BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỤC AN TOÀN THÔNG TIN

TÀI LIỆU HƯỚNG DẪN
ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN

Hà Nội – 2021

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT

Viết tắt	Viết đầy đủ	Nghĩa tiếng Việt
ATTT	An toàn thông tin	
ĐV	Đơn vị	
HT	Hệ thống	
HTTT	Hệ thống thông tin	
Events		Sự kiện
Threats		Mối đe dọa
Vulnerabilities		Lỗ hổng bảo mật

CHƯƠNG 1

PHẠM VI, ĐỐI TƯỢNG ÁP DỤNG

1.1. Phạm vi áp dụng

Tài liệu này đưa ra hướng dẫn đánh giá và quản lý rủi ro an toàn thông tin, bao gồm các nội dung liên quan đến xác định mức rủi ro, quy trình đánh giá và quản lý rủi ro, các biện pháp kiểm soát.

1.2. Đối tượng áp dụng

1. Cơ quan, tổ chức liên quan đến hoạt động đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong cơ quan, tổ chức nhà nước.

2. Khuyến khích cơ quan, tổ chức tham khảo, áp dụng tài liệu hướng dẫn này để tăng cường bảo đảm an toàn, an ninh mạng cho hệ thống thông tin thuộc phạm vi quản lý của mình.

1.3. Giải thích từ ngữ, định nghĩa

Trong hướng dẫn này, một số từ ngữ được hiểu như sau:

1. *Khả năng xảy ra (likelihood):* Khả năng xảy ra một sự kiện, có thể được định nghĩa, được đo lường hay được xác định một cách chủ quan hay khách quan, dưới dạng định tính hay định lượng và được mô tả bằng cách sử dụng thuật ngữ chung hoặc bằng toán học (như xác suất hoặc tần suất trong một khoảng thời gian nhất định).

2. *Rủi ro (risk):* Sự kết hợp giữa hậu quả của một sự kiện an toàn thông tin và khả năng xảy ra kèm theo. Rủi ro an toàn thông tin liên quan đến những vấn đề tiềm ẩn mà những mối đe dọa có thể khai thác những điểm yếu của một hoặc một nhóm tài sản thông tin và do đó gây ra thiệt hại đối với tổ chức.

3. *Đánh giá rủi ro (risk assessment):* Quy trình tổng thể bao gồm nhận biết rủi ro, phân tích rủi ro và ước lượng rủi ro.

4. *Quản lý rủi ro (risk management):* Quá trình nhận biết, kiểm soát và giảm thiểu hay loại bỏ rủi ro có thể gây ảnh hưởng đến hệ thống thông tin. Quản lý rủi ro bao gồm: đánh giá, xử lý và chấp nhận rủi ro.

5. *Xử lý rủi ro (risk treatment):* Quá trình điều chỉnh rủi ro. Xử lý rủi ro để giải quyết các hậu quả tiêu cực, có thể được thực hiện bằng một trong các phương án như giảm nhẹ rủi ro, loại bỏ rủi ro, ngăn chặn rủi ro và giảm bớt rủi ro.

6. *Mối đe dọa (Threat):* Nguyên nhân tiềm ẩn gây ra sự cố không mong muốn, kết quả là có thể gây thiệt hại cho một hệ thống hay tổ chức.

7. *Điểm yếu (Vulnerability):* Nhược điểm của một tài sản hay kiểm soát có khả năng bị khai thác bởi một hay nhiều mối đe dọa.

8. *Phân tích rủi ro (Risk analysis):* Quá trình đánh giá mối nguy (threats) và điểm yếu (Vulnerabilities) của tài sản thông tin.

1.4. Nguyên tắc quản lý rủi ro an toàn thông tin

Cơ quan, tổ chức khi thực hiện quản lý rủi ro an toàn thông tin cần dựa trên các nguyên tắc dưới đây:

a) Quản lý rủi ro phải được thực hiện thường xuyên, liên tục theo quy chế, chính sách quy trình bảo đảm an toàn thông tin của cơ quan, tổ chức.

b) Việc xử lý rủi ro cần được thực hiện trên cơ sở trọng tâm, trọng điểm, bảo đảm tính khả thi trên cơ sở cân đối giữa nguồn lực thực hiện và giá trị đem lại.

c) Tuân thủ nguyên tắc phân tán rủi ro thông qua các biện pháp phi tập trung, tránh, chuyển giao, giảm thiểu rủi ro.

1.5. Tiêu chuẩn tham chiếu

1. 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.

2. TCVN 10295:2014- Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý rủi ro ATTT.

3. ISO/IEC 27005:2011, Informatinon Technology Security Techniques Informatinon Security Risk management system.

4. NIST SP 800-30r1, Guide for Conducting Risk Assessments.

CHƯƠNG 2

HƯỚNG DẪN XÁC ĐỊNH MỨC RỦI RO AN TOÀN THÔNG TIN

Khi thực hiện đánh giá và quản lý rủi ro an toàn thông tin, cơ quan, tổ chức cần xây dựng một bức tranh đầy đủ về các rủi ro an toàn thông tin mà tổ chức có khả năng gặp phải, đánh giá sắp xếp mức độ ưu tiên và xây dựng hệ thống các biện pháp kiểm soát tổng thể, thống nhất và đầy đủ để giảm thiểu rủi ro.

Trong chương này, nội dung hướng dẫn tập trung vào việc xác định tài sản, các điểm yếu và mối đe dọa đối với mỗi tài sản để từ đó xác định hậu quả, mức ảnh hưởng đến cơ quan, tổ chức khi xảy ra rủi ro đối với tài sản đó, cụ thể như hướng dẫn dưới đây.

2.1. Nhận biết tài sản

Tài sản là vấn đề cần xem xét đầu tiên khi thực hiện quản lý rủi ro an toàn thông tin. Theo đó, cơ quan, tổ chức tổ chức cần xác định và thu thập thông tin đầy đủ về tài sản của mình đang quản lý, đặc biệt là các thông tin liên quan đến đặc điểm, nơi lưu trữ, mức độ quan trọng và giá trị, đặc thù của tài sản.

Mỗi tài sản sau khi được xác định, cần được đánh giá các nguy cơ, điểm yếu đối với tài sản đó, từ đó có thể đánh giá xem mỗi tài sản khi gặp rủi ro thì sẽ gây ra hậu quả, mức độ ảnh hưởng thế nào đối với cơ quan, tổ chức. Mức độ ảnh hưởng và khả năng xảy ra sự cố sẽ quyết định các mức rủi ro mà cơ quan, tổ chức cần phải xử lý.

Hướng dẫn này tập trung vào việc hướng dẫn 02 loại tài sản cần bảo vệ là thông tin và hệ thống thông tin. Trong đó, việc xác định tài sản thông tin và hệ thống thông tin, cơ quan, tổ chức cần chú ý như sau:

Coi thông tin là đơn vị tài sản thành phần của hệ thống thông tin, khi hệ thống thông tin được bảo vệ thì thông tin cũng được bảo vệ. Trường hợp, hệ thống có nhiều loại thông tin khác nhau, các thông tin có cùng mức độ quan trọng, có thể tồn tại những điểm yếu và mối đe dọa giống nhau thì có thể đưa vào thành một nhóm để thực hiện đánh giá và quản lý rủi ro.

Một hệ thống thông tin lớn có thể được chia thành nhiều hệ thống thông tin thành phần tương đối độc lập nhau về chức năng, mục đích sử dụng. Việc áp dụng biện pháp đánh giá và quản lý rủi ro được áp dụng cho từng hệ thống thành phần theo mức rủi ro xác định được.

Thông tin bao gồm nhưng không giới hạn các loại sau: Thông tin công khai, thông tin riêng, thông tin cá nhân và thông tin bí mật nhà nước. Thông tin bí mật

nhà nước được chia làm 03 mức: Mật, Tối Mật và Tuyệt Mật. Để xác định đầy đủ các tài sản thông tin có trong hệ thống, ta có thể xác định các loại thông tin có cùng loại ở trên. Ví dụ thông tin công khai bao gồm thông tin lịch họp, thông tin thông cáo báo trí…; thông tin riêng bao gồm thông tin về quy trình nghiệp vụ….

Hệ thống thông tin bao gồm nhưng không giới hạn các loại hình: Hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, tổ chức; Hệ thống thông tin phục vụ người dân, doanh nghiệp; Hệ thống cơ sở hạ tầng thông tin; Hệ thống thông tin Điều khiển công nghiệp. Việc xác định các hệ thống thông tin cụ thể được quy định tại Điều 4 Thông tư 03/2017/TT-BTTTT ngày 24/4/2017.

Để xác định được giá trị của tài sản, ta có thể dựa vào yêu cầu đối với các tính bí mật (C), tính nguyên vẹn (I) và tính sẵn sàng (A) của mỗi tài sản. Giá trị của tài sản sẽ được chia làm 05 mức theo thang điểm được tính từ tích của các giá trị C, I, A như ví dụ dưới đây:

- Đối với thuộc tính bí mật thì giá trị được xác định vào loại thông tin hoặc loại thông tin hệ thống đó xử lý. Ví dụ: thông tin công khai thang điểm 1; thông tin riêng, thông tin cá nhân thang điểm 2; thông tin Mật thang điểm 3; thông tin Tối Mật thang điểm 4; thông tin Tuyệt Mật thang điểm 5.

- Đối với thuộc tính nguyên vẹn thì giá trị được xác định vào yêu cầu đối với mức độ nguyên vẹn của thông tin hoặc loại thông tin mà hệ thống đó xử lý. Ví dụ: tính nguyên vẹn thấp thang điểm 1; tính nguyên vẹn trung bình thang điểm 2; tính nguyên vẹn cao thang điểm 3; tính nguyên vẹn rất cao điểm 4; tính nguyên vẹn tuyệt đối thang điểm 5.

- Đối với thuộc tính sẵn sàng thì giá trị được xác định vào yêu cầu đối với mức sẵn sàng của thông tin hoặc hệ thống thông tin đó. Ví dụ: tính sẵn sàng thấp thang điểm 1; tính tính sẵn sàng trung bình thang điểm 2; tính tính sẵn sàng cao thang điểm 3; tính tính sẵn sàng rất cao điểm 4; tính tính sẵn sàng tuyệt đối thang điểm 5.

Theo đó, giá trị tài sản sẽ được xác định theo giá trị của các thuộc tính C, A, I như sau:

Giá trị tài sản	Giá trị C+I+A
Thấp (1)	1-3
Trung bình (2)	4-6
Cao (3)	7-9
Rất cao (4)	10-12
Cực cao (5)	13-15

Bảng 1. Bảng giá trị tài sản

Căn cứ vào giá trị tài sản, ta có thể xác định loại tài sản nào là quan trọng cần ưu tiên bảo vệ. Căn cứ vào mỗi thuộc tính C, A, I của tài sản ta có thể xác định được những điểm yếu, mối đe dọa làm cơ sở để xác định hậu quả, mức ảnh hưởng tới cơ quan, tổ chức khi xảy ra rủi ro đối với tài sản đó.

Cơ quan, tổ chức có thể tham khảo ví dụ về danh mục tài sản và các giá trị tương ứng tại Phụ lục 3 Hướng dẫn này.

2.2. Điểm yếu

Điểm yếu có thể được hiểu là điểm mà có thể bị khai thác gây ra các mối đe dọa cho tài sản. Các điểm yếu có thể có nhiều tiêu chí xác định và được phân làm các nhóm khác nhau.

