TCVN | **TIÊU CHUẨN QUỐC GIA**

DỰ THẢO

TCVN XXXXX: 2026
ISO/IEC 27400:2022

Xuất bản lần 1

AN NINH MẠNG — BẢO MẬT VÀ QUYỀN RIÊNG TƯ IOT — HƯỚNG DẪN

Cybersecurity — IoT security and privacy — Guidelines

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu

TCVN XXXXX: 2026 hoàn toàn tương đương với ISO/IEC 27400:2022.

TCVN XXXXX:2026 do Ban Cơ yếu Chính phủ biên soạn, Bộ trưởng Bộ Quốc phòng đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

An toàn thông tin là một mối quan tâm lớn của bất kỳ hệ thống công nghệ thông tin và truyền thông (CNTT-TT) nào và các hệ thống Internet vạn vật (IoT) cũng không ngoại lệ. Các hệ thống IoT đặt ra những thách thức đặc biệt đối với an toàn thông tin ở chỗ chúng có tính phân tán cao và liên quan đến một số lượng lớn các thực thể đa dạng. Điều này dẫn đến bề mặt tấn công rất lớn và một thách thức đáng kể đối với hệ thống quản lý an toàn thông tin (HTQL ATTT) trong việc áp dụng và duy trì các biện pháp kiểm soát bảo mật phù hợp trên toàn bộ hệ thống.

Quyền riêng tư hay bảo vệ thông tin nhận dạng cá nhân (TTNDCN) là một vấn đề quan trọng đối với một số loại hệ thống IoT. Khi một hệ thống IoT thu thập hoặc sử dụng TTNDCN, thường có các luật và quy định áp dụng cho việc thu thập, lưu trữ và xử lý TTNDCN. Ngay cả khi các quy định không phải là một mối quan tâm, việc xử lý TTNDCN bởi một hệ thống IoT vẫn là một mối quan tâm về uy tín và lòng tin đối với các tổ chức liên quan, ví dụ, nếu TTNDCN bị đánh cắp hoặc bị lạm dụng, có khả năng gây ra một số hình thức tổn hại cho những người được xác định bởi thông tin đó.

Các biện pháp kiểm soát bảo mật và quyền riêng tư trong tiêu chuẩn này được phát triển cho các bên liên quan trong môi trường hệ thống IoT, nhằm được sử dụng bởi mỗi bên liên quan tới IoT trong suốt vòng đời của hệ thống IoT.

TIÊU CHUẨN QUỐC GIA **TCVN XXXXX: 2026**

An ninh mạng — Bảo mật và quyền riêng tư IoT — Hướng dẫn

Cybersecurity — IoT security and privacy — Guidelines

1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp các hướng dẫn về rủi ro, nguyên tắc và biện pháp kiểm soát liên quan đến bảo mật và quyền riêng tư của các giải pháp Internet vạn vật (IoT).

2 Tài liệu viện dẫn

Không có tài liệu viện dẫn mang tính quy định trong tiêu chuẩn này.

3 Thuật ngữ và định nghĩa

3.1
điện toán đám mây (cloud computing)

mô hình cho phép truy cập mạng vào một quỹ tài nguyên vật lý hoặc ảo có thể chia sẻ, có khả năng mở rộng và co giãn, với khả năng cung cấp và quản lý tự phục vụ theo yêu cầu.

CHÚ THÍCH 1: Các ví dụ về các tài nguyên bao gồm các máy chủ, hệ điều hành, mạng, phần mềm, ứng dụng và thiết bị lưu trữ.

[NGUỒN: Khuyến nghị ITU-T Y.3500 | TCVN 12480:2019 (ISO/IEC 17788:2014), 3.2.5]

3.2
dịch vụ đám mây (cloud service)

một hoặc nhiều khả năng được cung cấp thông qua điện toán đám mây (3.1) được gọi qua một giao diện xác định

[NGUỒN: Khuyến nghị ITU-T Y.3500 | TCVN 12480:2019 (ISO/IEC 17788:2014), 3.2.8]

3.3
thiết bị IoT (IoT device)

thực thể của một hệ thống IoT tương tác và giao tiếp với thế giới vật lý thông qua cảm biến hoặc truyền động

3.4
nhà phát triển thiết bị IoT (IoT device developer)

thực thể tạo ra một thiết bị IoT hoàn chỉnh được lắp ráp

CHÚ THÍCH 1: "Hoàn chỉnh" trong định nghĩa này có nghĩa là giai đoạn bàn giao cho nhà phát triển dịch vụ IoT trong quá trình lắp ráp.

3.5
nền tảng IoT (IoT platform)

cơ sở hạ tầng cho phép triển khai, quản lý và vận hành các thiết bị IoT

3.6
hệ thống IoT (IoT system)

hệ thống cung cấp các chức năng của Internet vạn vật

CHÚ THÍCH 1: Hệ thống IoT bao gồm các thiết bị IoT, cổng IoT, cảm biến và bộ truyền động.

CHÚ THÍCH 2: Trong ngữ cảnh của tiêu chuẩn này, hệ thống IoT cũng bao gồm các ứng dụng và hệ thống phía sau (backend) hỗ trợ các giải pháp IoT.

3.7
giải pháp IoT (IoT solution)

một gói tích hợp liền mạch các công nghệ, có khả năng bao gồm các cảm biến, cổng kết nối và bộ truyền động

CHÚ THÍCH 1: Những điều này có thể giải quyết một vấn đề hoặc nhu cầu cụ thể hoặc chúng có thể được sử dụng để tạo ra chức năng bổ sung trong các giải pháp khác ngoài IoT.

3.8
hệ sinh thái (ecosystem)

cơ sở hạ tầng và các dịch vụ dựa trên một mạng lưới các tổ chức và các bên liên quan

CHÚ THÍCH 1: Các tổ chức có thể bao gồm các cơ quan công quyền.

[NGUỒN: ISO/IEC TS 27570:2021, 3.8]

4 Thuật ngữ viết tắt

ASD	Application and Service Domain	Miền ứng dụng và dịch vụ
CRM	Customer Relationship Management	Quản lý quan hệ khách hàng
DoS	Denial of Service	Từ chối dịch vụ
IC	Integrated Circuit	Mạch tích hợp
ICT	Information and Communications Technology	Công nghệ thông tin và truyền thông
IoT	Internet of Things	Internet vạn vật
ISAC	Information Sharing and Analysis Centre	Trung tâm chia sẻ và phân tích thông tin
ITS	Intelligent Traffic System	Hệ thống giao thông thông minh
OMD	Operations and Management Domain	Miền vận hành và quản lý
OTA	Over The Air	Qua vô tuyến
PED	Physical Entity Domain	Miền thực thể vật lý
PII	Personally Identifiable Information	Thông tin nhận dạng cá nhân
RAID	Resource Access and Interchange Domain	Miền truy cập và trao đổi tài nguyên
SCD	Sensing and Controlling Domain	Miền cảm biến và điều khiển
UD	User Domain	Miền người dùng
Wi-Fi	Wireless Fidelity	Độ trung thực không dây

5 Các khái niệm IoT

5.1 Tổng quan

Điều này cung cấp phần giới thiệu khái quát về các khái niệm và mô hình tham chiếu IoT hữu ích trong bối cảnh bảo mật và quyền riêng tư. Thông tin chi tiết về các chủ đề này được cung cấp trong TCVN 13117:2020 (ISO/IEC 30141).

5.2 Đặc tính của hệ thống IoT

Các ứng dụng của hệ thống IoT là rất đa dạng, làm cho việc định nghĩa một bộ đặc điểm chung áp dụng cho mỗi hệ thống IoT là không thực tế. Như một cách tiếp cận thực tế để mô tả các đặc điểm của hệ thống IoT, "các đặc điểm chung" và "các đặc điểm cụ thể cho các lĩnh vực ứng dụng" có thể được xác định.

Các hệ thống IoT chia sẻ các đặc điểm chung sau đây.

- Các hệ thống IoT bao gồm các thiết bị IoT, là các thiết bị phần cứng và phần mềm cụ thể được sử dụng kết hợp với hoặc gắn vào các vật thể hoặc vật liệu vật lý.
- Các thiết bị IoT được kết nối với mạng và có khả năng truyền và nhận dữ liệu. Cả mạng có dây và không dây đều có thể được sử dụng.
- Các thiết bị IoT thường có khả năng cảm biến, ví dụ như để phát hiện trạng thái môi trường hoặc chuyển động.
- Các thiết bị IoT có thể có khả năng truyền động, ví dụ như nhận dữ liệu điều khiển để khởi tạo các hành động vật lý.
- Các hệ thống IoT bao gồm các ứng dụng IoT để xử lý dữ liệu từ các thiết bị IoT, để tạo và gửi dữ liệu điều khiển và để cho phép tích hợp với các hệ thống khác.
- Các hệ thống IoT bao gồm các thành phần vận hành cho phép thiết lập và vận hành các thiết bị và ứng dụng IoT.
- Các hệ thống IoT hỗ trợ người dùng là con người hoặc người dùng kỹ thuật số (để biết thêm thông tin, tham khảo TCVN 13117:2020 (ISO/IEC 30141)).

Tùy thuộc vào lĩnh vực hoặc mục đích sử dụng hệ thống IoT, có những yêu cầu cụ thể. Xem danh sách các ví dụ sau đây.

- Đối với các hệ thống IoT dành cho người tiêu dùng, giá cả rất nhạy cảm, do đó chi phí sản xuất và vận hành thiết bị IoT thấp là rất quan trọng. Tùy thuộc vào dữ liệu được xử lý, quyền riêng tư dữ liệu cũng có thể rất quan trọng.
- Các hệ thống IoT công nghiệp có thể thay thế hoặc được sử dụng kết hợp với một nhà máy công nghiệp và các hệ thống điều khiển và do đó, phải tuân theo các yêu cầu tương tự như tính sẵn sàng cao hoặc tính an toàn. Tính an toàn của quá trình sử dụng hệ thống IoT có thể phụ thuộc vào các đặc tính bảo mật của một thiết bị IoT.
- Các hệ thống IoT được sử dụng trong các phương tiện giao thông được sử dụng trong bối cảnh các chức năng liên quan đến độ tin cậy hoặc tính an toàn. Trong khi ở trường hợp sử dụng liên quan đến độ tin cậy, các yêu cầu về quyền riêng tư có thể cần được xem xét, một trường hợp sử dụng liên quan đến an toàn có thể đặt ra các yêu cầu cao về tính toàn vẹn và tính sẵn sàng.

Để biết thêm thông tin và thảo luận về các trường hợp sử dụng cụ thể cho các hệ thống IoT, tham khảo ISO/IEC TR 22417:2017.

Các nhà cung cấp dịch vụ IoT thường sử dụng cơ sở hạ tầng đám mây để triển khai các dịch vụ của mình. Đặc biệt khi sử dụng các dịch vụ đám mây công cộng, điều này cho phép chi phí ban đầu thấp và khả năng mở rộng cao.

Một nhà cung cấp dịch vụ IoT, với tư cách là người tiêu dùng của một dịch vụ đám mây, cần đảm bảo rằng dịch vụ đám mây đó có các biện pháp kiểm soát bảo mật phù hợp. Các biện pháp kiểm soát này, thường kết hợp với các biện pháp kiểm soát bổ sung tại phía nhà cung cấp dịch vụ IoT, cần đáp ứng đầy đủ các yêu cầu về bảo mật và quyền riêng tư của người dùng IoT (ví dụ: liên quan đến việc bảo vệ TTNDCN), trong đó nhà cung cấp dịch vụ IoT đóng vai trò là nhà cung cấp.

