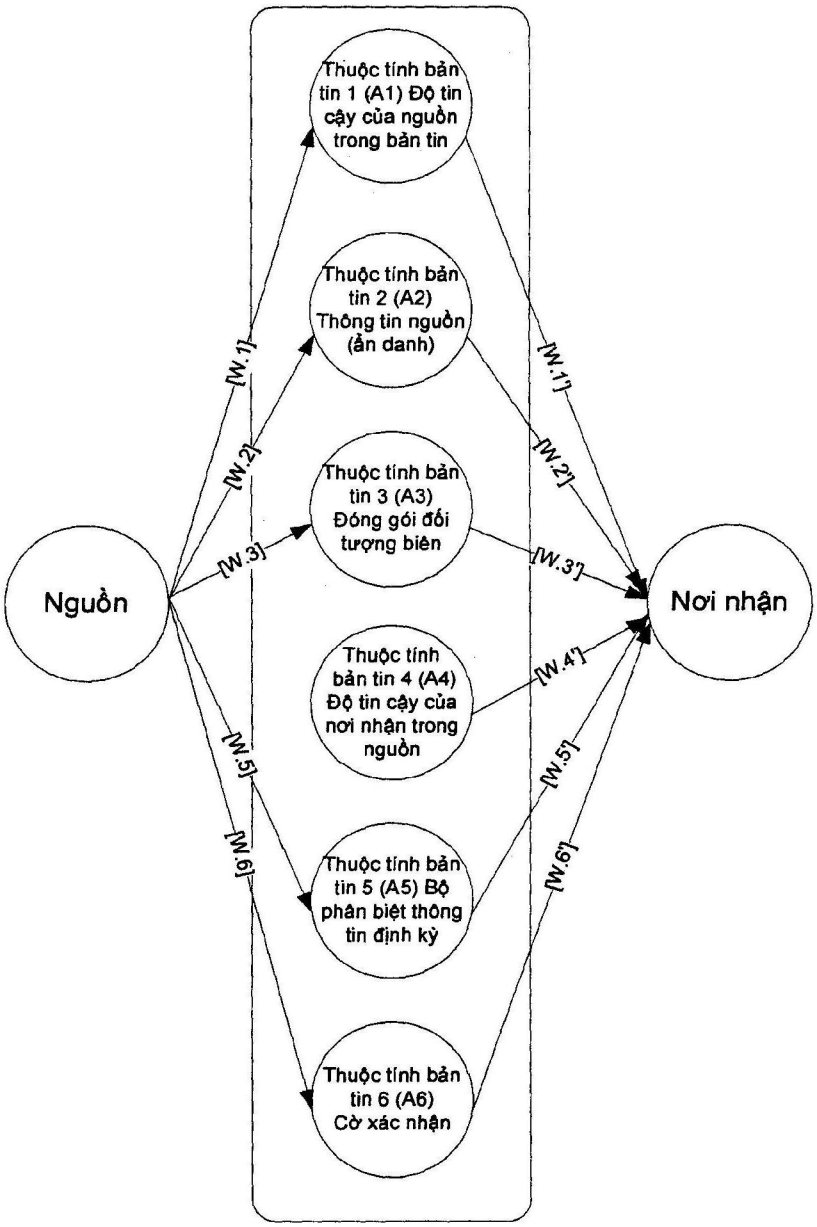
Các thành phần của một cách tiếp cận như vậy có thể là:

a) Bên khởi tạo thông tin nên gán một mức độ tin cậy cho thông tin khi họ phát hành. Sự hữu dụng của cách tiếp cận này đã được xác nhận hợp lệ bởi Trung tâm bảo vệ cơ sở hạ tầng quốc gia Vương quốc Anh, trong đó phương thức này được sử dụng để tự động mô tả sơ lược và phổ biến thông tin cảnh báo tới nhiều hình thức cộng đồng chia sẻ thông tin khác nhau.

b) Tất cả các thông tin được xác định rõ ràng với nguồn gốc của nó, lý tưởng nhất là sử dụng một định dạng dữ liệu có cấu trúc.

