TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11780:2017
ISO/IEC 27032:2012

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - HƯỚNG DẪN VỀ AN TOÀN KHÔNG GIAN MẠNG

Information technology - Security techniques - Guidelines for cybersecurity

HÀ NỘI - 2017

Mục lục

Lời nói đầu

TCVN 11780:2017 hoàn toàn tương đương tiêu chuẩn ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity.

TCVN 11780:2017 do Học viện Công nghệ Bưu chính Viễn thông 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.

Lời giới thiệu

Không gian mạng là một môi trường phức tạp, là kết quả của sự tương tác giữa con người, phần mềm và dịch vụ với nhau trên Internet, được hỗ trợ bởi các thiết bị và mạng lưới công nghệ thông tin và truyền thông trên toàn thế giới. Tuy nhiên vẫn có những vấn đề an toàn mà an toàn thông tin, an toàn Internet, an toàn mạng và an toàn ICT hiện tại không đề cập đến, như là các kẽ hở giữa các miền này, cũng như việc thiếu trao đổi thông tin liên lạc giữa các tổ chức và các nhà cung cấp trong không gian mạng. Đó là do các kết nối mạng, các thiết bị hỗ trợ trong không gian mạng có rất nhiều chủ thể. Mỗi chủ thể có những mối quan tâm khác nhau về quản lý, điều hành và các nghiệp vụ khác nhau. Không chỉ các tổ chức hay các nhà cung cấp dịch vụ chia sẻ ít hoặc không chia sẻ thông tin đầu vào, mà mỗi đối tượng còn có một sự tập trung khác nhau khi giải quyết vấn đề an toàn không gian mạng. Tình trạng như vậy sẽ dẫn đến việc phân mảnh an toàn trong không gian mạng.

Như vậy, trọng tâm đầu tiên của tiêu chuẩn này là tập trung giải quyết những vấn đề về an toàn không gian mạng hoặc các vấn đề về an ninh mạng nhằm lấp các kẽ hở giữa các miền an toàn khác nhau trong không gian mạng. Trong phần này, tiêu chuẩn đưa ra các hướng dẫn kĩ thuật để giải quyết các rủi ro an toàn không gian mạng phổ biến, bao gồm:

- Các tấn công sử dụng kỹ thuật xã hội;
- Xâm nhập (hacking);
- Sự gia tăng của các phần mềm độc hại (malware);
- Phần mềm gián điệp;
- Các phần mềm không mong muốn tiềm ẩn khác.

Các hướng dẫn kĩ thuật này cung cấp các biện pháp kiểm soát để giải quyết các rủi ro, bao gồm:

- Chuẩn bị cho các cuộc tấn công gây bởi phần mềm độc hại, tội phạm cá nhân hoặc tổ chức tội phạm trên Internet;
- Phát hiện và giám sát các cuộc tấn công;
- Đối phó với các cuộc tấn công.

Khu vực tập trung thứ hai của tiêu chuẩn này là sự hợp tác, như một sự cần thiết để chia sẻ phối hợp thông tin và xử lý sự cố hiệu quả và năng suất giữa các bên liên quan trong không gian mạng. Sự hợp tác này không những phải an toàn và đáng tin cậy mà còn bảo vệ sự riêng tư của các cá nhân có liên quan. Các bên liên quan có thể nằm trong khu vực địa lý và múi giờ khác nhau và có thể sẽ được quản lý bởi nhiều yêu cầu khác nhau. Các bên liên quan bao gồm:

- Người dùng, có thể là các tổ chức hoặc cá nhân;
- Các nhà cung cấp, bao gồm cả các nhà cung cấp dịch vụ.

Vì vậy, tiêu chuẩn này cung cấp một khung cho

- Chia sẻ thông tin;
- Phối hợp;
- Giải quyết các sự cố.

Bộ khung bao gồm

- Các yếu tố chính trong việc xem xét các thiết lập tin tưởng.

- Các quy trình cần thiết cho sự hợp tác và trao đổi, chia sẻ thông tin,
- Các yêu cầu kĩ thuật cho việc tích hợp và tương tác hệ thống giữa các bên liên quan khác nhau.

Do phạm vi của tiêu chuẩn này, các biện pháp kiểm soát được cung cấp cần thiết phải ở mức cao. Chi tiết tiêu chuẩn đặc tả kỹ thuật và hướng dẫn phù hợp đối với từng phần được tham chiếu trong tiêu chuẩn này.

Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn về an toàn không gian mạng

Information technology - Security techniques - Guidelines for cybersecurity

1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra hướng dẫn để tăng cường trạng thái an toàn không gian mạng, phác thảo những khía cạnh đặc thù về hoạt động đó (tăng cường an toàn không gian mạng) và các phụ thuộc của hoạt động này trên các miền an toàn khác, cụ thể là:

- an toàn thông tin,
- an toàn mạng,
- an toàn Internet,
- bảo vệ hạ tầng thông tin trọng yếu (CIIP).

Tiêu chuẩn này bao gồm các thực hành an toàn cơ bản cho các bên liên quan trong không gian mạng. Tiêu chuẩn này cung cấp:

- tổng quan về an toàn không gian mạng,
- giải thích rõ mối quan hệ giữa an toàn không gian mạng và các loại an toàn khác,
- định nghĩa về các bên liên quan và mô tả vai trò của họ trong an toàn không gian mạng,
- hướng dẫn về giải quyết các vấn đề phổ biến trong an toàn không gian mạng,
- bộ khung cho phép các bên liên quan hợp tác giải quyết vấn đề an toàn không gian mạng.

2 Khả năng áp dụng

2.1 Đối tượng sử dụng

Tiêu chuẩn này được áp dụng cho các nhà cung cấp các dịch vụ trong không gian mạng, bao gồm cả người dùng sử dụng các dịch vụ đó. Trường hợp các tổ chức cung cấp dịch vụ trong không gian mạng cho người sử dụng tại nhà hay tại các tổ chức khác, họ có thể cần chuẩn bị các hướng dẫn dựa trên tiêu chuẩn này, bao gồm các giải thích bổ sung hay các ví dụ để giúp người dùng hiểu và làm theo.

2.2 Giới hạn

Tiêu chuẩn này không giải quyết:

- Điều kiện an toàn không gian mạng,
- Tội phạm không gian mạng,
- Bảo vệ hạ tầng thông tin trọng yếu (CIIP),
- Điều kiện an toàn Internet (Internet safety),
- Tội phạm liên quan tới Internet.

Tiêu chuẩn này thừa nhận mối quan hệ tồn tại giữa các miền được đề cập với an toàn không gian mạng. Tuy nhiên, việc giải quyết các mối quan hệ đó và sự chia sẻ các biện pháp kiểm soát giữa các miền vượt quá phạm vi của tiêu chuẩn này.

Điều quan trọng cần lưu ý là khái niệm về tội phạm không gian mạng, mặc dù được đề cập tới nhưng không được giải quyết ở tiêu chuẩn này. Tiêu chuẩn này không cung cấp hướng dẫn về các khía cạnh pháp luật liên quan tới không gian mạng, hay các quy định của an toàn không gian mạng.

Hướng dẫn trong tiêu chuẩn này giới hạn thực hiện trong không gian mạng trên Internet, bao gồm cả các thiết bị đầu cuối. Tuy nhiên, việc mở rộng không gian mạng để đại diện cho các không gian khác thông qua các nền tảng và phương tiện truyền thông, cũng như các khía cạnh an toàn vật lý của chúng không được giải quyết ở đây.

VÍ DỤ 1 Việc bảo vệ các yếu tố hạ tầng, như vật mang thông tin truyền thông không được giải quyết ở đây.

VÍ DỤ 2 Việc an toàn vật lý cho điện thoại di động kết nối vào không gian mạng để tải về và/hoặc thao tác nội dung không được giải quyết ở đây.

VÍ DỤ 3 Chức năng nhắn tin văn bản và tán gẫu bằng giọng nói (voice chat) của điện thoại không được giải quyết ở đây.

3 Tài liệu viện dẫn

Các tài liệu viện dẫn dưới đây là cần thiết để áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng 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).

TCVN 11238 *Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng.*

4 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa sau đây trong TCVN 11238.

4.1

Phần mềm quảng cáo (Adware)

Ứng dụng đẩy các quảng cáo tới người dùng và/hoặc thu thập các hành vi trực tuyến của người dùng.

CHÚ THÍCH Ứng dụng này có thể được cài đặt hoặc không được cài đặt tùy theo hiểu biết hay sự cho phép của người dùng hoặc bị ép buộc thông qua điều khoản cấp phép cho các phần mềm khác.

4.2

Ứng dụng (Application)

Giải pháp công nghệ thông tin, bao gồm cả các phần mềm ứng dụng, dữ liệu và thủ tục ứng dụng, được thiết kế để giúp người dùng của tổ chức thực hiện các nhiệm vụ đặc thù hay giải quyết các kiểu vấn đề đặc thù về công nghệ thông tin bằng cách tự động hóa chức năng và quy trình nghiệp vụ.

[ISO/IEC 27304-1:2011]

4.3

Nhà cung cấp dịch vụ ứng dụng (Application service provider)

Các nhà điều hành cung cấp các giải pháp phần mềm lưu trữ, cung cấp các dịch vụ ứng dụng, bao gồm các mô hình cung cấp dựa trên nền web hay máy trạm-chủ.

VÍ DỤ Các nhà điều hành game trực tuyến, các nhà cung cấp ứng dụng văn phòng và các nhà cung cấp kho lưu trữ trực tuyến.

4.4

Dịch vụ ứng dụng (Application services)

Phần mềm với chức năng cung cấp theo yêu cầu tới các thuê bao thông qua mô hình trực tuyến, bao gồm cả ứng dụng dựa trên nền web hay máy trạm-chủ.

4.5

Phần mềm ứng dụng (Application software)

Phần mềm thiết kế để giúp người sử dụng thực hiện các nhiệm vụ hay giải quyết các vấn đề cụ thể, khác biệt với các phần mềm giúp kiểm soát chính bản thân máy tính.

[ISO/IEC 18019]

4.6

Tài sản (Asset)

Là bất kỳ thứ gì có giá trị cho một cá nhân, tổ chức hay chính phủ.

CHÚ THÍCH Chấp nhận theo TCVN 11238:2015 cho phù hợp để tạo điều khoản cho các cá nhân, tách biệt chính phủ khỏi các tổ chức (4.37).

4.7

Hình đại diện (Avatar)

Thể hiện của một cá nhân tham gia vào không gian mạng.

CHÚ THÍCH 1 Một hình đại diện có thể liên quan đến bản thân của người đó.

CHÚ THÍCH 2 Một hình đại diện có thể là một "đối tượng" đại diện cho hiện thân của người sử dụng.

4.8

Tấn công (Attack)

Cố gắng phá hủy, làm lộ, thay đổi, vô hiệu hóa, đánh cắp, giành quyền truy cập trái phép hay thực thi việc sử dụng trái phép một tài sản.

[TCVN 11238:2015]

4.9

Khả năng tấn công (Attack potential)

Khả năng nhận biết cho sự thành công của một cuộc tấn công, nếu cuộc tấn công xảy ra, thì được thể hiện qua chuyên môn, tài nguyên và động cơ của đối tượng tấn công.

[TCVN 8709-1:2011]

4.10

Véc-tơ tấn công (Attack vector)

Là con đường hay cách thức mà đối tượng tấn công có thể truy cập vào một máy tính hay máy chủ mạng để chuyển các phần mềm độc hại vào.

4.11

Tấn công hỗn hợp (Blended attack)

Là cuộc tấn công kết hợp nhiều phương thức tấn công nhằm gây mức độ thiệt hại và tốc độ lây lan cao nhất.

4.12

Chương trình phần mềm tự động (Bot, robot)

Là các chương trình phần mềm tự động thực hiện các nhiệm vụ cụ thể.

CHÚ THÍCH 1 Thuật ngữ này thường được dùng để mô tả các chương trình chạy trên một máy chủ, tự động hóa các tác vụ như chuyển tiếp hay phân loại thư điện tử.

CHÚ THÍCH 2 Một chương trình phần mềm tự động (bot) cũng được mô tả như một chương trình hoạt động như một tác nhân người dùng hay chương trình khác hay mô phỏng hoạt động của con người. Trên internet, các chương trình phần mềm tự động (bot) phổ biến nhất là các chương trình truy cập vào các trang web, thu thập nội dung cho các chỉ số công cụ tìm kiếm (spider hay crawler).

4.13

Mạng máy tính ma (Botnet)

Là phần mềm kiểm soát từ xa, tập hợp các chương trình phần mềm độc hại, tự động chạy và chạy độc lập trên các máy tính bị xâm hại.

4.14

Cookie

<Kiểm soát truy cập> Khả năng hay thẻ trong hệ thống kiểm soát truy cập.

4.15

Cookie

<IPsec> Dữ liệu trao đổi bằng ISAKMP để ngăn chặn tấn công từ chối dịch vụ DoS trong quá trình thiết lập một liên kết an toàn.

4.16

Cookie

<HTTP> Dữ liệu trao đổi giữa một máy chủ HTTP và một trình duyệt để lưu trữ thông tin trạng thái bên phía máy khách và có thể lấy lại sau đó để máy chủ sử dụng.

CHÚ THÍCH Một trình duyệt web có thể nằm trên một máy khách hoặc một máy chủ.

4.17

Biện pháp kiểm soát (Control)

Biện pháp đối phó (Countermeasure)

Biện pháp quản lý các rủi ro, bao gồm các chính sách, các thủ tục, hướng dẫn, thực hành hay cơ cấu tổ chức, có thể mang tính kĩ thuật, quản lý, pháp lý hay tính chất hành chính.

[TCVN 11238:2015]

CHÚ THÍCH TCVN 9788:2013 (ISO Guide 73:2009) định nghĩa biện pháp kiểm soát đơn giản là một biện pháp để điều chỉnh rủi ro.

4.18

Tội phạm không gian mạng (Cybercrime)

Các hoạt động phạm tội mà trong đó coi các ứng dụng và dịch vụ trong không gian mạng được sử dụng hay là mục tiêu của tội phạm, hoặc coi không gian mạng là tài nguyên, công cụ, mục tiêu hay địa điểm của tội phạm.

4.19

Điều kiện an toàn không gian mạng (Cybersafety)

Điều kiện được bảo vệ chống lại tác nhân vật lý, xã hội, tôn giáo, tài chính, chính trị, tình cảm, nghề nghiệp, tâm lý, giáo dục hoặc các tác nhân khác hoặc hậu quả của thất bại, hư hỏng, lỗi, tai nạn, thiệt hại hay bất cứ sự kiện nào khác trong không gian mạng không mong muốn.

CHÚ THÍCH 1 Điều này có thể mang hình thức được bảo vệ khỏi các sự kiện hay việc làm lộ thông tin gây mất mát về sức khỏe và kinh tế. Nó có thể bao gồm cả việc bảo vệ con người và tài sản.

CHÚ THÍCH 2 Tổng quát, điều kiện an toàn cũng được định nghĩa là trạng thái chắc chắn rằng một vài tác nhân trong các điều kiện xác định sẽ không thể gây ảnh hưởng bất lợi.

4.20

An toàn không gian mạng (Cybersecurity - Cyberspace security)

Bảo toàn tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin trong không gian mạng.

CHÚ THÍCH 1 Ngoài ra, các đặc tính khác, như tính xác thực, kiểm soát, chống chối bỏ và độ tin cậy cũng có thể liên quan.

CHÚ THÍCH 2 Chấp nhận theo định nghĩa về an toàn thông tin trong TCVN 11238:2015.

4.21

Không gian mạng (the Cyberspace)

Là một môi trường phức tạp, là tập hợp sự tương tác giữa con người, phần mềm và dịch vụ trên Internet với nhau, bằng các thiết bị công nghệ và mạng lưới kết nối với nó, không có bất cứ yếu tố vật lý nào.

4.22

Các dịch vụ ứng dụng không gian mạng (Cyberspace application services)

Các dịch vụ ứng dụng (4.4) cung cấp qua không gian mạng.

4.23

Bên chiếm giữ không gian mạng (Cyber-squatter)

Là các cá nhân hay các tổ chức đăng kí và giữ các URL giống với tham chiếu hay tên của các tổ chức khác trong thế giới thực hay trong không gian mạng.

4.24

Phần mềm lừa đảo (Deceptive software)

Là phần mềm thực hiện các hoạt động trên máy tính người dùng mà không thông báo trước cho người dùng về chính xác những điều mà phần mềm sẽ làm trên máy tính hoặc không hỏi người dùng về việc cho phép các hành động này.

VÍ DỤ 1 Một chương trình ngăn chặn việc cấu hình của người dùng.

VÍ DỤ 2 Một chương trình tạo ra các quảng cáo bật ra liên tục không ngừng, người dùng rất khó để có thể tắt được nó.

VÍ DỤ 3 Phần mềm quảng cáo và phần mềm gián điệp.

4.25

Xâm nhập (Hacking)

Cố ý truy cập vào hệ thống máy tính mà không có sự cho phép của người dùng hoặc chủ nhân của nó.

4.26

Tin tặc (Hactivism)

Là xâm nhập (hacking) với động cơ chính trị hay xã hội.

4.27

Tài sản thông tin (Information asset)

Là kiến thức hay dữ liệu có giá trị đối với cá nhân hay tổ chức.

CHÚ THÍCH Chấp nhận theo TCVN 11238:2015.

4.28

Liên mạng (internet – internetwork)

Tập hợp các mạng máy tính liên kết với nhau.

CHÚ THÍCH 1 Được chấp nhận theo TCVN 9801-1:2013

CHÚ THÍCH 2 Trong ngữ cảnh này, nó được gọi là "an internet". Định nghĩa "an internet" và "the internet" là khác nhau.

4.29

Mạng Internet (the Internet)

Hệ thống mạng máy tính liên kết toàn cầu trong miền công khai.

[TCVN 9801-1:2013]

CHÚ THÍCH "Mạng Internet" và "Liên mạng" là khác nhau.

4.30

Tội phạm Internet (Internet crime)

Các hoạt động phạm tội tại nơi mà các dịch vụ hoặc các ứng dụng trên mạng Internet được sử dụng hoặc là mục tiêu của tội phạm hoặc tại nơi mà Internet là nguồn gốc, công cụ, mục tiêu hoặc vị trí của tội phạm.

4.31

Điều kiện an toàn Internet (Internet Safety)

Điều kiện được bảo vệ chống lại tác nhân vật lý, xã hội, tôn giáo, tài chính, chính trị, tình cảm, nghề nghiệp, tâm lý, giáo dục hay các tác nhân khác hoặc hậu quả của thất bại, hư hỏng, lỗi, tai nạn, thiệt hại hoặc bất cứ sự kiện nào khác trong Internet mà được coi là ko mong muốn.

4.32

An toàn Internet (Internet Security)

Bảo toàn tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin trên Internet.

4.33

Dịch vụ Internet (Internet Services)

Dịch vụ cung cấp cho người sử dụng để cho phép truy cập vào Internet thông qua một địa chỉ IP, bao gồm cả xác thực, cấp quyền và dịch vụ tên miền.

4.34

Nhà cung cấp dịch vụ Internet (Internet Service Provider)

Các tổ chức cung cấp dịch vụ Internet cho người sử dụng và cho phép khách hàng truy cập vào Internet.

CHÚ THÍCH Ngoài ra đôi khi được gọi là một nhà cung cấp truy cập Internet.

4.35

Phần mềm độc hại (Malicious software)

Phần mềm được thiết kế với mục đích gây hại, chứa các tính năng hoặc khả năng có thể gây ra thiệt hại trực tiếp hoặc gián tiếp cho người sử dụng và/hoặc hệ thống máy tính.

VÍ DỤ Virus, sâu, trojan.

4.36

Nội dung độc hại (Malicious contents)

Các ứng dụng, tài liệu, tập tin, dữ liệu hoặc các nguồn tài nguyên khác có các tính năng độc hại được nhúng vào, ngụy trang hoặc ẩn trong chúng.

4.37

Tổ chức (Organization)

Nhóm người và cơ sở vật chất cùng một thỏa thuận về trách nhiệm, quyền hạn và mối quan hệ.

[TCVN ISO 9000: 2007]

CHÚ THÍCH 1 Trong ngữ cảnh của tiêu chuẩn này, một cá nhân khác với một tổ chức.

CHÚ THÍCH 2 Tổng quát, một chính phủ cũng được coi như một tổ chức. Trong ngữ cảnh của tiêu chuẩn này, chính phủ có thể được xem xét một cách riêng biệt với các tổ chức khác một cách rõ ràng.

4.38

Tấn công giả mạo (Phishing)

Quá trình gian lận để cố gắng có được thông tin riêng tư hay bí mật bằng cách giả mạo như là một thực thể đáng tin cậy trong truyền thông điện tử.

CHÚ THÍCH Tấn công giả mạo có thể được thực hiện bằng cách sử dụng các kỹ thuật xã hội hoặc lừa đảo kỹ thuật.

4.39

Tài sản vật lý (Physical asset)

Tài sản hữu hình hoặc vật chất đang tồn tại.

CHÚ THÍCH Tài sản vật lý thường nhắc đến tiền mặt, thiết bị, hàng hóa và tài sản thuộc sở hữu của cá nhân, tổ chức. Phần mềm được coi là một tài sản vô hình hoặc một tài sản phi vật chất.

4.40

Các phần mềm không mong muốn tiềm ẩn (Potentially unwanted software)

Phần mềm lừa đảo, bao gồm cả phần mềm độc hại và không độc hại, thể hiện các đặc tính của phần mềm lừa đảo.

4.41

Lừa đảo (Scam)

Gian lận hoặc lừa dối tính bí mật.

4.42

Thư rác (Spam)

Lạm dụng hệ thống nhắn tin điện tử để gửi thư điện tử số lượng cực lớn bất hợp pháp và/hoặc không mong muốn.

CHÚ THÍCH Trong khi loại phổ biến nhất của spam là thư điện tử rác, thuật ngữ này cũng được áp dụng đối với các lạm dụng tương tự trong các phương tiện truyền thông khác: tin nhắn tức thời rác, diễn đàn thảo luận thông tin toàn cầu (Usernet newsgroup) rác, công cụ tìm kiếm web rác, thư rác trong blogs, bách khoa toàn thư tự do (wiki) rác, tin nhắn di động rác, thư rác trong các diễn đàn Internet, thư rác trong fax.

4.43

Phần mềm gián điệp (Spyware)

Phần mềm lừa đảo thu thập thông tin cá nhân hoặc bí mật từ một người sử dụng máy tính.

CHÚ THÍCH Các thông tin có thể bao gồm các nội dung như các trang web thường xuyên truy cập hoặc các thông tin nhạy cảm chẳng hạn như mật khẩu.

4.44

Bên liên quan (Stakeholder)

<Quản lý rủi ro> người hoặc tổ chức có thể gây ảnh hưởng, bị ảnh hưởng hoặc tự cảm thấy mình bị ảnh hưởng bởi một quyết định hoặc hoạt động.

[TCVN 9788:2013 (ISO Guide 73:2009)]

4,45

Bên liên quan (Stakeholder)

<Hệ thống> cá nhân hoặc tổ chức có quyền, chia sẻ, yêu cầu hoặc quan tâm đến một hệ thống hoặc sở hữu các đặc tính đáp ứng nhu cầu và mong đợi của họ [ISO/IEC 12207:2008]

4.46

Mối đe dọa (Threat)

Nguyên nhân tiềm ẩn của một sự cố không mong muốn, có thể gây hại cho hệ thống cá nhân hoặc tổ chức.

CHÚ THÍCH Chấp nhận theo TCVN 11238:2015.

4.47

Mã Trojan (Trojan - Trojan horse)

Là phần mềm độc hại ẩn mình dưới dạng một chương trình hữu ích có những chức năng mong muốn.

4.48

Thư điện tử không mong muốn (Unsolicited email)

Thư điện tử không được chào đón hoặc không được yêu cầu hoặc được mời.

4.49

Tài sản ảo (Virtual asset)

Đại diện của một tài sản trong không gian mạng

CHÚ THÍCH Trong ngữ cảnh này, tiền tệ có thể được xác định là một phương tiện trao đổi hoặc một tài sản có giá trị trong một môi trường cụ thể, chẳng hạn như một trò chơi video hoặc một bài tập mô phỏng giao dịch tài chính.

4.50

Tiền ảo (Virtual currency)

Tài sản ảo tiền tệ.

4.51

Thế giới ảo (Virtual world)

Môi trường mô phỏng truy cập bởi nhiều người dùng thông qua một giao diện trực tuyến.

CHÚ THÍCH 1 Các môi trường mô phỏng thường tương tác với nhau.

CHÚ THÍCH 2 Thế giới vật chất nơi mọi người sống và các đặc tính liên quan, sẽ được gọi là "thế giới thực" để phân biệt nó với thế giới ảo.

4.52

Điểm yếu (Vulnerability)

Yếu điểm của tài sản hoặc biện pháp kiểm soát dẫn đến việc có thể bị khai thác bởi một mối đe dọa [TCVN 11238:2015]

4.53

Máy tính ma (Zombie – Zombie computer – Drone)

Máy tính có chứa phần mềm ẩn mà cho phép kiểm soát từ xa máy tính đó, thường là để thực hiện một cuộc tấn công vào một máy tính khác.

CHÚ THÍCH Nói chung, một máy bị xâm hại chỉ là một trong nhiều máy trong mạng máy tính ma (botnet) và sẽ được sử dụng để thực hiện các hoạt động độc hại theo chỉ đạo từ xa.

5 Thuật ngữ viết tắt

Các thuật ngữ viết tắt dưới đây được sử dụng trong tiêu chuẩn này.