Để có thêm hướng dẫn về quan hệ với nhà cung cấp trong các dịch vụ đám mây, tham khảo ISO/IEC 27036-4. Để có hướng dẫn về các biện pháp kiểm soát bảo mật cho các dịch vụ đám mây dựa trên ISO/IEC 27002, tham khảo ISO/IEC 27017 và hướng dẫn thêm về bảo vệ TTNDCN trong đám mây công cộng được cung cấp trong ISO/IEC 27018.

5.3 Các bên liên quan của hệ thống IoT

5.3.1 Tổng quan

Để có thể triển khai bảo mật và quyền riêng tư cho một hệ thống IoT, điều quan trọng là phải xác định các bên liên quan của hệ thống. Tùy thuộc vào vai trò của họ, họ có thể xác định mức độ bảo mật và quyền riêng tư cần thiết cho hệ thống dựa trên mức độ chấp nhận rủi ro của mình, hoặc họ đóng góp vào các biện pháp kiểm soát hiệu quả để đạt được các yêu cầu này.

TCVN 13117:2020 (ISO/IEC 30141) định nghĩa ba loại vai trò: nhà cung cấp dịch vụ IoT, nhà phát triển dịch vụ IoT và người dùng IoT. Tiêu chuẩn này cũng định nghĩa một số vai trò phụ và các hoạt động, một số trong đó liên quan đến bảo mật và quyền riêng tư.

Trong mục 5.3, các bên liên quan chung có liên quan đến hầu hết các hệ thống IoT đã được giới thiệu.

5.3.2 Nhà cung cấp dịch vụ IoT

Một nhà cung cấp dịch vụ IoT quản lý và vận hành các dịch vụ của một hệ thống IoT được cung cấp cho những người dùng IoT.

Các dịch vụ phổ biến được cung cấp bởi các nhà cung cấp dịch vụ IoT bao gồm các dịch vụ kết nối, dịch vụ thu thập và quản lý dữ liệu cũng như dịch vụ quản lý đối với các tài sản liên quan đến IoT như thiết bị IoT.

Dịch vụ IoT cần phải phù hợp với nhu cầu của người dùng IoT và phụ thuộc vào một trường hợp sử dụng cụ thể hoặc một hệ sinh thái IoT có liên quan.

Các nhà cung cấp dịch vụ IoT cần hiểu các yêu cầu chức năng và phi chức năng của người dùng IoT đối với các dịch vụ được cung cấp và đáp ứng nhu cầu của người dùng IoT thông qua các dịch vụ, đặc biệt là về mặt bảo mật và quyền riêng tư.

Để đạt được điều này, các nhà cung cấp dịch vụ IoT cũng cần hiểu đầy đủ về các tác nhân đe dọa (threat vectors) liên quan để có thể thực hiện đánh giá rủi ro và lựa chọn các phương án xử lý rủi ro hiệu quả.

Đối với các biện pháp kiểm soát cụ thể mà một nhà cung cấp dịch vụ IoT phải xem xét, tham khảo các biện pháp kiểm soát được đưa ra tại Điều 7, trong đó "Nhà cung cấp dịch vụ IoT" là đối tượng được chỉ định.

5.3.3 Nhà phát triển dịch vụ IoT

Các nhà phát triển dịch vụ IoT chịu trách nhiệm về việc thiết kế, triển khai và tích hợp các dịch vụ IoT.

Các nhà phát triển dịch vụ IoT có thể được chuyên môn hóa hơn, ví dụ như đảm nhận vai trò kiến trúc sư cho các giải pháp hoặc nền tảng IoT, như nhà thiết kế và/hoặc người triển khai cho các ứng dụng IoT, nhà thiết kế hoặc người triển khai cho các thiết bị IoT.

Trong mỗi vai trò, các nhà phát triển dịch vụ IoT cần tuân theo các thực hành tốt nhất về thiết kế và phát triển, ví dụ như tuân thủ các nguyên tắc bảo mật và quyền riêng tư theo thiết kế hoặc sử dụng các vòng đời phát triển phần mềm an toàn.

Một trong những vai trò phụ của các nhà phát triển dịch vụ IoT là nhà phát triển thiết bị IoT. Vai trò này thực hiện việc thiết kế kỹ thuật và sản xuất các thiết bị phần cứng cụ thể để sử dụng trong các hệ thống IoT, đặc biệt là các thiết bị IoT.

Các thiết bị IoT có thể được vận hành và sử dụng trực tiếp bởi một người dùng IoT hoặc bởi một nhà cung cấp dịch vụ IoT, và cùng một thiết bị kỹ thuật có thể được sử dụng trong các trường hợp sử dụng IoT khác nhau. Điều quan trọng đối với một nhà phát triển thiết bị IoT là phải xem xét các yêu cầu về bảo mật và quyền riêng tư của các kịch bản sử dụng tiềm năng cho thiết bị trong giai đoạn thiết kế, để có thể cung cấp các thiết bị có bộ chức năng và tính năng phù hợp để đáp ứng nhu cầu của khách hàng.

Các nhà phát triển dịch vụ IoT cần hiểu và xem xét các kỳ vọng và yêu cầu về bảo mật và quyền riêng tư của các nhà cung cấp dịch vụ IoT cũng như của người dùng IoT, để lựa chọn các biện pháp kiểm soát cần thiết nhằm đảm bảo xử lý rủi ro của hệ thống IoT một cách phù hợp.

Để biết thêm thông tin về các biện pháp kiểm soát mà nhà phát triển dịch vụ IoT cần xem xét, tham khảo các biện pháp kiểm soát được đưa ra trong Điều 7, trong đó "Nhà phát triển dịch vụ IoT" là đối tượng được chỉ định.

5.3.4 Người dùng IoT

Người dùng IoT là người dùng đầu cuối của một dịch vụ IoT và có thể được phân loại thành người dùng là con người và người dùng kỹ thuật số. Người dùng là con người là một cá nhân sử dụng dịch vụ IoT. Người dùng kỹ thuật số là một người dùng không phải con người của dịch vụ IoT; đó có thể là một dịch vụ tự động hoạt động thay cho một người dùng là con người.

Trong trường hợp người dùng là con người, họ có thể được đại diện bởi một cá nhân, ví dụ, trong trường hợp các hệ thống IoT cấp tiêu dùng, hoặc bởi một tổ chức, ví dụ, trong trường hợp các hệ thống IoT công nghiệp.

Trong mọi trường hợp, người dùng IoT trực tiếp đặt ra hoặc ít nhất là ảnh hưởng đến các yêu cầu chức năng và phi chức năng đối với một hệ thống IoT hoặc một dịch vụ IoT.

Điều cốt lõi đối với người dùng IoT là một hệ thống IoT hoặc dịch vụ IoT có thể được sử dụng mà không gây ra các rủi ro không thể chấp nhận được trong lĩnh vực bảo mật và quyền riêng tư.

Mức độ bảo mật và quyền riêng tư cần được cung cấp trong một hệ thống hoặc dịch vụ IoT chủ yếu được quyết định bởi các kỳ vọng hoặc các cân nhắc về rủi ro của người dùng IoT. Tuy nhiên, người dùng IoT thường có thể không nhận thức được các tác động bảo mật của các công nghệ này.

Đối với bất kỳ trường hợp sử dụng nào, việc hiểu rõ người dùng IoT và nhu cầu cũng như yêu cầu của họ là rất quan trọng.

Để có thể xử lý các rủi ro liên quan đến IoT một cách thích hợp, cũng có những biện pháp kiểm soát mà một người dùng IoT cần xem xét và triển khai. Để biết thêm thông tin về các biện pháp kiểm soát này, tham khảo các biện pháp kiểm soát được đưa ra trong Điều 7, trong đó "Người dùng IoT" là đối tượng được chỉ định.

5.4 Hệ sinh thái IoT

Sự phụ thuộc lẫn nhau giữa các nhà cung cấp dịch vụ IoT, nhà phát triển dịch vụ IoT và những người dùng IoT trong bối cảnh bảo mật và quyền riêng tư trong một hệ thống IoT có thể được mô tả như một hệ sinh thái, tương tự như khái niệm trong sinh thái học. Các sự phụ thuộc trong bảo mật và quyền riêng tư trong IoT bao gồm:

a) Các mối quan hệ nhà cung cấp sản phẩm và dịch vụ;
b) Việc cung cấp các biện pháp bởi các thực thể khác trong hệ sinh thái cần thiết trong việc triển khai các biện pháp kiểm soát bảo mật và quyền riêng tư (xem Điều 7); và
c) Các tác động ngoại lai tiềm ẩn của hậu quả trong các kịch bản rủi ro có thể xảy ra không nằm trong phạm vi của một thực thể (xem Điều 6), ví dụ, việc sai sót trong việc triển khai một biện pháp kiểm soát bởi một nhà cung cấp dịch vụ IoT hoặc một nhà phát triển dịch vụ IoT làm phát sinh rủi ro về bảo mật và quyền riêng tư cho những người dùng IoT.

Hơn nữa, có những lo ngại về các tác động tiêu cực đối với các tổ chức khác ngoài tác động giữa các bên liên quan được giả định trong một hệ thống IoT duy nhất, chẳng hạn như các cuộc tấn công mạng nhằm chống lại các tổ chức và quốc gia bên ngoài lợi dụng các hệ thống và thiết bị IoT dễ bị tấn công. Những tác động tiêu cực này cần được giải quyết trong một hệ sinh thái mở rộng bao gồm các thực thể có khả năng bị ảnh hưởng và các tổ chức có trách nhiệm cần triển khai các biện pháp kiểm soát (Điều 7) để giải quyết chúng.

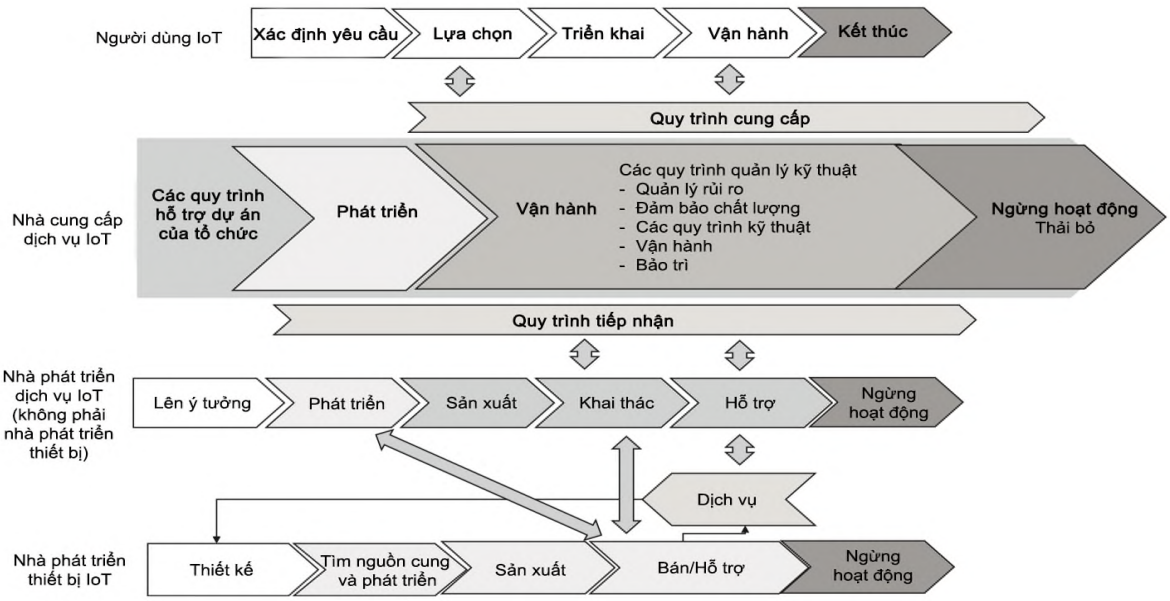
5.5 Các vòng đời dịch vụ IoT

Một dịch vụ IoT bao gồm nhiều vòng đời khác nhau, có thể được ánh xạ tới các bên liên quan của một hệ thống IoT.