c) Mặc dù có khái niệm về định danh nguồn gốc, cũng nên hỗ trợ báo cáo ẩn danh, như kinh nghiệm từ thế giới an toàn đã chỉ ra rằng cung cấp các ẩn danh làm tăng một cách đáng kể việc chia sẻ thông tin.

d) Khái niệm về một Đối tượng Biên được sử dụng để đóng gói nội dung của bất kỳ thông tin trao đổi. Các Đối tượng Biên là các tập hợp có cấu trúc của thông tin có mức độ công nhận lẫn nhau trong cộng đồng quan tâm, và cho phép trao đổi thông tin thông qua các biên giới về miền và ngôn ngữ: thành công của các sáng kiến như thông báo Liệt kê các điểm yếu chung (CVE) của Mitre đã đóng góp một phần cho việc được chấp nhận thực tế như là những Đối tượng Biên.



Khóa:

W.n phán quyết của bên khởi tạo về độ tin cậy của thông tin trong bản tin

W.n' phán quyết của bên nhận về độ tin cậy của thông tin trong bản tin

Hình B.1 – Đánh giá độ tin cậy của nội dung bản tin

e) Cả bên khởi tạo và bên nhận trong trao đổi thông tin tin cậy nên cung cấp một đánh giá về việc có hay không, và bao nhiêu lần, thông tin này hỗ trợ cho nội dung đã nhận được trước đó: mặc dù có một vài khả năng tự động phân tích cú pháp thông tin cho mục đích này, cần phải nhận thấy là tự động phân tích cú pháp cho bản tin cho các mục đích như vậy trong trình độ kỹ thuật hiện tại là không đáng tin. Để giảm thiểu rủi ro của việc tăng cường ở bề ngoài, cần áp dụng một Hàm Phân bố Tích lũy trả về kết quả giảm dần để áp dụng đếm số lượng các trường hợp trước đó, có nghĩa là giá trị trọng số của thông tin bổ sung giảm khi số đếm tăng.

f) Nguồn hoặc bên nhận gắn một cờ để xem thông tin có được xác nhận độc lập hay không, để bảo vệ chống lại sự cất giữ thông tin có ích. Sự cất giữ này làm tăng thêm sự hoài nghi về thông tin nhận được.

g) Bên nhận thông tin nên gán một đánh giá chủ quan cho nguồn gốc, dựa trên quy tắc của mô hình "5-5" (xem B.1).

Khi được gắn trọng số phù hợp, các tiêu chí như vậy có thể cho phép các thành viên của cộng đồng chia sẻ thông tin định lượng độ tin cậy của họ đối với thông tin mà họ nhận được từ các thành viên khác của cộng đồng. Điều này được minh họa trong Hình B.1.

Phụ lục C

(Tham khảo)

Giao thức đèn giao thông

Phụ lục này mô tả giao thức đèn giao thông, một cơ chế được sử dụng rộng rãi trong các cộng đồng chia sẻ thông tin để chỉ thị việc phổ biến thông tin được cho phép. Mặc dù khái niệm cơ bản này được hiểu rộng rãi, có một số biến thể với khác biệt nhỏ được sử dụng. Mô tả này được thực hiện theo Hướng dẫn thực hành tốt cho trao đổi thông tin bảo mật trong mạng được phát hành bởi Cơ quan an toàn mạng và thông tin Châu Âu (ENISA) [6]. Khái niệm ban đầu được phát triển bởi Trung tâm bảo vệ cơ sở hạ tầng quốc gia Vương quốc Anh (CPNI).

Giao thức đèn giao thông (TLP) được tạo ra để khuyến khích chia sẻ nhiều hơn các thông tin nhạy cảm giữa các tổ chức. Bên khởi tạo cần báo hiệu họ muốn thông tin của họ được phân phát tới các đối tượng nhận trung gian một cách rộng rãi như thế nào.

TLP dựa trên khái niệm thông tin ghi nhãn bên khởi tạo với một trong bốn màu để chỉ thị việc phổ biến tiếp theo của thông tin, nếu có, có thể được xử lý bởi bên nhận. Bên nhận phải tham khảo ý kiến bên khởi tạo nếu được yêu cầu phổ biến rộng rãi hơn.