AS	Autonomous System	Hệ thống tự quản
AP	Access Point	Điểm truy cập
CBT	Computer Based Training	Đào tạo dựa trên máy tính
CERT	Computer Emergency Response Team	Trung tâm ứng cứu khẩn cấp máy tính
CIRT	Computer Incident Response Team	Trung tâm ứng cứu sự cố máy tính
CSIRT	Computer Security Incident Response	Trung tâm ứng cứu sự cố an toàn máy tính
CIIP	Critical Information Infrastructure Protection	Bảo vệ hạ tầng thông tin trọng yếu
DoS	Denial-of-Service	Từ chối dịch vụ
DDoS	Distributed Denial-of-Service	Từ chối dịch vụ phân tán
HIDS	Host-based Intrusion Detection System	Hệ thống phát hiện xâm nhập máy chủ
IAP	Independent Application Provider	Nhà cung cấp ứng dụng độc lập
ICMP	Internet Control Message Protocol	Giao thức bản tin điều khiển Internet
ICT	Information and Communications Technology	Công nghệ thông tin và Truyền thông
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập

IP	Internet Protocol	Giao thức Internet
IPO	Information Providing Organization	Tổ chức cung cấp thông tin
IPS	Intrusion Prevention System	Hệ thống ngăn chặn xâm nhập
IRO	Information Receiving Organization	Tổ chức tiếp nhận thông tin
ISP	Internet Service Provider	Nhà cung cấp dịch vụ Internet
ISV	Independent Software Vendor	Nhà cung cấp phần mềm độc lập
IT	Information Technology	Công nghệ thông tin
MMORPG	Massively Multiplayer Online Role-Playing Game	Trò chơi nhập vai trực tuyến nhiều người chơi
NDA	Non-Disclosure Agreement	Thỏa thuận không tiết lộ
SDLC	Software Development Life-cycle	Vòng đời phát triển phần mềm
SSID	Service Set Identifier	Định danh tập dịch vụ
TCP	Transmission Control Protocol	Giao thức điều khiển giao vận
UDP	User Datagram Protocol	Giao thức dữ liệu người dùng
URI	Uniform Resource Identifier	Định danh tài nguyên thống nhất
URL	Uniform Resource Locator	Định vị tài nguyên thống nhất

6 Tổng quan

6.1 Giới thiệu

An toàn trên Internet và trong không gian mạng là một chủ đề ngày càng được quan tâm. Các bên liên quan đã thiết lập đại diện của họ trong không gian mạng thông qua các trang web và bây giờ đang cố gắng để tiếp tục tận dụng thế giới ảo đó.

VÍ DỤ Các bên liên quan cố gắng tăng số lượng các cá nhân sử dụng ngày càng nhiều thời gian cùng đại diện ảo của họ cho các trò chơi nhập vai trực tuyến nhiều người chơi MMORPG.

Trong khi một số người rất cẩn thận trong việc quản lý định danh trực tuyến của họ, hầu hết mọi người đều tải lên chi tiết hồ sơ cá nhân của mình để chia sẻ với người khác. Các hồ sơ trên nhiều trang web, đặc biệt là các trang web mạng xã hội và các phòng chat, có thể được tải về và lưu trữ bởi các thành viên khác. Điều này có thể dẫn đến việc tạo ra một hồ sơ kỹ thuật số các dữ liệu cá nhân, có thể bị lợi dụng, tiết lộ cho các bên khác hoặc sử dụng để thu thập dữ liệu thứ cấp. Trong khi tính chính xác và toàn vẹn của dữ liệu này vẫn là một câu hỏi, họ tạo ra các liên kết đến các cá nhân và tổ chức, các liên kết này thường không thể xóa hoàn toàn. Sự phát triển trong truyền thông, giải trí, vận chuyển, mua sắm, tài chính, bảo hiểm, chăm sóc sức khỏe và các lĩnh vực khác tạo ra những rủi ro mới tới các bên liên quan trong không gian mạng. Rủi ro có thể liên quan với việc mất tính riêng tư.

Sự hội tụ của công nghệ thông tin và truyền thông, sự dễ dàng đi vào không gian mạng và thu hẹp không gian cá nhân giữa các cá nhân đang tạo nên sự chú ý tới các tội phạm cá nhân và tổ chức tội phạm. Những thành phần này đang sử dụng các cách hiện có, chẳng hạn như tấn công giả mạo, thư

rác và phần mềm gián điệp, cũng như phát triển các kỹ thuật tấn công mới để khai thác những điểm yếu mà chúng phát hiện ra trong không gian mạng. Trong những năm gần đây, các cuộc tấn công an toàn không gian mạng đã phát triển từ việc xâm nhập (hacking) vì sự nổi tiếng cá nhân thành phạm tội có tổ chức hay tội phạm không gian mạng. Hiện nay, rất nhiều công cụ và quy trình xuất hiện trước đó trong các sự cố an toàn không gian mạng đang được sử dụng kết hợp với nhau trong các cuộc tấn công đa hỗn hợp, nhằm đạt mục tiêu độc hại xa hơn. Các mục tiêu này trải từ các cuộc tấn công cá nhân, trộm cắp định danh, gian lận hay trộm cắp tài chính, đến các cuộc xâm nhập vì mục đích chính trị, xã hội. Các diễn đàn chuyên biệt giúp làm nổi bật các vấn đề bảo mật tiềm ẩn và cũng chỉ ra các kỹ thuật tấn công và cơ hội phạm tội.

Các hình thức giao dịch nghiệp vụ đa dạng được thực hiện trong không gian mạng đang trở thành mục tiêu của tổ chức tội phạm không gian mạng. Trong các dịch vụ từ doanh nghiệp tới doanh nghiệp, doanh nghiệp tới người dùng, người dùng tới người dùng, những rủi ro đều rất phức tạp. Những khái niệm như là những thứ tạo ra một giao dịch hoặc một thỏa thuận phụ thuộc vào sự diễn giải của pháp luật và làm thế nào để mỗi bên quản lý trách nhiệm của họ. Thông thường, các vấn đề trong việc sử dụng số liệu thu thập được trong quá trình giao dịch hay mối quan hệ không được giải quyết thỏa đáng. Điều này có thể dẫn đến các vấn đề an toàn chẳng hạn như rò rỉ thông tin.

Những thách thức về pháp luật và kỹ thuật gây ra bởi các vấn đề an toàn không gian mạng mang tính sâu rộng và toàn cầu. Những thách thức này chỉ có thể được giải quyết bằng cộng đồng công nghệ an toàn thông tin, cộng đồng pháp lý, các quốc gia và cộng đồng các quốc gia kết hợp với nhau theo một chiến lược thống nhất. Chiến lược này phải tính đến vai trò của mỗi bên liên quan và các sáng kiến hiện có trong khung hợp tác quốc tế.

Ví DỤ Một ví dụ về một thách thức từ thực tế là các không gian mạng vẫn cho phép các cuộc tấn công lén lút và nặc danh làm cho việc phát hiện hết sức khó khăn. Điều này ngày càng gây khó khăn cho các cá nhân và tổ chức khi tạo dựng sự tin tưởng và giao dịch, cũng như cho các cơ quan thực thi pháp luật khi thực thi các chính sách có liên quan. Ngay cả khi nguồn gốc của cuộc tấn công có thể được xác định, vấn đề biên giới pháp lý cũng thường xuyên ngăn chặn các cuộc điều tra.

Các vấn đề an toàn không gian mạng ngày càng gia tăng và phát triển và việc tiến hành giải quyết những thách thức này hiện tại đang bị cản trở bởi nhiều vấn đề. Có rất nhiều các mối đe dọa an toàn không gian mạng, và cũng có rất nhiều cách để chống lại chúng mặc dù không được chuẩn hóa. Tiêu chuẩn này tập trung vào các vấn đề chính sau đây:

- các cuộc tấn công bởi phần mềm độc hại và không mong muốn tiềm ẩn;
- các cuộc tấn công khai thác thông tin xã hội;
- phối hợp và chia sẻ thông tin.

Ngoài ra, một số công cụ an toàn không gian mạng cũng sẽ được thảo luận ngắn gọn trong tiêu chuẩn này. Những công cụ này và các khu vực liên quan chặt chẽ tới việc ngăn chặn, phát hiện, đối phó và điều tra tội phạm không gian mạng. Thông tin chi tiết có thể được tìm thấy trong phụ lục A.

6.2 Bản chất của không gian mạng

Không gian mạng có thể được mô tả như một môi trường ảo, không tồn tại bất kỳ hình thức vật lý nào, đúng hơn nữa, là một môi trường hoặc không gian phức tạp hình thành lên do sự xuất hiện của Internet, cùng với con người, các tổ chức và các hoạt động trên tất cả các thiết bị công nghệ và mạng lưới kết nối tới nó. An toàn của không gian mạng, hay an toàn không gian mạng là nói về an toàn của thế giới ảo này.

Nhiều thế giới ảo có một loại tiền ảo, chẳng hạn như sử dụng để mua vật phẩm trong trò chơi. Có sự liên quan về giá trị trong thế giới thực với đồng tiền ảo và thậm chí với cả các vật phẩm trong trò chơi. Những vật phẩm ảo thường được giao dịch với tiền thật trên các trang web đấu giá trực tuyến và một số trò chơi thậm chí còn có một kênh chính thức công bố tỷ giá trao đổi tiền ảo với tiền thật cho các vật phẩm ảo. Đó là những kênh lưu hành tiền tệ, làm cho thế giới ảo này trở thành mục tiêu của tấn công, thường là tấn công giả mạo hoặc dùng các kỹ thuật khác để ăn cắp thông tin tài khoản.

6.3 Bản chất của an toàn không gian mạng

Các bên liên quan trong không gian mạng ngoài việc bảo vệ tài sản của mình, phải đóng một vai trò tích cực để phát huy tính hữu ích của không gian mạng. Các ứng dụng trong không gian mạng đang mở rộng, từ các mô hình doanh nghiệp đến người dùng và từ người dùng đến người dùng, trở thành một mô hình tương tác và giao dịch nhiều – nhiều. Các yêu cầu mở rộng cho các cá nhân và các tổ chức được chuẩn bị để giải quyết các rủi ro và thách thức an toàn đang nổi lên, để ngăn chặn và đối phó hiệu quả với việc lạm dụng và việc khai thác của tội phạm.

An toàn không gian mạng liên quan đến các hành động mà các bên liên quan dùng để thiết lập và duy trì an toàn trong không gian mạng.

An toàn không gian mạng dựa trên cơ sở của an toàn thông tin, an toàn ứng dụng, an toàn mạng và an toàn Internet. An toàn không gian mạng là một trong những hoạt động cần thiết cho CIIP, đồng thời, việc bảo vệ đầy đủ các dịch vụ hạ tầng trọng yếu góp phần vào các nhu cầu an toàn cơ bản (ví dụ, tính bảo mật, độ tin cậy và tính sẵn sàng của hạ tầng trọng yếu) để đạt được các mục tiêu của an toàn không gian mạng.

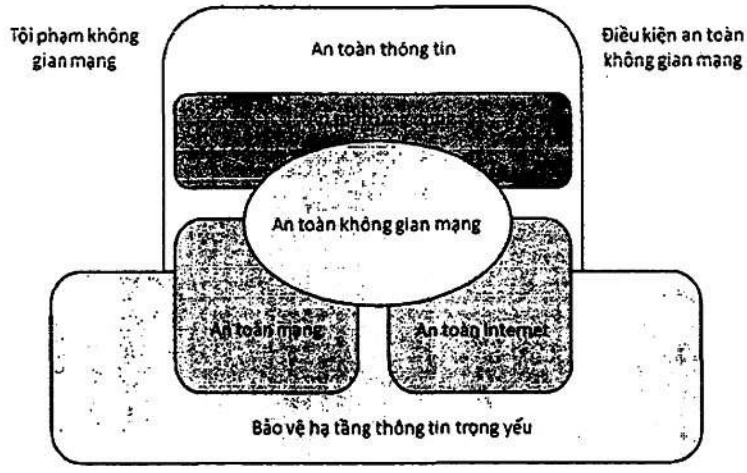
Tuy nhiên, an toàn không gian mạng không đồng nghĩa với an toàn Internet, an toàn mạng, an toàn ứng dụng, an toàn thông tin hoặc CIIP. Nó có một phạm vi duy nhất yêu cầu các bên liên quan đóng một vai trò tích cực để duy trì, cải thiện tính hữu ích và đáng tin cậy của không gian mạng. Tiêu chuẩn này phân biệt an toàn không gian mạng với các miền an toàn khác như sau:

- An toàn thông tin liên quan đến việc bảo vệ tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin nói chung, phục vụ nhu cầu của người sử dụng thông tin.
- An toàn ứng dụng là một quy trình thực hiện để áp dụng các biện pháp kiểm soát và đo lường tới các ứng dụng của tổ chức để quản lý rủi ro khi sử dụng chúng. Các biện pháp kiểm soát và đo lường có thể được áp dụng cho chính bản thân các ứng dụng (các quy trình, các thành

phần, phần mềm và kết quả của nó), cho dữ liệu của nó (dữ liệu cấu hình, dữ liệu người dùng, dữ liệu tổ chức) và cho tất cả các công nghệ, quy trình và các yếu tố liên quan trong vòng đời ứng dụng.

- An toàn mạng liên quan đến việc thiết kế, triển khai và vận hành của mạng để đạt được các mục đích an toàn thông tin trên mạng trong các tổ chức, giữa các tổ chức, giữa tổ chức và người dùng.
- An toàn Internet liên quan đến việc bảo vệ các dịch vụ liên quan đến Internet, các hệ thống và mạng ICT liên quan như một phần mở rộng của an toàn mạng trong các tổ chức và hộ gia đình, để đạt được mục đích an toàn. An toàn Internet cũng đảm bảo tính sẵn sàng và độ tin cậy của các dịch vụ Internet.
- CIIP liên quan đến việc bảo vệ các hệ thống được cung cấp hoặc được vận hành bởi các nhà cung cấp hạ tầng trọng yếu, chẳng hạn như các ban ngành năng lượng, viễn thông và nước. CIIP đảm bảo rằng các hệ thống và mạng lưới được bảo vệ và chống lại các rủi ro an toàn thông tin, rủi ro an toàn mạng, rủi ro an toàn Internet, cũng như rủi ro an toàn không gian mạng.

Hình 1 tổng kết các mối quan hệ giữa an toàn không gian mạng và các miền an toàn khác. Mối quan hệ giữa các miền an toàn và an toàn không gian mạng là rất phức tạp. Một số dịch vụ hạ tầng trọng yếu, ví dụ như nước và giao thông vận tải, cần không tác động trực tiếp hoặc tác động không đáng kể đến tình trạng an toàn không gian mạng. Tuy nhiên, việc thiếu an toàn không gian mạng có thể có tác động tiêu cực tới tính sẵn sàng của hệ thống hạ tầng thông tin trọng yếu được cung cấp bởi các nhà cung cấp hạ tầng trọng yếu.



Hình 1 – Mối quan hệ giữa an toàn không gian mạng và các miền an toàn khác

Mặt khác, tính sẵn sàng và độ tin cậy của không gian mạng đều dựa vào tính sẵn sàng và độ tin cậy của các dịch vụ hạ tầng trọng yếu liên quan, chẳng hạn như hạ tầng mạng lưới viễn thông. An toàn không gian mạng cũng liên quan chặt chẽ đến an toàn Internet và an toàn thông tin mạng doanh

nghiệp/ hộ gia đình nói chung. Cần lưu ý rằng các miền an toàn được xác định trong phần này có mục tiêu và phạm vi tập trung của riêng nó. Để giải quyết các vấn đề an toàn không gian mạng, cần đòi hỏi sự phối hợp và truyền thông thực chất giữa các đơn vị cá nhân và cộng đồng từ các tổ chức và các nước khác nhau. Các dịch vụ hạ tầng trọng yếu được quan tâm bởi một số chính phủ, như các dịch vụ liên quan đến an toàn quốc gia, có thể không được thảo luận hoặc tiết lộ công khai. Hơn nữa, kiến thức về các điểm yếu của hạ tầng trọng yếu, nếu không được sử dụng một cách thích hợp có thể ảnh hưởng trực tiếp đến an toàn quốc gia. Do đó, bộ khung cơ sở để ban hành, chia sẻ thông tin hoặc phối hợp sự cố là cần thiết để thu hẹp khoảng cách và đảm bảo an toàn cho các bên liên quan trong không gian mạng.

6.4 Mô hình chung

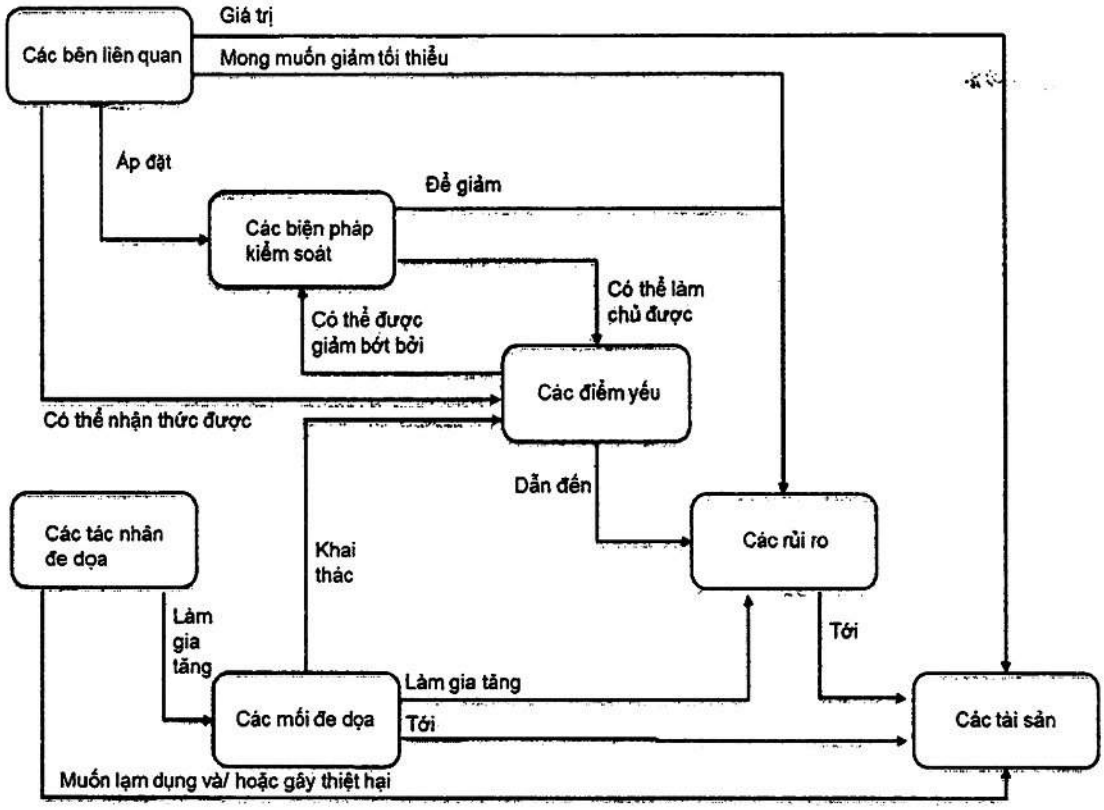
6.4.1 Giới thiệu

Điều này giới thiệu một mô hình chung được dùng xuyên suốt trong tiêu chuẩn này. Nó cũng thừa nhận một số kiến thức về an toàn nhưng không phải với mục đích như một hướng dẫn trong Điều này. Tiêu chuẩn này thảo luận về an toàn sử dụng một tập hợp các khái niệm và thuật ngữ an toàn. Việc hiểu các khái niệm và thuật ngữ là một điều kiện tiên quyết để sử dụng có hiệu quả tiêu chuẩn này. Tuy nhiên, các khái niệm bản thân nó cũng khá tổng quát và không nhằm mục đích hạn chế các vấn đề về an toàn công nghệ thông tin mà tiêu chuẩn này áp dụng.

6.4.2 Ngữ cảnh an toàn chung

An toàn liên quan đến việc bảo vệ tài sản khỏi các mối đe dọa, các mối đe dọa được phân loại theo khả năng lạm dụng các tài sản được bảo vệ. Tất cả các loại mối đe dọa nên được xem xét; tuy nhiên, trong miền an toàn cần chú ý nhiều hơn tới những mối đe dọa liên quan đến hành động của những người có ý đồ xấu. Hình 2 minh họa những khái niệm và mối quan hệ ở mức cao.

CHÚ THÍCH Hình 2 chấp nhận theo theo TCVN 8709-1:2011, Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá về an toàn Công nghệ Thông tin - Phần 1: Giới thiệu và mô hình tổng quát.



Hình 2 – Các mối quan hệ và khái niệm an toàn

Việc quan tâm bảo vệ tài sản là trách nhiệm của các bên liên quan, những người đặt giá trị của họ trên các tài sản đó. Thực tế là các tác nhân đe dọa cũng có thể đặt giá trị lên trên tài sản đó và tìm cách lợi dụng tài sản đó trái với lợi ích của các bên liên quan. Các bên liên quan sẽ nhận thấy được các mối đe dọa khi tài sản của họ bị suy giảm. Các hư hại đặc trưng về an toàn thường bao gồm, nhưng không giới hạn, thiệt hại về tiết lộ các tài sản cho người nhận trái phép (mất tính bí mật), thiệt hại tài sản qua sửa đổi trái phép (mất tính toàn vẹn) hoặc cướp quyền truy cập vào tài sản (mất tính sẵn sàng).

Các bên liên quan đánh giá các rủi ro liên quan tới tài sản của họ. Phân tích này có thể hỗ trợ việc lựa chọn các biện pháp kiểm soát để chống lại những rủi ro và giảm bớt nó tới mức chấp nhận được.

Các biện pháp kiểm soát được áp đặt để giảm bớt các điểm yếu hoặc các tác động và để đáp ứng yêu cầu an toàn của các bên liên quan (trực tiếp hoặc gián tiếp bằng cách cung cấp trực tiếp cho các bên khác). Sau khi áp đặt các biện pháp kiểm soát, một số điểm yếu có thể vẫn còn. Các điểm yếu này có thể bị khai thác bởi các tác nhân đe dọa tới các tài sản. Các bên liên quan sẽ tìm cách để giảm thiểu nguy cơ tạo bởi những ràng buộc khác.

Các bên liên quan sẽ cần phải chắc chắn rằng các biện pháp kiểm soát là đủ để chống lại các mối đe dọa đến tài sản trước khi họ cho phép các mối đe dọa cụ thể tiếp xúc với các tài sản đó. Bản thân các bên liên quan có thể không có khả năng đánh giá tất cả các khía cạnh của các biện pháp kiểm soát và có thể tìm được các đánh giá về các biện pháp kiểm soát từ các tổ chức bên ngoài.

6.5 Phương pháp tiếp cận

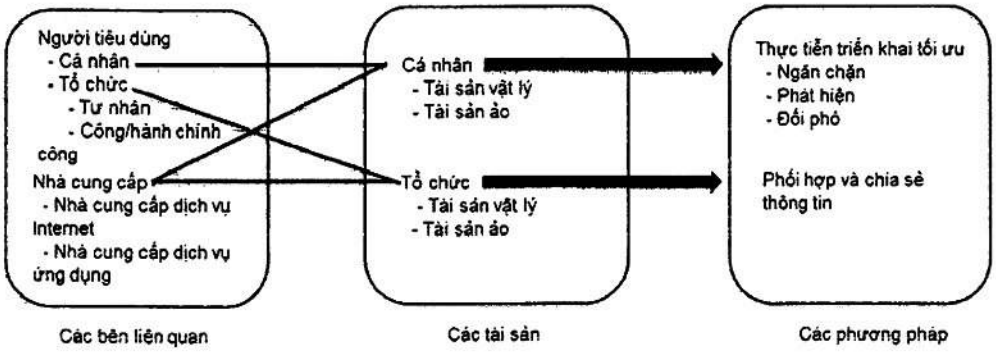
Một cách hiệu quả để đối đầu với những rủi ro an toàn không gian mạng là kết hợp nhiều chiến lược, thu hút sự quan tâm của các bên liên quan. Những chiến lược này bao gồm:

- Những thực tiễn triển khai tối ưu, cùng sự hợp tác của tất cả các bên liên quan để xác định và giải quyết vấn đề và rủi ro an toàn không gian mạng;
- Đào tạo đại trà cho người dùng và nhân viên, đưa ra một nguồn tài nguyên được tin cậy để làm thế nào nhận diện và giải quyết rủi ro an toàn không gian mạng cụ thể trong tổ chức cũng như trong không gian mạng;
- Cải tiến các giải pháp công nghệ để giúp bảo vệ người dùng khỏi các cuộc tấn công an toàn không gian mạng đã biết và chuẩn bị chống lại kiểu khai thác mới.

Hướng dẫn này tập trung vào việc cung cấp những thực tiễn triển khai tối ưu và giáo dục đại trà cho người dùng và nhân viên để hỗ trợ các bên liên quan trong không gian mạng trong việc đóng vai trò tích cực để giải quyết những thách thức an toàn không gian mạng. Nó bao gồm các hướng dẫn về:

- Vai trò;
- Chính sách;
- Phương pháp;
- Quy trình;
- Các kiểm soát kĩ thuật có thể áp dụng.

Hình 3 đưa ra tổng quan về những điểm nổi bật trong phương pháp tiếp cận đã đề cập trong tiêu chuẩn này. Tiêu chuẩn này không có ý định được sử dụng trực tiếp để cung cấp giáo dục đại trà cho người dùng. Thay vào đó, tiêu chuẩn này có ý định được sử dụng bởi các nhà cung cấp dịch vụ trong không gian mạng, cũng như các tổ chức cung cấp giáo dục không gian mạng liên quan đến việc giáo dục cho người dùng, để chuẩn bị cơ sở vật chất cho việc giáo dục đại trà người dùng.



Hình 3 – Tổng quan về phương pháp tiếp cận

7 Các bên liên quan trong không gian mạng

7.1 Tổng quan

Không gian mạng không thuộc bất cứ ai; tất cả mọi người đều có thể tham gia và là một phần trong đó.

Theo mục đích của tiêu chuẩn này, các bên liên quan trong không gian mạng được phân chia thành các nhóm sau:

- người tiêu dùng, bao gồm:
  - cá nhân;
  - các tổ chức tư nhân và tổ chức hành chính công;
- các nhà cung cấp, bao gồm nhưng không giới hạn là:
  - các nhà cung cấp dịch vụ internet;
  - các nhà cung cấp dịch vụ ứng dụng.