Cụ thể hơn, một dịch vụ IoT là:

a) được phát triển bởi một nhà phát triển dịch vụ IoT và (các) nhà phát triển thiết bị IoT;
b) được cung cấp bởi một nhà cung cấp dịch vụ IoT; và
c) được sử dụng bởi những người dùng IoT.

Các quá trình của các bên liên quan này tạo thành một tập hợp các vòng đời phụ thuộc lẫn nhau của việc phát triển thiết bị, phát triển dịch vụ, cung cấp dịch vụ và sử dụng dịch vụ. Hình 1 thể hiện các vòng đời này của dịch vụ IoT và mối quan hệ giữa chúng.



Hình 1 — Các vòng đời của dịch vụ IoT

Trong vòng đời của thiết bị IoT, nhà phát triển thiết bị IoT thiết kế, phát triển, sản xuất, bán và hỗ trợ cho các nhà phát triển dịch vụ IoT, các nhà cung cấp dịch vụ IoT hoặc người dùng IoT. Khi thiết bị hết vòng đời (hết hạn sử dụng), nhà phát triển thiết bị IoT ngừng việc hỗ trợ thiết bị IoT đó. Các yêu cầu về bảo mật và quyền riêng tư được xem xét trong quá trình thiết kế và phát triển thiết bị IoT và được triển khai như các tính năng của thiết bị IoT, ví dụ:

d) các cơ chế xác thực người dùng và kiểm soát truy cập của thiết bị;
e) tính năng bảo mật vật lý như vỏ thiết bị an toàn; và
f) cơ chế cập nhật phần mềm và phần sụn (firmware) của thiết bị và hoạt động của chúng.

Trong quá trình hợp tác với nhà cung cấp, thông tin về các tính năng này được cung cấp và sử dụng bởi các nhà phát triển dịch vụ IoT và các nhà cung cấp dịch vụ IoT ở các giai đoạn phù hợp trong vòng đời của chúng. Một nhà phát triển thiết bị IoT cần đảm bảo rằng thông tin thiết bị đầy đủ và cập nhật, bao gồm thông tin liên quan đến bảo mật, luôn sẵn có cho tất cả các bên liên quan.

Nhà phát triển dịch vụ IoT thiết kế, phát triển, sản xuất và hỗ trợ hệ thống IoT để dịch vụ IoT sẵn sàng. Khi hết vòng đời, nhà phát triển dịch vụ IoT ngừng hỗ trợ hệ thống IoT. Dựa trên các yêu cầu cho một dịch vụ IoT được định hướng bởi nhu cầu của người dùng dự kiến của dịch vụ, các yêu cầu về bảo mật và quyền riêng tư được xem xét trong quá trình thiết kế và phát triển hệ thống IoT và được triển khai như các tính năng của hệ thống IoT, ví dụ:

g) các cơ chế xác thực người dùng và kiểm soát truy cập của dịch vụ;
h) bảo vệ chống phần mềm độc hại;
i) độ dự phòng của các thành phần và mạng;
j) cơ chế cập nhật phần mềm và vận hành; và
k) các chức năng và quy trình cho các hoạt động của hệ thống.

Thông tin của các tính năng này được cung cấp và sử dụng bởi các nhà cung cấp dịch vụ IoT ở các giai đoạn tương ứng trong vòng đời của dịch vụ và chúng cần phải tương thích với các tính năng bảo mật của các thiết bị IoT được sử dụng.

Nhà cung cấp dịch vụ IoT phát triển và vận hành dịch vụ IoT được mua từ nhà phát triển dịch vụ IoT. Khi hết vòng đời, nhà cung cấp dịch vụ IoT ngừng cung cấp dịch vụ. Các hoạt động của các giai đoạn này của vòng đời, tức là phát triển, vận hành và ngừng cung cấp là việc thực hiện các quá trình vòng đời hệ thống được quy định trong ISO/IEC 15288 bao gồm nhưng không giới hạn ở:

l) quá trình thu mua;
m) quá trình cung cấp;
n) các quá trình hỗ trợ dự án của tổ chức;

o) các quá trình quản lý kỹ thuật;
   1) quá trình quản lý rủi ro;
   2) quá trình đảm bảo chất lượng;
p) các quá trình kỹ thuật;
   3) quá trình vận hành;
   4) quá trình bảo trì; và
   5) quá trình loại bỏ.

Trong số các quá trình này, quá trình quản lý rủi ro và quá trình đảm bảo chất lượng là yếu tố then chốt đảm bảo bảo mật và quyền riêng tư trong dịch vụ IoT. Trong quá trình quản lý rủi ro, các rủi ro về bảo mật và quyền riêng tư được đánh giá và xử lý bằng cách áp dụng các tính năng của thiết bị IoT và hệ thống IoT, đồng thời triển khai các hoạt động an toàn. Thông qua quá trình đảm bảo chất lượng, hệ thống IoT và phần mềm được đảm bảo loại trừ các lỗ hổng bảo mật và thành phần độc hại, đồng thời có các chức năng an toàn cần thiết để đảm bảo tính sẵn sàng của hệ thống IoT cùng các khía cạnh an toàn khác.

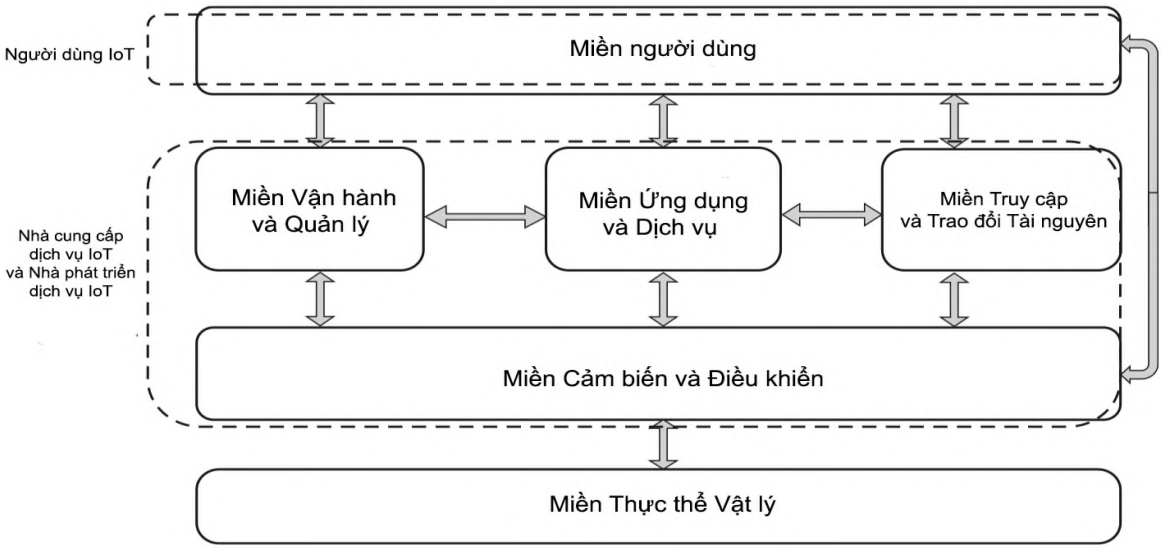
Thông qua quá trình cung cấp, thông tin liên quan đến bảo mật và quyền riêng tư trong việc sử dụng dịch vụ IoT và các bản cập nhật phần mềm được cung cấp cho người dùng IoT.

Người dùng IoT chọn dịch vụ IoT đáp ứng các yêu cầu về dịch vụ và chức năng cùng với các yêu cầu về bảo mật và quyền riêng tư. Thông tin liên quan đến bảo mật và quyền riêng tư được cung cấp bởi nhà cung cấp dịch vụ IoT và nhà phát triển thiết bị IoT và được người dùng IoT xem xét ở giai đoạn này. Sau khi mua dịch vụ IoT, người dùng IoT áp dụng các bản cập nhật phần mềm và phần sụn (firmware) và sử dụng thông tin khác được cung cấp bởi nhà cung cấp dịch vụ IoT và nhà phát triển thiết bị IoT để duy trì mức độ bảo mật và quyền riêng tư trong quá trình vận hành cho đến khi thiết bị IoT ngừng hoạt động.

Cần lưu ý rằng các vấn đề về bảo mật và quyền riêng tư có thể xảy ra do thiếu sự nhất quán giữa các vòng đời của các bên liên quan. Ví dụ, các nhà cung cấp dịch vụ IoT cần nhận thức được khả năng thời gian hỗ trợ của một thiết bị IoT cụ thể kết thúc trong quá trình vận hành dịch vụ IoT, hoặc nhà phát triển thiết bị IoT hoặc nhà phát triển dịch vụ IoT khác không còn tồn tại trên thị trường, trong khi người dùng IoT vẫn tiếp tục sử dụng thiết bị IoT đó dù có biết hay không việc kết thúc hỗ trợ.

5.6 Mô hình tham chiếu dựa trên miền

Các mô hình tham chiếu IoT được trình bày trong TCVN 13117:2020 (ISO/IEC 30141) cung cấp các góc nhìn về các hệ thống IoT. Một trong những mô hình tham chiếu là mô hình tham chiếu dựa trên miền, đây là khung chức năng cấu thành hệ thống IoT và các hoạt động của nó. Hình 2 được trích dẫn từ ISO/IEC 30141:2018, Hình 13. Người dùng IoT, nhà cung cấp dịch vụ IoT và nhà phát triển dịch vụ IoT được thêm vào hình này để thể hiện sự liên quan của các bên liên quan này đến các miền IoT.



Hình 2 — Mô hình tham chiếu dựa trên miền

Hình 2 cho thấy các miền IoT sau:

- Miền Người dùng (UD) bao gồm người dùng là con người và người dùng kỹ thuật số;
- Miền Thực thể Vật lý (PED) bao gồm các thực thể vật lý trong một hệ thống IoT;
- Miền Cảm biến và Điều khiển (SCD) bao gồm các thiết bị IoT và cổng IoT;
- Miền Vận hành và Quản lý (OMD) bao gồm hệ thống hỗ trợ vận hành và hệ thống hỗ trợ kinh doanh;
- Miền Truy cập và Trao đổi Tài nguyên (RAID) cung cấp các cơ chế mà qua đó các thực thể bên ngoài có thể truy cập vào các khả năng của hệ thống IoT; và
- Miền Ứng dụng và Dịch vụ (ASD) bao gồm các ứng dụng và dịch vụ được cung cấp bởi các nhà cung cấp dịch vụ IoT.

Mô hình tham chiếu dựa trên miền cung cấp cấu trúc tổng thể của các thành phần trong một hệ thống IoT để xem xét vấn đề bảo mật và quyền riêng tư trong IoT. Các nguồn rủi ro có thể được xác định liên quan đến các miền IoT (xem 6.2). Mỗi biện pháp kiểm soát bảo mật và quyền riêng tư có thể liên quan đến một hoặc nhiều miền IoT (xem Điều 7).

6 Các nguồn rủi ro đối với các hệ thống IoT

6.1 Tổng quan

Mục này cung cấp hướng dẫn và thông tin về các yếu tố và đầu vào đặc thù của IoT cần được xem xét khi xác định các nguồn rủi ro cho các hệ thống IoT.

Dựa trên các nguồn rủi ro đã xác định, quản lý rủi ro cho các hệ thống IoT cần được thực hiện bằng cách sử dụng các cách tiếp cận và phương pháp đã được tiêu chuẩn hóa.