Bốn màu và ý nghĩa của chúng như sau:

- Màu Đỏ - Chỉ cho cá nhân bên nhận có tên. Ví dụ trong bối cảnh của một cuộc họp, thông tin màu Đỏ được giới hạn cho những người có mặt trong cuộc họp. Trong phần lớn các trường hợp, thông tin màu Đỏ được truyền bằng lời nói hoặc cho bên nhận.
- Màu Vàng - Phổ biến giới hạn. Bên nhận có thể chia sẻ thông tin màu Vàng với người khác trong tổ chức của họ, nhưng chỉ trên cơ sở "cần phải biết". Bên khởi tạo phải chỉ ra giới hạn nhắm tới cho việc chia sẻ này.
- Màu Xanh – Cộng đồng rộng. Thông tin thuộc thể loại này có thể được phát hành rộng rãi trong một cộng đồng cụ thể. Tuy nhiên, thông tin có thể không được phát hành hoặc đăng trên Internet, cũng như phát hành bên ngoài cộng đồng.
- Màu Trắng – Không giới hạn. Tùy theo các quy định chuẩn về bản quyền, thông tin màu Trắng có thể tự do phổ biến mà không bị hạn chế.

Thông tin nhạy cảm được cung cấp bởi bên khởi tạo nào cũng nên được đánh dấu tại thời điểm tiết lộ thông tin phù hợp với TLP. Tất cả thông tin nhạy cảm được xem như thông tin màu Vàng trừ trường hợp được phát biểu hoặc viết khác đi. Tuy nhiên, theo mặc định hoặc trừ khi có quy định khác cụ thể tại thời điểm tiết lộ thông tin, định danh về nguồn gốc của thông tin nhạy cảm luôn là màu Đỏ.

TLP cũng có thể tương thích để sử dụng trong một tổ chức, ví dụ nơi chỉ có một vài cá nhân được cấp phép truy nhập đầy đủ tới tất cả thông tin được chia sẻ. Xem Hình 2.

Phụ lục D

(Tham khảo)

Các mô hình tổ chức một cộng đồng chia sẻ thông tin

D.1 Giới thiệu

Có một vài cách tổ chức cộng đồng chia sẻ thông tin, từ sự kết hợp lỏng lẻo của các đối tác ngang hàng đến các tổ chức có pháp nhân được quản lý tập trung và cấu trúc ở mức cao. Phụ lục này mô tả hai dạng tổ chức cộng đồng có thể gặp trong thực tế và hỗ trợ quản lý an toàn thông tin có hiệu quả.

D.2 Thực thể truyền thông thông tin tin cậy

D.2.1 Giới thiệu

Thực thể truyền thông thông tin tin cậy là một tổ chức tự trị hỗ trợ trao đổi thông tin giữa các thành viên của một cộng đồng chia sẻ thông tin bằng cách hành động như là một cổng thông tin và điều phối tập trung. Nó có thể trở thành thành phần cốt lõi của một hệ thống quản lý an toàn thông tin hiệu lực cho trao đổi thông tin liên tổ chức, liên ngành. TICE có thể đảm bảo trao đổi thông tin an toàn và hiệu lực giữa các thành viên của cộng đồng chia sẻ thông tin và trợ giúp cho họ trong viiệc giám sát, phân tích và quản lý hiệu quả các phản ứng với sự cố và rủi ro.

Thực thể truyền thông thông tin tin cậy (TICE) bao gồm một nhóm các đối tượng chuyên gia có nghiệp vụ chính là:

- Đảm bảo trao đổi thông tin thích hợp giữa TICE và các thành viên cộng đồng;
- Phân tích và ứng phó với các sự cố an toàn thông tin;
- Xử lý sự cố và hỗ trợ các thành viên cộng đồng khôi phục từ vi phạm;
- Cung cấp cho các thành viên cộng đồng nhận thức về an toàn thông tin có liên quan đến bằng cách:
    - Đưa ra tư vấn về các điểm yếu trong các thiết bị đang sử dụng,
    - Thông báo cho đại diện của các thành viên cộng đồng về các lỗ hổng và các virus đang lợi dụng các lỗi này, do đó các thành viên được phép có thể thực hiện hiệu quả các phần cập nhật và vá lỗi.