7.2 Người dùng

Như mô tả trong hình 3, người dùng liên quan tới các người dùng cá nhân cũng như các tổ chức tư nhân và tổ chức hành chính công. Các tổ chức tư nhân bao gồm các doanh nghiệp vừa và nhỏ (SMEs), cũng như các doanh nghiệp lớn. Chính phủ và các cơ quan hành chính công khác được gọi chung là các tổ chức hành chính công. Một cá nhân hoặc một tổ chức trở thành người dùng khi họ truy cập vào không gian mạng hoặc vào bất kỳ dịch vụ nào sẵn có trong không gian mạng.

Một người dùng cũng có thể là một nhà cung cấp nếu họ cung cấp một dịch vụ trong không gian mạng hoặc cho phép người dùng khác truy cập vào không gian mạng. Một người dùng sử dụng dịch vụ thế giới ảo có thể trở thành một nhà cung cấp bằng cách tạo ra các sản phẩm và dịch vụ ảo sẵn có cho người dùng khác.

7.3 Nhà cung cấp

Các nhà cung cấp liên quan tới các nhà cung cấp dịch vụ trong không gian mạng, cũng như các nhà cung cấp dịch vụ Internet cho phép người dùng truy cập vào không gian mạng và các dịch vụ khác nhau sẵn có trong không gian mạng.

Các nhà cung cấp cũng có thể được hiểu như là nhà vận chuyển hoặc nhà bán buôn, trái ngược với các nhà phân phối và nhà bán lẻ dịch vụ truy cập. Sự khác biệt này là rất quan trọng trong an toàn và đặc biệt là trong quan điểm thực thi pháp luật, bởi vì, trong trường hợp một nhà phân phối hoặc bán lẻ không thể cung cấp an toàn đầy đủ hoặc truy cập hợp pháp, các dịch vụ hỗ trợ mặc định sẽ trở lại nhà vận chuyển hoặc nhà bán buôn. Hiểu được bản chất của một nhà cung cấp dịch vụ là một yếu tố hữu ích trong việc quản lý rủi ro không gian mạng.

Các nhà cung cấp dịch vụ ứng dụng tạo ra các dịch vụ sẵn sàng cho người tiêu dùng thông qua phần mềm của họ. Những dịch vụ này có nhiều hình thức, bao gồm sự kết hợp của danh sách không đầy đủ như sau:

- việc chỉnh sửa, lưu trữ, phân phối tài liệu;
- môi trường ảo trực tuyến cho việc giải trí, truyền thông và tương tác giữa người sử dụng với nhau;
- kho phương tiện số trực tuyến cho các dịch vụ tổng hợp, lập chỉ mục, tìm kiếm, lưu trước, catalô, mua sắm và thanh toán;
- chức năng quản lý nguồn lực doanh nghiệp như nguồn nhân lực, tài chính và bảng lương, quản lý chuỗi cung ứng, mối quan hệ khách hàng, hóa đơn.

8 Tài sản trong không gian mạng

8.1 Tổng quan

Tài sản là bất cứ thứ gì có giá trị đối với cá nhân hoặc tổ chức. Có nhiều loại tài sản, danh sách chưa đầy đủ bao gồm:

a) Thông tin;
b) Phần mềm, ví dụ như một chương trình máy tính;
c) Tài sản vật lý, ví dụ như một máy tính;
d) Dịch vụ;
e) Con người, bao gồm năng lực, kỹ năng và kinh nghiệm của người đó;
f) Tài sản vô hình, ví dụ như danh tiếng và hình ảnh.

CHÚ THÍCH 1 Tài sản thường được coi đơn giản như là tài nguyên hay thông tin.

CHÚ THÍCH 2 Tiêu chuẩn TCVN 8709-1:2011 xác định một tài sản như thông tin hay tài nguyên được bảo vệ bởi các biện pháp kiểm soát của một TOE (mục tiêu đánh giá).

CHÚ THÍCH 3 Tiêu chuẩn ISO/IEC 19770-1 cho phép một tổ chức chứng minh rằng nó thực hiện quản lý tài sản phần mềm (SAM) tới tiêu chuẩn đủ để đáp ứng yêu cầu quản trị doanh nghiệp và đảm bảo hỗ trợ hiệu quả cho việc quản lý dịch vụ IT nói chung. ISO/IEC 19770 được thiết kế để gắn kết chặt chẽ và hỗ trợ ISO/IEC 20000.

CHÚ THÍCH 4 Tiêu chuẩn ISO/IEC 20000-1 khuyến khích việc chấp nhận một phương pháp tiếp cận quy trình tích hợp khi tiến hành thiết lập, triển khai, vận hành, giám sát, đo lường, đánh giá và cải thiện một hệ thống quản lý dịch vụ (SMS) để thiết kế và cung cấp các dịch vụ đáp ứng nhu cầu nghiệp vụ và yêu cầu khách hàng.

Với mục đích của tiêu chuẩn này, tài sản trong không gian mạng được phân thành các lớp sau đây:

- cá nhân;
- tổ chức.

Đối với cả hai lớp, một tài sản cũng có thể được phân loại thành

- tài sản vật chất, dạng hình thức tồn tại trong thế giới thực,
- tài sản ảo, chỉ tồn tại trong không gian mạng và không thể nhìn thấy hay chạm vào trong thế giới thực.

8.2 Tài sản cá nhân

Một trong các tài sản ảo chính là định danh cá nhân trực tuyến của người tiêu dùng và thông tin thẻ tín dụng trực tuyến của họ. Định danh trực tuyến được coi như là một tài sản, vì nó là định danh quan trọng đối với bất kỳ người tiêu dùng cá nhân nào trong không gian mạng.

Tài sản ảo khác của người tiêu dùng cá nhân cũng được tham chiếu trong thế giới ảo. Trong thế giới ảo, các thành viên thường sử dụng hình đại diện ảo để đại diện cho định danh của họ. Thông thường, tiền ảo được sử dụng cho các giao dịch ảo. Các hình đại diện và tiền tệ có thể được coi là tài sản của người tiêu dùng cá nhân.

Ví DỤ Một số ngân hàng hoạt động trong thế giới ảo sử dụng tiền trong thế giới ảo như một loại tiền chính thức.

Phần cứng và phần mềm công nghệ thông tin, cũng như các thiết bị kỹ thuật số cá nhân hoặc thiết bị đầu cuối, cho phép người tiêu dùng kết nối và giao tiếp trong không gian mạng, cũng được coi là tài sản trong ngữ cảnh của tiêu chuẩn này.

8.3 Tài sản tổ chức

Một khía cạnh quan trọng của không gian mạng là hạ tầng tạo lên nó. Hạ tầng này là một mạng lưới kết nối của các mạng, máy chủ và ứng dụng, thuộc nhiều nhà cung cấp dịch vụ. Tuy nhiên, độ tin cậy và tính sẵn sàng của hạ tầng là rất quan trọng trong việc đảm bảo các dịch vụ và ứng dụng không gian mạng luôn sẵn sàng cho bất cứ ai trong không gian mạng. Trong khi bất kỳ hạ tầng nào, được coi là một tài sản vật lý, cũng cho phép bất kỳ người dùng kết nối với không gian mạng hoặc truy cập các dịch vụ trong không gian mạng, thì có thể có sự chồng chéo với các biện pháp an toàn được đề xuất, như CIIP, an toàn Internet và an toàn mạng. Tuy nhiên, tiêu chuẩn này tập trung về việc đảm bảo rằng các vấn đề an toàn mà có thể ảnh hưởng đến các tài sản của tổ chức được giải quyết thích hợp mà không cần quá nhấn mạnh đến các vấn đề khác không nằm trong phạm vi của tiêu chuẩn này.

Bên cạnh tài sản vật chất, tài sản ảo của tổ chức cũng ngày càng đa dạng hơn. Các nhãn hiệu trực tuyến và các đại diện khác của tổ chức trong không gian mạng xác định duy nhất được tổ chức trong không gian mạng, cũng quan trọng như gạch và vữa của tổ chức đó.

Ví DỤ 1 Thông tin website và URL của một tổ chức là tài sản.

Ví DỤ 2 Các nước thậm chí còn thiết lập đại sứ quán trong một thế giới ảo chủ yếu để bảo vệ đại diện của đất nước.

Tài sản tổ chức khác bị lộ qua các điểm yếu trong không gian mạng bao gồm sở hữu trí tuệ (công thức, quy trình độc quyền, bằng sáng chế, kết quả nghiên cứu), kế hoạch và chiến lược nghiệp vụ (chiến lược giới thiệu và tiếp thị sản phẩm, thông tin cạnh tranh, thông tin tài chính và dữ liệu báo cáo).

9 Các mối đe dọa đối với an toàn không gian mạng

9.1 Các mối đe dọa

9.1.1 Tổng quan

Các mối đe dọa tồn tại trong không gian mạng được thảo luận liên quan tới tài sản trong không gian mạng.

Các mối đe dọa đến không gian mạng có thể được chia thành:

- các mối đe dọa đến tài sản cá nhân:
- các mối đe dọa đến tài sản tổ chức;

9.1.2 Các mối đe dọa đến tài sản cá nhân

Mối đe dọa đến tài sản cá nhân tập trung chủ yếu về các vấn đề định danh, bị công khai do rò rỉ hoặc bị đánh cắp thông tin cá nhân.

VÍ DỤ 1 Thông tin tín dụng có thể bị bán trên thị trường chợ đen, nơi có thể dễ dàng đánh cắp định danh trực tuyến.

Nếu một định danh trực tuyến của một người bị đánh cắp hoặc giả mạo, người đó có thể bị tước quyền truy cập dịch vụ và ứng dụng. Nghiêm trọng hơn, những hậu quả có thể trải dài từ các sự cố cấp tài chính tới các sự cố cấp quốc gia.

Truy cập trái phép vào thông tin tài chính của một người cũng tạo ra nguy cơ trộm cắp và gian lận tiền của người đó.

Mối đe dọa khác là các thiết bị đầu cuối có khả năng bị biến thành các máy tính ma (zombie) hoặc các chương trình phần mềm tự động (bot). Các thiết bị máy tính cá nhân có thể bị xâm hại và trở thành một phần của mạng máy tính ma (botnet) lớn hơn.

Bên cạnh đó, các tài sản ảo khác đang bị nhắm tới là các tài sản cá nhân trong thế giới ảo và trò chơi trực tuyến. Tài sản trong thế giới ảo hay thế giới của trò chơi trực tuyến có thể là mục tiêu tấn công và khai thác rất tốt.

VÍ DỤ 2 Trong một số trường hợp, chi tiết hình đại diện và tiền ảo sẽ là mục tiêu hàng đầu, có thể bị truy vết và chuyển đổi trở lại thế giới thực.

Trộm ảo và cướp ảo là một số thuật ngữ được tạo mới dành cho kiểu tấn công này. Trong trường hợp này, an toàn sẽ phụ thuộc vào việc bao nhiêu thông tin thế giới thực có thể bị truy cập, cũng như bản thân bộ khung an toàn của thế giới ảo được người quản trị xác định và triển khai đến đâu.

Các quy tắc và quy định về việc bảo vệ các tài sản vật chất thực tế có liên quan đến không gian mạng vẫn đang được viết, những vấn đề liên quan đến tài sản ảo hầu như không được đề cập. Phải thật cẩn thận và thận trọng bằng cách tiến hành khảo sát để đảm bảo việc bảo vệ thích hợp tài sản ảo của nó.

9.1.3 Các mối đe dọa đến tài sản của tổ chức

Các hình ảnh trực tuyến và các nghiệp vụ trực tuyến của tổ chức thường là mục tiêu của kẻ tội phạm có ý định xấu chứ không đơn thuần là nghịch ngợm.

Ví DỤ 1 Tổ chức tội phạm không gian mạng thường đe dọa các tổ chức rằng website của họ sẽ bị gỡ xuống hoặc website của họ sẽ phải chịu những hành động phá hoại khác như thay đổi nội dung website (deface).

Ví DỤ 2 Nếu URL của một tổ chức bị đăng ký hoặc bị đánh cắp bởi những kẻ trung gian và bán cho tổ chức không liên quan trong thế giới thực, các tổ chức nạn nhân có thể mất đi sự tin tưởng trực tuyến của người dùng.

Trong trường hợp cuộc tấn công thành công, thông tin cá nhân của các nhân viên, khách hàng, đối tác hay nhà cung cấp có thể bị lộ và bị dùng để chống lại các tổ chức. Nếu nó đã được tìm thấy nhưng được quản lý, bảo vệ không đầy đủ, sẽ góp phần vào sự mất mát của tổ chức.

Các quy định về lưu trữ tài chính cũng có thể bị phá vỡ nếu kết quả tổ chức bị lộ một cách trái phép.

Chính phủ không chỉ giữ thông tin về các vấn đề an toàn quốc gia, chiến lược, quân sự, tình báo trong số rất nhiều yếu tố khác liên quan đến chính phủ và nhà nước, mà còn giữ một loạt các thông tin về cá nhân, tổ chức và xã hội.

Chính phủ phải bảo vệ thông tin và hạ tầng của họ khỏi các truy cập và khai thác trái phép. Cùng với sự phát triển và mở rộng xu hướng cung cấp dịch vụ chính phủ điện tử qua không gian mạng, đây cũng là một kênh mới để phát động các cuộc tấn công và truy cập các thông tin trên, nếu thành công, có thể dẫn đến những rủi ro nghiêm trọng đối với quốc gia, chính phủ và xã hội của đất nước đó.

Trên một quy mô lớn hơn, hạ tầng hỗ trợ Internet, không gian mạng có thể là đích nhắm rất tốt của kẻ có ý đồ xấu. Điều này sẽ không ảnh hưởng đến các chức năng của không gian mạng vĩnh viễn, nhưng nó sẽ ảnh hưởng đến độ tin cậy và tính sẵn sàng của hạ tầng, thành phần góp phần vào sự an toàn của không gian mạng.

Ở cấp độ quốc gia hoặc quốc tế, không gian mạng là một vùng màu xám, nơi có chủ nghĩa khủng bố phát triển mạnh. Một trong những lý do đó là sự truyền thông dễ dàng được cung cấp bởi không gian mạng. Do bản chất của không gian mạng, đặc biệt là những thách thức trong việc xác định ranh giới và biên giới, rất khó để điều chỉnh và kiểm soát cách thức mà nó có thể được sử dụng.

Các nhóm khủng bố có thể mua hợp pháp các ứng dụng, dịch vụ và tài nguyên tạo thuận lợi cho họ hoặc họ có thể dùng đến các phương tiện bất hợp pháp giúp bảo mật tài nguyên của họ tránh bị phát hiện và theo dõi, đó có thể bao gồm một số lượng máy tính lớn thông qua mạng máy tính ma.

9.2 Các tác nhân đe dọa

Một tác nhân đe dọa là một cá nhân hay một nhóm người có vai trò trong việc thực hiện hay hỗ trợ tấn công.

Việc hiểu rõ về động cơ (tôn giáo, chính trị, kinh tế , ...), năng lực (kiến thức, nguồn tài trợ, quy mô, ...) và ý định (vui vẻ, tội phạm, gián điệp, ...) của họ là rất quan trọng trong việc đánh giá điểm yếu và rủi ro, cũng như trong việc phát triển và triển khai các biện pháp kiểm soát.

9.3 Các điểm yếu

Một điểm yếu là một yếu điểm của một tài sản hoặc biện pháp kiểm soát có thể bị khai thác bởi một hay nhiều mối đe dọa. Trong ngữ cảnh của một hệ thống thông tin, ISO/IEC TR 19791:2006 cũng xác định điểm yếu này là một lỗi, điểm yếu hay đặc tính của việc thiết kế hay triển khai một hệ thống thông tin (bao gồm cả biện pháp kiểm soát an toàn của nó) hoặc môi trường của nó, có thể là vô ý hay cố ý khai thác gây ảnh hưởng xấu đến tài sản hay hoạt động của tổ chức.

Việc đánh giá điểm yếu phải diễn ra liên tục. Khi hệ thống nhận được các bản vá lỗi, bản cập nhật hay các yếu tố mới được thêm vào, các điểm yếu mới có thể cũng được đề cập tới. Các bên liên quan cần phải có kiến thức và hiểu biết toàn diện về tài sản hoặc biện pháp kiểm soát, các tác nhân đe dọa và rủi ro liên quan, để thực hiện một đánh giá toàn diện.

CHÚ THÍCH TCVN 10295:2016 cung cấp hướng dẫn về việc xác định các điểm yếu.

Các điểm yếu đã biết, bao gồm tài sản hay biện pháp kiểm soát, nên được lưu giữ với các giao thức truy cập hạn chế và tách biệt, cả về vật lý và logic. Nếu xảy ra vi phạm truy cập và kho lưu trữ điểm yếu bị xâm hại, thì kho điểm yếu này sẽ là một trong những công cụ hiệu quả nhất mà các tác nhân đe dọa sử dụng để phát động cuộc tấn công.

Giải pháp khắc phục điểm yếu phải được tìm kiếm, triển khai và khi một giải pháp không thể thực hiện được, thì các biện pháp kiểm soát phải được đưa vào sử dụng. Phương pháp này nên áp dụng trên cơ sở ưu tiên để các điểm yếu có nguy cơ cao sẽ được giải quyết đầu tiên. Các thủ tục công bố thông tin điểm yếu có thể được thấy trong bộ khung về việc chia sẻ và phối hợp thông tin tại Điều 13 của tiêu chuẩn này.

CHÚ THÍCH Tiêu chuẩn ISO/IEC 29147 cung cấp hướng dẫn về việc phát hiện điểm yếu.

9.4 Cơ chế tấn công

9.4.1 Giới thiệu

Nhiều cuộc tấn công trong không gian mạng được thực hiện bằng cách sử dụng phần mềm độc hại, chẳng hạn như phần mềm gián điệp, sâu và virus. Thông tin thường được thu thập thông qua các kỹ thuật tấn công giả mạo. Tấn công có thể xảy ra như là một con đường tấn công đơn lẻ hoặc thực hiện như một cơ chế tấn công hỗn hợp. Những cuộc tấn công có thể được lan truyền qua các trang web đáng ngờ, dữ liệu tải về chưa được xác minh, thư rác, việc khai thác từ xa và thiết bị di động bị lây nhiễm.

Các cuộc tấn công được phân loại thành:

- Các cuộc tấn công từ bên trong mạng riêng;
- Các cuộc tấn công từ bên ngoài mạng riêng.

Có những trường hợp cuộc tấn công là kết hợp của cả hai tấn công từ bên trong và bên ngoài mạng riêng. Ngày càng có nhiều kĩ thuật khác tinh vi hơn được sử dụng để thực hiện các cuộc tấn công, như là dựa vào các trang web mạng xã hội và việc sử dụng các tập tin đã bị thay đổi trên các trang web hợp pháp.

Các cá nhân có xu hướng tin tưởng các thông điệp và nội dung nhận được từ những người liên lạc đã được chấp nhận trước đó trong hồ sơ của họ trên các trang web mạng xã hội của họ. Khi đối tượng tấn công đánh cắp được định danh, hắn có thể cải trang như một người liên lạc hợp pháp và tạo ra con đường mới để thực hiện nhiều kiểu tấn công.

Các trang web hợp pháp cũng có thể bị xâm nhập vào và một số tập tin của nó có thể bị thay đổi và sử dụng như một phương tiện để thực hiện các cuộc tấn công. Cá nhân có xu hướng tin tưởng các trang web thường truy cập, thường được đánh dấu trong các trình duyệt Internet của họ trong một thời gian dài và thậm chí còn sử dụng cơ chế an toàn như SSL (Secure Sockets Layer). Trong khi tính xác thực và tính toàn vẹn của thông tin được truyền đi hoặc nhận được vẫn còn ở đó, SSL không phân biệt giữa nội dung ban đầu và nội dung bị thay đổi mới được tạo bởi một đối tượng tấn công, do đó làm lộ thông tin người dùng của trang web bị tấn công.

Mặc dù biết được các kiểu tấn công, như trong các trường hợp ở trên, các cá nhân vẫn nên tuân theo các sự phòng ngừa nêu tại Điều 11 để bảo vệ tốt hơn cho mình.

9.4.2 Các cuộc tấn công từ bên trong mạng riêng

Những cuộc tấn công thường diễn ra bên trong mạng riêng của tổ chức, điển hình là mạng cục bộ, có thể khởi tạo bởi nhân viên hay người nào đó có quyền truy cập vào một máy tính hoặc mạng trong một tổ chức.

VÍ DỤ 1 Một trường hợp là người quản trị hệ thống có thể tận dụng các đặc quyền truy cập hệ thống mà họ nắm giữ, chẳng hạn như truy cập vào thông tin mật khẩu người dùng và sử dụng nó để khởi tạo một cuộc tấn công. Mặt khác, người quản trị hệ thống cũng có thể trở thành mục tiêu của một cuộc tấn công, trở thành phương tiện để những đối tượng tấn công có được thêm thông tin (tên người dùng, mật khẩu, ...), trước khi tiến hành tấn công mục tiêu dự định ban đầu của chúng.
Đối tượng tấn công có thể sử dụng các kĩ thuật như phần mềm nghe lén gói tin để lấy được mật khẩu hoặc thông tin nhận dạng khác. Ngoài ra, đối tượng tấn công có thể giả mạo thành một thực thể có thẩm quyền và hoạt động như người đứng giữa (man-in-the-middle) để ăn cắp thông tin nhận dạng.

VÍ DỤ 2 Một ví dụ là việc sử dụng các điểm truy cập giả (AP) để ăn cắp định danh. Trong trường hợp này, đối tượng tấn công có thể ngồi trong một quán cà phê, sân bay hoặc một nơi công cộng khác có cung cấp truy cập Wi-Fi miễn phí ra Internet. Trong một số trường hợp, những đối tượng tấn công thậm chí có thể giả mạo thành chủ sở hữu hợp pháp của các điểm truy cập không dây bằng cách sử dụng các Định danh tập dịch vụ (SSID). Nếu người dùng truy cập vào AP giả mạo này, đối tượng tấn công có thể hành động như người ở giữa (man-in-the-middle) và có được thông tin định danh và mật khẩu có giá trị của người sử dụng, ví dụ như thông tin tài khoản và mật khẩu ngân hàng, thư điện tử, ...

VÍ DỤ 3 Thông thường, chỉ cần ở gần một mạng Wi-Fi không được bảo vệ, chẳng hạn như ngồi trong một chiếc xe bên ngoài một ngôi nhà, là có thể ăn cắp thông tin trên mạng.

Bên cạnh các cuộc tấn công gây ra bởi con người, các máy tính bị lây nhiễm phần mềm độc hại cũng khởi động nhiều cuộc tấn công khác nhau bên trong mạng riêng.

VÍ DỤ 4 Nhiều phần mềm độc hại thường xuyên gửi các gói dữ liệu tới mạng riêng để tìm các máy tính xung quanh và sau đó cố gắng khai thác máy tính phát hiện ra.

VÍ DỤ 5 Một số phần mềm độc hại sử dụng chế độ hỗn độn của giao diện mạng của máy tính bị tiêm nhiễm để nghe lén lưu lượng truyền đi trong mạng riêng.

VÍ DỤ 6 Trình theo dõi thao tác bàn phím (key logger) là các ứng dụng phần cứng hoặc phần mềm sẽ bắt tất cả phím bấm trên hệ thống mục tiêu. Điều này có thể được thực hiện bí mật để theo dõi hành động của người dùng. Trình theo dõi thao tác bàn phím (key logger) thường được sử dụng để bắt thông tin xác thực từ các trang đăng nhập ứng dụng.

9.4.3 Các cuộc tấn công từ bên ngoài mạng riêng (ví dụ như Internet)

Có rất nhiều cuộc tấn công khác nhau có thể được thực hiện từ bên ngoài mạng riêng, bao gồm cả Internet.

Trong khi các cuộc tấn công ban đầu thường nhắm đến các hệ thống giao tiếp ra bên ngoài (ví dụ như bộ định tuyến, máy chủ, tường lửa, trang web, ...), đối tượng tấn công cũng có thể tìm cách khai thác các tài sản trong mạng riêng.

Các phương pháp tấn công cũ liên tục được cải thiện và các phương pháp mới luôn được phát triển. Những đối tượng tấn công đang ngày càng khôn ngoan hơn, thường kết hợp các kỹ thuật và cơ chế tấn công khác nhau để tối đa hóa thành công của chúng, làm cho việc phát hiện tấn công và phòng ngừa ngày càng khó khăn hơn.

Các công cụ quét cổng là một trong những công cụ lâu đời nhất và vẫn còn rất hiệu quả thường được đối tượng tấn công sử dụng. Chúng quét tất cả các cổng hiện có trên máy chủ để xác nhận cổng nào đang "mở". Đây thường là một trong những bước thực hiện đầu tiên khi đối tượng tấn công muốn tấn công vào hệ thống mục tiêu.

Những cuộc tấn công khai thác giao thức hoặc điểm yếu thiết kế của ứng dụng có thể biến thành nhiều cuộc tấn công DoS khác nhau vào các máy chủ ứng dụng hoặc thiết bị mạng khác.

VÍ DỤ Với sự giúp đỡ của mạng máy tính ma, một số lượng lớn các cuộc tấn công DoS có thể được thực hiện, có thể làm giảm mạnh lượng truy cập của quốc gia trong không gian mạng.

Với sự phát triển của các ứng dụng ngang hàng, thường được sử dụng để chia sẻ các tập tin như âm nhạc kỹ thuật số, video, hình ảnh, ..., những đối tượng tấn công đang trở nên ngày càng tinh vi hơn trong cách che giấu bản thân và mã độc hại của chúng bằng cách sử dụng các tập tin trao đổi như một mã Trojan cho các cuộc tấn công của chúng.

Tràn bộ đệm – buffer overflow là một phương pháp phổ biến khác về xâm hại các máy chủ trên Internet. Bằng cách khai thác các điểm yếu trong mã chương trình và gửi các chuỗi ký tự dài hơn so với thông thường, những đối tượng tấn công làm cho máy chủ hoạt động vượt quá môi trường (được kiểm soát) bình thường của nó, do đó thuận lợi cho việc chèn/thực hiện các mã độc hại.
Một kỹ thuật khác là giả mạo IP, những đối tượng tấn công sẽ ngụy trang địa chỉ IP liên quan tới tin nhắn của hắn như một nguồn đã biết đáng tin cậy, nhờ vậy có thể truy cập trái phép vào hệ thống.