Để thuận tiện cho việc xác định các điểm yếu, trong hướng dẫn này các điểm yếu được phân nhưng không giới hạn các nhóm sau:

- Nhóm các điểm yếu liên quan đến tồn tại lỗ hổng, điểm yếu an toàn thông tin trong hệ thống;

- Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp quản lý: Không có quy định về sử dụng mật khẩu an toàn; không có quy định về lưu trữ có mã hóa, không có quy định về quy trình xử lý sự cố.v.v.

- Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp kỹ thuật: Không có biện pháp phòng chống xâm nhập, không có biện pháp phòng chống mã độc, không có biện pháp phòng chống tấn công.v.v.

Để xác định được các điểm yếu tồn tại trong hệ thống, cơ quan, tổ chức cần thực hiện kiểm tra, đánh giá an toàn thông tin để tìm ra các lỗ hổng, điểm yếu tồn tại trên hệ thống. Thực hiện rà soát quy chế, chính sách bảo đảm an toàn thông tin để tìm ra các điểm yếu từ việc chưa đáp ứng các biện pháp quản lý theo quy định. Thực hiện kiểm tra, đánh giá hiện trạng của hệ thống để xác định các điểm yếu

xuất phát từ việc chưa đáp ứng các biện pháp kỹ thuật theo quy định. Bên cạnh đó, từ kết quả đánh giá thực tế, cơ quan, tổ chức có thể xác định thêm các điểm yếu khác của hệ thống, ngoài các điểm yếu xuất phát từ yêu cầu đáp ứng các yêu cầu an toàn cơ bản theo quy định.

Cơ quan, tổ chức có thể tham khảo ví dụ về mối liên hệ giữa tài sản, mối đe dọa và điểm yếu tại Phụ lục 1, Phụ lục 3 Hướng dẫn này.

2.3. Mối đe dọa

Mối đe dọa được xác định khi mỗi điểm yếu có nguy cơ bị khai thác thì sẽ gây ra tác động gì đối với tài sản cần bảo vệ. Các mối đe dọa có thể xuất phát từ những lý do khách quan hay chủ quan, cũng có thể là do cố ý hoặc vô ý.

Một mối đe dọa có thể phát sinh từ bên trong hoặc bên ngoài tổ chức. Một số mối đe dọa có thể gây ảnh hưởng đồng thời lên nhiều tài sản và gây ra các tác động khác nhau tùy thuộc vào tài sản nào bị ảnh hưởng.

Như đã phân tích ở trên, các mối đe dọa có thể được xác định dựa vào các điểm yếu của thông tin, hệ thống thông tin. Do đó, việc xác định các mối đe dọa có thể dựa vào việc phân nhóm các điểm yếu ở mục 2.2.

Trên cơ sở đó, các mối đe dọa có thể được phân, nhưng không giới hạn các nhóm như sau: (1) Nhóm các mối đe dọa từ việc tồn tại, điểm yếu, lỗ hổng trong hệ thống; (2) Nhóm các mối đe dọa từ việc thiếu hoặc không đáp úng các biện pháp quản lý; (3) Nhóm các mối đe dọa từ việc thiếu hoặc không đáp úng các biện pháp kỹ thuật.

Cơ quan, tổ chức có thể tham khảo ví dụ về các mối đe dọa tại Phụ lục 2 Hướng dẫn này.

2.4. Đánh giá hậu quả

Hậu quả là được xác định khi mối đe dọa xảy ra với tài sản sẽ gây tổn hại thế nào đối với cơ quan, tổ chức. Mức ảnh hưởng (Impact) là giá trị được sử dụng để xác định giá trị định lượng của hậu quả.

Việc xác định mức ảnh hưởng có thể dựa vào đối tượng bị ảnh hưởng như: quyền và lợi ích hợp pháp của tổ chức, cá nhân, sản xuất, lợi ích công cộng và trật tự, an toàn xã hội quốc phòng, an ninh. Việc xác định mức ảnh hưởng có thể dựa vào phạm vi bị ảnh hưởng như: cấp quốc gia, cơ quan, tổ chức hay cá nhân.

Việc xác định hậu quả, mức ảnh hưởng có thể dựa vào các thuộc tính C, A, I đối với tài sản như sau:

Mức ảnh hưởng	Tính bảo mật (C)	Tính toàn vẹn (I)	Tính sẵn sàng (A)
Đặc biệt nghiêm trọng (5)	Việc bị lộ thông tin trái phép làm ảnh hưởng nghiêm trọng đến quốc phòng, an ninh	Việc sửa đổi hoặc phá hủy trái phép thông tin làm ảnh hưởng nghiêm trọng đến quốc phòng, an ninh	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm ảnh hưởng nghiêm trọng đến quốc phòng, an ninh
Nghiêm trọng (4)	Việc bị lộ thông tin trái phép làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia
Vừa phải (3)	Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia
Nhỏ (2)	Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng
Không đáng kể (1)	Việc bị lộ thông tin trái phép làm tổn hại tới quyền và lợi ích	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại tới quyền và lợi ích	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại tới quyền và

	hợp pháp của tổ chức, cá nhân	hợp pháp của tổ chức, cá nhân	lợi ích hợp pháp của tổ chức, cá nhân

Bảng 2. Bảng giá trị Mức ảnh hưởng

Chú ý, việc đưa ra các tiêu chí xác định hậu quả, mức ảnh hưởng là phụ thuộc vào mục tiêu, chiến lược, yêu cầu thực tế của mỗi của cơ quan, tổ chức.

2.5. Khả năng xảy ra sự cố

Khả năng xảy ra được xác định là xác suất cơ quan, tổ chức phải đối mặt với hậu quả. Việc xác định khả năng xảy ra sự cố có thể được xem xét dựa vào các yếu tố sau:

1. Điểm yếu và khả năng khai thác: Khả năng thu thập thông tin về điểm yếu và các mối đe dọa đối với tài sản; Khả năng khai thác điểm yếu của tài sản; Khả năng thực hiện tấn công lặp lại, duy trì, mở rộng tấn công.

2. Thông qua những sự cố đã ghi nhận trong quá khứ: Việc theo dõi, giám sát an toàn thông tin cho hệ thống, ta có thể xác định được tần suất thông tin bị lộ lọt, bị phá hủy, bị thay đổi, bị mã hóa đòi tiền chuộc; hệ thống thông tin bị tấn công làm ngừng hoạt động, bị chiếm quyền điều khiển, bị lợi dụng để tấn công các hệ thống thông tin khác, bị tấn công mã độc, bị tấn công từ chối dịch vụ.v.v.

3. Giả định về khả năng xảy ra: Việc xác định khả năng xảy ra cũng có thể dựa trên các giả định về mối đe dọa hoặc dữ liệu về mối đe dọa thực tế từ các nguồn thông tin công khai. Ví dụ: dữ liệu lịch sử về các cuộc tấn công mạng, các loại tấn công mạng, xu hướng tấn công mạng, tần suất tấn công, dữ liệu lịch sử về hành vi tội phạm mạng. Cơ quan, tổ chức có thể sử dụng dữ liệu thu thập được và thực hiện phân tích, thống kê để xác định xác suất xảy ra sự cố.

Khả năng xảy ra sự cố có thể được chia làm 05 mức cùng tiêu chí xác định như sau (tối thiểu 01 tiêu chí thỏa mãn sẽ xác định được khả năng xảy ra sự cố):

Khả năng xảy ra	**Tiêu chí xác định**
Chắc chắn (5)	(1) Khả năng khai thác: - Lỗ hổng có thể được thu thập từ các nguồn thông tin công khai; - Có thể thực hiện tấn công từ bên ngoài Internet mà không cần quyền truy cập vào hệ thống; có thể sử dụng các công cụ khai thác tự động được công khai trên mạng và không yêu cầu có trình độ về an toàn thông tin để thực hiện. - Có thể thực hiện tấn công lặp lại mà không cần thay đổi thiết lập và các điều kiện kỹ thuật sau lần tấn công đầu tiên.

	(2) Tần suất: Nhiều hơn 1 lần/tháng (3) Khả năng xảy ra: >90% (4) Cơ hội: Dự kiến, chắc chắn sẽ xảy ra trong hầu hết các trường hợp
Cao (4)	(1) Khả năng khai thác: - Lỗ hổng có thể được thu thập thông qua việc tương tác thụ động với hệ thống từ bên ngoài; - Việc thực hiện tấn công yêu cầu có quyền người dùng tối thiểu; có thể sử dụng các công cụ khai thác tự động được công khai trên mạng và yêu cầu có trình độ về an toàn thông tin cơ bản để thực hiện. - Có thể thực hiện tấn công lặp lại bằng cách thay đổi thiết lập và các điều kiện kỹ thuật cơ bản mà không cần nắm được quy luật thay đổi. (2) Tần suất: Nhiều hơn 1 lần/quý nhưng ít hơn 1 lần/tháng (3) Khả năng xảy ra: >60% (4) Cơ hội: Có khả năng xảy ra trong hầu hết các trường hợp
Trung bình (3)	(1) Khả năng khai thác: - Lỗ hổng có thể được thu thập thông qua việc sử dụng các công cụ dò quét từ bên ngoài; - Việc thực hiện tấn công yêu cầu có tài khoản đặc quyền; có thể sử dụng các công cụ khai thác tự động và yêu cầu có trình độ về an toàn thông tin để thực hiện. - Có thể thực hiện tấn công lặp lại và xác định được chắc chắn các tham số cần thiết lập để thực hiện tấn công lặp lại. (2) Tần suất: Có khả năng xảy ra một số lần (3) Khả năng xảy ra: >=10% (4) Cơ hội: Có khả năng xảy ra một số lần
Thấp (2)	(1) Khả năng khai thác: - Lỗ hổng có thể được thu thập thông qua việc sử dụng các công cụ dò quét trực tiếp từ bên trong hệ thống; - Việc thực hiện tấn công yêu cầu có tài khoản đặc quyền; yêu cầu sử dụng các công cụ khai thác chuyên dụng và yêu cầu có trình độ cao về an toàn thông tin để thực hiện. - Có thể thực hiện tấn công lặp lại bằng cách thay đổi thiết lập và các điều kiện kỹ thuật cơ bản nhưng yêu cầu nắm được quy luật thay đổi. (2) Tần suất: Ít hơn 1 lần/năm (3) Khả năng xảy ra: <10%

	(4) Cơ hội: Chỉ xảy ra trong một số trường hợp
Ít khi (1)	(1) Khả năng khai thác: - Lỗ hổng có thể được thu thập yêu cầu nắm được sâu về thiết kế, cấu trúc hệ thống, mã nguồn ứng dụng; - Việc thực hiện tấn công yêu cầu có tài khoản đặc quyền; yêu cầu sử dụng các công cụ khai thác chuyên dụng và yêu cầu có trình độ chuyên gia về an toàn thông tin để thực hiện; việc khai thác điểm yếu yêu cầu cần thực hiện lặp lại nhiều lần. - Có thể thực hiện tấn công lặp lại bằng cách thay đổi thiết lập và các điều kiện kỹ thuật nhưng yêu cầu nắm được quy luật thay đổi và các tham số yêu cầu mức độ ngẫu nhiên nhất định. (2) Tần suất: Nhiều hơn 1 lần/quý nhưng ít hơn 1 lần/tháng (3) Khả năng xảy ra: <5% (4) Cơ hội: Chỉ xảy ra trong một số trường hợp đặc biệt

Bảng 3. Ví dụ Bảng giá trị Khả năng xảy ra sự cố

2.6. Xác định mức rủi ro

Mức rủi ro chia thành 05 mức và được xác định dựa vào hai tham số giá trị tài sản, mức ảnh hưởng và khả năng xảy ra:

Mức rủi ro	**Giá trị tài sản+Mức ảnh hưởng+Khả năng xảy ra**
Thấp (1)	1-3
Trung bình (2)	4-6
Cao (3)	7-9
Rất cao (4)	10-12
Cực cao (5)	13-15

Bảng 3. Bảng giá trị Mức rủi ro

Căn cứ vào mức rủi ro, cơ quan, tổ chức xác định được tài sản, điểm yếu, mối đe dọa nào cần ưu tiên xử lý.

