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.

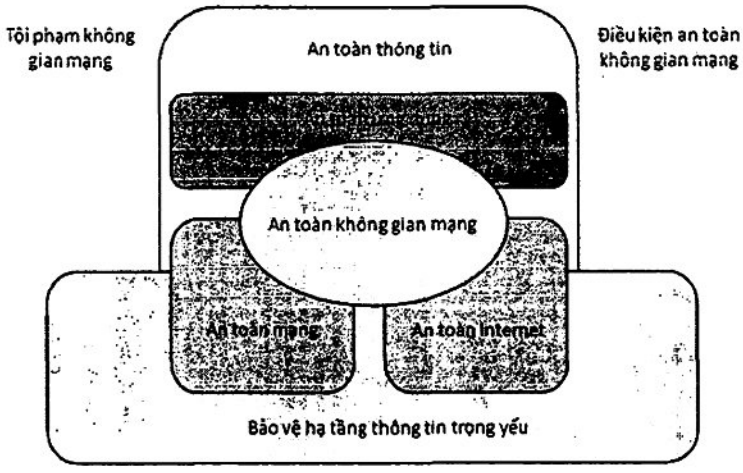
Tuy nhiên, an toàn không gian mạng không đồng nghĩa với an toàn Internet, an toàn mạng, an toàn ứng dụng, an toàn thông tin hoặc CIIP. Nó có một phạm vi duy nhất yêu cầu các bên liên quan đóng một vai trò tích cực để duy trì, cải thiện tính hữu ích và đáng tin cậy của không gian mạng. Tiêu chuẩn này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