10 Vai trò các bên liên quan trong an toàn không gian mạng

10.1 Tổng quan

Để cải thiện tình trạng an toàn không gian mạng, các bên liên quan trong không gian mạng cần phải đóng vai trò tích cực trong việc sử dụng và phát triển của Internet. Những vai trò này có thể trùng với

vai trò cá nhân và tổ chức của họ trong mạng lưới cá nhân hay tổ chức của họ. Thuật ngữ mạng tổ chức đề cập về việc kết hợp mạng riêng (mạng intranet đặc thù), mạng riêng mở rộng (mạng extranet) và mạng mở công cộng của tổ chức. Với mục đích của tiêu chuẩn này, các mạng hiển thị công khai là những mạng tiếp xúc với Internet, ví dụ để lưu trữ một trang web. Vì sự trùng lặp này, các vai trò này có thể không có lợi ích trực tiếp hoặc không đáng kể đối với các cá nhân và tổ chức có liên quan. Tuy nhiên, chúng lại rất quan trọng để tăng cường an toàn không gian mạng khi mà tất cả các hành động đều liên quan tới nhau.

10.2 Vai trò của người dùng

10.2.1 Giới thiệu

Người dùng có thể xem hoặc thu thập thông tin, cũng như cung cấp thông tin cụ thể trong không gian ứng dụng của không gian mạng hoặc mở cho các thành viên hoặc nhóm giới hạn trong không gian của ứng dụng hoặc cộng đồng chung. Hành động của người dùng trong những vai trò này có thể là thụ động hay chủ động và có thể đóng góp trực tiếp và gián tiếp đến tình trạng an toàn không gian mạng.

10.2.2 Vai trò của các cá nhân

Người dùng cá nhân trong không gian mạng có thể có các vai trò khác nhau trong ngữ cảnh và ứng dụng khác nhau. Vai trò của người dùng có thể bao gồm, nhưng không giới hạn, những điều sau đây:

- Người dùng ứng dụng không gian mạng nói chung, hay người dùng nói chung, như là người chơi trò chơi trực tuyến, người sử dụng tin nhắn tức thời hoặc lướt web;
- Người mua/ bán, tham gia trong việc đặt hàng và dịch vụ trên các trang đấu giá hay chợ trực tuyến cho những người mua quan tâm và ngược lại;
- Người viết blog và những người đóng góp nội dung khác (ví dụ, tác giả của một bài viết trên wiki), trong đó thông tin văn bản và đa phương tiện (ví dụ, video clip) được công khai tới cộng đồng chung hoặc một số lượng hạn chế đối tượng;
- Nhà cung cấp ứng dụng độc lập (IAP) trong một ngữ cảnh ứng dụng (chẳng hạn như một trò chơi trực tuyến) hoặc không gian mạng nói chung;
- Thành viên của một tổ chức (như một nhân viên của một công ty hoặc các hình thức khác có liên kết với công ty);
- Các vai trò khác. Đó có thể là một người sử dụng bị chỉ định một vai trò không có chủ ý hoặc không có sự đồng ý của người đó.

VÍ DỤ Khi người dùng ghé thăm một trang web đòi hỏi xác nhận quyền và vô tình truy cập được, người dùng có thể bị coi là một kẻ xâm nhập.

Trong mỗi vai trò, các cá nhân có thể xem hoặc thu thập thông tin, cũng như cung cấp một số thông tin cụ thể trong không gian ứng dụng của không gian mạng hoặc mở cho các thành viên hoặc các nhóm giới hạn trong không gian của ứng dụng hoặc cộng đồng chung. Hành động của cá nhân trong những

vai trò này có thể là thụ động hay chủ động và có thể đóng góp trực tiếp và gián tiếp đến tình trạng an toàn không gian mạng.

VÍ DỤ 1 Nếu một IAP cung cấp một ứng dụng có chứa điểm yếu an toàn, điểm yếu này có thể bị tội phạm không gian mạng lợi dụng như một kênh tiếp cận người dùng của ứng dụng.

VÍ DỤ 2 Những người viết blog hay người đóng góp nội dung khác có thể nhận được một yêu cầu trả lời các câu hỏi về nội dung của họ. Trong các trả lời ấy, họ có thể vô tình tiết lộ thêm thông tin cá nhân hoặc công ty nhiều hơn so với mong muốn.

VÍ DỤ 3 Một cá nhân, đóng vai trò là người mua hoặc người bán có thể vô tình tham gia vào các giao dịch tội phạm bán hàng hóa bị đánh cắp hoặc các hoạt động rửa tiền.

Do đó, như ở thế giới thực, mỗi cá nhân tiêu dùng cần sử dụng thận trọng trong từng vai trò và mọi vai trò họ đảm nhiệm trong không gian mạng.

10.2.3 Vai trò của các tổ chức

Các tổ chức thường xuyên sử dụng không gian mạng để quảng bá thông tin công ty, các thông tin liên quan, như thị trường sản phẩm và dịch vụ. Các tổ chức cũng sử dụng không gian mạng như một phần của mạng lưới của họ để gửi và nhận các thông điệp điện tử (ví dụ, thư điện tử) và các tài liệu khác (ví dụ, tập tin truyền đi).

Cùng các quy tắc để trở thành tập thể tốt, các tổ chức phải mở rộng trách nhiệm tập thể đến không gian mạng bằng các bảo đảm chủ động rằng sự chủ động và các hành động của họ trong không gian mạng không tạo ra các rủi ro an toàn trong tương lai ở trong không gian mạng. Một số biện pháp chủ động bao gồm:

- quản lý an toàn thông tin thích hợp bằng cách thực hiện và vận hành một hệ thống quản lý an toàn thông tin hiệu quả (ISMS);

CHÚ THÍCH 1 TCVN ISO/IEC 27001:2009 cung cấp các yêu cầu cho hệ thống quản lý an toàn thông tin.

- giám sát và phản ứng an toàn thích hợp;
- kết hợp an toàn như một phần của vòng đời phát triển phần mềm (SDLC), nơi mà mức độ an toàn được xây dựng trong các hệ thống cần phải được xác định dựa trên mức độ quan trọng của các dữ liệu của tổ chức;
- giáo dục an toàn thường xuyên cho người dùng trong tổ chức, liên tục cập nhật công nghệ và theo dõi sự phát triển công nghệ mới nhất;
- hiểu và sử dụng các kênh thích hợp để truyền thông với các đối tác và các nhà cung cấp dịch vụ về các vấn đề an toàn phát hiện ra trong quá trình sử dụng.

CHÚ THÍCH 2 Tiêu chuẩn ISO/IEC 29147 sẽ cung cấp các hướng dẫn về phát hiện điểm yếu.

CHÚ THÍCH 3 Tiêu chuẩn ISO/IEC 27031 cung cấp hướng dẫn về sự sẵn sàng ICT cho duy trì nghiệp vụ liên tục.

CHÚ THÍCH 4 ISO/LEC 27035 cung cấp hướng dẫn quản lý sự cố an toàn thông tin.

CHÚ THÍCH 5 Tiêu chuẩn ISO/IEC 27034-1 cung cấp hướng dẫn về an toàn ứng dụng.

Chính phủ, các cơ quan quản lý và thực thi pháp luật chính, có thể có vai trò quan trọng sau đây:

- tư vấn vai trò và trách nhiệm của các tổ chức trong không gian mạng;

- chia sẻ thông tin với các bên liên quan về các xu hướng và sự phát triển công nghệ mới nhất;
- chia sẻ thông tin với các bên liên quan về những rủi ro an toàn phổ biến hiện nay;
- là nơi tiếp nhận bất kỳ thông tin nào, dù đóng hay mở, liên quan đến những rủi ro an toàn cho không gian mạng;
- là người điều phối chính để phổ biến thông tin và sắp xếp các nguồn lực cần thiết, cả ở cấp quốc gia lẫn cấp độ doanh nghiệp, trong thời gian phát sinh khủng hoảng do một cuộc tấn công mạng quy mô lớn.

10.3 Vai trò của nhà cung cấp

Các tổ chức cung cấp dịch vụ có thể bao gồm:

- nhà cung cấp việc truy cập cho các nhân viên và đối tác tới không gian mạng,
- nhà cung cấp dịch vụ cho người dùng của không gian mạng hoặc cho một cộng đồng khép kín (ví dụ, người dùng đã đăng ký) hoặc cộng đồng chung, thông qua việc cung cấp các ứng dụng không gian mạng.

VÍ DỤ Các dịch vụ này có thể là chợ giao dịch trực tuyến; dịch vụ diễn đàn thảo luận nền tảng; dịch vụ viết blog, dịch vụ mạng xã hội.

Các nhà cung cấp dịch vụ cũng là các tổ chức tiêu dùng. Họ cũng được mong đợi sẽ thực hiện các vai trò và trách nhiệm giống như các tổ chức tiêu dùng. Là nhà cung cấp dịch vụ, họ có thêm trách nhiệm trong việc duy trì hoặc thậm chí tăng cường an toàn của không gian mạng bằng cách:

- cung cấp sản phẩm và dịch vụ an toàn và bảo mật;
- cung cấp hướng dẫn an toàn và bảo mật cho người dùng cuối;
- cung cấp đầu vào an toàn cho các nhà cung cấp khác và cho người dùng về các xu hướng và việc theo dõi lưu lượng truy cập trong mạng lưới và dịch vụ của họ.

11 Hướng dẫn cho các bên liên quan

11.1 Tổng quan

Điều này tập trung hướng dẫn vào ba miền chính:

- hướng dẫn an toàn cho người dùng;
- quản lý rủi ro an toàn thông tin nội bộ của một tổ chức;
- các yêu cầu an toàn mà các nhà cung cấp nên chỉ rõ cho người dùng thực hiện.

Các khuyến nghị được cấu trúc như sau:

a) giới thiệu về cách đánh giá và xử lý rủi ro;
b) các hướng dẫn cho người dùng;
c) các hướng dẫn cho các tổ chức, bao gồm cả các nhà cung cấp dịch vụ:
   - quản lý rủi ro an toàn thông tin trong nghiệp vụ;
   - các yêu cầu an toàn cho dịch vụ lưu trữ và các dịch vụ ứng dụng khác.

11.2 Đánh giá và xử lý rủi ro

TCVN 31000, *Quản lý rủi ro - Các nguyên tắc và hướng dẫn*, cung cấp các nguyên tắc và các hướng dẫn về quản lý rủi ro, trong khi tiêu chuẩn TCVN 10295, *Công nghệ thông tin - Kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin,* cung cấp các hướng dẫn và quy trình quản lý rủi ro an toàn thông tin trong một tổ chức, hỗ trợ cho các yêu cầu của ISMS theo tiêu chuẩn TCVN ISO/IEC 27001. Những hướng dẫn và quy trình này được soát xét đủ để giải quyết vấn đề quản lý rủi ro trong ngữ cảnh của không gian mạng.

TCVN 10295:2016 không đưa ra bất kỳ một phương pháp cụ thể nào về quản lý rủi ro an toàn thông tin. Điều đó phụ thuộc vào việc người dùng và các nhà cung cấp xác định phương pháp tiếp cận của họ để quản lý rủi ro. Một số phương pháp hiện tại có thể được sử dụng theo bộ khung mô tả trong TCVN 10295 để triển khai các yêu cầu của một ISMS.

Khi xác định một phương pháp tiếp cận để quản lý rủi ro, cần chú ý đến các khía cạnh sau:

- Xác định các tài sản quan trọng: Việc kết nối đến hoặc sử dụng không gian mạng sẽ mở rộng phạm vi của việc xác định tài sản. Việc xác định các tài sản quan trọng không phải là cách hiệu quả để bảo vệ tất cả tài sản, nhưng là điều cần thiết vì các tài sản quan trọng cần được xác định để có những biện pháp bảo vệ chúng thích hợp hơn. Việc xác định nên được thực hiện trong ngữ cảnh nghiệp vụ, thông qua việc xem xét các tác động của việc mất mát hoặc suy giảm của một tài sản trong nghiệp vụ.
- Xác định các rủi ro: Các bên liên quan nên xem xét và giải quyết một cách thích hợp các rủi ro, các mối đe dọa và cuộc tấn công khi tham gia vào không gian mạng.
- Trách nhiệm: Khi tham gia vào không gian mạng, một bên liên quan phải chấp nhận thêm trách nhiệm đối với các bên liên quan khác. Điều này bao gồm:
    - Sự công nhận: Nhận thức được nguy cơ tiềm năng mà các bên liên quan tham gia có thể giới thiệu trong không gian mạng nói chung và đặc biệt là trong các hệ thống thông tin khác của các bên liên quan.
    - Báo cáo: Là cần thiết, bao gồm cả các báo cáo mà các bên liên quan bên ngoài tổ chức đưa ra, liên quan đến những rủi ro, sự cố và các mối đe dọa.
    - Chia sẻ thông tin: Cũng giống báo cáo, nó là cần thiết để chia sẻ thông tin có liên quan với các bên liên quan khác.
    - Đánh giá rủi ro: Nó là cần thiết để xác định phạm vi rủi ro mà hành động của một bên liên quan có thể gây ra cho các bên liên quan khác.
    - Quy định/ Lập pháp: Khi kết nối với không gian mạng, ranh giới pháp lý trở nên khó phân biệt, hơn nữa đôi khi còn gây mâu thuẫn, các yêu cầu cần được áp dụng.
- Chấm dứt hoạt động hệ thống hoặc dịch vụ: Khi một hệ thống hoặc dịch vụ không còn cần thiết, chúng cần được chấm dứt hoạt động mà vẫn đảm bảo rằng các dịch vụ hoặc các giao

diện có liên quan không bị ảnh hưởng. Mọi thông tin liên quan đến an toàn phải được chấm dứt hiệu lực để đảm bảo rằng hệ thống mà nó giao tiếp hoặc có liên quan không bị ảnh hưởng.

- Tính nhất quán: Các phương pháp quản lý rủi ro được áp dụng trên toàn bộ không gian mạng. Trong các phương pháp này, người dùng và các nhà cung cấp không gian mạng được phân công trách nhiệm các hoạt động cụ thể, chẳng hạn như lên kế hoạch dự phòng, khôi phục thảm họa, việc phát triển và triển khai các chương trình bảo vệ cho các hệ thống dưới các biện pháp kiểm soát của họ.

Nói chung, phương pháp quản lý rủi ro trong TCVN 10295 bao phủ toàn bộ vòng đời của một hệ thống nói chung, do đó rất hữu dụng cho các hệ thống an toàn mới cũng như cho các hệ thống kế thừa. Khi được gắn liền với việc xử lý hệ thống, nó rất phù hợp để áp dụng cho tất cả các mô hình nghiệp vụ. Các quy trình trong bộ khung này coi các hệ thống mạng và dịch vụ như một hệ thống nhúng, bao gồm các hệ thống con cung cấp dịch vụ công cộng và hệ thống con cá nhân cung cấp các dịch vụ nội bộ; hoặc coi mỗi dịch vụ cá nhân tách biệt với nhau (ví dụ, lưu trữ web) và mô tả các điều khoản trong các hệ thống tương tác riêng biệt. Nó có thể có lợi thế là xem xét tất cả mọi thứ cần thiết để hỗ trợ cho các dịch vụ của nhà cung cấp như việc một hệ thống lớn có thể được chia thành các hệ thống nhỏ hơn, mỗi trong số đó cung cấp dịch vụ thị trường hoặc một phần của hạ tầng.

Các khía cạnh quan trọng cần nhớ khi xem xét các mục tiêu, mục đích của an toàn không gian mạng là:

a) bảo vệ an toàn tổng thể của không gian mạng;

b) lên kế hoạch cho các trường hợp khẩn cấp và khủng hoảng qua việc thực hành, cập nhật các kế hoạch đối phó và kế hoạch cho vận hành liên tục;

c) giáo dục các bên liên quan về an toàn không gian mạng và thực hành quản lý rủi ro;

d) đảm bảo chia sẻ thông tin về các mối đe dọa kịp thời, phù hợp và chính xác giữa bên thực thi pháp luật, cộng đồng trí thức và những người có quyết định quan trọng liên quan đến không gian mạng;

e) Thiết lập sự phối hợp giữa các bên liên quan và liên ngành có hiệu quả để giải quyết các vấn đề phụ thuộc lẫn nhau quan trọng, bao gồm cả việc nhận thức tình huống sự cố và quản lý sự cố của các bên liên quan và liên ngành.

Mục đích và mục tiêu a) tới c) liên quan trực tiếp đến các nhà cung cấp dịch vụ, người chịu trách nhiệm cho các thiết bị và dịch vụ mà họ kiểm soát. Mục đích và mục tiêu d) và e) liên quan trực tiếp tới các nhà cung cấp dịch vụ tham gia tích cực vào hoạt động chia sẻ thông tin và phối hợp.

Mục tiêu của nhà cung cấp dịch vụ cụ thể, chẳng hạn như là các dịch vụ để cung cấp, liên quan tới ngữ cảnh nghiệp vụ.

11.3 Hướng dẫn cho người dùng

Tiêu chuẩn này không hướng tới các cá nhân cụ thể trong không gian mạng, mà tập trung vào các tổ chức cung cấp dịch vụ cho người dùng và các tổ chức yêu cầu nhân viên hay người dùng cuối của họ tập luyện sử dụng không gian mạng an toàn để quản lý rủi ro an toàn không gian mạng có hiệu quả. Trong ngữ cảnh về các chương trình đào tạo và nâng cao nhận thức và cung cấp dịch vụ cho người dùng, các hướng dẫn về các vai trò và an toàn của người dùng trong không gian mạng và cách làm thế nào để họ có ảnh hưởng tích cực đến tình trạng của an toàn không gian mạng được đưa ra như một hướng dẫn cho việc thiết kế và phát triển nội dung bởi các tổ chức này.

Như đã giải thích tại Điều 10.2, người dùng có thể xem hoặc thu thập thông tin, cũng như cung cấp thông tin cụ thể nhất định trong một không gian mạng hoặc mở cho một số lượng thành viên hay nhóm giới hạn trong không gian ứng dụng của không gian mạng hoặc cộng đồng chung. Hành động của người dùng trong vai trò này, có thể là thụ động hay chủ động, có thể đóng góp trực tiếp và gián tiếp đến tình trạng an toàn không gian mạng.

Ví dụ, như một IAP, nếu ứng dụng được cung cấp có chứa điểm yếu bảo mật, nó có thể bị khai thác bởi tội phạm không gian mạng và tận dụng nó như một kênh để tiếp cận tới người dùng vô tội của ứng dụng. Những người viết blog hoặc những người đóng góp nội dung khác, họ có thể nhận được một yêu cầu trả lời các câu hỏi tưởng như vô hại về nội dung của họ, khi đó họ có thể vô tình tiết lộ thêm thông tin cá nhân hoặc công ty nhiều hơn so với mong muốn. Là một người mua hoặc người bán, một người dùng có thể vô tình tham gia vào các giao dịch phạm tội bán hàng hóa bị đánh cắp hoặc các hoạt động rửa tiền. Do đó, cũng như trong thế giới vật chất, người dùng cần phải thận trọng trong từng vai trò của họ trong không gian mạng.

Nhìn chung, người dùng nên lưu ý hướng dẫn như sau:

a) Học và hiểu chính sách bảo mật và riêng tư của các trang web và ứng dụng liên quan, như trang web đó được công bố bởi nhà cung cấp nào.

b) Học và hiểu được rủi ro an toàn và riêng tư liên quan và xác định các biện pháp kiểm soát áp dụng thích hợp. Tham gia vào các diễn đàn thảo luận trực tuyến có liên quan hoặc hỏi những người biết thông tin về trang web hoặc ứng dụng trước khi cung cấp thông tin cá nhân hay tổ chức hoặc các thông tin tham gia và đóng góp cho các cuộc thảo luận đó.

c) Thiết lập và thực hiện một chính sách riêng tư cá nhân để bảo vệ định danh bằng cách xác định các loại thông tin cá nhân hiện có và chia sẻ các yếu tố liên quan đến thông tin đó.

d) Quản lý định danh trực tuyến. Sử dụng định danh khác nhau cho các ứng dụng web khác nhau và hạn chế tối đa việc chia sẻ thông tin cá nhân cho mỗi trang web hoặc ứng dụng yêu cầu thông tin đó. Đăng ký định danh trực tuyến trên các trang web mạng xã hội phổ biến ngay cả khi tài khoản đó không hoạt động.

VÍ DỤ Đăng nhập một lần (SSO) là một hình thức quản lý định danh trực tuyến.

e) Báo cáo sự kiện hoặc cuộc gặp gỡ đáng ngờ với các cơ quan có thẩm quyền liên quan (xem Phụ lục B có ví dụ về danh sách địa chỉ liên lạc công khai).

f) Là một bên mua hoặc bên bán, việc đọc và hiểu chính sách an toàn và bảo mật các trang web mua bán trực tuyến và thực hiện các bước để xác minh tính xác thực của các bên liên quan tham gia là cần thiết. Không chia sẻ dữ liệu cá nhân, bao gồm cả thông tin ngân hàng, trừ khi có mối quan tâm thật về việc mua hay bán. Sử dụng một cơ chế thanh toán đáng tin cậy.

g) Là một IAP, thực hiện phát triển phần mềm an toàn và cung cấp một giá trị băm của mã trực tuyến để các đối tác nhận được có thể xác minh giá trị khi cần thiết, đảm bảo tính toàn vẹn của mã này. Cung cấp tài liệu về các chính sách riêng tư, an toàn cho mã, thực hiện và tôn trọng sự riêng tư của mã người dùng.

h) Là một người viết blog hay những người đóng góp nội dung khác (bao gồm cả người bảo trì trang web), đảm bảo rằng sự riêng tư của các bên liên quan và các thông tin nhạy cảm không bị tiết lộ qua các blog hoặc các ấn phẩm trực tuyến. Các ý kiến nhận xét và thông tin đăng trên trang web cần được đảm bảo rằng chúng không chứa bất kỳ nội dung độc hại nào như các liên kết đến các trang web giả mạo trực tuyến hay liên kết tải về các phần mềm độc hại.

i) Là một thành viên của một tổ chức, một người dùng cá nhân nên học và hiểu chính sách an toàn thông tin doanh nghiệp và đảm bảo rằng thông tin nhạy cảm không bị phát tán do cố ý hay do sự cố trên bất kỳ trang web nào trong không gian mạng, trừ khi có sự cho phép trước đó.

j) Các vai trò khác. Khi một người dùng truy cập vào một trang web yêu cầu cấp quyền và khi vô tình truy cập được, người dùng có thể bị coi là một kẻ xâm nhập. Thoát khỏi trang web ngay lập tức và báo cáo cho cơ quan có liên quan, vì thực tế là việc trang web có thể truy cập được có thể là một dấu hiệu trang web đó đã bị xâm hại.

11.4 Hướng dẫn cho các tổ chức và các nhà cung cấp dịch vụ

11.4.1 Tổng quan

Các biện pháp kiểm soát quản lý rủi ro an toàn không gian mạng phụ thuộc đáng kể vào tính thuần thục của các quy trình quản lý an toàn bên trong tổ chức (kể cả bên cung cấp dịch vụ). Trong khi hướng dẫn đưa ra ở đây là tùy ý thực hiện đối với các tổ chức, nhưng vẫn khuyến nghị rằng các nhà cung cấp dịch vụ hãy coi các hướng dẫn này là biện pháp cơ bản bắt buộc.

Các hướng dẫn tại điều này có thể được tổng kết thành:

- Quản lý rủi ro an toàn thông tin trong nghiệp vụ.
- Giải quyết các yêu cầu an toàn cho dịch vụ lưu trữ web cũng như các dịch vụ ảo khác.
- Cung cấp hướng dẫn an toàn cho các người dùng.

11.4.2 Quản lý rủi ro an toàn thông tin trong nghiệp vụ

11.4.2.1 Hệ thống quản lý an toàn thông tin

Ở cấp độ doanh nghiệp, các tổ chức kết nối với không gian mạng nên thực hiện một hệ thống quản lý an toàn thông tin (ISMS) để xác định và quản lý rủi ro an toàn thông tin liên quan đến nghiệp vụ. Bộ Tiêu chuẩn TCVN 11238:2015 về hệ thống quản lý an toàn thông tin cung cấp các hướng dẫn cần thiết và thực tiễn nhất để triển khai một hệ thống như vậy.

Một xem xét quan trọng trong việc thực hiện một ISMS là cần đảm bảo rằng tổ chức này có một hệ thống xác định, đánh giá, xử lý và quản lý rủi ro an toàn thông tin liên quan đến nghiệp vụ của mình một cách liên tục, bao gồm cả các điều khoản về các dịch vụ trên Internet, hướng trực tiếp tới người dùng cuối hoặc thuê bao.

CHÚ THÍCH 1 Theo tiêu chuẩn TCVN 10295, Công nghệ thông tin - Kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin, cung cấp hướng dẫn quản lý rủi ro an toàn thông tin trong một tổ chức, hỗ trợ các yêu cầu của ISMS theo tiêu chuẩn TCVN ISO/IEC 27001.

CHÚ THÍCH 2 Tiêu chuẩn TCVN 31000, Quản lý rủi ro - Các nguyên tắc và hướng dẫn, cung cấp các nguyên tắc và hướng dẫn về quản lý rủi ro.

Các tổ chức cũng có thể xem xét một chứng nhận chính thức theo các yêu cầu ISMS, chẳng hạn như tiêu chuẩn TCVN ISO/IEC 27001.

Như một phần của việc triển khai ISMS, một tổ chức cũng nên thiết lập một bộ phận giám sát, ứng cứu sự cố an toàn và phối hợp các hoạt động ứng phó sự cố của họ với các tổ chức CIRT, CERT, hay CSIRT bên ngoài. Các điều khoản của ứng cứu sự cố khẩn cấp nên bao gồm việc giám sát và đánh giá tình trạng an toàn về việc sử dụng các của dịch vụ của tổ chức bởi người dùng cuối và khách hàng và cung cấp các hướng dẫn hỗ trợ các bên có liên quan để ứng phó sự cố an toàn có hiệu quả.

CHÚ THÍCH Tiêu chuẩn ISO/IEC 27035, Công nghệ thông tin - Kỹ thuật an toàn - Quản lý sự cố an toàn thông tin, cung cấp hướng dẫn về quản lý sự cố an toàn thông tin.