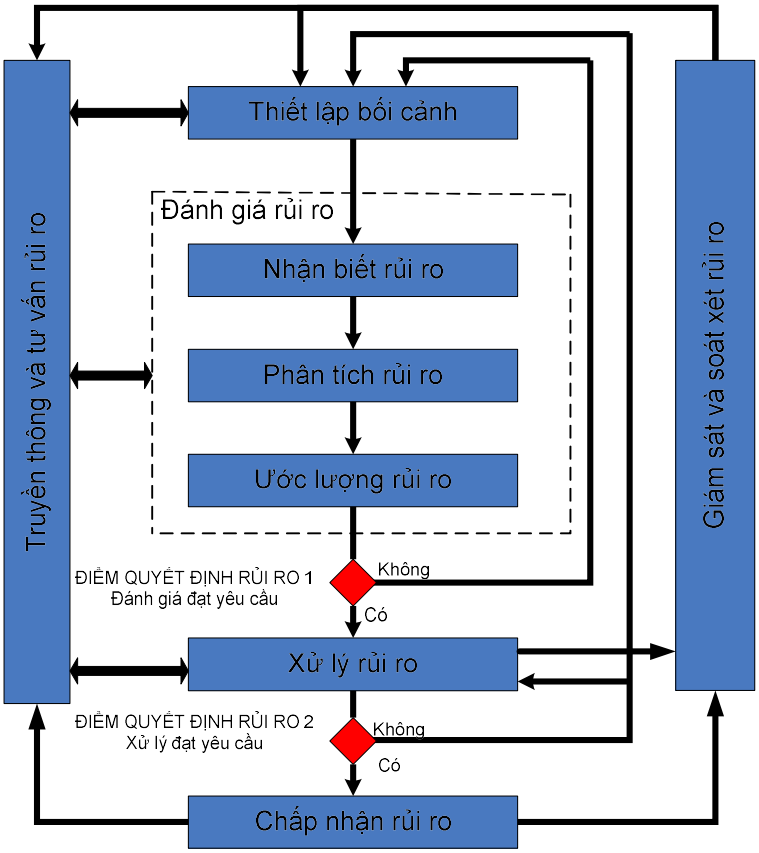
CHƯƠNG 3

QUY TRÌNH ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

Nội dung chương 2 tập trung hướng dẫn cơ quan, tổ chức việc xác định tài sản, điểm yếu, mối đe dọa liên quan đến tài sản để từ đó xác định được hậu quả và mức ảnh hưởng và khả năng xảy ra tương ứng.

Nội dung chương 3 tập trung hướng dẫn cơ quan, tổ chức việc xây dựng, lên phương án, kế hoạch và tổ chức triển khai quy trình đánh giá và quản lý rủi ro an toàn thông tin tổng thể, cụ thể như dưới đây.

3.1. Quy trình tổng quan về đánh giá và xử lý rủi ro



Về cơ bản, hoạt động đánh giá và quản lý rủi ro bao gồm các 04 bước: (1) Thiết lập bối cảnh; (2) Đánh giá rủi ro; (3) Xử lý rủi ro; (4) Chấp nhận rủi ro và 02 quá trình cần thực hiện song song: Truyền thông và tư vấn rủi ro, Giám sát và soát xét rủi ro. Cụ thể như sau:

a) Bước thiết lập bối cảnh, cơ quan, tổ chức cần đưa ra thông tin tổng quan, mục tiêu, quy mô, phạm vi và các thành phần của hệ thống cần bảo vệ.

b) Bước đánh giá rủi ro, cơ quan, tổ chức cần thực hiện nhận biết rủi ro, phân tích rủi ro và ước lượng rủi ro. Kết quả của việc thực hiện nội dung này là cần xác định tài sản, điểm yếu, mối đe dọa, hậu quả và mức ảnh hưởng đối với cơ quan, tổ chức khi rủi ro xảy ra đối với tài sản.

c) Bước xử lý rủi ro, cơ quan, tổ chức cần xác định các phương án xử lý rủi ro, bao gồm các biện pháp quản lý và kỹ thuật để có thể xử lý, giảm thiểu các mối đe dọa có thể xảy ra đối với tài sản, dẫn tới hậu quả cho cơ quan, tổ chức.

d) Bước xác định mức chấp nhận rủi ro, cơ quan, tổ chức cần xác định mức chấp nhận rủi ro và các rủi ro còn lại sau khi xử lý. Bởi vì có thể hệ thống tồn tại những rủi ro không có phương án xử lý triệt để mà chỉ có thể giảm thiểu.

đ) Quá trình truyền thông và tư vấn rủi ro là quá trình cơ quan, tổ chức cần trao đổi, tham vấn ý kiến của các bên liên quan để có thông tin đầu vào khi thực hiện các bước ở trên; thực hiện tuyên truyền, phổ biến các nguy cơ, rủi ro có thể xảy ra.

e) Quá trình giám sát và soát xét rủi ro, cơ quan, tổ chức giám sát và đánh giá tuân thủ, tính hiệu quả của việc thực hiện việc đánh giá và xử lý rủi ro.

Cụ thể các bước được trong quy trình đánh giá và xử lý rủi ro hướng dẫn chi tiết như dưới đây.

3.2. Thiết lập bối cảnh

3.2.1. Thông tin tổng quan về hệ thống thông tin

Bước này, cơ quan, tổ chức cần đưa ra thông tin tổng quan, mục tiêu, quy mô, phạm vi và các thành phần của hệ thống cần bảo vệ, bao gồm nhưng không giới hạn các thông tin sau:

1. Thông tin Chủ quản hệ thống thông tin

2. Thông tin Đơn vị vận hành

3. Chức năng, nhiệm vụ, cơ cấu tổ chức của đơn vị vận hành

4. Các cơ quan, tổ chức liên quan

5. Phạm vi, quy mô của hệ thống.

3.2.2. Tiêu chí chấp nhận rủi ro

Việc xử lý toàn bộ rủi ro được xác định là khó khả thi với bất kỳ cơ quan, tổ chức nào. Do đó, các rủi ro có thể xem xét giảm thiểu đến mức chấp nhận được.

Tiêu chí chấp nhận rủi ro phụ thuộc vào các chính sách, mục đích, mục tiêu bảo đảm an toàn thông tin của cơ quan, tổ chức và các lợi ích của các bên liên quan.

Mỗi tổ chức cần phải xác định mức chấp nhận rủi ro của riêng tổ chức mình. Việc xác định các tiêu chí chấp nhận rủi ro cần xem xét đến các yếu tố như: Nguồn lực để xử lý rủi ro so với hiệu quả mang lại sau khi rủi ro được xử lý; Khả năng xử lý rủi ro theo điều kiện thực tế của cơ quan, tổ chức của mình.v.v.

Tiêu chí chấp nhận rủi ro có thể bao gồm nhiều ngưỡng với các tiêu chí tương ứng, căn cứ theo mục tiêu bảo đảm an toàn thông tin mà tổ chức đưa ra. Hướng dẫn này đưa ra khuyến nghị về một số tiêu chí chấp nhận rủi ro như sau:

1. Hệ thống thông tin cấp độ cấp độ 5 không chấp nhận tồn tại rủi ro.

2. Hệ thống thông tin cấp độ 3 hoặc cấp độ 4, chỉ chấp nhận tồn tại các rủi ro ở mức thấp.

3. Hệ thống thông tin cấp độ 1 hoặc cấp độ 2, không chấp nhận tồn tại các rủi ro mức trung bình.

3.2.3. Phạm vi và giới hạn

Cơ quan, tổ chức cần xác định rõ phạm vi thực hiện đánh giá và quản lý rủi ro để bảo toàn bộ tài sản được bảo vệ trong quy trình thực hiện. Để xác định phạm vi, giới hạn, cơ quan, tổ chức cần xác định rõ thông tin liên quan (bao gồm nhưng không giới hạn) sau:

1. Phạm vi quản lý an toàn thông tin

a) Các mục tiêu bảo đảm an toàn thông tin của cơ quan, tổ chức

b) Các quy định pháp lý phải tuân thủ

c) Quy chế, chính sách bảo đảm an toàn thông tin của tổ chức.

2. Phạm vi kỹ thuật

a) Sơ đồ tổng thể (vật lý, logic) và các thành phần trong hệ thống (thiết bị mạng, bảo mật, máy chủ, thiết bị đầu cuối…).

b) Xác định các hệ thống thông tin khác có liên quan hoặc có kết nối đến hoặc có ảnh hưởng quan trọng tới hoạt động bình thường của hệ thống thông tin được đề xuất; trong đó, xác định rõ mức độ ảnh hưởng đến hệ thống thông tin đang được đề xuất cấp độ khi các hệ thống này bị mất an toàn thông tin;

c) Danh mục các nguy cơ tấn công mạng, mất an toàn thông tin đối với hệ thống và các ảnh hưởng.

3.2.4. Tổ chức thực hiện đánh giá và quản lý rủi ro

Cơ quan, tổ chức cần xây dựng phương án, kế hoạch thực hiện đánh giá và quản lý rủi ro an toàn thông tin. Nội dung phương án, kế hoạch, trách nhiệm của các đơn vị, bộ phận liên quan cần đưa vào quy chế bảo đảm an toàn thông tin của cơ quan, tổ chức để thực hiện.

Dưới đây là một số nội dung cần thực hiện (bao gồm nhưng không giới hạn) để tổ chức thực hiện đánh giá và quản lý rủi ro an toàn thông tin:

1. Phương án, kế hoạch thực hiện đánh giá và quản lý rủi ro.

2. Quy trình tổ chức thực hiện đánh giá và quản lý rủi ro.

3. Cơ chế phối hợp với các bên liên quan trong quá trình thực hiện.

4. Phương án, kế hoạch giám sát quy trình đánh giá và quản lý rủi ro.

Cơ quan, tổ chức có thể tham khảo nội dung hướng dẫn xác định các hậu quả tại mục 7 tiêu chuẩn TCVN 10295:2014.

3.3. Đánh giá rủi ro

3.3.1. Nhận biết rủi ro

Nhận biết rủi ro là các bước để xác định ra các rủi ro, hậu quả và mức thiệt hại tương ứng. Như đã hướng dẫn ở Chương 2 tại mục 2.1 đến 2.3, để xác định được rủi ro, cơ quan, tổ chức cần thực hiện các bước sau:

1. Nhận biết về tài sản để xác định danh mục các tài sản của cơ quan, tổ chức cần bảo vệ bao gồm thông tin, hệ thống thông tin.