Thông tin về các cách tiếp cận hoặc phương pháp này đã được đề cập trong các Tiêu chuẩn Quốc tế khác, cụ thể là:

- ISO 31000, đưa ra các hướng dẫn chung về quản lý rủi ro;
- TCVN 10295:2014 (ISO/IEC 27005), đưa ra các hướng dẫn cụ thể về quản lý rủi ro an toàn thông tin;
- IEC 62443 (tất cả các phần), đưa ra hướng dẫn trong lĩnh vực tự động hóa và hệ thống điều khiển công nghiệp;
- ISO/IEC 29134, đưa ra các hướng dẫn về đánh giá tác động đến quyền riêng tư.

Trong các trường hợp việc áp dụng hệ thống quản lý an toàn thông tin là bắt buộc, các Tiêu chuẩn Quốc tế sau đây cũng có liên quan:

- TCVN ISO/IEC 27001:2019 (ISO/IEC 27001), cung cấp các yêu cầu đối với hệ thống quản lý an toàn thông tin;
- ISO/IEC 27701, cung cấp các yêu cầu mở rộng đối với các yêu cầu của hệ thống quản lý an toàn thông tin phục vụ việc quản lý thông tin riêng tư.

Có những nguồn rủi ro cụ thể của IoT cần được xem xét khi đánh giá rủi ro của các hệ thống IoT; các nguồn này được mô tả chi tiết hơn trong 6.2.

6.2 Các nguồn rủi ro

6.2.1 Tổng quan

Nguồn rủi ro là yếu tố có khả năng tiềm ẩn gây ra rủi ro, dù là riêng lẻ hay kết hợp với các yếu tố khác (xem định nghĩa về nguồn rủi ro trong ISO/IEC 31000). Khi xác định các kịch bản rủi ro và rủi ro trong hệ thống IoT, ứng dụng hoặc dịch vụ, các nguồn rủi ro liên quan cần được xác định một cách toàn diện để đưa vào các kịch bản rủi ro. Xem Phụ lục A: Kịch bản rủi ro mẫu cho camera giám sát IoT để có hướng dẫn chi tiết về việc thực hiện đánh giá rủi ro. Có nhiều loại nguồn rủi ro khác nhau, bao gồm nhưng không giới hạn ở:

a) lỗ hổng bảo mật của hệ thống, ứng dụng hoặc dịch vụ IoT;
b) thiếu kiến thức và kỹ năng của những người có vai trò trong việc cung cấp hoặc sử dụng hệ thống, ứng dụng hoặc dịch vụ IoT;

c) lỗi con người của những người có vai trò trong việc cung cấp hoặc sử dụng hệ thống, ứng dụng hoặc dịch vụ IoT;
d) sự tồn tại của những người có ý đồ xấu nhằm tấn công hệ thống, ứng dụng hoặc dịch vụ IoT;
e) chất lượng của hệ thống, ứng dụng hoặc dịch vụ IoT và các thành phần của chúng;
f) sự tồn tại của các hệ thống và thiết bị bên ngoài có thể bị lợi dụng để tạo ra các cuộc tấn công vào hệ thống, ứng dụng hoặc dịch vụ IoT;
g) sự tồn tại của các hiện tượng tự nhiên, ví dụ như sét, lũ lụt và động đất; và
h) sự thiếu hụt quản trị tổ chức trong các bên liên quan của hệ thống IoT.

Mục 6.2.2 cung cấp các nguồn rủi ro mẫu cho từng miền của hệ thống IoT, 6.2.3 liệt kê các nguồn rủi ro bắt nguồn từ bên ngoài các miền IoT và 6.2.4 thảo luận về các nguồn rủi ro liên quan đến quyền riêng tư.

6.2.2 Các nguồn rủi ro mẫu liên quan đến các miền IoT

6.2.2.1 Miền cảm biến và điều khiển

Sau đây là danh sách các nguồn rủi ro cần được xem xét trong miền cảm biến và điều khiển.

- Phần mềm và phần sụn (firmware) của một thiết bị IoT hoặc một cổng IoT có các lỗ hổng kỹ thuật.
- Phần mềm và phần sụn của một thiết bị IoT hoặc một cổng IoT không có hoặc có cơ chế cập nhật không an toàn.
- Một thiết bị IoT hoặc một cổng IoT không có hoặc có chức năng bảo mật yếu, ví dụ như chức năng xác thực yếu, không có mã hóa và dự phòng.
- Một thiết bị IoT hoặc một cổng IoT có thể bị cấu hình theo cách không an toàn.
- Một thiết bị IoT hoặc một cổng IoT không đạt mức chất lượng đảm bảo hoạt động liên tục trong một khoảng thời gian lâu dài.
- Một nhà phát triển của một thiết bị IoT hoặc một cổng IoT không có năng lực cần thiết để phát triển một thiết bị IoT hoặc một cổng IoT an toàn.
- Một nhà phát triển của một thiết bị IoT hoặc một cổng IoT không có năng lực để triển khai chất lượng đảm bảo hoạt động liên tục trong một khoảng thời gian lâu dài.
- Một thiết bị IoT hoặc một cổng IoT được đặt tại một địa điểm không được bảo vệ bởi cơ sở vật chất an toàn.
- Thiết bị IoT hoặc cổng IoT được đặt tại một vị trí không có nhân viên trực/giám sát.
- Thiết bị IoT hoặc cổng IoT hoạt động dưới ảnh hưởng của thời tiết và các điều kiện môi trường khác.
- Thiết bị IoT hoặc cổng IoT được sản xuất thông qua chuỗi cung ứng CNTT-TT.

6.2.2.2 Miền vận hành và quản lý

Sau đây là danh sách các nguồn rủi ro cần được xem xét trong miền vận hành và quản lý.

- Một nhà cung cấp dịch vụ IoT không có năng lực cần thiết để vận hành hệ thống IoT một cách an toàn.
- Quy trình vận hành hệ thống hoặc dịch vụ IoT đã được ban hành nhưng tồn tại các lỗ hổng bảo mật.
- Quy trình để vận hành một hệ thống hoặc dịch vụ IoT được ban hành nhưng không được người vận hành hệ thống tuân thủ.
- Một quản trị viên hoặc một người vận hành một hệ thống hoặc dịch vụ IoT thực hiện sai sót trong quá trình vận hành.
- Một quản trị viên hoặc một người vận hành của một hệ thống hoặc dịch vụ IoT có ý đồ xấu.
- Một nhà cung cấp dịch vụ IoT thiếu nhận thức về quyền riêng tư trong quá trình sử dụng các hệ thống quản lý quan hệ khách hàng (CRM).

Các nguồn rủi ro trong miền này có khả năng ảnh hưởng đến tính toàn vẹn và tính sẵn sàng của dữ liệu của bộ cảm biến hoặc các lệnh điều khiển bộ truyền động.

Các vấn đề về tính toàn vẹn hoặc các thay đổi trái phép của dữ liệu này có thể khó phát hiện - ví dụ, dữ liệu hiệu chuẩn cảm biến bị thay đổi vẫn có thể dẫn đến dữ liệu cảm biến có vẻ hợp lý, nhưng có thể không phản ánh đúng thực tế.

6.2.2.3 Miền ứng dụng và dịch vụ

Sau đây là danh sách các nguồn rủi ro cần được xem xét trong miền ứng dụng và dịch vụ.

- Một nhà phát triển dịch vụ IoT không có năng lực để phát triển một ứng dụng và dịch vụ IoT an toàn.
- Một nhà phát triển dịch vụ IoT không có năng lực để triển khai chất lượng đảm bảo hoạt động liên tục trong một khoảng thời gian lâu dài.
- Phương pháp luận đã được thiết lập không được tuân theo trong quá trình phát triển một hệ thống, ứng dụng hoặc dịch vụ.
- Một nhà phát triển của một hệ thống, ứng dụng hoặc dịch vụ IoT mắc lỗi trong quá trình phát triển.
- Một hệ thống, ứng dụng hoặc dịch vụ IoT có các lỗ hổng bảo mật.
- Một nhà phát triển của một hệ thống, ứng dụng hoặc dịch vụ có ý đồ xấu.

6.2.2.4 Miền truy cập và trao đổi tài nguyên

Sau đây là danh sách các nguồn rủi ro cần được xem xét trong miền truy cập và trao đổi tài nguyên.

- Một hệ thống, ứng dụng hoặc dịch vụ IoT không có hoặc có chức năng bảo mật yếu, ví dụ như chức năng xác thực và ủy quyền yếu hoặc kiểm soát truy cập yếu.
- Một hệ thống, ứng dụng hoặc dịch vụ IoT không có mức chất lượng đảm bảo hoạt động liên tục trong một khoảng thời gian dài.
- Một nhà phát triển dịch vụ IoT không có năng lực để thiết kế và áp dụng các cài đặt an toàn cho một hệ thống, ứng dụng hoặc dịch vụ IoT.

Các nguồn rủi ro trong miền này có khả năng ảnh hưởng đến tính toàn vẹn và tính sẵn sàng của dữ liệu cảm biến hoặc các lệnh điều khiển bộ truyền động.

Các sự cố gây ra bởi nguồn rủi ro của miền này cũng có thể khó phát hiện - ví dụ, dữ liệu cảm biến từ một cảm biến sai nhưng cùng chủng loại với cảm biến đúng rất có thể vẫn nằm trong một phạm vi hợp lệ.

6.2.2.5 Miền người dùng

Sau đây là danh sách các nguồn rủi ro cần được xem xét trong miền người dùng.

- Một người dùng IoT không nhận thức được các rủi ro về bảo mật và quyền riêng tư trong việc sử dụng một thiết bị IoT và một dịch vụ IoT.
- Một người dùng IoT không có năng lực để chọn thiết bị IoT hoặc dịch vụ IoT an toàn.
- Một người dùng IoT không có năng lực để cài đặt và vận hành một thiết bị IoT và một dịch vụ IoT một cách an toàn.
- Một người dùng IoT không biết điểm liên hệ cung cấp hỗ trợ cho việc sử dụng an toàn thiết bị IoT hoặc dịch vụ IoT.
- Một người dùng IoT thiếu kiến thức về các lỗ hổng kỹ thuật.
- Một người dùng IoT không biết thời điểm kết thúc thời gian hỗ trợ đối với thiết bị IoT và/hoặc các dịch vụ IoT.

Các sự cố gây ra bởi nguồn rủi ro của miền này cũng có thể khó phát hiện - ví dụ, vì dữ liệu cảm biến sai vẫn có thể nằm trong một phạm vi hợp lệ và có thể không có tác động tức thời nào hiển thị rõ đối với người dùng.

Sau đây là một nguồn rủi ro về quyền riêng tư cần được xem xét trong miền người dùng IoT:

- Người dùng IoT thiếu kiến thức và nhận thức về khung quyền riêng tư theo thiết kế.

6.2.3 Các nguồn rủi ro từ bên ngoài các miền IoT

Sau đây là danh sách các nguồn rủi ro có thể được xác định trong các khu vực bên ngoài một hệ thống IoT. Mục 6.2.2 cung cấp các ví dụ về nguồn rủi ro mẫu cho từng miền của hệ thống IoT và trong 6.2.3 các ví dụ khác về nguồn rủi ro mẫu bắt nguồn từ bên ngoài các miền hệ thống IoT được nêu ra.

- Có những người có ý đồ xấu tấn công, xâm nhập hoặc lạm dụng hệ thống, ứng dụng hoặc dịch vụ IoT.