11.4.2.2 Cung cấp sản phẩm an toàn

Một số tổ chức phát triển và phát hành thanh công cụ, trình quay số hoặc mã chương trình trên trình duyệt web của riêng mình để cung cấp dịch vụ giá trị gia tăng cho người dùng hoặc tạo điều kiện dễ dàng truy cập vào các dịch vụ hoặc các ứng dụng của tổ chức. Trong những trường hợp như vậy, cần có một thỏa thuận người dùng cuối thích hợp với một ngôn ngữ thích hợp, kết hợp với tuyên bố về chính sách mã hóa, chính sách riêng tư của tổ chức. Người dùng có thể thay đổi quyết định của họ sau này hoặc báo cáo vượt cấp bất kỳ vấn đề nào mà họ có quan tâm đến các chính sách và thực tiễn. Khi một thỏa thuận được sử dụng, nó nên được kiểm soát theo phiên bản và tổ chức phải đảm bảo rằng người dùng cuối ký tên đồng ý.

Để có độ tin cậy ở mức độ cao về sự an toàn của các sản phẩm phần mềm, chúng cần được xác nhận độc lập theo Chương trình tiêu chuẩn chung (Common Criteria scheme), như mô tả ở TCVN 8709.

Các tổ chức nên cung cấp tài liệu về hành vi mã chương trình và đưa ra đánh giá về việc liệu các hành vi có thể hoạt động sai khi ở các khu vực tiềm ẩn (có thể chứa phần mềm gián điệp hoặc phần mềm lừa đảo) hay không. Trong trường hợp này, cần thuê một chuyên gia đánh giá chất lượng phù hợp để xem mã chương trình hoạt động sai theo tiêu chí khách quan của nhà cung cấp phần mềm chống gián điệp có gắn liền với các thực tiễn tối ưu hay không để công cụ phần mềm mà tổ chức cung cấp cho người dùng cuối không bị các nhà cung cấp phần mềm chống gián điệp gán nhãn là phần mềm gián điệp hay phần mềm quảng cáo. Nhiều nhà cung cấp phần mềm chống gián điệp công khai các tiêu chí mà họ đánh giá phần mềm.

Các tổ chức cần thực hiện ký số cho những chương trình của họ để các nhà cung cấp chống phần mềm độc hại và chống phần mềm gián điệp có thể dễ dàng xác định chủ sở hữu của một tập tin và nhà cung cấp phần mềm độc lập ISV, những người sản xuất phần mềm phù hợp thực tiễn nhất sẽ được phân loại là an toàn trước khi phân tích.

Nên có một tổ chức tìm ra các công nghệ phần mềm hữu ích có thể giúp giảm thiểu các vấn đề phần mềm gián điệp hoặc phần mềm độc hại, tổ chức nên xem xét hợp tác và làm việc với các nhà cung cấp để mở rộng thêm quy mô.

Để đáp ứng các yêu cầu này, giáo dục an toàn cho các nhà phát triển là rất quan trọng. Một vòng đời phát triển phần mềm an toàn nên được sử dụng để giảm thiểu tối đa các điểm yếu phần mềm có, nhờ đó cung cấp một sản phẩm phần mềm an toàn hơn.

CHÚ THÍCH Tiêu chuẩn ISO/IEC 27034, Công nghệ thông tin - Kỹ thuật an toàn – An toàn ứng dụng, cung cấp hướng dẫn để xác định, phát triển, triển khai, quản lý, hỗ trợ và chấm dứt một ứng dụng.

11.4.2.3 Giám sát mạng và ứng phó

Giám sát mạng thường được các tổ chức sử dụng để đảm bảo độ tin cậy và chất lượng của các dịch vụ mạng của họ. Đồng thời, điều này có thể được tận dụng để tìm kiếm các lưu lượng mạng đặc biệt và phát hiện các hoạt động độc hại mới nổi trên mạng. Nhìn chung, các tổ chức cần thực hiện như sau:

- Hiểu được lưu lượng trên mạng lưới– Thế nào là bình thường, thế nào là bất thường.
- Sử dụng một công cụ quản lý mạng để xác định những đột biến về lưu lượng truy cập, lưu lượng/ cổng bất thường và đảm bảo rằng có các công cụ để xác định và xử lý các vấn đề.
- Kiểm tra trước khả năng ứng phó cần thiết đối với một sự kiện có thật. Tinh chỉnh các công nghệ, quy trình và các công cụ dựa trên kết quả của việc diễn tập thường xuyên.
- Hiểu về các hành vi cơ bản của một cá nhân - nếu một người bình thường không hoạt động, đột nhiên chiếm 100% băng thông có sẵn, khi đó có thể cần thiết phải cô lập người sử dụng trái phép này cho đến khi tìm thấy nguyên nhân. Việc cô lập mạng lưới có thể ngăn chặn sự lây lan của phần mềm độc hại, việc triển khai có thể cần yêu cầu sự đồng ý của người sử dụng hoặc cập nhật Điều khoản Dịch vụ.

- Hãy xem xét giám sát các hoạt động từ các điểm chính yếu trong mạng như DNS và bộ lọc các bản tin, để áp dụng cho các thiết bị cờ (flag devices) đã bị xâm hại với phần mềm độc hại, nhưng vì nhiều lý do không được phát hiện bằng phần mềm chống virus hay các dịch vụ IDS.

VÍ DỤ Do khối lượng thông tin trên mạng, các công cụ như IDS và IPS có thể được sử dụng để giám sát các trường hợp ngoại lệ có thể báo cáo được.

11.4.2.4 Hỗ trợ và báo cáo vượt cấp

Các doanh nghiệp, bao gồm cả các nhà cung cấp dịch vụ và các tổ chức chính phủ thường có một dịch vụ hỗ trợ khách hàng để trả lời các câu hỏi, hỗ trợ kỹ thuật và giải quyết các vấn đề của khách hàng. Với sự phát triển ngày càng tăng của phần mềm độc hại trên Internet, một tổ chức cung cấp dịch vụ có thể nhận được các báo cáo liên quan đến việc nhiễm phần mềm độc hại và phần mềm gián điệp và các vấn đề an toàn không gian mạng khác. Những thông tin này rất quan trọng và hữu ích cho các nhà cung cấp có liên quan để đánh giá rủi ro và tình hình phần mềm độc hại, cập nhật và cung cấp các công cụ cần thiết để đảm bảo rằng bất kỳ phần mềm độc hại hoặc phần mềm gián điệp mới phát hiện được có thể được gỡ bỏ hoặc vô hiệu hóa một cách hiệu quả. Về vấn đề này, một tổ chức cần thiết lập liên lạc với các nhà cung cấp an toàn và cung cấp các báo cáo có liên quan cùng các mẫu phần mềm độc hại để các nhà cung cấp đó theo dõi - đặc biệt là khi các phần mềm độc hại này có dấu hiệu lây lan. Hầu hết các nhà cung cấp đều có một danh sách thư điện tử để nhận báo cáo hoặc các mẫu để phân tích và theo dõi. Ví dụ, xem Bảng B.1 trong Phụ lục B.

11.4.2.5 Giữ cập nhật mới nhất

Là một phần của việc triển khai ISMS để quản lý các rủi ro an toàn thông tin doanh nghiệp và cũng đảm bảo rằng các tổ chức tiếp tục thực hiện các thực tiễn triển khai tối ưu, cập nhật các điểm yếu và tình hình khai thác/ tấn công mới nhất, các tổ chức nên tham gia vào các diễn đàn cộng đồng hoặc các diễn đàn công nghệ để chia sẻ kinh nghiệm và học hỏi từ các nhà cung cấp đồng nghiệp khác.

11.4.3 Các yêu cầu an toàn cho dịch vụ lưu trữ web và các dịch vụ ứng dụng không gian mạng khác

Hầu hết các nhà cung cấp dịch vụ cung cấp các dịch vụ lưu trữ trên mạng và trung tâm dữ liệu của họ như một phần của dịch vụ nghiệp vụ của họ. Những dịch vụ này, trong đó bao gồm cả ứng dụng web và các ứng dụng trực tuyến khác, thường được đóng gói lại và bán lại bởi các thuê bao lưu trữ cho các khách hàng khác, chẳng hạn như các doanh nghiệp nhỏ và người dùng cuối. Nếu các thuê bao lưu trữ thiết lập một máy chủ không an toàn, hay lưu trữ nội dung độc hại trong các trang web hoặc các ứng dụng của họ, sự an toàn của người dùng sẽ bị ảnh hưởng xấu. Như vậy, điều quan trọng là dịch vụ này ít nhất cần đáp ứng các tiêu chuẩn thực tiễn tối ưu bằng cách tuân thủ chính sách hoặc các điều khoản của thỏa thuận.

Trong trường hợp có nhiều nhà cung cấp được sử dụng, sự tương tác giữa các nhà cung cấp cần được phân tích và các thỏa thuận dịch vụ tương ứng nên giải quyết bất cứ tác động qua lại quan trọng

nào. Ví dụ, việc cập nhật hoặc vá lỗi cho hệ thống một nhà cung cấp nên được phối hợp với các nhà cung cấp khác.

Các điều khoản của thỏa thuận ít nhất phải bao gồm những điều sau đây:

a) Thông báo rõ ràng, mô tả các trang web trực tuyến hay an toàn ứng dụng và các thực hành riêng tư, thực hành thu thập dữ liệu và hành vi của bất kỳ mã chương trình nào (ví dụ, Browser Helper Object), rằng các trang web trực tuyến hoặc ứng dụng có thể phân phối và triển khai trên máy tính để bàn của người dùng cuối hoặc môi trường trình duyệt web.

b) Sự ưng thuận của người dùng, đồng ý hay không đồng ý với các điều khoản của dịch vụ được mô tả trong Thông báo. Điều này sẽ cho phép người dùng thực hiện các quyết định và xác định xem anh/ cô ấy có thể chấp nhận các điều khoản của dịch vụ hay không.

c) Quyền kiểm soát của người dùng, tạo điều kiện cho người dùng thay đổi các thiết lập của họ hoặc chấm dứt việc thừa nhận của họ bất cứ lúc nào trong tương lai sau thỏa thuận ban đầu.

Các điều khoản này rất quan trọng để đảm bảo rằng người dùng cuối nắm rõ về hành vi và thực tiễn của các ứng dụng hay trang web trực tuyến, liên quan đến sự riêng tư và an toàn của người dùng cuối. Các điều khoản cần được phát triển với sự trợ giúp của một chuyên gia pháp lý để đảm bảo rằng họ cũng sẽ đảm bảo cho các nhà cung cấp dịch vụ khi các hoạt động hợp pháp của người dùng cuối gây ra thiệt hại cụ thể do nội dung độc hại hoặc các chính sách và thực hành không rõ ràng trên trang web.

Ngoài các điều khoản riêng tư cá nhân và bảo vệ dữ liệu trên các trang web trực tuyến hoặc ứng dụng, các nhà cung cấp dịch vụ nên yêu cầu các trang web trực tuyến hoặc các ứng dụng được lưu trữ trên mạng của họ triển khai các kiểm soát an toàn thực tiễn tối ưu ở mức ứng dụng trước khi đưa ra. Những điều này bao gồm, nhưng không giới hạn, trong các ví dụ được đưa ra trong điều nhỏ 12.2. Là một phần của hạ tầng lưu trữ của nhà cung cấp dịch vụ, các máy chủ cần được bảo vệ chống truy cập trái phép và nguy cơ lưu trữ nội dung độc hại. Xem ví dụ về các biện pháp kiểm soát tại điều nhỏ 12.3.

Cho phép thực thi các biện pháp kiểm soát an toàn, đặc biệt là các vấn đề liên quan đến an toàn ứng dụng và trang web trực tuyến, các nhà cung cấp dịch vụ nên xem xét kết hợp các điều khoản này tại các điều khoản của thỏa thuận dịch vụ.

11.4.4 Hướng dẫn an toàn cho người dùng

Các nhà cung cấp dịch vụ sẽ cung cấp hướng dẫn cho người dùng về cách giữ an toàn trực tuyến. Các nhà cung cấp dịch vụ hoặc có thể tạo ra các hướng dẫn trực tiếp hoặc giới thiệu người dùng đến các trang web hướng dẫn có sẵn có thể cung cấp nội dung. Điều này rất quan trọng để giáo dục người dùng cuối về cách họ có thể đóng góp cho một Internet an toàn, trong mối quan hệ với các vai trò mà họ có thể làm trong không gian mạng, như mô tả trong Điều 7. Ngoài ra, người dùng cuối cần được tư vấn để có biện pháp an toàn kỹ thuật cần thiết, trong đó các nhà cung cấp dịch vụ cũng

có thể đóng một vai trò tích cực, như mô tả trong điều nhỏ 11.3. Các ví dụ về các hoạt động hướng dẫn có thể bao gồm:

a) Các bản tin an toàn định kỳ (ví dụ, hàng tháng), để tư vấn về kỹ thuật an toàn cụ thể (ví dụ, làm thế nào để lựa chọn một mật khẩu tốt); cập nhật về xu hướng an toàn; cung cấp chú ý về an toàn truyền thông trên web (webcast), video theo yêu cầu khác, chương trình phát thanh và các thông tin an toàn khác đang sẵn sàng từ cổng trang web của tổ chức hay các nhà cung cấp nội dung an toàn khác.

b) Chương trình phát sóng trực tiếp các video giáo dục an toàn theo yêu cầu hay truyền thông trên web (webcast) bao gồm một loạt các chủ đề an toàn để nâng cao nhận thức và thực tiễn an toàn đầu cuối của người sử dụng.

c) Kết hợp với một mục an toàn trong các bản tin giấy của nhà cung cấp dịch vụ được gửi tới nơi cư trú hay văn phòng của người dùng cuối để làm nổi bật sự kiện hoặc nội dung an toàn quan trọng.

d) Tổ chức các cuộc hội thảo an toàn hàng năm hoặc định kỳ cho người dùng cuối, có thể hợp tác với các ngành công nghiệp khác, các nhà cung cấp và chính phủ.

Các nhà cung cấp dịch vụ sử dụng thư điện tử là phương tiện chính để giao tiếp với người dùng cuối, đó là một cách giúp người dùng cuối chống lại các cuộc tấn công khai thác thông tin xã hội. Đặc biệt, người dùng nên nhớ rằng các thư điện tử không mong muốn từ các nhà cung cấp dịch vụ sẽ không bao giờ yêu cầu

- thông tin cá nhân;
- tên người dùng;
- mật khẩu;
- không bao giờ chứa các liên kết liên quan tới an toàn cho người đọc click vào.

Khi một nhà cung cấp dịch vụ muốn người dùng đến trang web của mình để xem thông tin thì họ sẽ cho người sử dụng biết cách để kết nối với các URL được yêu cầu một cách an toàn. Ví dụ, họ có thể yêu cầu người dùng gõ một URL trích dẫn vào trình duyệt của họ và chắc chắn rằng các URL được trích dẫn không có một liên kết có thể nhấp chuột vào.

Là một phần của giáo dục và hướng dẫn an toàn cho người dùng chống lại phần mềm lừa đảo và phần mềm gián điệp, các tổ chức và các nhà cung cấp dịch vụ cần phải tư vấn cho người dùng cuối của họ về việc sử dụng các biện pháp an toàn kỹ thuật phù hợp để bảo vệ hệ thống của họ chống lại các kiểu khai thác và tấn công đã biết. Theo hướng dẫn chung, người dùng được khuyến khích nên thực hiện các biện pháp kiểm soát tại điều nhỏ 12.4.

Phụ lục B cung cấp danh sách tài liệu tham khảo và các tài nguyên trực tuyến có thể được sử dụng để hỗ trợ việc thực hiện các khuyến nghị trên.

12 Biện pháp kiểm soát an toàn không gian mạng

12.1 Tổng quan

Khi các rủi ro đối với an toàn không gian mạng được xác định và các hướng dẫn phù hợp được phác thảo, các biện pháp kiểm soát an toàn không gian mạng hỗ trợ các yêu cầu an toàn có thể được lựa chọn và thực hiện. Điều khoản này đưa ra một cái nhìn tổng quan về các biện pháp kiểm soát an toàn không gian mạng chủ chốt có thể triển khai để hỗ trợ các hướng dẫn đặt ra trong Tiêu chuẩn này.

12.2 Biện pháp kiểm soát mức ứng dụng

Các biện pháp kiểm soát mức ứng dụng bao gồm:

a) Hiển thị các thông báo ngắn, cung cấp bản tóm tắt rõ ràng, ngắn gọn trong một trang (sử dụng ngôn ngữ đơn giản) về chính sách trực tuyến cần thiết của công ty. Với bản tóm tắt này, người dùng có thể lựa chọn nhiều thông tin hơn về việc chia sẻ thông tin trực tuyến của họ. Các thông báo ngắn nên phù hợp với tất cả yêu cầu quy định và cung cấp liên kết đến đầy đủ các cơ quan pháp lý và các thông tin khác có liên quan. Khách hàng muốn biết thêm chi tiết có thể dễ dàng bấm vào để đọc phiên bản đầy đủ hơn. Với một chú thích đơn giản, khách hàng có thể biết rõ hơn về tất cả các đặc tính của công ty, với cùng tiêu chuẩn riêng tư và mong muốn mở rộng cho nhiều trang web.

b) Xử lý an toàn các phiên làm việc đối với các ứng dụng web; điều này có thể bao gồm các cơ chế trực tuyến như cookies.

c) Xác nhận và xử lý đầu vào an toàn để ngăn chặn các cuộc tấn công phổ biến như SQL-Injection. Dựa trên thực tế là các trang web, thường được coi là đáng tin cậy, đang ngày càng được sử dụng để phân phối mã độc hại, việc xác nhận đầu vào và đầu ra phải được thực hiện theo nội dung hoạt động cũng như nội dung động.

d) An toàn cho mã kịch bản của trang web để ngăn chặn các cuộc tấn công phổ biến như tấn công chèn mã Cross-site Scripting.

e) Soát xét và kiểm tra an toàn mã hóa bằng các kỹ năng thích hợp.

f) Các dịch vụ của tổ chức, được cung cấp bởi tổ chức hoặc của một bên đại diện cho tổ chức, cần được cung cấp một cách để người dùng có thể xác thực các dịch vụ. Đó có thể là các nhà cung cấp sử dụng một tên miền phụ từ tên miền tổ chức chính và có thể sử dụng thông tin HTTPS đăng ký cho tổ chức. Dịch vụ này nên tránh việc sử dụng các phương pháp lừa đảo khiến người dùng có thể gặp khó khăn trong việc xác định với người mà họ đang tiếp xúc.

12.3 Bảo vệ máy chủ

Các biện pháp kiểm soát sau đây có thể được sử dụng để bảo vệ máy chủ chống truy cập trái phép và lưu trữ các nội dung độc hại trên máy chủ:

a) Cấu hình các máy chủ, kể cả các hệ điều hành cơ bản tuân theo hướng dẫn cấu hình an toàn định chuẩn. Hướng dẫn này bao gồm định nghĩa về người sử dụng máy chủ so với người quản trị, tuân theo sự kiểm soát truy cập vào chương trình và thư mục, tập tin hệ thống và cho phép kiểm toán các dấu vết, đặc biệt về an toàn và các sự kiện thất bại khác trên hệ thống. Hơn nữa, nên cài đặt một hệ thống tối thiểu trên một máy chủ nhằm giảm thiểu vector tấn công.

b) Triển khai một hệ thống để kiểm tra và triển khai các bản cập nhật an toàn, đảm bảo hệ thống điều hành máy chủ và các ứng dụng được cập nhật kịp thời khi bản cập nhật mới xuất hiện.

c) Giám sát việc thực thi an toàn của máy chủ thông qua việc đánh giá kiểm toán thường xuyên.

d) Soát xét các cấu hình an toàn.

e) Sử dụng các phần mềm chống nội dung độc hại (chẳng hạn như chống virus và chống phần mềm gián điệp) trên máy chủ.

f) Quét tất cả các nội dung được lưu trữ và tải lên thường xuyên, sử dụng phần mềm chống độc hại đã được cập nhật. Phải luôn coi rằng một tập tin có thể vẫn là phần mềm gián điệp hoặc phần mềm độc hại ngay cả khi không được phát hiện bởi các biện pháp kiểm soát hiện tại do những hạn chế của thông tin chưa đầy đủ.

g) Thực hiện đánh giá điểm yếu và kiểm tra an toàn thường xuyên cho các trang web và các ứng dụng trực tuyến để đảm bảo an toàn của chúng được duy trì đầy đủ.

h) Thường xuyên rà quét các máy bị xâm hại.

12.4 Biện pháp kiểm soát người dùng cuối

Sau đây là một danh sách chưa đầy đủ các biện pháp kiểm soát mà người dùng cuối có thể sử dụng để bảo vệ hệ thống của họ chống lại các kiểu khai thác và tấn công đã biết:

a) Việc sử dụng các hệ điều hành được hỗ trợ có cài đặt các bản vá lỗi an toàn cập nhật mới nhất. Người dùng tổ chức có trách nhiệm phải nhận thức được và làm theo các chính sách tổ chức liên quan đến hệ điều hành được hỗ trợ. Người dùng cá nhân cần phải nhận thức được và xem xét sử dụng hệ điều hành được nhà cung cấp khuyến nghị. Trong mọi trường hợp, hệ điều hành cần luôn luôn được cập nhật phiên bản mới nhất.

b) Sử dụng các ứng dụng phần mềm hỗ trợ gần đây nhất được cập nhật các bản vá lỗi mới nhất. Người dùng tổ chức có trách nhiệm phải nhận thức được và làm theo chính sách liên quan đến việc hỗ trợ phần mềm ứng dụng. Người dùng cá nhân cần phải nhận thức và soát xét sử dụng phần mềm ứng dụng được nhà cung cấp khuyến nghị. Trong mọi trường hợp, hệ điều hành cần luôn luôn được cập nhật phiên bản mới nhất.

c) Sử dụng các công cụ chống virus và chống phần mềm gián điệp. Nếu khả thi, một nhà cung cấp dịch vụ như một ISP nên xem xét hợp tác với các nhà cung cấp an toàn đáng tin cậy để

cung cấp tới người sử dụng những công cụ này như một phần của gói thuê bao dịch vụ để các biện pháp kiểm soát an toàn được thực hiện kể từ ngày ký kết các thuê bao hoặc khi đổi mới. Người dùng tổ chức có trách nhiệm phải nhận thức được và làm theo chính sách tổ chức liên quan đến việc sử dụng các công cụ phần mềm bảo mật. Người dùng cá nhân nên sử dụng các công cụ phần mềm bảo mật. Họ nên tìm đến các nhà cung cấp khi có bất kỳ đề nghị, cung cấp hoặc chấm dứt sử dụng phần mềm bảo mật. Trong tất cả các trường hợp, các phần mềm bảo mật phải được cập nhật các bản vá lỗi an toàn và cơ sở dữ liệu chữ ký.

d) Triển khai các biện pháp chống virus và chống phần mềm gián điệp thích hợp. Trình duyệt web và thanh công cụ trình duyệt web phổ biến hiện nay có khả năng chặn pop-up, tức là chặn các trang web độc hại hiển thị trên cửa sổ màn hình có chứa phần mềm gián điệp hoặc phần mềm lừa đảo có thể khai thác điểm yếu hệ thống hoặc trình duyệt hoặc sử dụng kỹ thuật tấn công khai thác thông tin xã hội để lừa người dùng tải về và cài đặt chúng lên trên hệ thống của họ. Các tổ chức phải thiết lập một chính sách để cho phép việc sử dụng các công cụ như vậy. Các tổ chức cung cấp dịch vụ phải đối chiếu danh sách các công cụ được đề nghị và khuyến khích người dùng sử dụng, hướng dẫn về cách cho phép cấp quyền cho các trang web mà người dùng có nhu cầu.

e) Kích hoạt tính năng chặn mã kịch bản. Kích hoạt tính năng chặn mã kịch bản hay một thiết lập an toàn web cao hơn để đảm bảo rằng chỉ có mã kịch bản từ các nguồn đáng tin cậy mới được thực hiện trên một máy tính nội bộ.

f) Sử dụng bộ lọc chống tấn công giả mạo. Trình duyệt web và thanh công cụ trình duyệt phổ biến thường kết hợp khả năng này, có thể xác định xem một trang web mà người dùng đang truy cập có tìm thấy trong cơ sở dữ liệu các trang web giả mạo được biết đến hoặc chứa các mẫu mã kịch bản tương tự như các trang web giả mạo hay không. Các trình duyệt sẽ cung cấp các cảnh báo, thường ở dạng mã màu nổi bật, để cảnh báo người dùng về nguy cơ tiềm ẩn. Các tổ chức phải thiết lập một chính sách để cho phép việc sử dụng các công cụ như vậy.

g) Sử dụng các tính năng an toàn có sẵn trên trình duyệt web. Theo thời gian, khi nguy cơ an toàn không gian mạng mới xuất hiện, nhà cung cấp trình duyệt web và thanh công cụ trình duyệt sẽ thêm khả năng an toàn mới để bảo vệ người dùng chống lại các rủi ro. Người dùng cuối nên theo kịp sự phát triển bằng cách cập nhật thường xuyên các công cụ mà nhà cung cấp khuyến nghị. Các tổ chức và nhà cung cấp dịch vụ tương tự nên xem xét những khả năng mới và cập nhật các chính sách và dịch vụ liên quan để phục vụ tốt hơn các nhu cầu của các tổ chức và khách hàng của họ và giải quyết các rủi ro an toàn không gian mạng liên quan.

h) Kích hoạt tường lửa cá nhân và HIDS. Tường lửa cá nhân và HIDS là công cụ quan trọng để kiểm soát việc truy cập các dịch vụ mạng vào hệ thống của người dùng. Một số hệ điều hành mới hơn có tường lửa cá nhân và HIDS kết hợp. Chúng được kích hoạt theo mặc định, người sử dụng hoặc các ứng dụng có thể vô hiệu hóa chúng, dẫn đến các rủi ro an toàn mạng không

mong muốn. Các tổ chức cần có một chính sách về việc sử dụng tường lửa cá nhân và HIDS, các công cụ hoặc các sản phẩm phù hợp để triển khai để sử dụng mặc định cho tất cả nhân viên. Các nhà cung cấp dịch vụ nên khuyến khích việc sử dụng chức năng tường lửa cá nhân và HIDS và/hoặc đề nghị các sản phẩm tường lửa cá nhân và HIDS khác của bên thứ ba đã được đánh giá đáng tin cậy và giáo dục giúp người dùng trong việc đảm bảo an toàn mạng cơ bản ở mức hệ thống người dùng cuối.

i) Kích hoạt tính năng cập nhật tự động. Trong khi các biện pháp an toàn kỹ thuật trên có khả năng đối phó với hầu hết các phần mềm độc hại ở mức hoạt động tương ứng của mình, nó lại không hiệu quả chống lại các khai thác điểm yếu tồn tại trong hệ điều hành và các sản phẩm ứng dụng. Để ngăn chặn việc khai thác như vậy, chức năng cập nhật có sẵn trong hệ điều hành, được cung cấp bởi các ứng dụng tin cậy (ví dụ, các sản phẩm chống virus, chống gián điệp của bên thứ ba là đáng tin cậy), nên được kích hoạt để việc cập nhật diễn ra tự động. Điều này sẽ đảm bảo rằng hệ thống được cập nhật với các bản vá lỗi bảo mật mới nhất, thu hẹp khoảng thời gian mà việc khai thác có thể diễn ra.