2. Nhận biết về mối đe dọa để xác định các mối đe dọa đối với mỗi tài sản.

3. Nhận biết về điểm yếu để xác định các điểm yếu có thể tồn tại đối với mỗi tài sản.

Kết quả của bước nhận biết rủi ro là danh mục các mối đe dọa và điểm yếu đối với các tài sản được xác định.

3.3.2. Phân tích rủi ro

Phân tích rủi ro để xác định ra các mức ảnh hưởng, các hậu quả đối với cơ quan, tổ chức trên cơ sở thực hiện bước nhận biết rủi ro ở trên. Như đã hướng dẫn ở Chương 2 tại mục 2.4 và 2.5, để phân tích rủi ro, cơ quan, tổ chức cần thực hiện các bước sau:

1. Đánh giá các hậu quả để xác định mức ảnh hưởng đối với cơ quan, tổ chức khi tài sản bị khai thác điểm yếu gây ra các mối nguy.

2. Đánh giá khả năng xảy ra đối với từng loại sự cố.

Kết quả của bước phân tích rủi ro là xác định được các hậu quả, mức ảnh hưởng mà cơ quan, tổ chức phải xử lý.

3.3.3. Ước lượng rủi ro

Ước lượng rủi ro để xác định ra các rủi ro và mức rủi ro tương ứng mà cơ quan, tổ chức phải xử lý. Mức rủi ro được xác định dựa vào 02 tham số được xác định ở bước trên là mức ảnh hưởng và khả năng xảy ra sự cố (Như đã hướng dẫn ở Chương 2 tại mục 2.6).

3.4. Xử lý rủi ro

Cơ quan, tổ chức có thể lựa chọn các phương án xử lý rủi ro khác nhau để bảo đảm đạt được các mục tiêu bảo đảm an toàn thông tin của đơn vị mình. Việc thực hiện xử lý rủi ro có thể được thực hiện bởi một hoặc kết hợp nhiều phương án sau: thay đổi rủi ro, duy trì rủi ro, tránh rủi ro và chia sẻ rủi ro, cụ thể như dưới đây.

3.4.1. Thay đổi rủi ro

Thay đổi rủi ro là phương án thực hiện các biện pháp xử lý, khắc phục nhằm giảm mức rủi ro đã được xác định nhằm xác định các rủi ro tồn đọng được đánh giá lại ở mức chấp nhận được.

Để thực hiện phương án này, cơ quan, tổ chức cần xây dựng một hệ thống các biện pháp kiểm soát phù hợp. Các biện pháp được lựa chọn căn cứ vào các tiêu chí liên quan đến chi phí, đầu tư và thời gian triển khai, trên cơ sở cân đối giữa nguồn lực bỏ ra và lợi ích đem lại đối với tổ chức khi thực hiện xử lý rủi ro đó. Các biện pháp kiểm soát rủi ro được chia thành 02 nhóm quản lý và kỹ thuật, được hướng dẫn chi tiết tại Chương 4.

3.4.2. Duy trì rủi ro

Duy trì rủi ro là phương án chấp nhận rủi ro đã xác định mà không đưa ra các phương án xử lý để giảm thiểu rủi ro. Việc xác định rủi ro nào có thể được chấp nhận dựa vào mức rủi ro và tiêu chí chấp nhận rủi ro.

3.4.3. Tránh rủi ro

Tránh rủi ro là phương án xử lý khi cơ quan, tổ chức phải đối mặt với mức rủi ro quá cao bằng cách làm thay đổi, loại bỏ hoặc dừng hoạt động của hệ thống,

quy trình nghiệp vụ hoặc hoạt động của cơ quan, tổ chức để không phải phải đối mặt với rủi ro đã xác định. Tránh rủi ro là phương án thích hợp khi rủi ro được xác định vượt quá khả năng chấp nhận rủi ro của tổ chức.

3.4.4. Chia sẻ rủi ro

Chia sẻ rủi ro là phương án chuyển rủi ro, một phần rủi ro phải đối mặt cho cơ quan, tổ chức khác. Phương án chia sẻ rủi ro thường được thực hiện khi cơ quan, tổ chức xác định rằng việc giải quyết rủi ro yêu cầu chuyên môn hoặc nguồn lực được cung cấp tốt hơn bởi các tổ chức khác.

3.5. Chấp nhận rủi ro

Chấp nhận rủi ro là việc xem xét, đánh giá các rủi ro tồn đọng, chưa được xử lý hoàn toàn để đánh giá lại mức rủi ro sau xử lý có thể được chấp nhận hay không.

Rủi ro tồn đọng được chấp nhận khi mức rủi ro được xác định là thấp hơn mức rủi ro mà cơ quan, tổ chức có thể chấp nhận dựa vào tiêu chí chấp nhận rủi ro tại Mục 3.2.2.

3.6. Truyền thông và tư vấn rủi ro an toàn thông tin

Truyền thông và tư vấn rủi ro an toàn thông tin là hoạt động nhằm tuyên truyền nâng cao nhận thức cho các bên liên quan đến hoạt động đánh giá và quản lý rủi ro. Bên cạnh đó, việc này cũng nhằm đạt được sự thống nhất giữa các bên liên quan. Ví dụ trong trường hợp lựa chọn phương án chia sẻ rủi ro.

Cơ quan, tổ chức cần xây dựng kế hoạch truyền thông rủi ro định kỳ hoặc đột xuất. Hoạt động truyền thông rủi ro phải được thực hiện liên tục và thường xuyên.

Cơ quan, tổ chức có thể tham khảo nội dung hướng dẫn xác định các hậu quả tại mục 11 tiêu chuẩn TCVN 10295:2014.

3.7. Giám sát và soát xét rủi ro an toàn thông tin

Giám sát và soát xét rủi ro nhằm bảo đảm hoạt động đánh giá và quản lý rủi ro an toàn thông tin được thực hiện thường xuyên liên tục theo quy chế, chính sách bảo đảm an toàn thông tin của cơ quan, tổ chức.

3.7.1. Giám sát và soát xét các yếu tố rủi ro

Các rủi ro là không ổn định, các mối đe dọa, những điểm yếu, khả năng xảy ra hoặc những hậu quả có thể thay đổi mà không có bất kì dấu hiệu nào. Do đó, việc kiểm tra liên tục là cần thiết để phát hiện những thay đổi này.

Việc giám sát và soát xét các yếu tố rủi ro cần bảo đảm các yếu tố sau:

1. Quản lý được các tài sản mới, sự thay đổi của tài sản, giá trị của tài sản.

2. Sự thay đổi, xuất hiện mới các mối đe dọa

3. Sự thay đổi, xuất hiện mới các điểm yếu

4. Sự thay đổi, xuất hiện mới các rủi ro.

Kết quả của việc giám sát và soát xét các yếu tố rủi ro là việc cập nhật thường xuyên, liên tục sự thay đổi đối với các yếu tố rủi ro được đề cập ở trên.

3.7.2. Giám sát soát xét và cải tiến quản lý rủi ro

Để bảo đảm hoạt động đánh giá và quản lý rủi ro an toàn thông tin được mang lại hiệu quả, việc giám sát, soát xét và cải tiến quy trình quản lý rủi ro an toàn thông tin cần được thực hiện thường xuyên, liên tục.

Các tiêu chí được sử dụng để giám sát soát xét và cải tiến quản lý rủi ro có thể bao gồm, nhưng không giới hạn các yếu tố sau: Các yếu tố liên quan đến quy định pháp lý, Phương pháp tiếp cận đánh giá rủi ro, Các loại tài sản và giá trị tài sản, Tiêu chí tác động, Tiêu chí ước lượng rủi ro, Tiêu chí chấp nhận rủi ro; Các nguồn lực cần thiết...

Cơ quan, tổ chức có thể tham khảo nội dung hướng dẫn xác định các hậu quả tại mục 12 tiêu chuẩn TCVN 10295:2014.

CHƯƠNG 4

BIỆN PHÁP KIỂM SOÁT RỦI RO

4.1. Hướng dẫn chung

Theo quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, hệ thống thông tin phải đáp ứng các yêu cầu an toàn cơ bản, tối thiểu. Tuy nhiên, mỗi hệ thống thông tin khác nhau sẽ có sẽ có đặc thù riêng và yêu cầu mức độ an toàn khác nhau phù hợp với yêu cầu thực tế của mỗi cơ quan, tổ chức. Do đó, trên cơ sở đánh giá và quản lý rủi ro, cơ quan, tổ chức cần rà soát, bổ sung các yêu cầu an toàn (sau đây gọi là biện pháp kiểm soát rủi ro) cho phù hợp với yêu cầu thực tế. Khi triển khai các biện pháp kiểm soát rủi ro, trước hết cơ quan, tổ chức cần xem xét các biện pháp cần thiết đã có trong yêu cầu cơ bản hay chưa. Trường hợp, biện pháp kiểm soát đã nằm trong yêu cầu cơ bản thì cần thực hiện theo quy định. Trường hợp cần bổ sung các yêu cầu an toàn mới để đáp ứng yêu cầu thực tế thì cần đưa ra phương án cụ thể để thực hiện.

Các biện pháp kiểm soát cơ bản đối với hệ thống thông tin được quy định tại Điều 19 Nghị định 85/2016/NĐ-CP ngày 10/7/2016, Điều 8, 9 Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 và hướng dẫn chi tiết tại tiêu chuẩn quốc gia TCVN 11930:2017. Các yêu cầu an toàn được chia làm nhóm các yêu cầu về quản lý và các yêu cầu về kỹ thuật. Trong đó, các yêu cầu về kỹ thuật đưa ra các yêu cầu liên quan đến thiết kế, thiết lập, các biện pháp, giải pháp công nghệ đối với hệ thống trong quá trình xây dựng và thiết lập. Các yêu cầu về quản lý đưa ra chính sách, quy chế, quy trình, tổ chức bộ máy bảo đảm an toàn thông tin nhằm bảo đảm an toàn thông tin cho hệ thống thông tin trong quá trình vận hành, khai thác.

Các biện pháp kiểm soát đưa ra trong TCVN 11930:2017 được phân thành 05 mức theo cấp độ của hệ thống thông tin cần bảo vệ. Do đó, biện pháp kiểm soát rủi ro khi lựa chọn cần dựa vào mức rủi ro để xác định các biện pháp kiểm soát phù hợp trong TCVN 11930:2017 và các tiêu chuẩn khác liên quan. Ví dụ, mức ảnh hưởng được xác định là mức 5 thì biện pháp kiểm soát được lựa chọn sẽ là các biện pháp tương ứng với cấp độ 5 trong TCVN 11930:2017.

Các biện pháp bổ sung được xác định là các biện pháp được yêu cầu ở hệ thống thông tin ở cấp độ cao hơn. Ví dụ hệ thống thông tin được xác định là cấp độ 3, cần áp dụng các biện pháp kiểm soát yêu cầu với hệ thống thông tin cấp độ 4, thì các biện pháp này được coi là biện pháp bổ sung.

Bên cạnh đó, các biện pháp kiểm soát bổ sung, cơ quan, tổ chức có thể tham khảo từ hai bộ tiêu chuẩn ISP/IEC 27000 đối với các biện pháp về quản lý và SP800-53 đối với các biện pháp về kỹ thuật.

Các biện pháp kiểm soát kiểm soát cơ bản và bổ sung được hướng dẫn cụ thể như dưới đây.