TICE có thể hành động như một trung gian tin cậy để ẩn danh nguồn hoặc người nhận thông tin chia sẻ. Điều này cho phép các thành viên giữ bí mật thông tin từ một nguồn đáng tin, mà không cần che giấu danh tính của họ hoặc đặt sự tin tưởng vào các thành viên khác được ẩn danh.

TICE có thể dựa trên hoặc phát triển từ một tổ chức đang tồn tại và đã phục vụ cộng đồng liên quan như Nhóm ứng phó sự cố an toàn thông tin (ISIRT). Tuy nhiên, ISIRT cần được mở rộng để cung cấp chủ động dịch vụ TICE cũng như các dịch vụ tương tác nói chung được cung cấp bởi ISIRT.

D.2.2 Xem xét việc tổ chức TICE

D.2.2.1 Các đối tượng chuyên gia

Cấu trúc nên bao gồm các chuyên môn ngành và công cộng để đảm bảo sự tham gia của đúng người với các kỹ năng thích hợp, để đảm bảo các chuyên gia có thể quyết định sự phù hợp của bất kỳ thông tin trao đổi và bối cảnh hạ tầng thông tin liên quan.

Các chuyên gia được sử dụng để thực hiện phân tích, đặc biệt trong các lĩnh vực sau (nhưng không giới hạn):

- Quản lý nghiệp vụ;
- Cơ sở hạ tầng và an toàn IT;
- Vận hành;
- Quy định nội bộ;
- Quy định pháp lý.

Các chuyên gia có thể làm việc bán thời gian hoặc toàn thời gian và có thể được làm tại khu vực trung tâm, khu vực vận hành hoặc nơi kết hợp.

D.2.2.2 Cấu trúc tổ chức

Một TICE điển hình nên bao gồm tối thiểu các chức năng sau:

- Ban điều hành (cần thiết, chịu trách nhiệm đối với quản lý chiến lược của TICE và mối quan hệ với các thành viên cộng đồng).
- Nhóm kỹ thuật vận hành (cần thiết, chịu trách nhiệm phân tích các vấn đề rủi ro chuyên môn và kỹ thuật và quyết định áp dụng thích hợp cho các bản vá hoặc thay đổi).
- Chuyên viên kỹ thuật vận hành (tùy chọn, khuyến nghị có để cải tiến sự hiểu biết của TICE về môi trường hoạt động hoặc tài nguyên liên quan đến mức độ tập hợp thiết bị (khu vực nội bộ)).
- Chuyên gia pháp lý (tùy chọn, khuyến nghị có đặc biệt trong giai đoạn bắt đầu của TICE để giảm nhẹ các vấn đề về pháp lý).
- Chuyên gia truyền thông (tùy chọn, khuyến nghị có để tập trung vào các khó khăn về truyền đạt liên quan đến các vấn đề kỹ thuật để đưa ra những thông điệp có thể hiểu tốt hơn cho các thành viên). Các chuyên gia truyền thông có thể cung cấp thông tin phản hồi từ các thành viên cộng đồng đến nhóm kỹ thuật vận hành, hành động như một nhân viên hỗ trợ giữa hai nhóm này.

D.2.2.3 Quản lý thành viên cộng đồng

TICE nên hỗ trợ để xác thực, đánh giá, tiếp tục hiểu và quản lý thành viên cộng đồng hoặc đại diện của họ để đảm bảo mối quan hệ tin cậy đầy đủ.

D.2.2.4 Mô hình tổ chức

Mô hình tổ chức thích hợp cho TICE phụ thuộc nhiều vào kiến trúc hiện tại, bản chất của các thành viên cộng đồng và tiềm năng mở rộng và hỗ trợ đầy đủ dịch vụ của TICE. Nó cũng phụ thuộc vào khả năng truy nhập của đối tượng chuyên gia được thuê không thời hạn hoặc theo thời vụ.