12.5 Biện pháp kiểm soát chống lại các cuộc tấn công khai thác thông tin xã hội

12.5.1 Tổng quan

Tội phạm mạng đang ngày càng sử dụng nhiều đến các chiến thuật sử dụng các kỹ thuật tấn công khai thác thông tin xã hội, tâm lý để đạt thành công.

VÍ DỤ 1 Việc sử dụng thư điện tử mang URL hướng người dùng đến các trang web giả mạo mà không bị nghi ngờ.

VÍ DỤ 2 Các thư điện tử lừa đảo (scam mail) yêu cầu người dùng cung cấp thông tin nhận dạng cá nhân hoặc thông tin liên quan đến sở hữu trí tuệ của công ty.

Sự phát triển của các mạng xã hội và trang web truyền thông cung cấp các phương tiện mới cho phép xây dựng các lừa đảo lòng tin và gian trá tiến xa hơn. Các cuộc tấn công ngày càng tăng, vượt qua công nghệ, qua các hệ thống máy tính và kết nối mạng truyền thống, chúng còn tận dụng điện thoại di động, mạng không dây (bao gồm cả Bluetooth) và giọng nói qua IP (VoIP).

Điều khoản này cung cấp một bộ khung biện pháp kiểm soát được áp dụng để quản lý và giảm thiểu rủi ro an toàn không gian mạng liên quan đến các cuộc tấn công khai thác thông tin xã hội. Hướng dẫn cung cấp tại điều khoản này được dựa trên quan điểm cho rằng cách hiệu quả duy nhất để giảm thiểu mối đe dọa của các kỹ thuật tấn công khai thác thông tin xã hội là thông qua sự kết hợp của:

- công nghệ bảo mật;
- chính sách an toàn thiết lập các nguyên tắc nền tảng cho hành vi cá nhân của cả các cá nhân các nhân viên;
- giáo dục và đào tạo phù hợp.

Do đó, bộ khung bao gồm:

- các chính sách;
- các phương pháp và quy trình;

- con người và tổ chức;
- các kiểm soát kỹ thuật được áp dụng.

12.5.2 Chính sách

Phù hợp với thực tiễn chung về quản lý rủi ro an toàn thông tin, các chính sách cơ bản về việc khởi tạo, thu thập, lưu trữ, truyền tải, chia sẻ, xử lý và việc sử dụng các thông tin và sở hữu trí tuệ của tổ chức, cá nhân trên Internet và trong không gian mạng nên được xác định và cung cấp tài liệu. Đặc biệt, điều này liên quan đến các ứng dụng như tin nhắn tức thời, viết blog, chia sẻ tệp ngang hàng và mạng xã hội, thường vượt ra ngoài phạm vi của mạng doanh nghiệp và an toàn thông tin.

Là một phần trong chính sách của công ty, việc trình bày và các hình phạt liên quan đến sự lạm dụng của các ứng dụng không gian mạng cũng nên được kết hợp để ngăn chặn chống lại thực tiễn việc lạm dụng bởi những nhân viên và các bên thứ ba trên mạng công ty hoặc các hệ thống truy cập vào không gian mạng.

Các chính sách quản trị nhằm nâng cao nhận thức và hiểu biết về các rủi ro an toàn không gian mạng và khuyến khích (hoặc bắt buộc) học tập và phát triển kỹ năng chống lại các cuộc tấn công an toàn không gian mạng, đặc biệt là các cuộc tấn công khai thác thông tin xã hội, cần được xây dựng và ban hành. Điều này sẽ bao gồm các yêu cầu đối với người tham dự để chỉ dẫn và đào tạo.

Bằng cách thúc đẩy các chính sách và nhận thức phù hợp về rủi ro khai thác thông tin xã hội, các nhân viên sẽ có đủ hiểu biết về các rủi ro và các yêu cầu đó, đồng thời phát triển sự hiểu biết về thực tiễn và chính sách triển khai tối ưu mong muốn cho mạng xã hội bên ngoài và các ứng dụng không gian mạng khác, ví dụ, thỏa thuận chính sách an toàn của nhà cung cấp dịch vụ.

12.5.3 Các phương pháp và quy trình

12.5.3.1 Danh mục và phân loại thông tin

Để hỗ trợ các chính sách nhằm thúc đẩy nhận thức và bảo vệ các thông tin nhạy cảm của doanh nghiệp và cá nhân, bao gồm cả tài sản trí tuệ, các quy trình phân loại thông tin cần được triển khai.

Đối với mỗi danh mục và phân loại các thông tin có liên quan, các biện pháp kiểm soát an toàn cụ thể để bảo vệ chống lại việc vô ý bị lộ, cố ý truy cập trái phép cần được xây dựng và phát hành tài liệu.

Người dùng trong các tổ chức sau đó có thể phân biệt các loại danh mục và phân loại các thông tin mà họ tạo ra, thu thập và xử lý. Sau đó người dùng có thể có sự thận trọng cần thiết và các biện pháp phòng ngừa khi sử dụng không gian mạng.

Các thủ tục về cách xử lý tài sản trí tuệ của công ty, dữ liệu cá nhân và các thông tin bí mật khác cũng cần được phát triển và ban hành.

12.5.3.2 Nhận thức và đào tạo

Việc nhận thức và đào tạo an toàn, bao gồm việc thường xuyên cập nhật kiến thức và học tập liên quan về an toàn là một yếu tố quan trọng để chống lại các cuộc tấn công khai thác thông tin xã hội.

Là một phần của chương trình an toàn không gian mạng của tổ chức, các nhân viên và các bên nhà thầu thứ ba cần phải trải qua một số giờ tối thiểu về đào tạo nâng cao nhận thức để đảm bảo rằng họ nhận thức được vai trò và trách nhiệm của mình trong không gian mạng và các kiểm soát kỹ thuật sẽ triển khai như khi cá nhân sử dụng không gian mạng. Ngoài ra, như là một phần của chương trình để chống lại các cuộc tấn công khai thác thông tin xã hội, việc đào tạo nâng cao nhận thức nên bao gồm các nội dung như sau:

a) Các mối đe dọa và các hình thức tấn công khai thác thông tin xã hội mới nhất, ví dụ, cách tấn công giả mạo từ các trang web giả mạo đơn lẻ, đến việc kết hợp các kiểu tấn công thư rác, chèn mã Cross Site Scripting và SQL injection.

b) Làm thế nào thông tin cá nhân và công ty có thể bị đánh cắp và thao tác thông qua các cuộc tấn công khai thác thông tin xã hội, cung cấp hiểu biết về cách đối tượng tấn công có thể tận dụng được bản chất con người, chẳng hạn như là xu hướng thực hiện các yêu cầu được đưa ra bởi người có thẩm quyền (mặc dù nó có thể không phải là thật), thái độ thân thiện và việc đáp lại bằng thứ gì có giá trị hay giúp đỡ.

c) Những thông tin nào cần được bảo vệ và làm thế nào để bảo vệ nó, phù hợp với chính sách an toàn thông tin.

d) Khi nào thì báo cáo thường hoặc báo cáo vượt cấp một sự kiện đáng ngờ hoặc các ứng dụng độc hại cho các cơ quan có thẩm quyền hoặc cơ quan ứng cứu và thông tin tới các địa chỉ liên lạc có sẵn. Ví dụ, xem Phụ lục B.

Các tổ chức cung cấp các ứng dụng và dịch vụ không gian mạng trực tuyến phải cung cấp các tài liệu nâng cao nhận thức cho các thuê bao hoặc người dùng bao gồm các nội dung trên trong ngữ cảnh các ứng dụng hoặc dịch vụ của họ.

12.5.3.3 Kiểm tra

Nhân viên nên có hiểu biết về việc họ chấp nhận và hiểu nội dung của các chính sách an toàn của tổ chức. Là một phần của quá trình nâng cao nhận thức và đảm bảo quan tâm đúng mức tới các rủi ro, một tổ chức cần xem xét tiến hành các bài kiểm tra định kỳ để xác định mức độ nhận thức và tuân thủ chính sách và thực tiễn liên quan. Nhân viên có thể thực hiện một bài kiểm tra viết hoặc trải qua CBT để xác định xem họ hiểu nội dung của chính sách an toàn của tổ chức hay không. Việc thử nghiệm này có thể bao gồm nhưng không giới hạn, việc tạo ra các trang web lừa đảo, thư rác và thư tấn công giả mạo mục tiêu nhưng kiểm soát được bằng cách sử dụng các nội dung khai thác thông tin xã hội có thể tin cậy. Khi tiến hành kiểm tra như vậy, điều quan trọng cần đảm bảo rằng:

a) Các máy chủ và nội dung kiểm tra đều nằm trong tầm kiểm soát và chỉ đạo của nhóm kiểm tra;

b) Các chuyên gia có kinh nghiệm về việc kiểm tra cần tham gia nếu có thể;

c) Người sử dụng được chuẩn bị cho bài kiểm tra đó thông qua các chương trình đào tạo và nâng cao nhận thức;

d) Tất cả kết quả kiểm tra được trình bày ở dạng tổng hợp để bảo vệ sự riêng tư của một cá nhân cũng như nội dung trình bày trong các bài kiểm tra, do các bài kiểm tra có thể gây rắc rối cho các cá nhân và gây ra mối quan tâm riêng tư, nếu như không được quản lý thích hợp.

CHÚ THÍCH Các nguyên tắc và luật pháp của mỗi quốc gia phải được xem xét.

12.5.4 Con người và tổ chức

Trong khi các cá nhân là mục tiêu chính của các cuộc tấn công khai thác thông tin xã hội, một tổ chức cũng có thể là nạn nhân bị nhắm tới. Tuy nhiên, con người vẫn là điểm tấn công chính của các cuộc tấn công khai thác thông tin xã hội. Như vậy, mọi người cần phải nhận thức được những rủi ro liên quan trong không gian mạng và các tổ chức nên thiết lập các chính sách có liên quan và có các bước chủ động tài trợ cho các chương trình có liên quan để đảm bảo nhận thức và năng lực của con người.

Theo hướng dẫn chung, tất cả các tổ chức (bao gồm cả doanh nghiệp, các nhà cung cấp dịch vụ và chính phủ) nên khuyến khích người dùng trong không gian mạng tìm hiểu những rủi ro khai thác thông tin xã hội trong không gian mạng và các bước mà họ nên làm để bảo vệ mình chống lại các cuộc tấn công tiềm ẩn.

12.5.5 Kỹ thuật

Ngoài việc thiết lập các chính sách và thực hành chống lại các cuộc tấn công khai thác thông tin xã hội, các kiểm soát kỹ thuật cũng cần được xem xét để hạn chế tối đa các tấn công làm lộ thông tin tiềm ẩn.

Ở mức cá nhân, người sử dụng không gian mạng cần làm theo hướng dẫn thảo luận tại điều nhỏ 11.3.

Các tổ chức và nhà cung cấp dịch vụ cần làm theo các hướng dẫn cung cấp tại điều nhỏ 11.4. để dễ dàng cho người dùng làm theo và sử dụng các biện pháp an toàn kỹ thuật.

Tổ chức cung cấp dịch vụ cũng cần làm theo hướng dẫn cung cấp tại điều nhỏ 11.4. Điều này rất quan trọng, cung cấp các biện pháp kiểm soát định chuẩn chống lại các cuộc tấn công khai thác thông tin xã hội trong không gian mạng.

Ngoài ra, các kiểm soát kỹ thuật sau đây rất hữu ích để chống các cuộc tấn công sử dụng các kỹ thuật tấn công khai thác thông tin xã hội:

a) Trường hợp thông tin nhạy cảm cá nhân hoặc doanh nghiệp có liên quan đến các ứng dụng trực tuyến và/hoặc khi giao dịch quan trọng đang được thực hiện, cần xem xét việc cung cấp các giải pháp xác thực mạnh, như một phần của xác thực đăng nhập.Việc xác thực mạnh đề cập đến việc sử dụng hai hay nhiều yếu tố xác định định danh, yếu tố thứ nhất là việc sử dụng

tài khoản và mật mã. Yếu tố thứ 2 thêm vào có thể là thẻ thông minh, sinh trắc học hoặc thẻ bảo mật cầm tay khác.

b) Đối với các dịch vụ dựa trên web, các tổ chức cần xem xét sử dụng một "chứng nhận an toàn cấp cao" để cung cấp sự đảm bảo cho người sử dụng trực tuyến. Hầu hết các nhà cung cấp chứng chỉ số thương mại (Certification Authoritie - CA) và các trình duyệt Internet có khả năng hỗ trợ việc sử dụng các chứng chỉ như vậy, làm giảm nguy cơ các cuộc tấn công tấn công giả mạo.

c) Để đảm bảo an toàn khi máy tính người dùng kết nối với các tổ chức, hay các dịch vụ, website, ứng dụng của tổ chức trong không gian mạng, cần xem xét các biện pháp kiểm soát bổ sung để bảo đảm mức tối thiểu về an toàn, chẳng hạn như cài đặt các bản cập nhật an toàn mới nhất. Việc sử dụng các biện pháp kiểm soát như vậy nên được công khai trong Hợp đồng dịch vụ người dùng cuối và/hoặc Chính sách an toàn và riêng tư trang web được áp dụng.

12.6 Sẵn sàng an toàn không gian mạng

Phụ lục A mô tả các biện pháp kiểm soát kỹ thuật bổ sung được áp dụng để cải thiện tính sẵn sàng của an toàn không gian mạng của tổ chức trong vùng phát hiện ra sự kiện qua việc giám sát qua mạng ẩn (darknet), điều tra qua truy vết ngược (traceback) và đối phó qua hoạt động của máy chủ nhận các kết nối chuyển hướng (sinkhole).

12.7 Các biện pháp kiểm soát khác

Các biện pháp kiểm soát khác có thể bao gồm các biện pháp kiểm soát liên quan tới việc cảnh báo và cách ly các thiết bị có các hoạt động đáng ngờ như quan sát mối tương quan của các sự kiện từ các bộ phận bên cung cấp dịch vụ và/hoặc bộ phận doanh nghiệp như các máy chủ DNS, lưu lượng mạng định tuyến, bộ lọc tin nhắn gửi đi và truyền thông ngang hàng.

13 Khung chia sẻ và phối hợp thông tin

13.1 Tổng quan

Các sự cố an toàn không gian mạng thường vượt qua ranh giới địa lý quốc gia và ranh giới tổ chức và tốc độ của dòng chảy thông tin và thay đổi của sự kiện diễn ra thường xuyên làm giới hạn thời gian hành động của các cá nhân và tổ chức. Một hệ thống cần phải được thành lập để chia sẻ và phối hợp thông tin để giúp chuẩn bị và ứng phó với các sự kiện, sự cố an toàn không gian mạng. Đây là một bước quan trọng của các biện pháp an toàn không gian mạng của tổ chức. Một hệ thống để chia sẻ và phối hợp thông tin cần được an toàn, hiệu quả, đáng tin cậy và năng suất cao.

Hệ thống cần an toàn để đảm bảo rằng các thông tin được chia sẻ, bao gồm chi tiết về phối hợp hành động, được bảo vệ chống lại những truy cập trái phép. Bảo mật thông tin liên quan đến các sự kiện an toàn không gian mạng cũng là cần thiết để tránh hiểu lầm và gây hoảng loạn hoặc báo động quá mức cho cộng đồng. Đồng thời, tính toàn vẹn và xác thực của thông tin là rất quan trọng để đảm bảo độ

chính xác và độ tin cậy của nó cho khi thông tin đó được chia sẻ trong một nhóm khép kín hoặc cộng đồng công khai. Hệ thống cần có hiệu quả và năng suất cao với nguồn tài nguyên tối thiểu và trong thời gian và khôn gian cần thiết.

Điều này cung cấp một bộ khung cơ bản để triển khai một hệ thống chia sẻ và phối hợp thông tin. Khung bao gồm bốn phần để xem xét là chính sách, phương pháp và quy trình, con người và các yếu tố kỹ thuật.

CHÚ THÍCH ITU Study Group 17 đang tiến hành việc mở rộng trao đổi thông tin an toàn không gian mạng. Tham khảo Bảng C.17 - Trao đổi thông tin an toàn không gian mạng để biết thêm thông tin.

13.2 Chính sách

13.2.1 Tổ chức cung cấp thông tin và tổ chức tiếp nhận thông tin

Theo mục đích của bộ khung này, hai loại hình tổ chức chia sẻ thông tin được giới thiệu:

- IPO và
- IRO.

Với phía gửi, IPO, các chính sách cơ bản liên quan đến danh mục và phân loại các thông tin, mức độ nghiêm trọng của các sự kiện và các sự cố và các hình thức chia sẻ nên được xác định trước khi xảy ra một sự cố an toàn không gian mạng hoặc bất kỳ chia sẻ nào diễn ra (trong trường hợp IPO biến thành một IRO để chia sẻ thông tin nhận được với các đơn vị có thẩm quyền khác trong chuỗi thông tin).

Với phía nhận, IRO nên đồng ý để thực thi việc bảo vệ an toàn và các thủ tục có liên quan khi nhận được thông tin từ IPO, phù hợp với các thỏa thuận đạt được trước đó và dựa trên danh mục và phân loại các thông tin liên quan.

13.2.2 Danh mục và phân loại thông tin

IPO nên xác định các loại thông tin khác nhau mà họ thu thập, tổng hợp, giữ an toàn và phân phối. Ví dụ về các loại thông tin có thể bao gồm các sự kiện an toàn, các mối đe dọa an toàn, điểm yếu an toàn, các hồ sơ tội phạm đáng nghi/ đã xác nhận, các nhóm tổ chức, thông tin nạn nhân và các loại hồ sơ hệ thống công nghệ thông tin.

Đối với mỗi loại, cần được tiếp tục chia thành hai hoặc nhiều loại khác dựa trên nội dung của các thông tin liên quan. Việc phân loại tối thiểu có thể nhạy cảm và không hạn chế. Nếu thông tin có chứa dữ liệu cá nhân, phân loại riêng tư cũng có thể được áp dụng.

13.2.3 Tối giản thông tin

Đối với mỗi lớp và phân lớp, IPO nên thực hiện thận trọng để tối giản các thông tin được phân phối. Việc tối giản là cần thiết để tránh tình trạng quá tải thông tin tại bên nhận, để đảm bảo sử dụng hiệu quả các hệ thống chia sẻ. Mục tiêu khác của việc tối giản là bỏ đi thông tin nhạy cảm để bảo vệ sự riêng tư của mọi người trong IPO và IRO. Trong trường hợp này, IPO và IRO nên xác định chi tiết

mức độ mong muốn cho mỗi danh mục và phân loại thông tin có thể được xác định trước khi chia sẻ thực tế tại bất cứ nơi nào có thể.

13.2.4 Hạn chế đối tượng

Phù hợp với nguyên tắc tối giản, một chính sách để hạn chế đối tượng (có thể là một một người, nhóm hoặc tổ chức liên lạc) cho việc phân phối là cần thiết khi chia sẻ thông tin có chứa dữ liệu riêng tư hoặc bí mật. Với thông tin ít nhạy cảm hơn, một chính sách cần được xem xét để ngăn chặn tình trạng quá tải thông tin, trừ khi những lợi ích của việc phân phối tối đa (chẳng hạn như chia sẻ các cảnh báo an toàn quan trọng) lớn hơn những tác động của quá tải thông tin cho IRO.

13.2.5 Giao thức phối hợp

Một chính sách mức cao cho việc phối hợp theo yêu cầu và phân phối (cho dù đó là IPO hoặc IRO khởi xướng) cần được thành lập. Chính sách này chính thức hóa các giao thức liên quan, cung cấp một phương tiện để IPO và IRO phản ứng một cách hiệu quả và năng suất. Thủ tục xác thực, xác minh lẫn nhau có thể được xây dựng dựa trên giao thức như vậy để đảm bảo tính xác thực của nguồn gốc và bằng chứng về việc phân phối tới nơi mong muốn, đặc biệt là các thông tin nhạy cảm, riêng tư và bí mật.

13.3 Các phương pháp và quy trình

13.3.1 Tổng quan

Để đạt hiệu quả chính sách chia sẻ thông tin, đảm bảo tính nhất quán trong thực tế, tính hiệu quả và độ tin cậy khi thực hiện, các phương pháp và quy trình liên quan cần được xây dựng và triển khai thực hiện. Phương pháp và quy trình như vậy cần được dựa trên các tiêu chuẩn có sẵn. Nếu không, sau khi xác nhận hoạt động, chúng có thể được chính thức hóa cho việc tiêu chuẩn hóa. Các điều khoản sau đây cung cấp hướng dẫn về các phương pháp và quy trình thường được sử dụng bởi các tổ chức trong ngành công nghiệp để đạt được mục tiêu và chính sách chia sẻ và phối hợp thông tin có liên quan trong ngữ cảnh an toàn không gian mạng.

13.3.2 Danh mục và phân loại các thông tin

Thông tin được chia sẻ có thể đến từ cả hai nguồn mở và đóng. Thông tin nguồn mở thường được tìm thấy trên internet hoặc từ các nguồn công cộng khác, chẳng hạn như báo chí. Thông tin nguồn mở nói chung là mức phân loại thấp nhất, vì những người đưa ra thông tin có thể có nhiều hoặc vô danh, thời gian tạo lập thông tin có thể không xác định và đối tượng chính xác của câu hỏi không cụ thể. Thông tin nguồn đóng không được công bố công khai, thường do một nguồn gốc có thâm niên. Ví dụ các thông tin nguồn đóng được nghiên cứu và phân tích độc quyền hoặc các hiểu biết thu thập được theo kinh nghiệm.

CHÚ THÍCH Hướng dẫn cho Điều này có thể dựa trên kết quả của giai đoạn nghiên cứu về chủ đề này, tham khảo tiêu chuẩn nếu giai đoạn nghiên cứu chuyển sang giai đoạn phát triển hoặc áp dụng một bản tóm tắt văn bản từ giai đoạn nghiên cứu nếu nó kết thúc mà không cần phát triển hơn nữa.

13.3.3 Thỏa thuận không tiết lộ

Một NDA có thể được sử dụng cho ít nhất hai mục đích trong ngữ cảnh chia sẻ và phối hợp thông tin để cải thiện an toàn không gian mạng. Điển hình của sử dụng NDA là để đảm bảo xử lý và bảo vệ đầy đủ các thông tin nhạy cảm, cá nhân và/hoặc bí mật được chia sẻ giữa IPO và IRO và thiết lập trước các điều kiện của việc chia sẻ, phân phối và sử dụng các thông tin đó.

Trong ngữ cảnh ứng phó với các sự kiện an toàn không gian mạng, việc thành lập trước một NDA cho phép chia sẻ và phân phối nhanh chóng giữa các đơn vị có thẩm quyền diễn ra một cách hiệu quả, ngay cả khi phân loại thông tin vẫn chưa được xác định rõ ràng.

13.3.4 Quy tắc thực hành

Một phương pháp thường được sử dụng để đảm bảo chia sẻ và xử lý đầy đủ thông tin nhạy cảm là thành lập một bộ quy tắc thực hành, bao gồm chi tiết các thủ tục, trách nhiệm và cam kết của các tổ chức liên quan (ví dụ, IPO và IRO) cho các phản ứng và hành động được thực hiện bởi các đơn vị tương ứng tham gia cho mỗi danh mục và phân loại thông tin.

Ví dụ Xem Tiêu chuẩn ISO/IEC 29147, Công nghệ thông tin – Các kỹ thuật an toàn – Công bố điểm yếu.

13.3.5 Kiểm tra và diễn tập

Để đảm bảo tính hiệu quả và độ tin cậy, các phương pháp và quy trình cần được xây dựng để thực hiện việc kiểm tra và thực hiện kịch bản diễn tập thường xuyên.

Một phương pháp tiêu chuẩn nên được sử dụng cho kiểm tra an toàn, để phù hợp với mục tiêu và nhu cầu của tổ chức.

Kiểm tra an toàn có thể thực hiện trên tài sản có rủi ro cao. Điều này có thể được hỗ trợ bằng cách sử dụng các danh mục và phân loại dữ liệu của tổ chức.

Đánh giá an toàn phải được thực hiện một cách thường xuyên trên:

- Ứng dụng
- Hệ điều hành
- Hệ thống quản lý cơ sở dữ liệu

13.3.6 Thời gian và lịch trình chia sẻ thông tin

Yêu cầu chia sẻ thông tin hoặc chủ động hoặc trong suốt quá trình ứng phó sự cố sẽ thay đổi theo từng đơn vị. Một số tổ chức sẽ có yêu cầu cung cấp thông tin thời gian thực: họ sẽ muốn thời điểm một cảnh báo hoặc báo động xảy ra để phân tích thêm. Các đối tượng khác không có các nguồn lực để quản lý việc chia sẻ thông tin theo thời gian thực. Trong thực tế, nhiều tổ chức có thể không có khả năng quản lý lịch trình chia sẻ thông tin trong khoảng thời gian bất kỳ.