4.2. Biện pháp kiểm soát về quản lý

4.2.1. Các yêu cầu an toàn cơ bản theo TCVN 11930

4.2.1.1. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

Đưa ra mục tiêu, nguyên tắc bảo đảm an toàn thông tin của tổ chức.

4.2.1.2. Trách nhiệm bảo đảm an toàn thông tin.

Đưa ra các quy định về trách nhiệm bảo đảm an toàn thông tin của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin.

4.2.1.3. Phạm vi chính sách an toàn thông tin

Đưa ra phạm vi chính sách, đối tượng áp dụng chính sách bảo đảm an toàn thông tin của tổ chức.

4.2.1.4. Tổ chức bảo đảm an toàn thông tin

Cung cấp thông tin về cơ cấu, tổ chức bảo đảm an toàn thông tin của tổ chức, bao gồm: Đơn vị chuyên trách về an toàn thông tin; Cơ chế, đầu mối phối hợp với cơ quan/tổ chức có thẩm quyền trong hoạt động bảo đảm an toàn thông tin.

4.2.1.5. Bảo đảm nguồn nhân lực

Đưa ra chính sách/quy trình thực hiện quản lý bảo đảm nguồn nhân lực an toàn thông tin của tổ chức, bao gồm: Tuyển dụng cán bộ; quy chế/quy định bảo đảm an toàn thông tin trong quá trình làm việc và chấm dứt hoặc thay đổi công việc.

4.2.1.6. Quản lý thiết kế, xây dựng hệ thống

Đưa ra chính sách/quy trình thực hiện quản lý thiết kế, xây dựng hệ thống của tổ chức, bao gồm: Thiết kế an toàn hệ thống thông tin; Phát triển phần mềm thuê khoán; Thử nghiệm và nghiệm thu hệ thống.

4.2.1.7. Quản lý vận hành hệ thống

a) Quản lý an toàn mạng: Đưa ra chính sách/quy trình thực hiện quản lý an toàn hạ tầng mạng của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường

của hệ thống; Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố; Truy cập và quản lý cấu hình hệ thống; Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

b) Quản lý an toàn máy chủ và ứng dụng: Đưa ra chính sách/quy trình thực hiện quản lý an toàn máy chủ và ứng dụng của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ; Truy cập mạng của máy chủ; Truy cập và quản trị máy chủ và ứng dụng; Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố; Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống; Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống; Cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

c) Quản lý an toàn dữ liệu: Đưa ra chính sách/quy trình thực hiện quản lý an toàn dữ liệu của tổ chức, bao gồm: Yêu cầu an toàn đối với phương pháp mã hóa; Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa; Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu; Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ; Sao lưu dự phòng và khôi phục dữ liệu; Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

d) Quản lý an toàn thiết bị đầu cuối: Đưa ra chính sách/quy trình thực hiện quản lý an toàn thiết bị đầu cuối của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường cho thiết bị đầu cuối; Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa; Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống; Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng; Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối.

đ) Quản lý phòng chống phần mềm độc hại: Đưa ra chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại của tổ chức, bao gồm: Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng; Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động; Thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Kiểm tra và xử lý phần mềm độc hại.

e) Quản lý giám sát an toàn hệ thống thông tin: Đưa ra chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống giám sát; Đối tượng giám sát bao gồm; Kết nối và gửi nhật ký hệ thống; Truy cập và quản trị hệ thống giám sát;

Loại thông tin cần được giám sát; Lưu trữ và bảo vệ thông tin giám sát; Theo dõi, giám sát và cảnh báo sự cố; Bố trí nguồn lực và tổ chức giám sát.

g) Quản lý điểm yếu an toàn thông tin: Đưa ra chính sách/quy trình thực hiện quản lý điểm yếu an toàn thông tin của tổ chức, bao gồm: Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin; Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; Phân nhóm và mức độ của điểm yếu; Cơ chế phối hợp với các nhóm chuyên gia; Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin trước khi đưa hệ thống vào sử dụng; Quy trình khôi phục lại hệ thống.

h) Quản lý sự cố an toàn thông tin: Đưa ra chính sách/quy trình thực hiện quản lý sự cố an toàn thông tin của tổ chức, bao gồm: Phân nhóm sự cố an toàn thông tin; Phương án tiếp nhận, phát hiện, phân loại và xử lý thông tin; Kế hoạch ứng phó sự cố an toàn thông tin; Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin; Quy trình ứng cứu sự cố an toàn thông tin thông thường; Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng; Cơ chế phối hợp trong việc xử lý, khắc phục sự cố an toàn thông tin; Diễn tập phương án xử lý sự cố an toàn thông tin.

i) Quản lý an toàn người sử dụng đầu cuối: Đưa ra chính sách/quy trình thực hiện quản lý an toàn người sử dụng đầu cuối của tổ chức, bao gồm: Quản lý truy cập, sử dụng tài nguyên nội bộ; Quản lý truy cập mạng và tài nguyên trên Internet; Cài đặt và sử dụng máy tính an toàn.

4.2.2. Các yêu cầu an toàn bổ sung

Cơ quan, tổ chức có thể tham khảo các biện pháp kiểm sát được đưa ra tại tiêu chuẩn TCVN ISO/IEC 27002:2020, bao gồm các biện pháp kiểm soát được chia thành 15 nhóm như sau: Chính sách an toàn thông tin; Tổ chức bảo đảm an toàn thông tin; An toàn nguồn nhân lực; Quản lý tài sản; Kiểm soát truy cập; Mật mã; An toàn vật lý và môi trường; An toàn vận hành; An toàn truyền thông; Tiếp nhận, phát triển và bảo trì hệ thống; Các mối quan hệ với nhà cung cấp; Quản lý sự cố an toàn thông tin; Các khía cạnh an toàn thông tin trong quản lý hoạt động nghiệp vụ liên tục; Soát xét về an toàn thông tin.

4.3. Biện pháp kiểm soát về kỹ thuật

4.3.1. Các yêu cầu an toàn cơ bản theo TCVN 11930

4.3.1.1. Bảo đảm an toàn mạng

a) Thiết kế hệ thống

- Đưa ra yêu cầu về thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng.

- Đưa ra yêu cầu về các biện pháp bảo vệ cụ thể bao gồm: Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn, Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, Phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng, Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu, Có phương án chặn lọc phần mềm độc hại trên môi trường mạng, Phương án phòng chống tấn công từ chối dịch vụ, Phương án giám sát hệ thống thông tin tập trung, Phương án giám sát an toàn hệ thống thông tin tập trung, Phương án quản lý sao lưu dự phòng tập trung, Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung, Phương án phòng, chống thất thoát dữ liệu, Phương án bảo đảm an toàn cho mạng không dây, Phương án quản lý tài khoản đặc quyền, Phương án dự phòng hệ thống ở vị trí địa lý khác nhau

b) Kiểm soát truy cập từ bên ngoài mạng: Đưa ra biện pháp quản lý truy cập từ các mạng bên ngoài theo chiều đi vào hệ thống tới các máy chủ dịch vụ bên trong mạng, bao gồm: Các dịch vụ/ứng dụng cho phép từ truy cập từ bên ngoài; Thời gian mất kết nối; Phân quyền truy cập; Giới hạn kết nối; Thiết lập chính sách ưu tiên. Phương án cần mô tả chính sách đó được thiết lập trên thiết bị hệ thống nào.

c) Kiểm soát truy cập từ bên trong mạng: Đưa ra biện pháp quản lý truy cập từ các máy tính/máy chủ bên trong mạng theo chiều đi ra các mạng bên ngoài và các mạng khác bên trong mạng, bao gồm: Các ứng dụng/dịch vụ nào được truy cập; Quản lý truy cập theo địa chỉ thiết bị; phương án ưu tiên truy cập. Phương án cần mô tả chính sách đó được thiết lập trên thiết bị hệ thống nào.

d) Nhật ký hệ thống: Đưa ra biện pháp quản lý nhật ký hệ thống (log) trên các thiết bị hệ thống về bật chức năng ghi log; thông tin ghi log; thời gian, dung lượng ghi log; quản lý log.

đ) Phòng chống xâm nhập: Đưa ra biện pháp triển khai/thiết lập cấu hình của thiết bị phòng, chống xâm nhập IDS/IPS hoặc chức năng IDS/IPS trên thiết bị tường lửa có trong hệ thống nhằm đáp ứng yêu cầu an toàn.

e) Phòng chống phần mềm độc hại trên môi trường mạng: Đưa ra biện pháp triển khai/thiết lập cấu hình của thiết bị để thực hiện chức năng phòng chống phần mềm độc hại trên môi trường mạng đáp ứng yêu cầu an toàn.

g) Bảo vệ thiết bị hệ thống: Đưa ra biện pháp triển khai/thiết lập cấu hình chức năng bảo mật trên các thiết bị có trong hệ thống nhằm bảo đảm bảo đảm an toàn cho thiết bị trong quá trình sử dụng và quản lý vận hành.

4.3.1.2. Bảo đảm an toàn máy chủ

a) Xác thực: Đưa ra biện pháp cấu hình/thiết lập chính sách xác thực trên máy chủ để bảo đảm việc xác thực khi đăng nhập vào máy chủ an toàn.

b) Kiểm soát truy cập: Đưa ra biện pháp cấu hình/thiết lập chính sách kiểm soát truy cập trên máy chủ để bảo đảm việc truy cập, sử dụng máy chủ an toàn sau khi đăng nhập thành công.

c) Nhật ký hệ thống: Đưa ra biện pháp quản lý nhật ký hệ thống (log) trên các máy chủ về: Bật chức năng ghi log; Thông tin ghi log; Thời gian, Dung lượng ghi log; Quản lý log.

d) Phòng chống xâm nhập: Đưa ra biện pháp cấu hình/thiết lập cấu hình bảo mật trên máy chủ để bảo bảo vệ tấn công xâm nhập từ bên ngoài.

đ) Phòng chống phần mềm độc hại: Đưa ra biện pháp cấu hình/thiết lập cấu hình bảo mật trên máy chủ về: Cài đặt phần mềm phòng chống mã độc; Dò quét mã độc; Xử lý mã độc; Quản lý tập trung phần mềm phòng chống mã độc...để phòng chống mã độc cho máy chủ.

e) Xử lý máy chủ khi chuyển giao: Đưa ra biện pháp xóa sạch dữ liệu; sao lưu dự phòng dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

4.3.1.3. Bảo đảm an toàn ứng dụng

a) Xác thực Đưa ra biện pháp cấu hình/thiết lập chính sách xác thực trên ứng dụng để bảo đảm việc xác thực khi đăng nhập vào máy chủ an toàn.

b) Kiểm soát truy cập: Đưa ra biện pháp cấu hình/thiết lập chính sách kiểm soát truy cập trên ứng dụng để bảo đảm việc truy cập, sử dụng ứng dụng an toàn sau khi đăng nhập thành công.

c) Nhật ký hệ thống: Đưa ra biện pháp quản lý nhật ký hệ thống (log) trên các ứng dụng về: Bật chức năng ghi log; Thông tin ghi log; Thời gian, dung lượng ghi log; Quản lý log.

d) Bảo mật thông tin liên lạc: Đưa ra biện pháp mã hóa và sử dụng giao thức mạng hoặc kênh kết nối mạng an toàn khi trao đổi dữ liệu qua môi trường mạng.

đ) Chống chối bỏ: Đưa ra biện pháp sử dụng và bảo vệ chữ ký số để bảo vệ tính bí mật và chống chối bỏ khi gửi/nhận thông tin quan trọng qua mạng.

e) An toàn ứng dụng và mã nguồn: Đưa ra biện pháp cấu hình/thiết lập chức năng bảo mật cho ứng dụng và phương án bảo vệ mã nguồn ứng dụng.