- Tồn tại các hệ thống và thiết bị dễ bị tấn công trên Internet và các mạng khác có thể bị lợi dụng để thực hiện các cuộc tấn công nhằm vào hệ thống, ứng dụng hoặc dịch vụ IoT.
- Có những hiện tượng tự nhiên, ví dụ như sét, lũ lụt và động đất, có thể làm tổn hại đến hoạt động của hệ thống, ứng dụng hoặc dịch vụ IoT.
- Tính khả dụng của hệ thống, ứng dụng hoặc dịch vụ IoT phụ thuộc vào tính sẵn sàng của nguồn cung cấp điện và các tiện ích hạ tầng khác.
- Tính khả dụng của hệ thống, ứng dụng hoặc dịch vụ IoT phụ thuộc vào tính sẵn sàng của các dịch vụ mạng.
- Sự phức tạp của hệ sinh thái CNTT-TT có thể dẫn đến vi phạm quyền riêng tư.

6.2.4 Các nguồn rủi ro liên quan đến quyền riêng tư

Quyền riêng tư là một mối quan tâm chính đối với các sản phẩm và dịch vụ hỗ trợ IoT trên mọi lĩnh vực. Trong khi các mô hình kinh doanh và dịch vụ mới đang được thiết kế trong các lĩnh vực khác nhau sử dụng dữ liệu được ghi lại bởi các cảm biến IoT và dữ liệu có nguồn gốc từ các dịch vụ IoT, điều này cũng đang làm dấy lên những lo ngại về việc bảo vệ quyền riêng tư của người dùng.

Nhiều dịch vụ IoT có xu hướng tập trung vào nhu cầu đơn giản hóa trách nhiệm của người dùng IoT, đặt những trách nhiệm đó lên các nhà phát triển thiết bị IoT và nhà cung cấp dịch vụ IoT. Người dùng có thể cảm thấy khó hiểu về kiến trúc của các sản phẩm và dịch vụ IoT này và dữ liệu mà các cảm biến IoT đang thu thập về họ, vì chi tiết về dữ liệu được thu thập hoặc không được các nhà sản xuất thiết bị và nhà cung cấp dịch vụ chia sẻ một cách rõ ràng hoặc người dùng có thể thiếu nhận thức rằng họ phải biết về cách thức hoạt động của thiết bị và dịch vụ IoT ở một mức độ nhất định vì lợi ích cá nhân của họ.

Khi các dịch vụ hỗ trợ IoT trở nên phổ biến, sự chồng chéo dần của các thiết bị và dịch vụ IoT với thói quen hàng ngày của chúng ta cũng sẽ dẫn đến những lo ngại gia tăng về quyền riêng tư của người dùng nếu nó không được giải quyết ngay từ giai đoạn thiết kế. Điều này là do khả năng giao tiếp của các thiết bị IoT với nhau (giao tiếp M2M) và khả năng kỹ thuật chia sẻ dữ liệu bối cảnh giữa các thiết bị này và các bên thứ ba có thể hỗ trợ việc lập hồ sơ người dùng và đánh giá hành vi người dùng bằng các phương pháp tổng hợp dữ liệu, xác định lại danh tính và phân tích, vì lợi ích kinh doanh, có thể diễn ra mà người dùng không hề hay biết hoặc không đồng ý. Vì các thiết bị IoT gần như luôn trực tuyến, chúng có thể để lại một dấu vết dữ liệu trên internet. Dữ liệu đó có thể được tích lũy để tạo ra một dấu vết kỹ thuật số của các thiết bị và chủ sở hữu thiết bị. Việc xâm nhập cookie của các thiết bị IoT cũng có thể gây ra vi phạm quyền riêng tư.

Ví dụ, một bản sao kỹ thuật số về cuộc sống hàng ngày của chúng ta có thể được tạo ra bằng cách theo dõi các thiết bị thông minh ở nhà, theo dõi vị trí của ô tô thông minh của chúng ta, theo dõi các thông số sức khỏe của chúng ta từ các thiết bị y tế thông minh hoặc bằng cách theo dõi các cuộc trò chuyện của chúng ta bằng các thiết bị thông minh dành cho một mục đích sử dụng khác. Các yếu tố không gian và thời gian của các sản phẩm và dịch vụ IoT có thể hỗ trợ việc tổng hợp dữ liệu cụ thể có thể giúp suy ra các đặc điểm khác nhau của người dùng. Các sản phẩm và dịch vụ thông minh có thể được kết nối và phụ thuộc lẫn nhau, như trong các thành phố thông minh, nơi hệ thống an ninh nhà có thể cung cấp dữ liệu và cảnh báo cho hệ thống giám sát thành phố do cảnh sát hoặc chính quyền thành phố duy trì, tủ lạnh thông minh có thể đặt hàng thực phẩm từ cửa hàng tạp hóa trực tuyến thay mặt cho chủ sở hữu, hoặc hệ thống theo dõi sức khỏe thông minh có thể gửi dữ liệu sức khỏe từ thiết bị theo dõi sức khỏe đeo được thông minh đến công ty bảo hiểm y tế. Các giao diện dịch vụ IoT có thể làm cho việc sử dụng dữ liệu ngữ cảnh trở nên không rõ ràng đối với những người bình thường, những người có thể để các thiết bị IoT ở cài đặt mặc định mà không có bất kỳ sự điều chỉnh nào để bảo vệ quyền riêng tư, cuối cùng dẫn đến vi phạm quyền riêng tư.

Những lỗi thiết kế này từ các nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT và sự thiếu nhận thức hoặc không có khả năng của người dùng IoT có thể dẫn đến việc lạm dụng thông tin cá nhân và xâm phạm quyền riêng tư, dẫn đến sự mất lòng tin và tai tiếng cho các thiết bị và dịch vụ thông minh. Quyền riêng tư cần được coi là một yếu tố then chốt để hiện thực hóa tiềm năng của công nghệ IoT, song song với các yếu tố tạo dựng lòng tin khác như bảo mật, an toàn, độ tin cậy và khả năng phục hồi. Những yếu tố này cùng nhau tạo thành nền tảng của một thế giới kết nối đáng tin cậy của 'vạn vật'.

7 Các biện pháp kiểm soát bảo mật và quyền riêng tư

7.1 Các biện pháp kiểm soát bảo mật

7.1.1 Tổng quan

Các biện pháp kiểm soát bảo mật được khuyến nghị ở đây cho các hệ thống IoT. Những biện pháp này dành cho nhà cung cấp dịch vụ IoT, nhà phát triển dịch vụ IoT và người dùng IoT.

Các biện pháp kiểm soát này được dự định sử dụng kết hợp với các biện pháp khác, không giới hạn ở các biện pháp kiểm soát cụ thể của IoT. Ví dụ, chúng có thể được áp dụng kết hợp với các biện pháp kiểm soát trong TCVN ISO/IEC 27002:2020.

Để mô tả các biện pháp kiểm soát, một định dạng chung được sử dụng:

Biện pháp kiểm soát XX — Biện pháp kiểm soát được nêu, trong đó XX là số thứ tự, được đưa ra để dễ dàng tham chiếu đến biện pháp kiểm soát.

Mục đích - giải thích mục đích của các biện pháp kiểm soát.

Đối tượng - nêu tên các bên liên quan có tham gia và cần được thông báo về biện pháp kiểm soát. Tham khảo 5.3 để biết danh sách các bên liên quan.

Miền IoT - liệt kê các miền mà biện pháp kiểm soát liên quan đến, dựa trên mô hình tham chiếu dựa trên miền được giới thiệu trong 5.6.

Hướng dẫn - cung cấp thông tin hướng dẫn để triển khai biện pháp kiểm soát.

7.1.2 Các biện pháp kiểm soát bảo mật cho nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT

7.1.2.1 Chính sách bảo mật cho IoT

Biện pháp kiểm soát-01

Một chính sách bảo mật cho IoT cần được xác định, được phê duyệt bởi ban quản lý, công bố, thông báo đến nhân sự liên quan và các bên ngoài có liên quan và được xem xét định kỳ hoặc khi có những thay đổi đáng kể.

CHÚ THÍCH: Khái niệm nhân sự bao gồm các thành viên của tổ chức, chẳng hạn như cơ quan quản trị, lãnh đạo cao nhất, nhân viên, nhân viên tạm thời, nhà thầu và tình nguyện viên.

Mục đích

Cung cấp định hướng và sự hỗ trợ của cấp quản lý đối với bảo mật IoT trong nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT, phù hợp với các yêu cầu kinh doanh và kỳ vọng của các bên liên quan.

Đối tượng**:** Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Nhà cung cấp dịch vụ IoT hoặc nhà phát triển dịch vụ IoT cần xác định chính sách bảo mật cho IoT của mình, thể hiện cam kết của ban lãnh đạo đối với bảo mật IoT.

Chính sách bảo mật cho IoT cần giải quyết các yêu cầu được xác định thông qua việc hiểu rõ:

a) trách nhiệm của tổ chức trong việc cung cấp các dịch vụ IoT;
b) các bên liên quan nội bộ và bên ngoài và kỳ vọng của họ; và
c) môi trường rủi ro.

Chính sách bảo mật cho IoT cần bao gồm các tuyên bố về:

1) định nghĩa về bảo mật IoT;
2) các mục tiêu của tổ chức về bảo mật IoT;
3) vai trò và trách nhiệm về bảo mật IoT trong tổ chức (xem 5.3).

Chính sách bảo mật cho IoT cần giải quyết các vấn đề liên quan đến an toàn thông tin và các khía cạnh khác bao gồm chất lượng của dịch vụ IoT có liên quan đến bảo mật IoT và có thể gây ra các sự cố bảo

mật IoT. Chính sách bảo mật cho IoT cũng cần xem xét hậu quả của các sự cố ảnh hưởng đến sự an toàn của các bên liên quan nội bộ và bên ngoài.

7.1.2.2 Tổ chức bảo mật IoT

Biện pháp kiểm soát-02

Các vai trò và trách nhiệm về bảo mật của IoT cần được xác định và phân công.

Mục đích

Thiết lập và duy trì một khung quản lý để khởi xướng và kiểm soát việc triển khai và vận hành bảo mật IoT trong nhà cung cấp dịch vụ IoT hoặc nhà phát triển dịch vụ IoT.

Đối tượng**:** Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT**:** Vận hành và Quản lý.

Hướng dẫn

Việc phân công vai trò và trách nhiệm về bảo mật của IoT cần được thực hiện theo chính sách bảo mật cho IoT (xem 7.1.2.1).

Các vai trò phụ của nhà cung cấp dịch vụ IoT và nhà phát triển dịch vụ IoT (xem 5.3.2 và 5.3.3) cần được phân công với các vai trò và trách nhiệm bảo mật IoT.

Các vai trò và trách nhiệm bảo mật IoT cần bao gồm nhưng không giới hạn ở những vai trò cho:

a) các hoạt động quản lý rủi ro (xem Điều 6);
b) thiết kế các biện pháp bảo mật cho các hệ thống, thiết bị và dịch vụ IoT;
c) triển khai và vận hành các biện pháp bảo mật trong việc phát triển và vận hành các hệ thống, thiết bị và dịch vụ IoT;
d) quản lý mối quan hệ với nhà cung cấp;
e) các chương trình nâng cao nhận thức, giáo dục và đào tạo; và
f) chương trình quản lý sự cố.

Các vai trò và trách nhiệm cần được ban hành dưới dạng văn bản, phổ biến trong tổ chức và được xem xét và cập nhật khi cần thiết.

7.1.2.3 Quản lý tài sản

Biện pháp kiểm soát-03

Cần xác định thông tin, các thiết bị và hệ thống IoT cùng các chức năng và hoạt động của chúng cần được bảo vệ.