Lịch trình và thời gian chia sẻ thông tin phải được xác định rõ ràng, với các mục tiêu cấp dịch vụ được xác định cụ thể cho mối quan hệ tự nguyện và thỏa thuận cấp dịch vụ cho các mối quan hệ thương mại.

13.4 Con người và tổ chức

13.4.1 Tổng quan

Con người và tổ chức là yếu tố quyết định cho sự thành công của an toàn không gian mạng. Con người ở đây là những cá nhân có liên quan trong việc thực hiện các phương pháp và quy trình chia sẻ và phối hợp thông tin để tạo ra sự khác biệt rõ ràng đến kết quả tích cực của các sự kiện an toàn không gian mạng. Các tổ chức là những nhóm người trong công ty hay toàn bộ công ty tham gia vào các hoạt động như vậy. Để đạt hiệu quả và năng suất, các nhu cầu của cả con người và các tổ chức cần được xem xét.

13.4.2 Liên lạc

Một danh sách liên lạc nên được biên soạn bởi các IPO và IRO và trao đổi với nhau để mỗi đơn vị có thể xác định người yêu cầu hoặc gửi thông tin tới cộng đồng chia sẻ.

Nhiều danh sách liên lạc chủ chốt cũng có thể được phát triển và chia sẻ phù hợp với đối tượng giới hạn (xem 13.2.4) và chính sách phân loại thông tin (xem 13.2.2).

Danh sách liên lạc không được chứa thông tin cá nhân nhạy cảm, để phù hợp với các chính sách tối giản thông tin (xem 13.2.3). Đối với mục đích riêng tư, một bí danh có thể được dùng thay cho tên đầy đủ. Các thông tin tối giản cho danh sách liên lạc nên bao gồm tên (hoặc bí danh), số liên lạc (điện thoại di động nếu có thể) và địa chỉ thư điện tử. Một liên lạc thay thế cũng có thể được thiết lập cho mỗi người quan trọng trong danh sách liên lạc.

Bên cạnh một danh sách liên lạc để chia sẻ và phối hợp thông tin, một danh sách liên lạc riêng biệt để báo cáo vượt cấp sự cố cũng có thể được biên dịch để tạo điều kiện báo cáo vượt cấp nhanh chóng. Một danh sách như vậy thường bao gồm địa chỉ liên lạc bên ngoài mà không phải là trong mạng chia sẻ. Ví dụ, xem Phụ lục B.

Ở mức tối thiểu, danh sách liên lạc cần được bảo vệ chống lại các sửa đổi trái phép để ngăn chặn việc sửa đổi và duy trì tính toàn vẹn. Các kiểm soát kỹ thuật (điều nhỏ 13.5) nên được áp dụng cho phù hợp.

13.4.3 Liên minh

Để tạo điều kiện chia sẻ thông tin và thiết lập các cách làm chung và nhất quán chi phối bởi một quy tắc thực hiện thống nhất và/hoặc NDA, tổ chức, nhóm cá nhân có thể hình thành các liên minh dựa vào các miền mà họ quan tâm, có thể là ngành công nghiệp, công nghệ hay các mối quan tâm đặc biệt

khác. Xem Phụ lục B về một danh sách mẫu các liên minh hiện tại và các tổ chức phi lợi nhuận phục vụ cho mục đích đó.

13.4.4 Sự nhận thức và đào tạo

Những người trong tổ chức phải nhận thức được các rủi ro an toàn không gian mạng mới đang nổi lên và được đào tạo để họ phát triển các kỹ năng và chuyên môn cần thiết để ứng phó một cách hiệu quả và năng suất khi họ gặp phải rủi ro cụ thể liên quan hoặc khi nhận được thông tin yêu cầu các hành động của họ để giảm thiểu hoặc cải thiện một tình huống nhất định. Để đạt được những mục tiêu này:

- Cuộc họp định kỳ về tình trạng và việc phát hiện nguy cơ an toàn không gian mạng liên quan đến tổ chức và ngành công nghiệp cần được thực hiện.
- Việc tập trung vào các buổi đào tạo dạng tất cả trong một về mô phỏng kịch bản tấn công không gian mạng và các buổi hội thảo về khu vực hành động đòi hỏi cụ thể nên được thiết kế, tổ chức và chuyển giao, cho cả những người mới vào nhóm/tổ chức và luôn được cập nhật thường xuyên.
- Kiểm tra thường xuyên, với các kịch bản liên quan từ đầu đến cuối để đảm bảo hiểu biết toàn diện và có khả năng để thực hiện các thủ tục và các công cụ cụ thể.

Việc nhận thức, đào tạo và kiểm tra có thể được thực hiện bởi các chuyên gia nội bộ có liên quan, chuyên gia tư vấn bên ngoài hoặc các chuyên gia từ các thành viên của liên minh tham gia vào việc chia sẻ và phối hợp thông tin.

Việc sử dụng kịch bản như là một phần của quá trình đào tạo và kiểm tra được khuyến khích như một cách tiếp cận cho phép các cá nhân đạt được kinh nghiệm gần với thực tế về các tình huống có liên quan, học và thực hành các ứng phó cần thiết. Ngoài ra, sự cố trước đó có thể được sử dụng như một phần của kịch bản để tối đa hóa việc chia sẻ các bài học kinh nghiệm và sự hiểu biết có được từ những tình huống như vậy.

13.5 Kỹ thuật

13.5.1 Tổng quan

Các kiểm soát kỹ thuật và tiêu chuẩn có thể được sử dụng để nâng cao hiệu quả, giảm lỗi của con người và tăng cường an toàn trong quá trình chia sẻ và phối hợp thông tin. Một số hệ thống kỹ thuật và các giải pháp có thể được thiết kế, phát triển và triển khai. Tiêu chuẩn này cung cấp một số phương pháp và kỹ thuật thường được sử dụng đã được chấp nhận và thực hiện bởi một số tổ chức và có thể được điều chỉnh thích hợp hơn để cải thiện nhu cầu và quy trình chia sẻ và phối hợp thông tin để đối phó với thay đổi môi trường rủi ro an toàn không gian mạng.

13.5.2 Tiêu chuẩn hóa dữ liệu cho hệ thống tự động

Là một phần của mạng chia sẻ, hệ thống tự động có thể được phát triển và triển khai giữa các tổ chức phối hợp để thu thập dữ liệu về sự tiến triển của các sự kiện an toàn không gian mạng theo thời gian thực, phân tích và đánh giá offline, để xác định tình trạng an toàn mới nhất trong không gian mạng trong ranh giới của các tổ chức liên quan. Những dữ liệu này có thể bao gồm dữ liệu lưu lượng truy cập mạng, các bản cập nhật bảo mật cho các hệ thống phần mềm và thiết bị phần cứng, các dữ liệu về điểm yếu an toàn và phần mềm độc hại, thư rác, dữ liệu về phần mềm gián điệp, bao gồm cả thông tin phụ tải và thông tin chặn bắt của chúng. Hệ thống tự động hỗ trợ những người ứng phó và các báo cáo vượt cấp sự cố đầu tiên, như mô tả trong điều nhỏ 13.4.2, cũng sẽ chứa các dữ liệu liên quan đến tổ chức và con người. Theo tính nhạy cảm và dung lượng của nội dung dữ liệu liên quan đến các hệ thống này, các tổ chức {đặc biệt, liên minh các tổ chức) nên đánh giá lược đồ và nội dung dữ liệu để xác định các kiểm soát kỹ thuật thích hợp để nâng cao hiệu quả, hiệu suất và an toàn. Điều này có thể bao gồm, nhưng không giới hạn:

a) Tiêu chuẩn hóa các lược đồ dữ liệu cho mỗi danh mục và phân loại dữ liệu thu thập để thực thi chính sách riêng tư và tối giản thông tin và cung cấp đảm bảo kỹ thuật cho tất cả các đơn vị tham gia và chủ sở hữu dữ liệu.

b) Tiêu chuẩn hóa định dạng dữ liệu để dễ dàng chia sẻ và cải thiện việc lưu trữ, truyền tải, xử lý và khả năng tương tác giữa các hệ thống. Ví dụ, xem ITU-T X.1205;

c) Tiêu chuẩn hóa các chức năng và thuật toán xử lý dữ liệu cơ bản được sử dụng, ví dụ, hàm băm và các thủ tục đồng bộ địa chỉ IP và các yêu cầu tiền xử lý khác.

13.5.3 Trực quan hóa dữ liệu

Xem xét sử dụng các kỹ thuật trực quan hóa dữ liệu để trình bày các sự kiện thông tin, giúp cải thiện khả năng hiển thị các thay đổi và sự cố an toàn mới nổi đang diễn ra mà không cần các nhà khai thác đọc các chi tiết của mỗi sự kiện khi nó xuất hiện. Ví dụ, Phụ lục A trình bày hình ảnh của hoạt động mạng ẩn (darknet), giúp hiển thị các phản ứng hiệu quả hơn đối với những thay đổi.

13.5.4 Trao đổi khóa mật mã và sao lưu phần mềm/ phần cứng

Để tạo điều kiện chia sẻ thông tin bí mật, một hệ thống mật mã, bao gồm một hệ thống trao đổi khóa có thể cần được triển khai nhanh chóng. Hệ thống này nên bao gồm các bản sao lưu đầy đủ cả phần mềm và phần cứng, cũng như các khóa được sử dụng để chuẩn bị cho mục đích chia sẻ và nhu cầu phục hồi khẩn cấp.

13.5.5 An toàn chia sẻ tập tin, tin nhắn tức thời, cổng thông tin điện tử và diễn đàn thảo luận

Để tạo điều kiện tương tác trực tuyến và chia sẻ thông tin nhanh chóng và an toàn, có thể bao gồm việc chia sẻ các nội dung kỹ thuật số như văn bản và các tập tin đa phương tiện và cả các cuộc thảo luận trực tuyến và ngoại tuyến, các tổ chức chia sẻ (IPO và IRO) nên cân nhắc áp dụng các công cụ

chia sẻ tập tin, tin nhắn tức thời và các công cụ diễn đàn thảo luận trực tuyến phù hợp để có thể đáp ứng nhu cầu an toàn, hiệu quả, hiệu suất và tin cậy.

Cổng thông tin điện tử cung cấp các tin tức về sự kiện và tình trạng an toàn không gian mạng cần được triển khai như một hình thức thông tin liên lạc cho cả cộng đồng và các cá nhân quan tâm và có liên quan. Trong trường hợp cổng thông tin web được sử dụng, cần phải có quyền sở hữu và trách nhiệm hành chính rõ ràng để đảm bảo sự an toàn và tính sẵn sàng của nó và các thông tin hạn chế đối tượng nên được cung cấp ở các khu vực riêng tư.

13.5.6 Hệ thống kiểm tra

Trong khi mỗi hệ thống kỹ thuật và các phương pháp và quy trình liên quan phải được kiểm tra một cách nghiêm ngặt để đảm bảo độ tin cậy và tính toàn vẹn của nó, nên cân nhắc một hoặc nhiều hệ thống kỹ thuật chuyên dùng để cải thiện hiệu quả và năng suất kiểm tra, đặc biệt là các kịch bản kiểm tra. Hệ thống này có thể là một hệ thống mô phỏng để mô phỏng các môi trường hoạt động của mỗi tổ chức trong không gian mạng và rút ra các tình huống an toàn không gian mạng, cung cấp khả năng giới thiệu một loạt các sự kiện an toàn để tạo điều kiện cho kiểm tra yêu cầu.

13.6 Hướng dẫn triển khai

Việc thực thi một bộ khung như vậy đòi hỏi các tổ chức, cá nhân hợp tác với nhau (ảo và thật) để xác định chính sách, biện pháp và các bước cụ thể cần thực hiện để đạt được mục tiêu chia sẻ, phối hợp thông tin an toàn, hiệu quả, hiệu suất và đáng tin cậy để ứng cứu các sự cố an toàn không gian mạng đang nổi cộm. Các bước mức cao sau đây được khuyến cáo như một hướng dẫn triển khai:

a) Xác định và thu thập các tổ chức, cá nhân có liên quan để hình thành cộng đồng mạng chia sẻ và phối hợp thông tin, cả không chính thức và chính thức;

b) Xác định các vai trò của từng tổ chức/ cá nhân liên quan như là IPO, IRO hoặc cả hai (điều nhỏ 13.2.1),

c) Thiết lập các loại thông tin và phối hợp cần thiết có thể mang lại lợi ích cho cộng đồng;

d) Thực hiện phân loại thông tin để xác định bất kỳ thông tin nhạy cảm và/hoặc riêng tư có liên quan (điều nhỏ 13.2.2);

e) Thiết lập các chính sách và nguyên tắc quản lý cộng đồng và các thông tin liên quan (điều nhỏ 13.2);

f) Xác định các phương pháp và quy trình cần thiết cho mỗi danh mục và phân loại các thông tin liên quan (điều nhỏ 13.3);

g) Xác định các yêu cầu và chỉ tiêu hiệu năng và thiết lập các quy tắc thực hành và ký tên NDA khi cần thiết (điều nhỏ 13.3.3 và 13.3.4);

h) Xác định các hệ thống kỹ thuật và tiêu chuẩn cần thiết và thích hợp để hỗ trợ việc triển khai và vận hành của cộng đồng (điều nhỏ 13.5);

i) Chuẩn bị cho việc vận hành; đối chiếu danh sách liên lạc; và tổ chức hội thảo nâng cao nhận thức và đào tạo để chuẩn bị cho các bên liên quan;

j) Tiến hành kiểm tra thường xuyên, bao gồm cả kịch bản và mô phỏng (điều nhỏ 13.5.5 và 13.5.6);

k) Tiến hành định kỳ, đánh giá sau kiểm tra, sau sự cố để cải thiện hệ thống chia sẻ và phối hợp hệ thống, bao gồm cả con người, quy trình và công nghệ liên quan; mở rộng hoặc giảm độ lớn của cộng đồng khi cần thiết.

CHÚ THÍCH Tiêu chuẩn TCVN ISO/IEC 27001:2009, Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Các yêu cầu và tiêu chuẩn ISO/IEC 27003, Công nghệ thông tin – Các kỹ thuật an toàn – Hướng dẫn triển khai hệ thống quản lý an toàn thông tin sẽ cung cấp các yêu cầu và hướng dẫn triển khai tương ứng.

Phụ lục A

(Tham khảo)

Sẵn sàng an toàn không gian mạng

A.1 Tổng quan

Các biện pháp kiểm soát an toàn không gian mang đã mô tả tại Điều 12 giảm thiểu sự lộ liễu và rủi ro của tổ chức và người dùng cuối trước hầu hết các tấn công không gian mạng đã biết. Khi có sự cố an toàn không gian mạng thì bộ khung chia sẻ và phối hợp thông tin đã miêu tả trong Điều 11 cung cấp việc thiết lập một hệ thống chia sẻ và phối hợp thông tin trong việc chuẩn bị đối phó với các sự kiện và sự cố an toàn không gian mạng. Những thông tin này được bảo vệ đầy đủ giữa IPO và IRO.

Trong khi các biện pháp kiểm soát giảm thiểu rủi ro và cải thiện việc quản lý và xử lý sự cố, tội phạm không gian mạng mạng vẫn tiếp tục phát triển các hình thức tấn công mới để vượt qua các hệ thống đang được bảo vệ. Do đó, các biện pháp kiểm soát cũng quan trọng cho các tổ chức trong việc triển khai các hệ thống và hạ tầng cho phép tiếp cận chủ động và chặt chẽ hơn để phát hiện, điều tra và có những hành động đáp trả kịp thời các cuộc tấn công.

ISO/IEC 27031 cung cấp hướng dẫn về các hệ thống quản lý và các quy trình liên quan để chuẩn bị một hệ thống công nghệ thông tin của tổ chức để phát hiện và ứng phó với các sự kiện an toàn đang nổi lên, bao gồm cả các sự kiện an toàn không gian mạng. Hướng dẫn này nhấn mạnh cách tiếp cận công nghệ bổ sung được áp dụng để cải thiện sự sẵn sàng an toàn không gian mạng của một tổ chức trong vùng phát hiện sự kiện thông qua hệ thống giám sát mạng ẩn (darknet), điều tra thông qua truy vết ngược (traceback) và đối phó thông qua hoạt động của máy chủ nhận các kết nối chuyển hướng (sinkhole).

Các tổ chức, đặc biệt là CIIPs nên cân nhắc tận dụng các phương pháp tiếp cận để cải thiện sự sẵn sàng an toàn không gian mạng của họ.

A.2 Giám sát mạng ẩn (darknet)

A.2.1 Giới thiệu

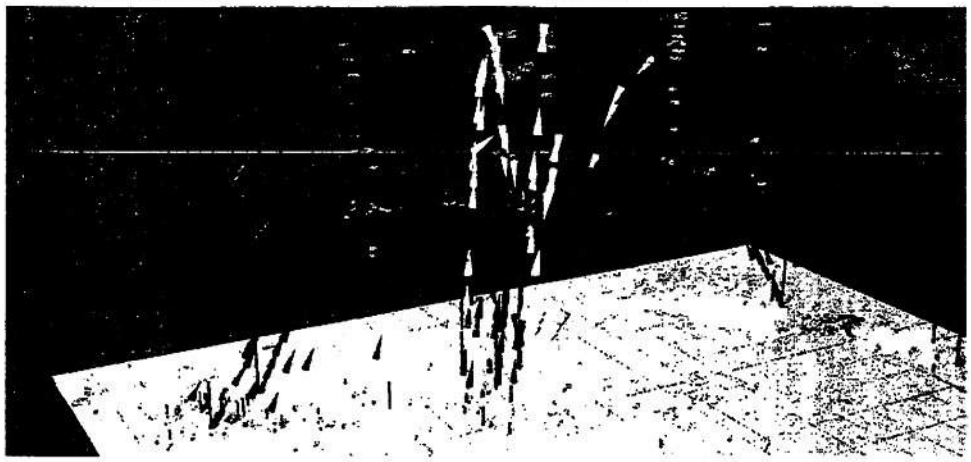
Mạng ẩn (darknet) là một tập hợp các địa chỉ IP mà không được sử dụng trong các tổ chức. Địa chỉ IP trong mạng ẩn (darknet) không được gán cho bất kỳ hệ thống máy chủ hay máy tính cá nhân nào. Bằng cách sử dụng các gói tin đã được giám sát trong vùng IP của mạng ẩn (darknet), các tổ chức có thể quan sát các cuộc tấn công mạng đang nổi lên, bao gồm việc rà quét mạng trong pha khởi tạo của phần mềm độc hại, hành vi lây nhiễm phần mềm độc hại và tán xạ ngược DDoS Backscatters. Dải địa chỉ IP của mạng ẩn (darknet) được công khai nhưng không được gán cho bất kì máy tính nào, tất cả lưu lượng truy cập đến vùng IP của mạng ẩn (darknet) có thể được suy ra như một hệ quả của hoặc hoạt động độc hại hoặc cấu hình không chính xác.

Nói chung, có ba phương pháp thường được sử dụng trong mạng ẩn (darknet) để quan sát các lưu lượng có liên quan đến các hoạt động phá hoại trên Internet, cụ thể là giám sát lỗ đen Internet (Black Hole), giám sát tương tác ở mức thấp và giám sát tương tác ở mức cao.

A.2.2 Giám sát lỗ đen Internet (Black Hole)

Giám sát Black Hole đề cập đến các hệ thống giám sát mà không phản ứng bất cứ điều gì đối với các gói tin được tìm thấy bên trong vùng IP của mạng ẩn (darknet). Loại hệ thống giám sát này thường được sử dụng để quan sát các hành vi quét cổng mạng bởi phần mềm độc hại, các hành vi lây nhiễm phần mềm độc hại (UDP với tải có chứa các đoạn mã shell code) và tán xạ ngược DDoS Backscatters. Quét cổng mạng thường được những đối tượng tấn công sử dụng đầu tiên để tìm kiếm các điểm yếu của hệ thống để có thể khai thác. Các hành vi lây nhiễm phần mềm độc hại thường được những đối tượng tấn công sử dụng ở bước tiếp theo sau khi xác định các điểm yếu trên hệ thống. Hành vi lây nhiễm thường được quan sát bằng cách sử dụng các gói tin UDP với phần tải được xây dựng sẵn trên hệ thống giám sát Black Hole. Hơn nữa, tán xạ ngược DDoS Backscatter cũng được giám sát bằng hệ thống giám sát Black Hole trong trường hợp giả mạo địa chỉ IP nguồn và mục tiêu của DDoS có thể được nhận ra bởi lưu lượng tán xạ ngược Backscatter đó. Hình A.1 mô tả một ảnh chụp màn hình một trường hợp các hành vi của phần mềm độc hại được phát hiện bởi một hệ thống giám sát Black Hole. Một liên kết video mẫu có thể tìm thấy tại địa chỉ:

https://www.youtube.com/watch?v=asemvKgkib4&feature=related



Hình A.1 – Ví dụ về trực quan hóa hành vi của phần mềm độc hại sử dụng hệ thống giám sát Black hole.

Các "mũi tên" trong hình A.1 mô tả chiều của các gói tin IP đi từ nguồn đến các mục tiêu. Các sắc thái khác nhau (màu sắc trong video) mô tả các loại dữ liệu (ví dụ như TCP SYN, TCP SYN-ACK, các dạng khác của TCP, UDP và ICMP). Độ cao của mỗi mũi tên tỉ lệ với số cổng (port) của nó.

A.2.3 Hệ thống giám sát tương tác ở mức thấp

Hệ thống giám sát tương tác ở mức thấp là hệ thống giám sát mạng ẩn (darknet), hệ thống này phản ứng khi phát hiện có gói tin IP mạng ẩn (darknet) bằng cách cố gắng kết nối lại với các hệ thống máy chủ đáng ngờ. Mục đích của việc cố gắng kết nối là để có được thêm thông tin về các hệ thống đang tấn công, đường đi của gói tin và các thông tin khác liên quan đến đối tượng tấn công nếu có thể. Hệ thống giám sát thường được cấu hình chính bản thân nó như là một hệ thống có nhiều điểm yếu để thu hút các đối tượng tấn công. Hệ thống giám sát tương tác ở mức thấp được sử dụng để quan sát các

phản ứng tiếp theo của các hoạt động và hành vi độc hại như việc thực hiện gửi đoạn mã shell code sau khi quét cổng mạng.

A.2.4 Hệ thống giám sát tương tác ở mức cao

Một hệ thống giám sát tương tác ở mức cao (còn được gọi là một hệ thống tài nguyên thông tin giả dạng-honeypot-tương tác cao) là một hệ thống giám sát mạng ẩn (darknet), hệ thống này cũng phản ứng khi phát hiện có gói tin IP mạng ẩn (darknet) bằng cách cố gắng kết nối lại với các hệ thống máy chủ đáng ngờ và tương tác với các hệ thống đó càng nhiều càng tốt. Mục đích của việc tương tác là có được các thông tin ở mức sâu hơn bao gồm cả chiến lược khai thác điểm yếu bảo mật, tiêm nhiễm phần mềm độc hại vào hệ thống sau khi tấn công và hành vi của các phần mềm độc hại đó. Hệ thống giám sát tương tác ở mức cao có thể được thực hiện, cài đặt trên hệ thống thật hoặc hệ thống ảo tồn tại nhiều điểm yếu để thu hút sự chú ý của đối tượng tấn công, bị khai thác và cuối cùng bắt được các mẫu phần mềm độc hại lây nhiễm đó.

A.3 Hệ thống nhận các kết nối chuyển hướng Sinkhole

Một hệ thống nhận các kết nối chuyển hướng (Sinkhole) được định nghĩa là một phương pháp để chuyển hướng lưu lượng từ một IP cụ thể đến một thiết bị sinkhole (ví dụ bộ định tuyến sinkhole) phục vụ cho mục đích phân tích lưu lượng, chuyển hướng các cuộc tấn công và phát hiện các hành vi bất thường trên mạng. Ví dụ, nếu hoạt động nghiệp vụ của một hệ thống mục tiêu bị phá vỡ bằng một cuộc tấn công DDoS, một trong những giải pháp hiệu quả là khởi tạo hệ thống nhận các kết nối chuyển hướng sinkhole bằng cách tạo một tuyến đường khác ở hệ thống mục tiêu để chuyển hướng lưu lượng DDoS đến hệ thống sinkhole thay vì đến mục tiêu ban đầu. Các thiết bị sinkhole có khả năng hấp thụ, phân tích và/hoặc loại bỏ lưu lượng DDoS. Việc định tuyến để chuyển hướng lưu lượng thường được thực hiện trên bộ định tuyến biên BGP. Hoạt động của hệ thống sinkhole bằng cách sử dụng cấu hình BGP (giao thức định tuyến liên miền) được mô tả trong RFC 3882. Một điểm bất lợi của phương pháp này là địa chỉ IP đang bị tấn công không thể sử dụng để giao tiếp với những mạng khác cho đến khi tuyến đường vừa tạo bị hủy bỏ.

Hệ thống sinkhole thường được sử dụng để bảo vệ chống lại các cuộc tấn công DDoS như mô tả ở trên. Nó cũng được triển khai để bảo vệ chống lại các cuộc tấn công mạng máy tính ma (botnet) bằng cách chuyển hướng trình điều khiển và ra lệnh (Command and Control C&C) mạng máy tính ma (botnet) tới các thiết bị sinkhole. Vì mỗi bot cần phải thiết lập kết nối tới một máy chủ C&C để nhận các hướng dẫn tấn công thông qua các tập lệnh được xây dựng từ trước, các bot này cần gửi các câu lệnh truy vấn DNS để phân giải ra URL của máy chủ C&C. Sau đó các máy chủ DNS gửi địa chỉ IP của thiết bị sinkhole đến cho bot thay vì địa chỉ IP thật của máy chủ C&C. Do đó, trình điều khiển mạng máy tính ma (botnet) bị chiếm các kết nối đến các con bot và như vậy bot không nhận được các tập lệnh hướng dẫn tấn công.