Có tối thiểu ba mô hình sau:

- Mô hình độc lập: TICE độc lập hành động như một tổ chức độc lập với người quản lý và nhân viên của nó.
- Mô hình lồng ghép: TICE lồng ghép được thiết lập trong một tổ chức sử dụng tài nguyên của mình để cung cấp dịch vụ. Số lượng tài nguyên được cấp phát có thể khác nhau để hỗ trợ các hoạt động trong điều kiện bình thường hoặc tình huống đặc biệt.

- Mô hình tự nguyện: TICE tự nguyện bao gồm các chuyên gia tư vấn và hỗ trợ các tổ chức khác dựa trên cơ sở tự nguyện. Nó nên được xem xét như một cộng đồng chuyên gia, phụ thuộc nhiều vào động lực của các người tham gia.

D.2.3 Dịch vụ cốt lõi và tùy chọn của TICE

Lựa chọn dịch vụ được cung cấp bởi TICE cho các thành viên cộng đồng là một giai đoạn quan trọng và nên dựa vào các yếu tố sau:

- Phạm vi và rủi ro tương ứng của trao đổi thông tin giữa các thành viên của cộng đồng chia sẻ thông tin;
- Phạm vi, tổ chức của TICE và bản chất của cộng đồng chia sẻ thông tin.

Ngoài ra, nó phụ thuộc nhiều vào vai trò được giả định của TICE trong bối cảnh cộng đồng (hoạt động như nhân viên hỗ trợ hoặc người khởi đầu chia sẻ thông tin giữa các thành viên).

Các dịch vụ cốt lõi tiềm năng của TICE là:

- Dịch vụ phản ứng: Dịch vụ phản ứng được thiết kế để phát hiện bất kỳ khả năng tấn công thiết bị hạ tầng thông tin, phân tích và báo cáo các tấn công và ảnh hưởng của các nguy cơ, đáp ứng với các yêu cầu hỗ trợ, báo cáo sự cố đến các thành viên cộng đồng,
- Dịch vụ chủ động: Dịch vụ chủ động được thiết kế để đảm bảo và tạo điều kiện thuận lợi cho trao đổi thông tin đầy đủ bằng cách cải tiến các quy trình an ninh của cộng đồng chia sẻ thông tin và hạ tầng thông tin liên quan trước khi bất kỳ sự cố nào xuất hiện hoặc bị phát hiện. Ngoài ra, một số dịch vụ chủ động được thiết kế để cải tiến ngăn ngừa sự cố thông qua nhận thức của các thành viên, giảm ảnh hưởng và phạm vi của chúng khi xuất hiện.

Các dịch vụ TICE tùy chọn tiềm năng là:

- Dịch vụ khảo sát mã độc: Dịch vụ khảo sát mã độc được thiết kế để:
  - Phân tích tệp tin hoặc đối tượng bất kỳ được tìm thấy trên thiết bị liên quan đến hoạt động độc hại.
  - Xử lý và phổ biến kết quả cho các thành viên cộng đồng, nhà cung cấp và đối tác liên quan khác. Để ngăn chặn sớm việc lây lan mã độc và giảm bớt rủi ro.
- Dịch vụ quản lý chất lượng và an toàn thông tin: Dịch vụ quản lý chất lượng và an toàn thông tin được thiết kế để hỗ trợ các thành viên cộng đồng phân tích, quản lý nghiệp vụ liên tục và nhận thức an toàn thông tin với mục tiêu dài hạn.
- Dịch vụ ẩn danh: Dịch vụ ẩn danh được thiết kế để cho phép các thành viên cộng đồng gửi và nhận thông tin đến thành viên khác mà không cần che giấu danh tính.

D.2.4 Kết luận

Mô hình TICE là một mô hình toàn diện có cấu trúc và được kiểm soát cho chia sẻ thông tin giữa các tổ chức. Nó đặc biệt thích hợp cho các môi trường quan trọng nơi việc phân tích và chia sẻ thông tin có phân định ưu tiên và nhanh chóng là quan trọng và các thành viên hoặc chính phủ có thể hỗ trợ các chi phí của hạ tầng trung tâm.