Mục đích

Xác định các tài sản của các thiết bị và hệ thống IoT để thiết kế các biện pháp bảo vệ phù hợp.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Các nhà cung cấp dịch vụ IoT cần xác định các tài sản liên quan đến vòng đời của dịch vụ IoT và lập thành văn bản mức độ quan trọng của chúng. Vòng đời của dịch vụ IoT phải bao gồm việc tạo, xử lý, lưu trữ, truyền, xóa, hủy bỏ. Các tài liệu liên quan đến các tài sản đã xác định cần được lưu trong một kho lưu trữ chuyên dụng hoặc hiện có khi cần.

Kho tài sản cần chính xác, cập nhật và nhất quán.

Các tài sản trong vòng đời của các thiết bị và hệ thống IoT có thể bao gồm những điều sau:

a) phần mềm và phần sụn được triển khai trên các thiết bị và hệ thống IoT;
b) các thuộc tính do nhà máy cài đặt để sử dụng ban đầu các thiết bị và hệ thống IoT;

c) dữ liệu cảm biến và dữ liệu điều khiển;
d) dữ liệu được truyền từ/đến các thiết bị và hệ thống IoT.

Thực hiện quản lý thiết bị IoT để quản lý cấu hình thiết bị IoT và luôn nắm rõ các tài sản vật lý mà các thiết bị IoT được ghép nối.

7.1.2.4 Thiết bị và tài sản nằm ngoài khu vực được bảo vệ vật lý

Biện pháp kiểm soát-04

Các biện pháp bảo mật cụ thể cần được áp dụng cho các thiết bị và tài sản IoT được đặt hoặc vận hành bên ngoài các khu vực được bảo vệ vật lý.

Mục đích

Ngăn chặn mất mát, hư hỏng, trộm cắp hoặc xâm phạm các thiết bị IoT và gián đoạn hoạt động của các dịch vụ IoT.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý.

Hướng dẫn

Khi các thiết bị IoT được đặt bên ngoài cơ sở của nhà cung cấp dịch vụ IoT, hướng dẫn sau đây cần được xem xét để giải quyết các rủi ro liên quan.

a) Đảm bảo bảo vệ vật lý đầy đủ cho các cảm biến và bộ truyền động. Các vỏ bảo vệ của cảm biến và bộ truyền động được lắp đặt ở khu vực công cộng phải có khả năng chống tháo mở hiệu quả, nhằm ngăn chặn hành vi trộm cắp, phá hủy hoặc can thiệp trái phép vào thiết bị.
b) Đảm bảo rằng vị trí của các cảm biến và bộ truyền động được kiểm tra thường xuyên, ví dụ như trong khuôn khổ các hoạt động quản lý tài sản.
c) Nếu chỉ có thể bảo vệ vật lý hạn chế cho các thiết bị IoT, bất kỳ người dùng nào của các thiết bị (ví dụ: người tiêu dùng các giá trị cảm biến) phải được thông báo về mức độ tin cậy hạn chế mà các thiết bị cung cấp.
d) Đảm bảo thông tin nhạy cảm, chẳng hạn như vật liệu khóa mật mã, được bảo vệ đầy đủ khỏi việc lộ lọt hoặc sửa đổi trái phép, bằng cách sử dụng lưu trữ an toàn dựa trên phần cứng hoặc các kỹ thuật tương tự.

7.1.2.5 Tiêu hủy hoặc tái sử dụng thiết bị một cách an toàn

Biện pháp kiểm soát-05

Tất cả các hạng mục thiết bị chứa phương tiện lưu trữ cần được xác minh để đảm bảo rằng mọi dữ liệu nhạy cảm và phần mềm được cấp phép đã được gỡ bỏ hoặc ghi đè an toàn trước khi tiêu hủy hoặc tái sử dụng.

Mục đích

Ngăn chặn rò rỉ thông tin và sử dụng trái phép thiết bị IoT và các thiết bị khác của hệ thống IoT khi loại bỏ hoặc tái sử dụng.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý hoặc Cảm biến và Điều khiển.

Hướng dẫn

Phương tiện lưu trữ phải được phá hủy vật lý, hoặc thông tin được lưu trữ trong phương tiện phải được phá hủy, xóa hoặc ghi đè bằng các kỹ thuật làm cho thông tin gốc không thể truy xuất được trước khi tiêu hủy hoặc tái sử dụng.

Việc tiêu hủy hoặc tái sử dụng các thiết bị IoT có nguy cơ khiến mã phần mềm hoặc dữ liệu bị truy xuất, phân tích, sửa đổi và lạm dụng. Hậu quả của việc tiêu hủy hoặc tái sử dụng không an toàn có thể là trộm cắp danh tính, giao dịch trái phép, tấn công vào hệ thống IoT, vi phạm các điều khoản cấp phép và các

sự cố khác ảnh hưởng đến người dùng IoT, nhà phát triển dịch vụ IoT, nhà cung cấp dịch vụ IoT và các thực thể khác.

7.1.2.6 Học hỏi từ các sự cố bảo mật

Biện pháp kiểm soát-06

Kiến thức thu được từ việc phân tích và giải quyết các sự cố bảo mật IoT cần được sử dụng để giảm khả năng xảy ra hoặc tác động của các sự cố trong tương lai.

Mục đích

Giảm các tác động tiêu cực của các sự cố trong việc cung cấp và sử dụng các dịch vụ IoT.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Nguồn kiến thức có thể là nội bộ hoặc bên ngoài.

a) Khi sự cố được xử lý bởi nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT được kết thúc, các nguyên nhân và hậu quả của sự cố được xác định.
b) Khi một sự cố bảo mật IoT được báo cáo bởi một cơ quan bên ngoài, tính liên quan của nó đến hệ thống và dịch vụ IoT được xem xét và xác định.

Dựa trên kiến thức, nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT cần sửa đổi khi cần thiết:

c) đánh giá rủi ro, ví dụ như xác định các nguồn rủi ro và đánh giá rủi ro;
d) xử lý rủi ro, ví dụ như các biện pháp kiểm soát được áp dụng và việc triển khai chúng; hoặc
e) các quá trình quản lý sự cố.

Ví dụ, kiến thức về:

- lỗ hổng phần mềm mới được công bố có thể ảnh hưởng đến các biện pháp bảo mật của dịch vụ IoT (c);
- một cuộc tấn công vào hệ thống IoT có thể yêu cầu sửa đổi hoặc bổ sung việc triển khai một biện pháp kiểm soát (d); hoặc
- một vấn đề vận hành có thể chỉ ra sự cần thiết phải thay đổi quá trình quản lý sự cố giữa nhà cung cấp dịch vụ IoT và người dùng IoT (e).

Thông tin khác

ISO/IEC 27035 (tất cả các phần) cung cấp các hướng dẫn về quản lý sự cố an toàn thông tin, bao gồm các bài học kinh nghiệm, là những hướng dẫn chung và áp dụng cho tất cả các tổ chức. Hướng dẫn của tiểu mục này nhấn mạnh các khía cạnh của các bài học kinh nghiệm liên quan đến các dịch vụ IoT.

7.1.2.7 Các nguyên tắc thiết kế kỹ thuật hệ thống IoT an toàn

Biện pháp kiểm soát-07

Các nguyên tắc thiết kế kỹ thuật hệ thống IoT an toàn giải quyết việc thiết kế và triển khai các chức năng bảo mật, phòng thủ theo chiều sâu và tăng cường bảo mật (hardening) của hệ thống và phần mềm cần được áp dụng cho việc phát triển các hệ thống IoT.

Mục đích

Đảm bảo rằng bảo mật được thiết kế và triển khai trong quá trình phát triển các hệ thống IoT.

Đối tượng: Nhà phát triển dịch vụ IoT.

Miền IoT: Ứng dụng và Dịch vụ, Cảm biến và Điều khiển hoặc Truy cập và Trao đổi Tài nguyên.

Hướng dẫn

Nhà phát triển dịch vụ IoT cần có các nguyên tắc để thiết kế hệ thống IoT an toàn.

Các nguyên tắc này cần yêu cầu xác định rủi ro của hệ thống IoT, xem xét các hậu quả có thể ảnh hưởng đến người dùng IoT, các nhà cung cấp dịch vụ IoT và các thực thể bên ngoài khác trên mạng.

Việc xác định rủi ro cần xem xét các khía cạnh khác nhau của hệ thống IoT. Các ví dụ về các khía cạnh đó là:

a) các giao diện giữa hệ thống IoT và các thực thể bên ngoài thông qua mạng;
b) gian lận nội bộ trong vận hành và bảo trì hệ thống;
c) các vấn đề về chất lượng của các sản phẩm và dịch vụ được mua từ các thực thể bên ngoài;
d) truy cập vật lý vào hệ thống và thiết bị IoT;
e) thay đổi trong các điều kiện môi trường; và
f) các quá trình sản xuất để cài đặt dữ liệu quan trọng, ví dụ như phần sụn, khóa mật mã và chứng chỉ.

Các nguyên tắc cần đề cập đến các lĩnh vực sau đây của các biện pháp bảo mật cần được xem xét trong quá trình phát triển hệ thống IoT:

g) các chức năng bảo mật;
h) các yêu cầu tăng cường bảo mật cho hệ thống và phần mềm;
i) các yêu cầu về phòng thủ theo chiều sâu, tức là thiết kế theo lớp của các chức năng bảo mật; và
j) các chức năng giám sát và ghi nhật ký.

Các nguyên tắc cần được áp dụng cho việc phát triển các hệ thống IoT với các khái niệm thiết kế bảo mật sau đây:

k) An toàn theo mặc định: khái niệm này bao gồm các hướng dẫn để lựa chọn các tùy chọn an toàn nhất có sẵn trong quá trình mua sắm và cấu hình, ví dụ:
- giảm thiểu bề mặt tấn công;
- sử dụng chuỗi cung ứng an toàn;
- sử dụng các tiêu chuẩn, thực hành tốt nhất và tái sử dụng các mã đã được xác thực;
- tăng cường bảo mật hệ thống và hoạt động với đặc quyền tối thiểu;
- giảm thời gian tiếp xúc.

l) Nghiêm ngặt trong phòng thủ: khái niệm này bao gồm các hướng dẫn để đảm bảo sự cẩn thận và đầy đủ trong việc kiến trúc hệ thống, ví dụ:
- phòng thủ theo chiều sâu (nhiều lớp);
- phòng thủ theo chiều rộng (đa dạng), bảo vệ đồng đều;
- phân vùng hệ thống (ví dụ: phân đoạn mạng);
- sử dụng đóng gói để quản lý quyền truy cập vào các chức năng;
- giám sát, phát hiện và báo cáo các bất thường, bao gồm cả việc sử dụng các honeypot (mồi nhử để phát hiện và phân tích hành vi của kẻ tấn công);
- đánh giá lỗ hổng và kiểm thử xâm nhập;
- sử dụng một phương pháp kỹ thuật an toàn;
- vòng đời hệ thống an toàn;
- vá lỗi thường xuyên/kịp thời.

m) Trách nhiệm giải trình: khái niệm này bao gồm các hướng dẫn để đảm bảo sự cẩn thận trong việc cấp và giám sát quyền truy cập vào tài sản trong quá trình vận hành. Nó cũng bao gồm trách nhiệm báo cáo và giảm thiểu các lỗ hổng đã biết, ví dụ:
- kết nối một cách cẩn thận và có chủ ý;
- đảm bảo phân chia nhiệm vụ;
- thiết lập và bảo vệ các dấu vết kiểm toán;
- thực hành minh bạch (ví dụ: công bố của nhà cung cấp, công bố vi phạm).

n) Khả năng phục hồi: khái niệm này bao gồm các hướng dẫn để đảm bảo khả năng chống lại hoặc phục hồi từ một sự cố bảo mật, ví dụ:
- thiết kế cho dự phòng;
- quản lý tính sẵn sàng;
- giả định vi phạm;
- thất bại một cách an toàn (ví dụ: mất thiết bị hoặc kết nối);
- quản lý lỗ hổng;
- sao lưu và phục hồi;

- kiểm thử khả năng mở rộng.