A.4 Truy vết ngược (traceback)

Để tự động hóa hoặc giải quyết việc theo dõi để chống lại các cuộc tấn công như tấn công DoS trong trường hợp máy chủ nguồn bị giả mạo, nhiều kỹ thuật truy vết ngược (traceback) đã được nghiên cứu. Các công nghệ truy vết ngược (traceback) được công nhận là kỹ thuật tái tạo lại con đường tấn công

và xác định vị trí các nút tấn công bằng cách hiệu chỉnh các lưu lượng tấn công, thông tin định tuyến, các gói tin được đánh dấu hoặc truy vết log các lưu lượng đó.

Chưa có kỹ thuật truy vết ngược (traceback) được dùng hay thực hành trên môi trường mạng thực tế có thể tái tạo lại được đường đi của cuộc tấn công qua vài miền mạng. Những khó khăn của việc triển khai các công nghệ truy vết ngược (traceback) liên miền (đi qua một vài miềnmạng) được bắt nguồn từ các vấn đề sau đây:

a) Đối với mục đích của việc truy vết ngược (traceback) liên miền, việc trao đổi các thông tin nhạy cảm như là chi tiết cấu hình mạng đường trục có thể gây ra những vấn đề nguy hiểm cho nhà vận hành mạng.

b) Hoạt động truy vết ngược (traceback) có thể được gắn chặt với an toàn mạng đường trục của các nhà cung cấp dịch vụ (ISP), việc thử nghiệm bất kỳ nỗ lực truy vết ngược (traceback) nào bởi những người không được cấp quyền sẽ không được chấp nhận ở hầu hết các ISP. Vì vậy, sẽ có sự đề phòng với các công nghệ truy vết ngược (traceback) trong trường hợp truy vết ngược (traceback) liên miền.

c) Nếu một công nghệ truy vết ngược (traceback) liên miền duy nhất được áp dụng qua một vài miền mạng thì công nghệ duy nhất này cần được phát triển với sự tham gia cùng lúc của các hệ thống tự quản (AS). Hơn nữa, đối tượng tấn công không sớm thì muộn cũng sẽ phát triển các công nghệ ẩn mình tinh vi hơn. Thực tế mà nói, nhiều ISP sử dụng nhiều công cụ phát hiện và truy vết ngược (traceback) trong chính mạng của họ.

Các vấn đề hoạt động trên sẽ này sinh khi việc thử nghiệm traceback cố gắng để mở rộng vượt qua ngoài ranh giới mạng. Kỹ thuật truy vết ngược (traceback) nên cân nhắc các ranh giới của hoạt động mạng và sự khác nhau của các chính sách an toàn trong mỗi miền mạng khác nhau đó. Chắc chắn rằng truy vết ngược (traceback) liên miền và các cơ chế giảm nhẹ tấn công cần phải được triển khai ở khắp nơi trên Internet.

Với sự phát triển của các công nghệ và hệ thống truy vết ngược (traceback) liên miền trong thực tế, kiến trúc truy vết ngược (traceback) sau nên được soát xét:

a) Đối với việc giữ ranh giới mạng, kiến trúc truy vết ngược (traceback) phải chỉ rõ hệ thống tự quản-AS chịu trách nhiệm theo dõi, nhận các yêu cầu theo chính sách hoạt động của mỗi AS;

b) Kiến trúc truy vết ngược (traceback) cũng phải chỉ rõ hệ thống tự quản AS quyết định là có hay không điều tra bên trong mạng riêng của họ và nếu cho phép thì điều tra ở mức độ nào.

c) Kiến trúc này cũng nên cho phép mỗi miền phụ của một AS quyết định có hay không việc kiểm tra hệ thống mạng của chính nó theo chính sách hoạt động. Các hoạt động của truy vết ngược (traceback) sẽ tiêu thụ nhiều tài nguyên trên các AS liên quan; Do đó, kiến trúc truy vết ngược (traceback) không nên tạo ra hay làm ngập bằng các yêu cầu vô nghĩa nếu có thể; Do đó, kiến trúc truy vết ngược (traceback) không nên chuyển tiếp thông điệp yêu cầu không có liên quan đến vụ tấn công đến các AS khác;

d) Để giảm thiểu thiệt hại của việc lạm dụng, bản tin không nên truyền đạt thông tin nhạy cảm, có thể làm sự rò rỉ bí mật hoặc tính bí mật của một AS; do đó, các kiến trúc truy vết ngược (traceback) không nên tiết lộ thông tin nhạy cảm của một AS cho AS khác;

e) Ngay cả khi việc sử dụng sai hoặc một hành động xâm hại xảy ra, việc truy vết nguồn gốc của thông điệp sẽ xác định *đối tượng tấn công* , do đó, một tin nhắn *trao đổi trong* kiến trúc cần phải có sự truy vết nguồn gốc riêng của chính nó để chứng minh hoặc xác nhận bên đưa ra;

f) Nếu kiến trúc phụ thuộc vào một kỹ thuật truy vết ngược (traceback) cụ thể, đối tượng tấn công sẽ phát triển cách né tránh và ẩn vị trí của các nút tấn công. Để đối phó với các cách né tránh đó, kiến trúc truy vết ngược (traceback) nên được độc lập với kỹ thuật truy vết ngược (traceback) cụ thể;

g) Nhiều hệ thống hoạt động hỗ trợ IPv4/ IPv6 dual stack và một số cuộc tấn công thực hiện thông qua đường hầm 6to4 IPv6. Nếu kiến trúc truy vết ngược (traceback) không thể theo dõi các cuộc tấn công trên mạng IPv6 hoặc các cuộc tấn công thông qua một vài bộ translator, phần lớn các cuộc tấn công sẽ chuyển thành một cuộc tấn công phức tạp. Do đó, kiến trúc truy vết ngược (traceback) nên theo dõi một cuộc tấn công trên môi trường dual stack, ngay cả khi cuộc tấn công sử dụng một số kỹ thuật chuyển dịch địa chỉ;

h) Để tự động hóa quá trình giảm nhẹ tấn công, kiến trúc nên xuất kết quả của một truy vết ngược (traceback) thử nghiệm để kích hoạt việc giảm nhẹ tấn công. Do đó, kiến trúc truy vết ngược (traceback) nên cho phép mỗi AS có hành động như lọc hoặc theo dõi khác với kết quả theo dõi.

i) Các kiến trúc nên có khả năng hợp tác với các hệ thống phát hiện và hệ thống bảo vệ;

j) Một đối tượng tấn công có thể thay đổi dạng lưu lượng tấn công để tránh ảnh hưởng của các hành động giảm nhẹ như vậy. Khi ứng phó với những thay đổi của một cuộc tấn công phức tạp, thời gian bỏ ra để truy vết một đường dẫn tấn công nên càng ngắn càng tốt. Do đó, kiến trúc nên loại trừ yếu tố con người càng nhiều càng tốt.

Phụ lục B
(Tham khảo)
Nguồn tài nguyên bổ sung

B.1 Tài liệu tham khảo an toàn trực tuyến và an toàn trực tuyến

Có một số trang web có thể được tham chiếu thêm thông tin liên quan đến điều kiện an toàn Internet và an toàn không gian mạng. Sau đây là một danh sách không đầy đủ các ví dụ:

- **Liên minh phần mềm chống gián điệp – ASC** (http://www.antispywarecoalition.org/) - Một nhóm chuyên xây dựng một sự đồng thuận về định nghĩa và thực hành tốt nhất trong các cuộc tranh luận về phần mềm gián điệp và các công nghệ không mong muốn tiềm năng khác. Liên minh bao gồm các công ty phần mềm, các viện nghiên cứu và các nhóm người dùng phần mềm chống gián điệp, ASC tìm cách mang lại đa dạng các quan điểm về các vấn đề biện pháp kiểm soát phần mềm gián điệp và các công nghệ không mong muốn tiềm năng khác..
- **APWG** (http://www.antiphishing.org) - Một trang web giáo dục và nhận thức về lừa đảo trực tuyến, cung cấp các bài báo cập nhật hàng quý về xu hướng tấn công, phân phối, tác động và tin tức các cuộc tấn công.
- **Be Web Aware** (http://www.bewebaware.ca) - Chương trình giáo dục cộng đồng song ngữ, quốc gia về điều kiện an toàn Internet được thiết kế để đảm bảo rằng lợi ích của người Canada từ mạng Internet được an toàn và trách nhiệm trong các hoạt động trực tuyến của họ.
- **Trung tâm về sử dụng Internet an toàn, trách nhiệm** (http://csriu.org) - Tổ chức cung cấp dịch vụ giải quyết các vấn đề về sử dụng Internet an toàn và trách nhiệm.
- **Childnet International** (http://www.childnet-int.org) - Tổ chức phi lợi nhuận hoạt động trong quan hệ đối tác với những thành phần khác trên toàn thế giới để giúp biến Internet thành một nơi tuyệt vời và an toàn cho trẻ em.
- **ECPAT** (http://www.ecpat.net) - Mạng lưới các tổ chức, cá nhân làm việc với nhau để loại bỏ việc khai thác tình dục trẻ em.
- **GetNetWise** (http://www.getnetwise.org) - Dịch vụ công cộng được cung cấp bởi một liên minh của các công ty ngành công nghiệp Internet và các tổ chức lợi ích công cộng muốn người dùng chỉ cần "một cú nhấp chuột" vào các nguồn tài nguyên mà họ cần để đưa ra quyết định về việc sử dụng Internet của họ và gia đình
- **Liên minh hạ tầng toàn cầu cho điều kiện an toàn Internet (GIAIS)** (http://www.microsoft.com/security/mrsa/default.mspx) - Một liên minh của một số nhà cung cấp dịch vụ, tổ chức để cải thiện an toàn và bảo mật trên Web, quản lý các mối đe dọa bằng cách mở rộng tầm nhìn, xác định và giảm thiểu các điểm yếu đang tồn tại.
- **INHOPE** (http://inhope.org) - Hiệp hội quốc tế hỗ trợ đường dây nóng Internet để xử lý các báo cáo về nội dung bất hợp pháp để giúp cho Internet an toàn hơn.

- **Nhóm điều kiện an toàn Internet** (www.netsafe.org.nz) - Trang web NetSafe là trang trực tuyến của Tập đoàn về điều kiện an toàn Internet của New Zealand (ISG) và Hector the Protector.
- **Interpol** (http://www.interpol.int) - Tổ chức cảnh sát quốc tế, tạo sự dễ dàng trong việc hợp tác cảnh sát xuyên biên giới và hỗ trợ tất cả các tổ chức, chính quyền và các dịch vụ có nhiệm vụ ngăn ngừa hoặc chống lại tội phạm quốc tế.
- **iSafe** (http://www.isafe.org) - Dẫn đầu trên toàn thế giới trong giáo dục điều kiện an toàn Internet, kết hợp chương trình giảng dạy lớp học với tiếp cận cộng đồng năng động để giúp cho sinh viên, giáo viên, phụ huynh, bên thực thi pháp luật và các vị thành niên có liên quan biến Internet thành một nơi an toàn hơn.
- **ISECOM** (http://www.isecom.org) - Phương pháp mã nguồn mở, miễn phí (FDL) về kiểm tra an toàn chuyên nghiệp (đánh giá điểm yếu, thử nghiệm thâm nhập, đạo đức hacking), kỹ thuật đánh giá rủi ro (RAVs, ...). ISECOM chạy OSSTMM (Open Source Security Testing Methodology Manual), một tiêu chuẩn về thực hiện kiểm tra an toàn IT/ICT (http://www.osstmm.org).
- **COP** (http://www.itu.int/cop/) - Bảo vệ trực tuyến trẻ em (COP) là một dự án đặc biệt được thực hiện bởi ITU (Liên minh Viễn thông Quốc tế) và các cơ quan/ công ty chuyên ngành khác, cung cấp hướng dẫn an toàn cho: Trẻ em, phụ huynh, người giám hộ và người giáo dục, công nghiệp và các nhà hoạch định chính sách.
- **An toàn Microsoft tại nhà** (http://www.microsoft.com/protect) - Thông tin và các nguồn tài nguyên để giúp mọi người bảo vệ máy tính của họ, bản thân họ và gia đình họ.
- **Viện quốc gia Công nghệ Viễn thông, INTECO** (http://www.inteco.es, http://cert.inteco.es, http://www.osi.es, http://observatorio.inteco.es) - Dịch vụ công cộng phi lợi nhuận được cung cấp bởi chính quyền Tây Ban Nha để thúc đẩy sự tin cậy và an toàn Internet cho người dân, doanh nghiệp nhỏ, người làm kỹ thuật, trẻ em, ..., thông qua một Trung tâm ứng cứu sự cố khẩn cấp (INTECO-CERT), một Security Helpdesk For Citizens (OSI) và một Đài quan sát an toàn thông tin.
- **Net Family News** (http://netfamilynews.org) - Dịch vụ công cộng phi lợi nhuận cung cấp một diễn đàn và tin tức công nghệ cho bé cho các gia đình và nhà giáo dục trên hơn 50 quốc gia.
- **NetAlert Limited** (http://www.netalert.net.au) - Tổ chức cộng đồng phi lợi nhuận được thành lập bởi chính phủ Úc để cung cấp tư vấn và giáo dục độc lập về quản lý truy cập nội dung trực tuyến.
- **NetSmartzKids** (http://www.netsmartzkids.org) - NetSmartz là một tài nguyên an toàn giáo dục tương tác giữa Trung tâm quốc gia về trẻ em mất tích và bị bóc lột (NCMEC) và Câu lạc bộ các bé trai và bé gái Mỹ (BGCA) cho trẻ em tuổi từ 5-17, cha mẹ, người giám hộ, các nhà giáo dục

và bên thực thi pháp luật ở độ tuổi phù hợp, các hoạt động 3-D để dạy trẻ em làm thế nào để giữ an toàn trên Internet.

- **Saferinternet.be** (www.saferinternet.be) - Trang web này cung cấp thông tin hữu ích về những rủi ro và nội dung độc hại chính mà trẻ vị thành niên trong độ tuổi có thể phải đối mặt khi trực tuyến và trong miền của ICT nói chung (do đó, cũng qua mạng điện thoại di động, ...) , ví dụ như khiêu dâm trẻ em, phân biệt chủng tộc và phân biệt đối xử, giáo phái, thực hiện thương mại bất hợp pháp và cuối cùng là các rủi ro kỹ thuật. Các trang web, mà còn trình bày các chiến lược để đối phó một cách chính xác với những rủi ro, bao gồm một số phần tập trung vào các nhóm đối tượng khác nhau. Nó cung cấp các tập tin kỹ thuật và những thứ sư phạm khác cho nhà giáo dục (phụ huynh và giáo viên), trò chơi cho trẻ em (từ 6 đến 12) và một trang web hoàn toàn riêng biệt (web4me.be) cho thanh thiếu niên.
- **SafeKids.com** (http://www.safekids.com) - Nguồn tài nguyên để giúp các gia đình tạo ra Internet và công nghệ vui vẻ, an toàn và hiệu quả.
- **StaySafe.org** (http://www.staysafe.org) - Trang web giáo dục nhằm giúp người dùng hiểu những khía cạnh tích cực của Internet cũng như làm thế nào để quản lý một loạt các vấn đề an toàn và bảo mật tồn tại trên mạng.
- **UNICEF** (http://www.unicef.org) – Quỹ nhi đồng liên hợp quốc, bảo vệ quyền lợi trẻ em chuyên cung cấp các hỗ trợ nhân đạo và phát triển lâu dài cho trẻ em và các bậc cha mẹ ở các nước đang phát triển.
- **Websafe Crackerz** (http://www.websafecrackerz.com) - Trò chơi tương tác và câu đố được thiết kế để giúp thanh thiếu niên và các chiến lược đề nghị đối phó với các tình huống khác nhau trực tuyến bao gồm cả thư rác, tấn công giả mạo và lừa đảo.

B2. Danh sách mẫu các địa chỉ liên lạc báo cáo vượt cấp sự cố

Bảng B.1 dưới đây cung cấp một danh sách không đầy đủ các ví dụ về các địa chỉ liên lạc báo cáo vượt cấp sự cố an toàn Internet:

Bảng B.1 - Danh sách mẫu các thông tin liên lạc khi báo cáo vượt cấp các vấn đề an toàn

Tổ chức	Liên hệ
Cisco Systems Inc.	mailto: safetyandsecurity@cisco.com http://www.cisco.com/security
Tập đoàn Microsoft	mailto: avsubmit@submit.microsoft.com mailto: secure@microsoft.com
Diễn đàn của Trung tâm an toàn và ứng cứu sự cố (FIRST)	http://www.first.org/about/organization/teams/
Trung tâm CERT quốc gia tương ứng	

(Ví dụ)	
Viện quốc gia về Công nghệ Viễn thông, INTECO, Tây Ban Nha	http://cert.inteco.es (English: http://cert.inteco.es/cert/INTECOCERT_1?postAction=getCertHome)
Viễn thông-ISAC Nhật Bản	https://www.telecom-isac.jp/contact/index.html
KrCERT/CC (Trung tâm an toàn Internet Hàn Quốc)	http://www.krcert.or.kr/index.jsp

Phụ lục C

(Tham khảo)

Ví dụ các tài liệu liên quan

C.1 Giới thiệu

Phụ lục này cung cấp một danh sách không đầy đủ các tài liệu có thể hữu ích khi xem xét an toàn không gian mạng. Đó không phải là một danh sách đầy đủ các Tiêu chuẩn và Báo cáo Kỹ thuật cho an toàn không gian mạng.

C.2 ISO và IEC

Bảng C.1 - Hệ thống quản lý an toàn thông tin

Tài liệu tham khảo	Tiêu đề
TCVN 11238:2015 (ISO/IEC 27000:2014)	Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng
ISO/IEC 27001 (TCVN ISO/IEC 27001:2009)	Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Các yêu cầu
ISO/IEC 27002 (TCVN ISO/IEC 27002:2011)	Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành quản lý an toàn thông tin
ISO/IEC 27003	Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn triển khai hệ thống quản lý an toàn thông tin
ISO/IEC 27010	Công nghệ thông tin - Các kỹ thuật an toàn – Quản lý an toàn thông tin quản lý cho truyền thông liên ngành

Bảng C.2 - Quản lý rủi ro

Tài liệu tham khảo	Tiêu đề
ISO/IEC 27005 (TCVN 10295:2016)	Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý rủi ro an toàn thông tin
ISO/IEC 16085	Kỹ thuật phần mềm và hệ thống - Quy trình vòng đời - Quản lý rủi ro

Bảng C.3 – Đánh giá an toàn IT

Tài liệu tham khảo	Tiêu đề
ISO/IEC 15408 (TCVN ISO/IEC 8709)	Công nghệ thông tin - Kỹ thuật an toàn - Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn IT
ISO/IEC 18045	Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn IT

ISO/IEC TR 19791	Công nghệ thông tin - Các kỹ thuật an toàn - Đánh giá an toàn hệ thống vận hành

Bảng C.4 - Đảm bảo an toàn

Tài liệu tham khảo	Tiêu đề
ISO/IEC 15443	Công nghệ thông tin - Các kỹ thuật an toàn – Bộ khung cho đảm bảo an toàn IT
ISO/IEC 15026	Kỹ thuật phần mềm và hệ thống - Đảm bảo phần mềm và hệ thống

Bảng C.5 -Thiết kế và triển khai

Tài liệu tham khảo	Tiêu đề
ISO/IEC 12207	Kỹ thuật phần mềm và hệ thống - Quy trình vòng đời phần mềm
ISO/IEC 14764	Kỹ thuật phần mềm - Quy trình vòng đời phần mềm - Bảo trì
ISO/IEC 15288	Kỹ thuật phần mềm và hệ thống - Quy trình vòng đời hệ thống
ISO/IEC 23026	Kỹ thuật phần mềm - Thực hành khuyến nghị cho Internet - Kỹ thuật Website, quản lý Website và vòng đời Website
ISO/IEC 42010	Kỹ thuật phần mềm và hệ thống - Mô tả kiến trúc

Bảng C.6 - Dịch vụ thuê ngoài và bên thứ ba

Tài liệu tham khảo	Tiêu đề
ISO/IEC TR 14516	Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn việc sử dụng và quản lý các dịch vụ của bên thứ ba được tin cậy
ISO/IEC 15945	Công nghệ thông tin - Các kỹ thuật an toàn - Đặc tả kỹ thuật của dịch vụ TTP để hỗ trợ các ứng dụng chữ ký số

Bảng C.7 - An toàn mạng và ứng dụng

Tài liệu tham khảo	Tiêu đề
ISO/IEC 18028	Công nghệ thông tin - Các kỹ thuật an toàn - An toàn mạng IT
ISO/IEC 18043	Công nghệ thông tin - Các kỹ thuật an toàn – Việc lựa chọn, triển khai và vận hành các hệ thống phát hiện xâm nhập
ISO/IEC 27033	Công nghệ thông tin - Các kỹ thuật an toàn - An toàn mạng
ISO/IEC 27034	Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn cho an toàn ứng dụng

Bảng C.8 – Quản lý sự cố và tính liên tục

Tài liệu tham khảo	Tiêu đề
ISO/IEC TR 18044	Công nghệ thông tin - Các kỹ thuật an toàn – Quản lý sự cố an toàn thông tin
ISO/IEC 24762	Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn các dịch vụ phục hồi thảm họa công nghệ thông tin và truyền thông
ISO/IEC 27031	Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn sẵn sàng ICT cho tính liên tục của nghiệp vụ
ISO/IEC 27035	Công nghệ thông tin - Các kỹ thuật an toàn – Quản lý sự cố an toàn thông tin

Bảng C.9 – Quản lý định danh

Tài liệu tham khảo	Tiêu đề
ISO/IEC 24760	Công nghệ thông tin - Các kỹ thuật an toàn – Bộ khung cho quản lý định danh.

Bảng C.10 – Tính riêng tư

Tài liệu tham khảo	Tiêu đề
ISO/IEC 29100	Công nghệ thông tin – Các kỹ thuật an toàn – Bộ khung về tính riêng tư.

Bảng C.11 Quản lý tài sản

Tài liệu tham khảo	Tiêu đề
ISO/IEC 19770	Công nghệ thông tin – Quản lý tài sản phần mềm

Bảng C.12 Quản lý dịch vụ

Tài liệu tham khảo	Tiêu đề
ISO/IEC 20000	Công nghệ thông tin – Quản lý dịch vụ

C.3 ITU-T

Bảng C.13 An toàn không gian mạng

Tài liệu tham khảo	Tiêu đề
ITU-T X.1200 – X.1299 Series	Series X: Mạng dữ liệu, An toàn và truyền thông hệ thống mở, An toàn viễn thông – An toàn không gian mạng
ITU-T X.1205	Series X: Mạng dữ liệu, An toàn và truyền thông hệ thống mở, An toàn viễn thông – Tổng quan an toàn không gian mạng

Bảng C.14: Quản lý sự cố và liên tục

Tài liệu tham khảo	Tiêu đề
ITU-T X.1206	Series X: Mạng dữ liệu, An toàn và truyền thông hệ thống mở, An toàn viễn thông - Một bộ khung nhà cung cấp trung lập cho các thông báo tự động về các thông tin về an toàn liên quan tới thông tin và các cập nhật phổ biến.

Bảng C.15 - Phần mềm không mong muốn

Tài liệu tham khảo	Tiêu đề
ITU-T X.1207	Series X: Mạng dữ liệu, An toàn và truyền thông hệ thống mở, An toàn viễn thông - Hướng dẫn cho các nhà cung cấp dịch vụ viễn thông về giải quyết rủi ro phần mềm gián điệp và phần mềm không mong muốn.

Bảng C.16 – Thư rác

Tài liệu tham khảo	Tiêu đề
ITU-T X.1231	Series X: Mạng dữ liệu, An toàn và truyền thông hệ thống mở, An toàn viễn thông - Chiến lược kỹ thuật cho chống thư rác
ITU-T X.1240	Series X: Mạng dữ liệu, An toàn và truyền thông hệ thống mở, An toàn viễn thông – Các công nghệ liên quan tới chống e-mail rác
ITU-T X.1241	Series X: Mạng dữ liệu, An toàn và truyền thông hệ thống mở, An toàn viễn thông – Bộ khung kỹ thuật cho chống e-mail rác
ITU-T X.1244	Series X: Mạng dữ liệu, An toàn và truyền thông hệ thống mở, An toàn viễn thông – Các khía cạnh chung về chống thư rác trong các ứng dụng đa phương tiện trên nền IP

Bảng C.17 – Trao đổi thông tin an toàn không gian mạng

Tài liệu tham khảo	Tiêu đề
ITU-T X.1500 -X.1598 Series (CYBEX)	Series X: Mạng dữ liệu, An toàn và truyền thông hệ thống mở, An toàn viễn thông – Trao đổi thông tin an toàn không gian mạng.

CHÚ THÍCH: Tính đến tháng 9 năm 2011, CYBEX hiện đang được tiến hành tại ITU-T, chỉ X.1500, X.1520, X.1521 và X.1570 là có sẵn khuyến nghị hoặc dự thảo. Một số khác sẽ làm trong tương lai, vì vậy nó được khuyến cáo rằng người sử dụng kiểm tra thông tin trang web của ITU-T sau này.

Thư mục tài liệu tham khảo

[1] ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity.

[2] ISO/IEC 12207:2008, Systems and software engineering – Software life cycle processes.

[3] ISO/IEC 19770-1, Information technology – Software asset management – Part 1: Processes and tiered assessment of conformance.

[4] ISO/IEC TR 19791, Information technology – Security techniques – Security assessment of operational systems.

[5] ISO/IEC 20000-1, Information technology – Service management – Part 1: Service management system requirements.

[6] ISO/IEC 27010, Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications.

[7] ISO/IEC 27031, Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity.

[8] ISO/IEC 27033, Information technology – Security techniques – Network security.

[9] ISO/IEC 27034, Information technology – Security techniques – Application security.

[10] ISO/IEC 27035, Information technology – Security techniques – Information security incident management.

[11] ISO/IEC 29147, Information technology – Security techniques – Vulnerability disclosure.

[12] TCVN 10295 ISO/IEC 27005, Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý rủi ro an toàn thông tin.

[13] TCVN 31000, Quản lý rủi ro – Nguyên tắc và hướng dẫn.

[14] TCVN 8709-1:2011, Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn công nghệ thông tin – Phần 1: Giới thiệu và mô hình chung.

[15] TCVN 9788:2013, Quản lý rủi ro – Từ vựng.

[16] TCVN ISO/IEC 27001, Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Các yêu cầu.

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