D.3 Điểm cảnh báo, tư vấn và báo cáo

D.3.1 Giới thiệu

Mô hình Điểm cảnh báo, tư vấn và báo cáo (WARP) [7] được dùng từ năm 2003 và cung cấp cơ chế đã được chứng minh để chia sẻ thông tin nhạy cảm giữa các tổ chức trong các ngành công cộng và tư nhân.

WARP chia sẻ thông tin giữa các cá nhân hoặc tổ chức có các quan tâm giống nhau, thường là trên cơ sở tự nguyện. WARP dựa trên mối quan hệ cá nhân giữa các đại diện của các thành viên của cộng đồng chia sẻ thông tin. Một WARP điển hình bao gồm một người điều hành có hiểu biết chút ít về đối tượng được quan tâm, nhưng chủ yếu là người được lựa chọn để truyền thông tốt với các thành viên. Thông thường có khoảng 20 đến 100 thành viên, nếu ngược lại thì WARP có thể bị mất khả năng liên lạc cá nhân, và các thành viên thuộc về một cộng đồng chia sẻ quan tâm mạnh (các doanh nghiệp nhỏ, chính quyền địa phương, các nhà cung cấp dịch vụ, các nhóm liên quan khác).

Thành viên WARP đồng ý làm việc với nhau như một phần của cộng đồng và chia sẻ thông tin để giảm thiểu rủi ro về tổn hại của hệ thống thông tin của họ, và do đó giảm rủi ro cho tổ chức của họ. Cộng đồng chia sẻ này có thể dựa trên một ngành công nghiệp hoặc thương mại, vị trí địa lý, tiêu chuẩn kỹ thuật, nhóm liên quan, nhóm rủi ro, hoặc bất cứ nghiệp vụ chia sẻ nào khác.

Một cách điển hình thì WARP là nhỏ, mang tính cá nhân và "phi lợi nhuận".

D.3.2 Các chức năng của WARP

Người điều hành WARP sử dụng website, email, điện thoại, SMS, và thỉnh thoảng họp (bất cứ nơi nào có thể) để gửi cảnh báo và tư vấn dịch vụ cá nhân đến các thành viên. Đây thường là lời tư vấn về an toàn IT (bởi vì nó tương đối nhiều và thay đổi khá nhanh), nhưng cũng có thể bao gồm các vấn đề khác (các nguy cơ khác, tội phạm mạng, kế hoạch dự phòng). Người điều hành cũng khai thác kiến thức của các thành viên để giúp đỡ các thành viên khác sử dụng bảng thông tin, hội họp và các kỹ năng truyền thông chung. Một WARP thành công là xây dựng đủ sự tin cậy để khuyến khích các thành viên nói về các sự cố và vấn đề của họ, một cách ẩn danh, cho lợi ích của những người còn lại (hơi giống kiểu "theo dõi hàng xóm").

D.3.3 Các dịch vụ WARP

D.3.3.1 Tổng quan

WARP thông thường cung cấp ba dịch vụ cốt lõi:

- Dịch vụ cảnh báo chọn lọc – trong đó các thành viên chỉ nhận thông tin được bảo mật mà họ muốn, được chọn thông qua danh sách đánh dấu trực tuyến;
- Dịch vụ tư vấn môi giới – trong đó các thành viên có thể học sáng kiến và kinh nghiệm từ các thành viên khác thông qua một bảng thông tin của thành viên;
- Dịch vụ chia sẻ tin cậy – trong đó các báo cáo được ẩn danh để thành viên có thể học từ sự cố và tấn công của từng thành viên, mà không sợ bị phản kháng hoặc lúng túng.

D.3.3.2 Cảnh báo chọn lọc

Dịch vụ cảnh báo chọn lọc cho phép thành viên WARP nhận cảnh báo và tư vấn được lọc theo các lĩnh vực quan tâm của họ. Phần mềm ứng dụng cảnh báo chọn lọc sử dụng một danh sách lựa chọn đăng ký dạng cây cho phép các thành viên WARP thay đổi dễ dàng và duy trì sự lựa chọn của họ. Phần

mềm cũng giúp những người điều hành WARP dễ dàng phân loại và phổ biến các cảnh báo và tư vấn kịp thời. Dịch vụ này cung cấp phần cảnh báo cho WARP.