7.1.2.8 Môi trường và quy trình phát triển an toàn

Biên pháp kiểm soát-08

Môi trường và quy trình phát triển an toàn cần được áp dụng cho việc phát triển các hệ thống IoT.

Mục đích

Tránh đưa các lỗ hổng bảo mật vào các hệ thống IoT trong quá trình phát triển.

Đối tượng: Nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ hoặc Cảm biến và Điều khiển.

Hướng dẫn

Một môi trường phát triển bao gồm con người, quá trình, công nghệ và cơ sở vật chất liên quan đến việc phát triển một hệ thống.

Nhà phát triển dịch vụ IoT cần đánh giá các rủi ro trong từng nỗ lực phát triển hệ thống IoT riêng lẻ và thiết lập các môi trường phát triển an toàn xem xét:

a) nhân sự làm việc trong môi trường;
b) các phương pháp luận phát triển được áp dụng và các quá trình xử lý phần mềm và dữ liệu;
c) sử dụng các sản phẩm và dịch vụ thuê ngoài;
d) môi trường vật lý và mạng; và
e) sự tương thích với các nỗ lực phát triển và vận hành khác.

Nhà phát triển dịch vụ IoT cần xác định môi trường phát triển và các quy trình liên quan để giảm thiểu các rủi ro. Các quy trình cần được phổ biến cho các cá nhân tham gia vào các nỗ lực phát triển.

Các quy trình phát triển phần mềm an toàn cần được áp dụng cho việc phát triển phần mềm IoT. Các phương pháp luận hỗ trợ các quy trình, không giới hạn ở những ứng dụng IoT, bao gồm những phương pháp giải quyết:

f) vòng đời phát triển phần mềm an toàn;
g) mô hình hóa mối đe dọa; và
h) lập trình an toàn.

Các quy trình phát triển phần mềm an toàn có thể được hỗ trợ bởi các công cụ môi trường phát triển tích hợp (IDE) và lập trình an toàn hỗ trợ việc triển khai các phương pháp luận.

7.1.2.9 Bảo mật của hệ thống IoT hỗ trợ an toàn

Biện pháp kiểm soát-09

Các nguyên tắc bảo mật hỗ trợ an toàn cần được áp dụng cho việc phát triển các hệ thống IoT.

Mục đích

Hỗ trợ an toàn trong các hệ thống IoT.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Trong một hệ thống IoT, các sự kiện và biện pháp kiểm soát có thể ảnh hưởng đến an toàn của hệ thống IoT, ví dụ:

a) dữ liệu điều khiển không chính xác hoặc bị hỏng có thể gây ra sự cố của hệ thống IoT;
b) cuộc tấn công bảo mật có thể làm cho chức năng an toàn của hệ thống IoT không hoạt động được; và

c) việc triển khai một biện pháp kiểm soát bảo mật có thể ảnh hưởng đến hiệu suất của hệ thống IoT và các chức năng an toàn của nó.

Nhà phát triển dịch vụ IoT cần xem xét các nguy cơ trong hệ thống IoT có thể ảnh hưởng đến hoạt động của hệ thống IoT và các chức năng an toàn của hệ thống đó như là những hậu quả có thể xảy ra của các sự kiện bảo mật.

Nhà phát triển dịch vụ IoT cũng cần xem xét các tác động của các biện pháp kiểm soát bảo mật đã triển khai đối với hoạt động của hệ thống IoT và các chức năng an toàn của hệ thống đó.

Thông tin khác

Có trường hợp "an toàn" được ưu tiên hơn "bảo mật". Điều này có thể được đề cập trong các tiêu chuẩn của ISO/IEC JTC 1/SC 41.

7.1.2.10 Bảo mật khi kết nối các thiết bị IoT đa dạng

Biện pháp kiểm soát-10

Một hệ thống IoT cần được thiết kế và triển khai để đảm bảo và duy trì bảo mật khi kết nối các thiết bị IoT đa dạng.

Mục đích

Duy trì bảo mật của hệ thống IoT khi kết nối các thiết bị IoT đa dạng, bao gồm cả những thiết bị không nhất thiết được xác minh bởi nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT thiết kế và triển khai một hệ thống IoT và yêu cầu các thiết bị IoT phải đáp ứng các thông số kỹ thuật đã xác định. Các thiết bị IoT được kiểm thử như là các thành phần của hệ thống IoT.

Có khả năng các thiết bị IoT chưa được kiểm thử như là các thành phần của hệ thống IoT vẫn được chấp nhận (đưa vào sử dụng). Điều này có thể xảy ra vì việc kiểm thử tất cả các mẫu thiết bị mới được hỗ trợ có thể không khả thi trên thực tế. Hoặc, người dùng IoT, với tư cách là người tiêu dùng, có thể chọn các thiết bị có sẵn trên thị trường.

Nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT cần thiết kế và triển khai hệ thống IoT an toàn được chuẩn bị trước cho tình huống này. Hệ thống IoT có thể có các khả năng sau đây khi cần thiết:

a) kết nối có chọn lọc thiết bị IoT thông qua danh sách cho phép (whitelist); hoặc
b) khi thích hợp, thu thập các thông số kỹ thuật (đặc tả) của thiết bị, ví dụ như tên nhà cung cấp, mẫu mã (model), năm sản xuất, sự tuân thủ với tiêu chuẩn liên quan và việc sử dụng các thực hành tốt nhất, khi thỏa thuận với thiết bị để kết nối và xác định xem yêu cầu kết nối có được chấp nhận hay từ chối, hoặc giới hạn phạm vi chức năng, dịch vụ hoặc thông tin sẽ được cung cấp sẵn.

7.1.2.11 Xác minh thiết bị IoT và thiết kế hệ thống

Biện pháp kiểm soát-11

Thiết kế và triển khai của các thiết bị IoT và hệ thống IoT cần được xác minh.

Mục đích

Đảm bảo bảo mật và an toàn cho thiết bị IoT và hệ thống IoT.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Một hệ thống IoT cấu thành từ các thiết bị IoT và các thiết bị khác. Trong trường hợp nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT thu thập và tích hợp các thiết bị IoT để xây dựng hệ thống IoT, họ cần xác minh rằng các thiết bị IoT và hệ thống IoT sau khi tích hợp hoạt động như dự kiến.

Nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT cần:

a) xác định các thiết bị IoT, các chức năng và giao diện cần được xác minh;
b) lập kế hoạch kiểm thử; và
c) thực hiện kiểm thử.

7.1.2.12 Giám sát và ghi nhật ký

Biện pháp kiểm soát-12

Các trạng thái, sự kiện và lưu lượng mạng của các thiết bị và hệ thống IoT cần được giám sát và ghi nhật ký.

Mục đích

Phát hiện và theo dõi các bất thường và sự cố của các thiết bị và hệ thống IoT.

Đối tượng: Nhà cung cấp dịch vụ IoT hoặc nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và Quản lý.

Hướng dẫn

Việc giám sát và ghi nhật ký cần được thiết kế và triển khai giải quyết các khía cạnh sau:

a) các chức năng và hoạt động để giám sát và ghi nhật ký các trạng thái, sự kiện và lưu lượng mạng của các hệ thống và thiết bị IoT bao gồm các cảm biến và bộ truyền động;
b) các chức năng và quá trình để phân tích nhật ký;
c) phản ứng của hệ thống, con người và tổ chức được kích hoạt bởi các phát hiện bất thường và sự cố được phát hiện. Các trạng thái, sự kiện và thông tin liên lạc cần được giám sát và ghi nhật ký có thể bao gồm những điều sau:
d) bảo mật;
- xác thực người dùng;
- vị trí của các thiết bị IoT;
- thay đổi cấu hình hệ thống IoT;
- lưu lượng mạng;
- sử dụng bộ xử lý và bộ nhớ;
- dấu hiệu của các cuộc tấn công và truy cập trái phép;
- sự cố;
- các giá trị vượt quá ngưỡng bình thường của dữ liệu cảm biến và truyền động;
- các giá trị chỉ ra bất kỳ sự can thiệp trái phép hoặc không chủ ý nào của dữ liệu cảm biến và truyền động; và

e) độ tin cậy;
- sự cố ngừng/gián đoạn hoạt động của thiết bị hoặc hệ thống IoT; và
- các điều kiện môi trường, ví dụ như nhiệt độ và độ ẩm.

Nếu một thiết bị IoT có khả năng tự xác định vị trí/định vị, tính năng này cần được sử dụng để giám sát việc di chuyển ngoài ý muốn của thiết bị.

Các tài nguyên có sẵn cho tính toán, lưu trữ và truyền thông cần được xem xét và các yêu cầu khác nhau về giám sát và ghi nhật ký cần được ưu tiên khi thiết kế các chức năng giám sát và ghi nhật ký. Cần lưu ý rằng có những thiết bị IoT có tài nguyên và chức năng hạn chế và không khả thi cho việc tự giám sát và ghi nhật ký. Đối với những thiết bị này, việc giám sát và ghi nhật ký cần được thiết kế để được thực hiện trên các máy chủ hoặc các nút mạng của hệ thống IoT.

Nhật ký của một hệ thống IoT có thể được thu thập trong một hệ thống ghi nhật ký để thuận tiện cho việc quản lý và vận hành. Các thiết bị IoT đặt ngoài cơ sở của nhà cung cấp dịch vụ IoT có thể bị gặp rủi ro trong việc duy trì nhật ký.

Đồng hồ trong một hệ thống IoT cần được đồng bộ hóa để đảm bảo phân tích nhất quán.

Đảm bảo thiết lập giám sát đầy đủ đối với các cảm biến IoT, bộ truyền động IoT và các thiết bị khác nhằm phát hiện sớm các sự cố ngừng hoạt động, trục trặc kỹ thuật hoặc các giá trị vượt quá ngưỡng bình thường - đây là những dấu hiệu cho thấy có sự truy cập trái phép hoặc không chủ ý, cũng như các hành vi thao túng dữ liệu cảm biến hoặc truyền động.

Cần đưa các thành phần IoT vào các hoạt động ghi nhật ký và giám sát nhằm xác định sớm mọi hành vi đáng ngờ của các thành phần này. Quá trình này cần bao gồm cả việc nhận diện các dấu hiệu truy cập trái phép cũng như các hành vi thao túng dữ liệu cảm biến hoặc dữ liệu bộ truyền động.

7.1.2.13 Bảo vệ nhật ký

Biện pháp kiểm soát-13

Nhật ký cho các thiết bị và hệ thống IoT cần được bảo vệ khỏi rò rỉ, phá hủy và thay đổi ngoài ý muốn.

Mục đích

Đảm bảo khả năng và độ tin cậy của việc ghi nhật ký.

Đối tượng: Nhà cung cấp dịch vụ IoT hoặc nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và Quản lý.

Hướng dẫn

Việc bảo vệ nhật ký cho các thiết bị và hệ thống IoT cần được thiết kế và triển khai. Các biện pháp để bảo vệ nhật ký có thể bao gồm:

a) kiểm soát truy cập của tệp nhật ký;
b) kiểm soát truy cập của thiết bị hoặc hệ thống xử lý nhật ký;
c) kiểm soát truy cập vật lý vào cơ sở lưu trữ phương tiện ghi nhật ký;
d) thực thi các quy trình xử lý nhật ký;
e) cấu hình dự phòng cho nhật ký;
f) phát hiện sự phá hủy hoặc thay đổi của nhật ký, ví dụ như sử dụng các giá trị băm;
g) mã hóa nhật ký;
h) các mục trong nhật ký có dấu thời gian; và
i) các tệp nhật ký chỉ nên ở chế độ "chỉ đọc" cho tất cả các đối tượng ngoại trừ tiến trình hệ thống.