4.3.1.4. Bảo đảm an toàn dữ liệu

a) Nguyên vẹn dữ liệu: Đưa ra biện pháp lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính nguyên vẹn của dữ liệu.

b) Bảo mật dữ liệu: Đưa ra biện pháp lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính bí mật của dữ liệu.

c) Sao lưu dự phòng: Đưa ra biện pháp sao lưu dự phòng dữ liệu: Các thông tin yêu cầu sao lưu dự phòng; Phân loại dữ liệu sao lưu dự phòng; Hệ thống sao lưu dự phòng…

4.3.2. Các yêu cầu an toàn bổ sung

Cơ quan, tổ chức có thể tham khảo các tiêu chuẩn quốc tế dưới đây để xác định các biện pháp bổ sung, bao gồm nhưng không giới hạn các nhóm, tiêu chuẩn sau: Quản lý sự cố an toàn thông tin, Quản lý giám sát, Kiểm tra, đánh giá an toàn thông tin, Kỹ thuật an toàn mạng, Kỹ thuật an toàn máy chủ, Kỹ thuật an toàn thông tin cho ứng dụng, Kỹ thuật an toàn dữ liệu, Kỹ thuật an toàn thiết bị đầu cuối. Danh mục các tiêu chuẩn cụ thể tại Phụ lục 4 hướng dẫn này.

TÀI LIỆU THAM KHẢO

[1]. 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.

[2]. TCVN 10295:2014- Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý rủi ro ATTT.

[3]. Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 cuả Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

[4] ISO/IEC 15408:2017 Information technology — Security techniques — Evaluation criteria for IT security

[5] ISO/IEC 27001:2005, Information technology - Security techniques - lnformation security management systems - Requirements

[6]. ISO/IEC 27005:2011, Informatinon technology-Security techniques-Informatinon Security Risk management system.

[7]. NIST SP 800-30r1, Guide for Conducting Risk Assessments.

[8]. NIST SP 800-53R4, Security and Privacy Controls for Federal Information Systems and Organizations.

PHỤ LỤC 1. DANH MỤC CÁC ĐIỂM YẾU THAM KHẢO

Bảng danh mục các điểm yếu dưới đây được phân thành 03 nhóm: Các điểm yếu, lỗ hổng tồn tại trong sản phẩm, thiết bị sử dụng trong hệ thống; Điểm yếu từ các biện pháp quản lý; Điểm yếu từ các biện pháp kỹ thuật.

Để thuận tiện cho việc tham chiếu, các điểm yếu, lỗ hổng tồn tại trong sản phẩm, thiết bị sử dụng trong hệ thống được ký hiệu bắt đầu là chữ V. Ví dụ V01, V02 v.v. Điểm yếu từ các biện pháp quản lý được ký hiệu bắt đầu bằng chữ M. Ví dụ M01, M02 v.v. Điểm yếu từ các biện pháp kỹ thuật được ký hiệu bắt đầu bằng chữ T. Ví dụ T01, T02 v.v.

Danh mục các điểm yếu bao gồm nhưng không giới hạn các điểm yếu dưới đây:

STT	Điểm yếu	Kí hiệu
I	**Nhóm điểm yếu liên quan đến tồn tại lỗ hổng, điểm yếu an toàn thông tin**	
1.1	Tồn tại điểm yếu trên hệ điều hành máy chủ	V01
1.2	Tồn tại điểm yếu trên hệ điều hành máy trạm	V02
1.3	Tồn tại điểm yếu trên ứng dụng	V03
1.4	Tồn tại điểm yếu trên hệ quản trị cơ sở dữ liệu	V04
1.5	Tồn tại điểm yếu trên firmware thiết bị mạng, thiết bị bảo mật	V05
1.6	Tồn tại điểm yếu trên ứng dụng hệ thống (DNS, DHCP, SSO,..)	V06
1.7	Tồn tại điểm yếu của các giao thức mạng	V07
1.8	Tồn tại điểm yếu của các thư viện lập trình	V08
II	**Nhóm điểm yếu liên quan đến biện pháp quản lý**	
2.1	Không xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin.	M01
2.2	Không xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng liên quan	M02

2.3	Không xác định phạm vi của hệ thống thông tin cần quản lý	M03
2.4	Không xác định các ứng dụng, dịch vụ hệ thống cung cấp	M04
2.5	Không có chính sách, quy định về nguồn nhân lực bảo đảm an toàn thông tin	M05
2.6	Không có chính sách, quy định về quản lý an toàn mạng.	M06
2.7	Không có chính sách, quy định về an toàn máy chủ và ứng dụng	M07
2.8	Không có chính sách, quy định về an toàn dữ liệu	M08
2.9	Không có chính sách, quy định về an toàn thiết bị đầu cuối	M09
2.10	Không có chính sách, quy định về phòng chống phần mềm độc hại	M10
2.11	Không có chính sách, quy định về quản lý điểm yếu an toàn thông tin	M11
2.12	Không có chính sách, quy định về quản lý giám sát an toàn hệ thống thông tin	M12
2.13	Không có chính sách, quy định về quản lý sự cố an toàn thông tin	M13
2.14	Không có chính sách, quy định về quản lý an toàn người sử dụng đầu cuối	M14
2.15	Không có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng	M19
2.16	Không có chính sách, quy định về tổ chức đào tạo về an toàn thông tin cho người sử dụng	M20
2.17	Không có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc	M21
2.18	Không có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin	M22
2.19	Không có chính sách, quy định về kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng	M23

2.20	Không có chính sách, quy định về kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng	M24
2.21	Không có chính sách, quy định về thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng	M25
2.22	Không có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống	M26
2.23	Không có chính sách, quy định về quản lý, vận hành hoạt động bình thường của hệ thống	M27
2.24	Không có chính sách, quy định về cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố	M28
2.25	Không có chính sách, quy định về truy cập và quản lý cấu hình hệ thống	M29
2.26	Không có yêu cầu an toàn đối với phương pháp mã hóa	M30
2.27	Không có chính sách, quy định về phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa	M31
2.28	Không có chính sách, quy định về kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa	M32
2.45	Không có chính sách, quy định về cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống	M33
2.29	Không có chính sách, quy định về cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng	M34
2.30	Không có chính sách, quy định về gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động	M35
2.31	Không có chính sách, quy định về thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống	M36
2.32	Không có quy định truy cập và quản trị hệ thống giám sát	M37
III	**Nhóm các điểm yếu liên quan đến biên pháp kỹ thuật**	
3.1	Không có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	T01
3.2	Không có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	T02

3.3	Không có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng	T03
3.4	Không có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	T04
3.5	Không có phương án chặn lọc phần mềm độc hại trên môi trường mạng	T05
3.6	Không có phương án phòng chống tấn công từ chối dịch vụ	T06
3.7	Không có phương án giám sát hệ thống thông tin tập trung	T07
3.8	Không có phương án giám sát an toàn hệ thống thông tin tập trung	T08
3.9	Không có phương án quản lý sao lưu dự phòng tập trung	T09
3.10	Không có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung	T10
3.11	Không có phương án phòng, chống thất thoát dữ liệu	T11
3.12	Không có phương án dự phòng kết nối mạng Internet	T12
3.13	Không có phương án bảo đảm an toàn cho mạng không dây	T13
3.14	Không có phương án quản lý tài khoản đặc quyền	T14
3.15	Không có phương án dự phòng hệ thống ở vị trí địa lý khác nhau	T15
3.16	Không có phương án dự phòng cho kết nối mạng giữa hệ thống chính và hệ thống dự phòng	T16
3.18	Không có biện pháp kiểm soát truy cập từ bên ngoài vào hệ thống	T18
3.19	Không phân quyền và cấp quyền truy cập từ bên ngoài vào hệ thống	T19
3.20	Không có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ	T20
3.21	Không lưu trữ và quản lý tập trung nhật ký hệ thống thu thập được từ các thiết bị hệ thống;	T21

3.22	Không có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống.	T23
3.24	Hệ thống không có phương án cân bằng tải và dự phòng nóng	T24
3.25	Không thiết lập cấu hình để vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định;	T25
3.26	Không thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối đến hệ thống	T26
3.25	Không thay đổi cổng quản trị mặc định của máy chủ	T25
3.26	Không sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ	T26
3.27	Không có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ.	T27
3.51	Không thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng.	T51
3.28	Không có biện pháp quản lý tập trung việc cập nhật và xử lý bản vá, điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ.	T28
3.29	Không thực hiện cấu hình tối ưu, tăng cường bảo mật cho máy chủ trước khi đưa vào sử dụng.	T29
3.30	Không có biện pháp phòng chống xâm nhập trên máy chủ và kiểm tra tính nguyên vẹn của các tập tin hệ thống	T30
3.31	Không có phương án kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt	T31
3.32	Không có cơ chế kiểm tra, xử lý mã độc của các phương tiện lưu trữ di động trước khi kết nối với máy chủ.	T32
3.33	Không có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF.	T33
3.34	Không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng	T34
3.35	Không có phương án chuyên dụng để quản lý, lưu trữ dữ liệu trong hệ thống bảo đảm tính nguyên vẹn.	T35

3.36	Không có phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu lưu trên hệ thống lưu trữ/phương tiện lưu trữ.	T36
3.37	Không có phương án khôi phục tính nguyên vẹn của thông tin dữ liệu.	T37
3.38	Không có hệ thống/phương tiện lưu trữ độc lập để sao lưu dự phòng.	T38

PHỤ LỤC 2. DANH MỤC CÁC MỐI ĐE DỌA THAM KHẢO

Bảng danh mục các mối đe dọa dưới đây được phân thành 03 nhóm: (1) Nhóm các mối đe dọa từ việc tồn tại, điểm yếu, lỗ hổng trong hệ thống; (2) Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp quản lý; (3) Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp kỹ thuật.

Để thuận tiện cho việc tham chiếu, các mối đe dọa trong quá trình thực hiện đánh giá và quản lý rủi ro, nhóm các mối đe dọa từ việc tồn tại, điểm yếu, lỗ hổng trong hệ thống được ký hiệu bắt đầu là Th-V. Ví dụ Th-V01, Th-V02..v.v. Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp quản lý được ký hiệu bắt đầu bằng Th-M. Ví dụ Th-M01, Th-M02.v.v. Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp kỹ thuật được ký hiệu bắt đầu bằng chữ Th-T. Ví dụ Th-T01, Th-T02.v.v.