D.3.3.3 Tư vấn môi giới

Dịch vụ này cho phép thành viên cộng đồng WARP thảo luận các vấn đề an toàn thông tin và thực hành tốt trong môi trường an toàn thông tin. Dịch vụ cũng cho phép các thành viên cung cấp kinh nghiệm và kỹ năng cho các thành viên khác, có thể trên cơ sở trao đổi, trong đó một người làm việc và những người khác theo dõi. Dịch vụ này cung cấp phần tư vấn cho WARP.

D.3.3.4 Chia sẻ tin cậy

Dịch vụ này cung cấp một môi trường tin cậy mà ở đó các thành viên WARP có thể chia sẻ thông tin nhạy cảm, như các dữ liệu sự cố hoặc nguy cơ, theo cách hiểu không gây hại hoặc gây bối rối. Báo cáo có thể thu được qua điện thoại, thư điện tử hoặc trực tiếp, với sự bảo vệ an ninh thích hợp. Khi đã được làm sạch và ẩn danh nếu phù hợp, những thông tin sự cố này cũng có thể được gửi cho các WARP khác hiện có mối quan hệ tin cậy và với Chính phủ để phục vụ đối chiếu và giám sát các xu hướng quốc gia. Dịch vụ này cung cấp phần báo cáo cho WARP.

D.3.3.5 Các dịch vụ khác

Các WARP cũng cung cấp các dịch vụ khác có lợi cho các thành viên cộng đồng. Tuy nhiên, các dịch vụ như vậy thường được thực hiện đơn giản để tối ưu thời gian và tài nguyên cần thiết từ người điều hành WARP để hỗ trợ họ.

D.3.4 Các lợi ích

WARP cung cấp an toàn thông tin hiệu quả và chi phí thấp cho các thành vên bằng cách cung cấp:

- Môi trường tin cậy;
- Lọc thông tin an toàn;
- Tiếp cận tới các tư vấn của chuyên gia;
- Cảnh báo sớm các nguy cơ;
- Hỗ trợ các quyết định chiến lược;
- Cải tiến nhận thức về an toàn thông tin.

Một số lợi ích tiềm năng gắn với việc thiết lập WARP là:

- Hiệu quả công việc: WARP thúc đẩy chia sẻ thông tin và việc phối hợp các nhiệm vụ chung, dẫn đến giảm trùng lặp trong công việc. Điều này sẽ có lợi cho doanh nghiệp hoặc chính phủ thông qua việc tăng hiệu quả công việc.
- Tránh thiệt hại danh tiếng: do các tổ chức chuyển sang hướng tiếp cận trực tuyến nhiều hơn để tương tác với cộng đồng, sự hiện diện của web trở thành yếu tố then chốt. Nếu một website không hoạt động hoặc bị thay đổi diện mạo thì sẽ gây ra các vấn đề danh tiếng và làm nản lòng việc thực hiện các dịch vụ web. Cộng đồng được phục vụ sẽ được bảo vệ tốt hơn khi là các thành viên WARP.
- Cảnh báo sớm: việc tìm ra các vấn đề và cách giải quyết chúng là những kinh nghiệm, và việc chia sẻ những kinh nghiệm này trong cộng đồng WARP sẽ tạo điều kiện thuận lợi cho một dịch

vụ cá nhân hóa và duy nhất, mà ngay cả một nhà cung cấp thương mại lớn cũng không thể so sánh được.