Danh mục các mối đe dọa bao gồm nhưng không giới hạn các mối đe dọa dưới đây:

STT	Mô tả	Ký hiệu
I	**Nhóm các mối đe dọa từ việc tồn tại, điểm yếu, lỗ hổng trong hệ thống**	
1.1	Thiết bị hệ thống tấn công truy cập trái phép, chiếm quyền điều khiển	Th-V01
1.2	Máy chủ hệ thống bị truy cập trái phép, chiếm quyền điều khiển	Th-V02
1.3	Ứng dụng, dịch vụ bị truy cập trái phép, chiếm quyền điều khiển	Th-V03
1.3	Dữ liệu trên máy chủ bị bị truy cập, sửa, xóa trái phép	Th-V04
1.4	Dữ liệu trên ứng dụng/dịch vụ bị truy cập, sửa, xóa trái phép	Th-V05
II	**Nhóm các mối đe dọa từ việc thiếu/không đáp ứng các biện pháp quản lý**	
2.1	Ban Lãnh đạo không nhận thức đúng về tầm quan trọng của bảo đảm an toàn thông tin cho hệ thống	Th-M01
2.2	Thiếu nguồn lực để triển khai các biện pháp bảo vệ cho hệ thống	Th-M02

2.3	Người sử dụng không có kỹ năng cơ bản để tự bảo vệ khi sử dụng mạng	Th-M03
2.4	Người sử dụng nhận thức hạn chế về các nguy cơ, rủi ro mất an toàn thông tin	Th-M04
2.5	Chính sách, quy định về quản lý an toàn mạng không được tuân thủ theo quy định	Th-M05
2.6	Chính sách, quy định về an toàn máy chủ và ứng dụng không được tuân thủ theo quy định	Th-M06
2.7	Chính sách, quy định về an toàn dữ liệu không được tuân thủ theo quy định	Th-M07
2.8	Chính sách, quy định về an toàn thiết bị đầu cuối không được tuân thủ theo quy định	Th-M08
2.9	Chính sách, quy định về phòng chống phần mềm độc hại không được tuân thủ theo quy định	Th-M09
2.10	Chính sách, quy định về quản lý điểm yếu an toàn thông tin không được tuân thủ theo quy định	Th-M10
2.11	Chính sách, quy định về quản lý giám sát an toàn hệ thống thông tin không được tuân thủ theo quy định	Th-M11
2.12	Chính sách, quy định về quản lý sự cố an toàn thông tin không được tuân thủ theo quy định	Th-M12
2.13	Chính sách, quy định về quản lý an toàn người sử dụng đầu cuối không được tuân thủ theo quy định	Th-M13
III	**Nhóm các mối đe dọa từ việc thiếu/không đáp ứng các biện pháp kỹ thuật**	
3.1	Hệ thống bị tấn công, chiếm quyền điều khiển từ xa	Th-T01
3.2	Hệ thống hoạt động không ổn định, thường xuyên bị gián đoạn hoạt động	Th-T02
3.3	Hệ thống bị lợi dụng, tấn công các hệ thống thông tin khác	Th-T05
3.4	Hệ thống bị truy cập, xóa, sửa thông tin trái phép	Th-T06

PHỤ LỤC 3. HƯỚNG DẪN ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO CHO HỆ THỐNG THÔNG TIN CỤ THỂ

1. Xác định tài sản

Ví dụ về xác định tài sản dưới đây hướng dẫn xác định tài sản dựa vào loại hình hệ thống thông tin là loại thông tin mà hệ thống đó xử lý. Một hệ thống thông tin của cơ quan, tổ chức có thể bao gồm nhiều loại hình hệ thống khác nhau. Trường hợp này, các hệ thống thông tin có thể được coi là hệ thống thông tin thành phần trong hệ thống thông tin tổng thể. Mỗi hệ thống thành phần được đánh giá và quản lý rủi ro theo tài sản được xác định.

Trường hợp hệ thống thông tin xử lý nhiều loại thông tin khác nhau thì việc xác định các giá trị C, I , A có thể dựa vào giá trị của loại thông tin quan trọng nhất, như dưới đây:

STT	Tên tài sản		C	I	A	C+I+A	Giá trị tài sản
	Hệ thống thông tin	Thông tin hệ thống xử lý					
1	Cổng thông tin nội bộ cấp độ 1	Thông tin công khai	1	2	3	6	2
2	Hệ thống quản lý văn bản và điều hành cấp độ 2	Thông tin riêng của cơ quan, tổ chức	2	3	3	8	3
3	Hệ thống cung cấp thông tin và dịch vụ công trực tuyến cấp độ 3	- Thông tin công khai - Thông tin riêng của tổ chức, cá nhân	2	3	3	8	3
4	Hệ thống thông tin quốc gia phục vụ phát triển Chính phủ điện tử cấp độ 4	- Thông tin công khai - Thông tin riêng của tổ chức, cá nhân	3	3	4	10	4
5	Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia	Thông tin bí mật nhà nước.	5	5	4	14	5

2. Xác định Điểm yếu và Mối đe dọa

Ví dụ về xác định tài sản dưới đây hướng dẫn xác định Điểm yếu, Mối đe dọa đối với từng tài sản được xác định ở bước trên. Việc xác định Điểm yếu và Mối đe dọa ở bước này là cơ sở để xác định khả năng xảy ra cũng như các biện pháp kiểm soát ở các bước tiếp theo.

TT	Tên tài sản	Điểm yếu	Mối đe dọa
1	Cổng thông tin nội bộ cấp độ 1	V01: Tồn tại điểu yếu trên hệ điều hành máy chủ	Th-V02: Máy chủ hệ thống bị truy cập trái phép, chiếm quyền điều khiển
		M02: Không có chính sách, quy định về quản lý an toàn mạng	Th-M05: Chính sách, quy định về quản lý an toàn mạng không được tuân thủ theo quy định
		T06: Không có phương án phòng chống tấn công từ chối dịch vụ	Th-T02: Hệ thống hoạt động không ổn định, thường xuyên bị gián đoạn hoạt động
2	Hệ thống quản lý văn bản và điều hành cấp độ 2	V03: Tồn tại điểu yếu trên ứng dụng	Th-V03: Ứng dụng, dịch vụ bị truy cập trái phép, chiếm quyền điều khiển
		M07: Không có chính sách, quy định về an toàn máy chủ và ứng dụng	Th-M06: Chính sách, quy định về an toàn máy chủ và ứng dụng không được tuân thủ theo quy định
		T02: Không có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Th-T01: Hệ thống bị tấn công, chiếm quyền điều khiển từ xa
3	Hệ thống cung cấp thông tin và dịch vụ công trực tuyến cấp độ 3	V02: Tồn tại điểu yếu trên hệ điều hành máy chủ	Th-V02: Máy chủ hệ thống bị truy cập trái phép, chiếm quyền điều khiển
		M11: Không có chính sách, quy định về quản lý điểm yếu an toàn thông tin	Th-M10: Chính sách, quy định về quản lý điểm yếu an toàn thông tin không được tuân thủ theo quy định
		T03: Không có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng	Th-T02: Hệ thống hoạt động không ổn định, thường xuyên bị gián đoạn hoạt động
4	Hệ thống thông tin quốc gia	V03: Tồn tại điểu yếu trên ứng dụng	Th-V03: Ứng dụng, dịch vụ bị truy cập trái phép, chiếm quyền điều khiển

	phục vụ phát triển Chính phủ điện tử cấp độ 4	M24: Không có chính sách, quy định về kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng	Th-M10: Chính sách, quy định về quản lý điểm yếu an toàn thông tin không được tuân thủ theo quy định
		T07: Không có phương án giám sát hệ thống thông tin tập trung	Th-T02: Hệ thống hoạt động không ổn định, thường xuyên bị gián đoạn hoạt động
5	Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia	V04: Tồn tại điểu yếu trên hệ quản trị cơ sở dữ liệu	Th-V05: Dữ liệu trên ứng dụng/dịch vụ bị truy cập, sửa, xóa trái phép
		M08: Không có chính sách, quy định về an toàn dữ liệu	Th-M07: Chính sách, quy định về an toàn dữ liệu không được tuân thủ theo quy định
		T11:Không có phương án phòng, chống thất thoát dữ liệu	Th-T06: Hệ thống bị truy cập, xóa, sửa thông tin trái phép

3. Xác định Mức ảnh hưởng

Như đã hướng dẫn tại mục 2.4, mức ảnh hưởng đối với danh sách tài sản được xác định như Bảng dưới đây.

TT	Tên tài sản	Điểm yếu	Mối đe dọa	Mức ảnh hưởng
1	Cổng thông tin nội bộ cấp độ 1	V01	Th-V02	Không đáng kể (1)
		M02	Th-M05	
		T06	Th-T02	
2	Hệ thống quản lý văn bản và điều hành cấp độ 2	V03	Th-V03	Nhỏ (2)
		M07	Th-M06	
		T02	Th-T01	
3	Hệ thống cung cấp thông tin và dịch vụ công trực tuyến cấp độ 3	V02	Th-V02	Vừa phải (3)
		M11	Th-M10	
		T03	Th-T02	
4	Hệ thống thông tin quốc gia phục vụ phát triển Chính phủ điện tử cấp độ 4	V03	Th-V03	Nghiêm trọng (4)
		M24	Th-M10	
		T07	Th-T02	
5	Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia	V04	Th-V05	Đặc biệt nghiêm trọng (5)
		M08	Th-M07	
		T11	Th-T06	

4. Xác định khả năng xảy ra

Như đã hướng dẫn tại mục 2.5, việc xác định khả năng xảy ra sự cố cần dựa vào khả năng điểm yếu bị khai thác trên cơ sở xác định các tiêu chí: Khả năng khai thác, Tần suất, Khả năng xảy ra và Cơ hội. Trên cơ sở đó, khả năng xảy ra đối với danh sách tài sản được xác định như Bảng dưới đây.

TT	Tên tài sản	Điểm yếu	Mối đe dọa	Khả năng xảy ra
1	Cổng thông tin nội bộ cấp độ 1	V01	Th-V02	Trung bình (3)
		M02	Th-M05	Trung bình (3)
		T06	Th-T02	Thấp (2)
2	Hệ thống quản lý văn bản và điều hành cấp độ 2	V03	Th-V03	Cao (4)
		M07	Th-M06	Cao (4)
		T02	Th-T01	Trung bình (3)
3		V02	Th-V02	Trung bình (3)

	Hệ thống cung cấp thông tin và dịch vụ công trực tuyến cấp độ 3	M11	Th-M10	Trung bình (3)
		T03	Th-T02	Cao (4)
4	Hệ thống thông tin quốc gia phục vụ phát triển Chính phủ điện tử cấp độ 4	V03	Th-V03	Cao (4)
		M24	Th-M10	Cao (4)
		T07	Th-T02	Trung bình (3)
5	Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia	V04	Th-V05	Trung bình (3)
		M08	Th-M07	Cao (4)
		T11	Th-T06	Trung bình (3)

5. Xác định mức rủi ro

Như đã hướng dẫn tại mục 2.6, việc xác định khả năng xảy ra sự cố cần dựa Giá trị tái sản, Mức ảnh hưởng, Khả năng xảy ra. Trên cơ sở đó, Mức rủi ro đối với danh sách tài sản được xác định như Bảng dưới đây.