- Hỗ trợ từ Chính phủ và các WARP khác: lợi thế thuộc về một cộng đồng được tập trung như vậy có nghĩa là khả năng chia sẻ và phổ biến những tư vấn hữu ích từ một nguồn tin cậy. Việc hỗ trợ về vận hành từ các WARP khác được thiết lập tốt thông qua Diễn đàn các nhà khai thác WARP. Cũng có thể có hợp tác ngang hàng thông qua Ứng dụng cảnh báo chọn lọc, cho phép phổ biến cảnh báo và tư vấn của các WARP khác một cách dễ dàng.
- Chi phí thấp: Mô hình này được thiết kế với chi phí thấp, với mức độ biên chế tối thiểu (hoặc các nhóm ảo).
- Bộ công cụ miễn phí toàn diện: Nhà cung cấp WARP có thể truy nhập bộ công cụ WARP được tạo ra từ kinh nghiệm của các WARP hiện hành. Nó bao gồm các thông tin nền, cách để bắt đầu, cách để xây dựng và chạy WARP, và một danh sách tải xuống rộng rãi, từ các bài báo đến các tài liệu tiếp thị.
- Bền vững: Các WARP hiện nay đang được thiết lập rộng rãi, nhiều tổ chức uy tín đã chấp nhận cách tiếp cận một cách thành công với độ bền vững được chứng minh.
- Phần mềm: Các nhà cung cấp WARP có thể truy nhập phần mềm đặc biệt được phát triển để hỗ trợ cả ba dịch vụ của WARP.
- Tăng độ tin tưởng: Tính chất "phi lợi nhuận" và sự kết hợp các thông lệ tốt hiện hành sẽ giúp đạt được sự tin cậy của cộng đồng và có thể hỗ trợ độ tin tưởng của tổ chức, đặc biệt là trong bối cảnh của các hoạt động "tốt cho công chúng".
- Tuân thủ: là thành viên của WARP sẽ giúp các tổ chức thành viên đáp ứng các biện pháp quản lý liên lạc mang tính tổ chức được xác định trong TCVN ISO/IEC 27002:2011.
- Tiềm năng tăng trưởng: Nhiều nhà cung cấp WARP hiện đang trong quá trình thiết lập thêm các WARP nữa, trên cơ sở hạ tầng và chuyên môn hiện tại, hỗ trợ cả chi phí thấp và độ bền vững cao. Các WARP hiện nay đang xuất hiện trong nhiều ngành, và đang bắt đầu lan rộng ra toàn thế giới.
- Trách nhiệm xã hội của doanh nghiệp: là thành viên của WARP sẽ nânng cao trách nhiệm xã hội của tổ chức thành viên, qua đó thu được độ tin cậy của cộng đồng và có khả năng hỗ trợ chiến lược kinh doanh của cả người điều hành lẫn thành viên.

D.3.5 Kết luận

Mô hình WARP là mô hình cộng tác, đơn giản trong việc chia sẻ thông tin giữa các tổ chức có cùng định hướng. Nó đặc biệt thích hợp với các trường hợp trong đó nguồn vốn bị giới hạn và hạ tầng trung tâm phải được cung cấp và hoạt động trên cơ sở tự nguyện.

Thư mục tài liệu tham khảo

[1] ISO/IEC Guide 2:1996, Standardization and related activities -- General vocabulary

[2] ISO/IEC Guide 73:2002, Risk management -- Vocabulary -- Guidelines for use in standards

[3] ISO/IEC 13335-1:2004, Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management

[4] ISO/IEC TR 13335-3:1998, Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security

[5] ISO/IEC 13888-1:1997, Information technology -- Security techniques -- Non-repudiation -- Part 1: General

[6] ISO/IEC 11770-1:1996, Information technology -- Security techniques -- Key management -- Part 1: Framework

[7] ISO/IEC 9796-2:2002, Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms

[8] ISO/IEC 9796-3:2000, Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms

[9] ISO/IEC 14888-1:1998, Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General

[10] ISO/IEC 15408-1:1999, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

[11] ISO/IEC TR 14516:2002, Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services

[12] BS ISO 15489-1:2001, Information and documentation - Records management – Part 1: General

[13] ISO 10007:2003, Guidelines for Configuration Management.

[14] ISO/IEC 12207:1995, Information technology -- Software life cycle processes

[15] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

[16] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

[17] OECD Guidelines for Cryptography Policy, 1997

[18] IEEE P1363 – 2000, Standard Specifications for Public-Key Cryptography

[19] ISO/IEC 18028-4, Information technology -- Security techniques – IT Netwwork security - Part

4: Securing remote access

[20] ISO/IEC TR 18044, Information technology – Security techniques – Information security incident management.