TT	Tên tài sản	Điểm yếu	Giá trị tài sản	Khả năng xảy ra	Mức ảnh hưởng	Mức rủi ro
1	Cổng thông tin nội bộ cấp độ 1	V01	2	3	1	Trung bình (2)
		M02	2	3	1	Trung bình (2)
		T06	2	2	1	Trung bình (2)
2	Hệ thống quản lý văn bản và điều hành cấp độ 2	V03	3	4	2	Cao (3)
		M07	3	4	2	Cao (3)
		T02	3	3	2	Cao (3)
3	Hệ thống cung cấp thông tin và dịch vụ công trực tuyến cấp độ 3	V02	3	3	3	Cao (3)
		M11	3	3	3	Cao (3)
		T03	3	4	3	Rất cao (4)
4	Hệ thống thông tin quốc gia phục vụ phát triển Chính phủ điện tử cấp độ 4	V03	4	4	4	Rất cao (4)
		M24	4	4	4	Rất cao (4)
		T07	4	3	4	Rất cao (5)
5	Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia	V04	5	3	5	Cực cao (5)
		M08	5	4	5	Cực cao (5)
		T11	5	3	5	Cực cao (5)

6. Xác định biện pháp xử lý rủi ro và biện pháp kiểm soát

Như đã hướng dẫn tại Chương 3, việc xác định các biện pháp kiểm soát, trước hết cần dựa vào việc lựa chọn biện pháp xử lý rủi ro. Các biện pháp kiểm soát chỉ được đưa ra khi lựa chọn biện pháp xử lý rủi ro là thay đổi rủi ro. Trường hợp việc

lựa chọn các biện pháp kiểm soát cần nguồn lực bỏ ra lớn hơn lợi ích mang lại thì biện pháp xử lý rủi ro nên được lựa chọn là chập nhận rủi ro. Bảng dưới đây là ví dụ về việc lựa chọn biện pháp xử lý rủi ro và biện pháp kiểm soát tương ứng.

TT	Tên tài sản	Điểm yếu	Mối đe dọa	Mức rủi ro	Biện pháp xử lý rủi ro	Biện pháp kiểm soát
1	Cổng thông tin nội bộ cấp độ 1	V01	Th-V02	Trung bình (2)	Chấp nhận rủi ro	N/A
		M02	Th-M05	Trung bình (2)	Chấp nhận rủi ro	N/A
		T06	Th-T02	Trung bình (2)	Chấp nhận rủi ro	N/A
2	Hệ thống quản lý văn bản và điều hành cấp độ 2	V03	Th-V03	Cao (3)	Thay đổi rủi ro	TCVN 11930: 7.2.2.4 Phòng chống xâm nhập
		M07	Th-M06	Cao (3)	Thay đổi rủi ro	TCVN 11930: 7.1.5.7 Quản lý điểm yếu an toàn thông tin
		T02	Th-T01	Cao (3)	Thay đổi rủi ro	TCVN 11930: 7.2.1.5 Phòng chống xâm nhập
3	Hệ thống cung cấp thông tin và dịch vụ công trực tuyến cấp độ 3	V02	Th-V02	Cao (3)	Thay đổi rủi ro	TCVN 11930: 8.2.2.4 Phòng chống xâm nhập
		M11	Th-M10	Cao (3)	Thay đổi rủi ro	TCVN 11930: 8.1.5.7 Quản lý điểm yếu an toàn thông tin
		T03	Th-T02	Rất cao (4)	Thay đổi rủi ro	TCVN 11930: 8.2.1.1 Thiết kế hệ thống.b (Phương án cân bằng tải, dự phòng nóng)
4	Hệ thống thông tin quốc gia phục vụ phát	V03	Th-V03	Rất cao (4)	Thay đổi rủi ro	TCVN 11930: 8.2.2.4 Phòng chống xâm nhập

	triển Chính phủ điện tử cấp độ 4	M24	Th-M10	Rất cao (4)	Thay đổi rủi ro	TCVN 11930: 8.1.5.7 Quản lý điểm yếu an toàn thông tin
		T07	Th-T02	Rất cao (5)	Thay đổi rủi ro	TCVN 11930: 8.2.1.1 Thiết kế hệ thống.b (Phương án giám sát hệ thống thông tin tập trung)
5	Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia	V04	Th-V05	Cực cao (5)	Thay đổi rủi ro	TCVN 11930: 9.2.2.3 Phòng chống xâm nhập; 9.2.4.2 Bảo mật dữ liệu
		M08	Th-M07	Cực cao (5)	Thay đổi rủi ro	TCVN 11930: 9.1.5.3 Quản lý an toàn dữ liệu
		T11	Th-T06	Cực cao (5)	Thay đổi rủi ro	TCVN 11930: 9.2.1.1 Thiết kế hệ thống.b (Phương án phòng, chống thất thoát dữ liệu)

PHỤ LỤC 4. CÁC YÊU CẦU AN TOÀN BỔ SUNG

Cơ quan, tổ chức có thể tham khảo các tiêu chuẩn quốc tế dưới đây để xác định các biện pháp bổ sung, bao gồm nhưng không giới hạn các nhóm, tiêu chuẩn sau:

1. Quản lý sự cố an toàn thông tin

a) ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management.

TCVN 11239:2015 Công nghệ thông tin - Các kỹ thuật an toàn- Quản lý sự cố an toàn thông tin.

b) ISO/IEC 27037:2019 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.

Công nghệ thông tin - Các kỹ thuật an toàn – Hướng dẫn xác định, thu thập và lưu giữ bằng chứng số.

c) ISO/IEC 27041:2019 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method.

Công nghệ thông tin - Các kỹ thuật an toàn – Các yêu cầu bảo đảm với điều tra sự cố.

d) ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence.

Công nghệ thông tin - Các kỹ thuật an toàn – Hướng dẫn phân tích chứng cứ số.

đ) ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes.

Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn nguyên tắc và quy trình điều tra sự cố.

e) NIST SP 800-61 Computer Security Incident Handling Guide.

Công nghệ thông tin - Các kỹ thuật an toàn – Hướng dẫn quản lý sự cố máy tính.

g) NIST SP 800-40 Guide to Enterprise Patch_Management Technologies

Quản lý điểm yếu an toàn thông tin.

2. Quản lý rủi ro an toàn thông tin

a) ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (bổ sung TCVN).

TCVN 10295:2014 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin.

b) NIST SP 800-30 Risk Management Guide for Information Technology Systems.

Hướng dẫn khung quản lý rủi ro cho các hệ thống công nghệ thông tin.

c) NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.

Hướng dẫn quản lý rủi ro cho các hệ thống công nghệ thông tin.

d) NIST SP 800-154 Guide to Data-Centric System Threat Modeling.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn quản lý dữ liệu tập trung.

3. Quản lý giám sát

a) NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.

Quản lý giám sát hệ thống thông tin.

b) NIST SP 800-137A Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment.

Đánh giá hệ thống giám sát an toàn thông tin.

4. Kiểm tra, đánh giá an toàn thông tin

a) NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.

Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn kiểm tra, đánh giá an toàn thông tin.

b) ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing.

TCVN 11779:2017 Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn đánh giá hệ thống quản lý an toàn thông tin.

c) ISO/IEC TR 27008:2008 Information technology — Security techniques — Guidelines for auditors on information security controls.

TCVN 27008:2018 Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn chuyên gia đánh giá về kiểm soát an toàn thông tin

5. Kỹ thuật an toàn mạng

a) NIST SP 800-41 Guidelines on Firewalls and Firewall Policy.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn bảo mật thiết bị tường lửa.

b) NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS).

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn bảo mật thiết bị phát hiện xâm nhập.

c) NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn bảo đảm an toàn thông tin khi kết nối các hệ thống thông tin.

d) NIST SP 800-53 Security and Privacy Controls forFederal Information Systemsand Organizations.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn các biện pháp kiểm soát bảo mật cho hệ thống thông tin.

đ) NIST SP 800-58 Security Considerations for Voice Over IP Systems.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn bảo đảm an toàn thông tin thoại qua nền tảng IP.

e) NIST SP 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn bảo mật mạng không dây 802.11i.

g) NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn bảo đảm an toàn thông tin cho hệ thống điều khiển công nghiệp ISC.

h) NIST SP 800-77 Guide to IPsec VPNs

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn bảo mật mạng riêng ảo.

l) NIST SP 800-119 Guidelines for the Secure Deployment of IPv6.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn bảo mật triển khai IPv6.

m) ISO/IEC 27033 IT network security.

Công nghệ thông tin - Kỹ thuật an toàn - An toàn mạng.

n) ISO/IEC 27033-1 Network security - Part 1: Overview and concepts.

TCVN 9807-1:2013 Công nghệ thông tin - Kỹ thuật an toàn - An ninh mạng – Tổng quan và khái niệm.

p) ISO/IEC 27033-2 Network security - Part 2: Guidelines for the design and implementation of network security.

TCVN 9801-2:2015 Công nghệ thông tin - Kỹ thuật an toàn - An toàn mạng – Hướng dẫn thiết kế và triển khai an toàn mạng.

q) ISO/IEC 27033-4 Network security - Part 4: Securing communications between networks using security gateways.

Công nghệ thông tin - Kỹ thuật an toàn - An toàn mạng – An toàn kết nối.

r) ISO/IEC 27033-5 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs).

Công nghệ thông tin - Kỹ thuật an toàn - An toàn mạng – Mạng riêng ảo.

s) ISO/IEC 27033-6 Network security - Part 6: Securing wireless IP network access.

Công nghệ thông tin - Kỹ thuật an toàn - An toàn mạng – An toàn mạng không dây.

6. Kỹ thuật an toàn máy chủ

a) NIST SP 800-123 Guide to General Server Security.

Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn bảo đảm an toàn thông tin cho máy chủ.

b) NIST SP 800-44 Guidelines on Securing Public Web Servers.

Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn bảo đảm an toàn thông tin cho ứng dụng Web.

c) NIST SP 800-125A Security Recommendations for Server-based Hypervisor Platforms.

Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn bảo đảm an toàn thông tin cho máy chủ ảo hóa.

d) NIST SP 800-147B BIOS Protection Guidelines for Servers.

Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn bảo đảm an toàn thông tin cho BIOS máy chủ.

7. Kỹ thuật an toàn thông tin cho ứng dụng

a) ISO/IEC 27034 Application security

Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn bảo đảm an toàn thông tin cho ứng dụng.

b) NIST SP 800-95 Guide to Secure Web Services.

Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn bảo đảm an toàn thông tin cho Web.

c) NIST SP 800-45 Guidelines on Electronic Mail Security.

Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn bảo đảm an toàn thông tin cho ứng dụng Email.

d) Secure Domain Name System (DNS) Deployment Guide.

Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn bảo đảm an toàn thông tin cho ứng dụng DNS.

đ) NIST SP 800-57 Recommendation for Key Management.

Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn bảo đảm an toàn thông tin cho ứng dụng quản lý khóa.

8. Kỹ thuật an toàn dữ liệu

a) NIST SP 800-92 Guide to Computer Security Log Management.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn quản lý nhật ký bảo mật hệ thống.

b) ISO/IEC 27040 Storage security.

Công nghệ thông tin - Kỹ thuật an toàn – Quản lý lưu trữ an toàn.

c) NIST SP 800-85B PIV Data Model Test Guidelines.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn kiểm tra dữ liệu.

9. Kỹ thuật an toàn thiết bị đầu cuối

a) NIST SP 800-164 Guidelines on Hardware-Rooted Security in Mobile Devices.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn bảo đảm an toàn thông tin cho phần cứng thiết bị di động.

b) NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn phòng chống và xử lý sự cố mã độc trên máy tính.

c) NIST SP 800-163 Vetting the Security of Mobile Applications.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn đánh giá bảo mật ứng dụng cho thiết bị di động.

d) NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn công nghệ lưu trữ mã hóa cho thiết bị đầu cuối.

đ) NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn quản lý bảo mật cho thiết bị di động trong hệ thống.

e) NIST SP 800-121 Guide to Bluetooth Security.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn bảo mật kết nối Bluetooth.

g) NIST SP 800-101 Guidelines on Mobile Device Forensics.

Công nghệ thông tin - Kỹ thuật an toàn – Hướng dẫn điều tra sự cố trên thiết bị di động./.