7.1.2.14 Sử dụng các mạng phù hợp cho các hệ thống IoT

Biện pháp kiểm soát-14

Các công nghệ mạng và truyền thông được áp dụng cho hệ thống và thiết bị IoT cần phải đáp ứng các yêu cầu về chức năng truyền thông, dung lượng và bảo mật, cũng như chức năng và hiệu năng của các thiết bị IoT.

Mục đích

Sử dụng mạng đáp ứng các nhu cầu về bảo mật, hiệu suất và các yêu cầu khác của hệ thống IoT.

Đối tượng: Nhà cung cấp dịch vụ IoT hoặc nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ hoặc Truy cập và Trao đổi Tài nguyên.

Hướng dẫn

Nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT cần xác định các yêu cầu về bảo mật, hiệu suất và các yêu cầu khác cho mạng. Các yêu cầu có thể liên quan đến:

a) vị trí địa lý của các thiết bị và hệ thống IoT;
b) tính di động của các thiết bị IoT;
c) các hạn chế về hiệu suất và chức năng của các thiết bị IoT sẽ được kết nối;
d) tính bảo mật và toàn vẹn của thông tin trong quá trình truyền tải;
e) tính sẵn sàng của quá trình truyền thông; và

f) băng thông của mạng.

Để đáp ứng các yêu cầu đã xác định, nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT cần xem xét:

g) lựa chọn thiết bị và dịch vụ truyền thông phù hợp, xem xét đến phạm vi phủ sóng, yêu cầu về truyền thông không dây và băng thông;
h) áp dụng mã hóa cho thông tin được truyền tải; và
i) sử dụng thiết bị cổng kết nối (gateway) để hỗ trợ thiết bị IoT có các chức năng hạn chế.

7.1.2.15 Các thiết lập và cấu hình an toàn trong quá trình phân phối thiết bị và dịch vụ IoT

Biên pháp kiểm soát-15

Các thiết bị và dịch vụ IoT cần được phân phối với các thiết lập và cấu hình an toàn.

Mục đích

Đảm bảo bảo mật của các thiết bị và dịch vụ IoT trong quá trình phân phối.

Đối tượng: Nhà cung cấp dịch vụ IoT hoặc nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Các thiết lập và cấu hình ban đầu của các thiết bị và dịch vụ IoT cần được thiết kế để góp phần vào việc bảo mật cho người dùng IoT.

Tùy thuộc vào các tính năng của thiết bị hoặc dịch vụ IoT, các cài đặt và cấu hình liên quan có thể bao gồm:

a) các phiên bản và bản vá của phần mềm;
b) các cổng mở và dịch vụ mạng; và
c) hạn chế truy cập vào các chức năng và dữ liệu của dịch vụ.

Nếu thiết bị hoặc dịch vụ IoT yêu cầu người dùng IoT nhập mật khẩu, giá trị khởi tạo của nó cần là duy nhất đối với từng thiết bị hoặc duy nhất đối với từng người dùng dịch vụ. Giá trị khởi tạo cần được thông báo cho người dùng IoT một cách an toàn.

7.1.2.16 Xác thực người dùng và thiết bị

Biện pháp kiểm soát-16

Chức năng xác thực của người dùng và thiết bị IoT để truy cập vào các hệ thống và dịch vụ IoT cần được triển khai và áp dụng.

Mục đích

Bảo vệ thông tin, thiết bị, hệ thống và dịch vụ IoT khỏi truy cập trái phép và các vi phạm bảo mật khác.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Yêu cầu xác thực người dùng IoT và thiết bị IoT cần được xác định dựa trên xem xét quá trình vận hành của dịch vụ IoT và các rủi ro bảo mật liên quan. Các yêu cầu này có thể bao gồm những yêu cầu xác thực đối với:

a) một người dùng là con người để truy cập vào thiết bị, hệ thống hoặc dịch vụ IoT; và
b) một thiết bị IoT khi kết nối vào hệ thống IoT.

Các công nghệ có thể áp dụng để triển khai mức độ xác thực theo yêu cầu có thể là:

c) đối với người dùng là con người, sử dụng:
- xác thực bằng mật khẩu;
- thông tin xác thực phần cứng, ví dụ như thẻ IC; hoặc
- sinh trắc học;

d) đối với các thiết bị IoT, sử dụng:
- định danh thiết bị; hoặc
- neo tin cậy sử dụng các biện pháp bảo vệ phần cứng.

Chức năng xác thực cần an toàn:

e) Quản lý mật khẩu cần an toàn trước việc sử dụng trái phép: quy trình giao nhận mật khẩu ban đầu và thay đổi mật khẩu cần an toàn, và cần áp dụng mật khẩu mạnh.
f) Thông tin xác thực cần được bảo vệ đầy đủ chống lại truy cập trái phép bất kể nó được lưu trữ trong thiết bị hoặc hệ thống IoT hay đang trong quá trình truyền tải.

7.1.2.17 Cung cấp các bản cập nhật phần mềm và phần sụn

Biện pháp kiểm soát-17

Cơ chế cập nhật phần mềm và phần sụn cho các thiết bị và hệ thống IoT cần được thiết kế, triển khai và vận hành.

Mục đích

Đảm bảo bảo mật cho việc cập nhật phần mềm và phần sụn của thiết bị và hệ thống IoT.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ hoặc Cảm biến và Điều khiển.

Hướng dẫn

Trong quá trình phát triển dịch vụ IoT, cơ chế cập nhật phần mềm và phần sụn của các thiết bị IoT cần được thiết kế và triển khai như một chức năng cơ bản.

Các bản cập nhật phần mềm và phần sụn cần được cung cấp thông qua nguồn và kênh đáng tin cậy như trang web được chứng nhận của nhà phát triển thiết bị IoT hoặc nhà cung cấp dịch vụ IoT.

Gói cập nhật phần mềm/phần sụn cần có chữ ký số, chứng chỉ ký và chuỗi chứng chỉ ký được thiết bị xác minh trước khi quá trình cập nhật bắt đầu.

Tính toàn vẹn và tính bí mật của các khóa mật mã được sử dụng để cập nhật cần được quản lý an toàn và vận hành một cách phù hợp.

Khi các bản cập nhật được thực hiện qua vô tuyến (OTA), các bản cập nhật cần được thực hiện qua các kênh truyền thông được mã hóa.

Khi thiết bị không thể tự xác minh tính xác thực của các bản cập nhật, nó cần khôi phục về cấu hình hoạt động ổn định gần nhất đã được lưu trữ trên thiết bị.

Các bản cập nhật sử dụng OTA cần thành công hoàn toàn hoặc nếu thất bại thì có thể phục hồi được. Ngoài ra, việc thực hiện các bản cập nhật không nên làm giảm mức độ bảo mật hiện có của các thiết bị và hệ thống IoT.

Cơ chế khôi phục lại phần mềm và phần sụn cũng cần được thiết kế và triển khai để giải quyết các trường hợp cập nhật thất bại.

Cần có một cơ chế để ngăn chặn việc hạ cấp hoặc quay trở lại một phiên bản cũ hơn một cách trái phép trong quá trình hoạt động bình thường.

7.1.2.18 Chia sẻ thông tin về lỗ hổng bảo mật

Biên pháp kiểm soát-18

Các lỗ hổng bảo mật của các thiết bị, hệ thống và dịch vụ IoT cần được giám sát và thông báo cho người dùng IoT và các bên liên quan cùng với các rủi ro liên quan.

Mục đích

Đảm bảo các bên liên quan được thông báo về các lỗ hổng của các thiết bị, hệ thống và dịch vụ IoT và nhận thức được các rủi ro phát sinh.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Thông tin về các lỗ hổng bảo mật cần được thu thập, phân tích và phổ biến đến các bên liên quan trong hệ sinh thái IoT; cuối cùng, cần thực hiện các biện pháp cần thiết như cập nhật phần sụn (xem mục 7.1.2.17).

Các nhà phát triển dịch vụ IoT và các nhà cung cấp dịch vụ IoT cần có các chức năng để:

a) điều tra các sự cố bảo mật liên quan đến dịch vụ IoT và xác định lỗ hổng của hệ thống hoặc thiết bị IoT có thể gây ra các sự cố;
b) thu thập thông tin về lỗ hổng bảo mật từ các nhà phát triển dịch vụ IoT cung cấp các thành phần của hệ thống, Trung tâm chia sẻ và phân tích thông tin (ISAC) và các bên liên quan khác;
c) phân tích tác động của thông tin về lỗ hổng thu được đối với các thiết bị/hệ thống và dịch vụ IoT;
d) dựa trên kết quả phân tích lỗ hổng và tác động của nó đối với người dùng IoT và các bên liên quan, xác định xem có cần thông báo cho họ hay không.

7.1.2.19 Các biện pháp bảo mật được điều chỉnh theo vòng đời của hệ thống và dịch vụ IoT

Biện pháp kiểm soát-19

Các biện pháp bảo mật của hệ thống và dịch vụ IoT cần được điều chỉnh và duy trì trong các giai đoạn của vòng đời, bao gồm phát triển, vận hành, bảo trì và hủy bỏ.

Mục đích

Duy trì bảo mật của hệ thống và dịch vụ IoT trong suốt vòng đời.

Đối tượng: Nhà cung cấp dịch vụ IoT hoặc nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và Quản lý hoặc Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Trong quá trình phát triển, các biện pháp bảo mật của hệ thống và dịch vụ IoT cần được thiết kế và triển khai theo các nguyên tắc kỹ thuật xây dựng hệ thống IoT bảo mật (7.1.2.7) và các biện pháp kiểm soát liên quan được đưa ra trong 7.1.2.8 đến 7.1.2.14.

Để chuẩn bị cho việc vận hành, bảo trì và hủy bỏ, nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT cần xác định các thực thể liên quan bao gồm người dùng IoT và các nhà phát triển và cung cấp dịch vụ IoT khác mà thông tin bảo mật phải được trao đổi.

Khi hệ thống và dịch vụ IoT được cài đặt và vận hành, các cấu hình và cài đặt bảo mật cần được thực thi liên tục. Điều này cần được hỗ trợ bằng cách chia sẻ thông tin về:

a) tăng cường bảo mật hệ thống và dịch vụ IoT;
b) sử dụng mật khẩu an toàn hoặc các thông tin xác thực người dùng khác;
c) các lỗ hổng bảo mật đã được công bố;
d) các bản cập nhật phần mềm;
e) các cảnh báo bảo mật và các giải pháp tạm thời; và
f) chấm dứt hỗ trợ kỹ thuật cho các thiết bị và phần mềm bởi các nhà cung cấp.

Khi hệ thống, dịch vụ hoặc các thành phần IoT kết thúc vòng đời:

g) thông tin bí mật cần được tiêu hủy một cách an toàn; và

h) người dùng IoT cần được thông báo về quá trình cần tuân theo khi chấm dứt hệ thống và dịch vụ IoT.

7.1.2.20 Hướng dẫn cho người dùng IoT về việc sử dụng đúng cách các thiết bị và dịch vụ IoT

Biện pháp kiểm soát-20

Người dùng IoT cần được cung cấp hướng dẫn về việc sử dụng đúng cách các thiết bị IoT cùng với các rủi ro và các tác động không mong muốn của hệ thống và dịch vụ IoT có thể phát sinh từ việc sử dụng không đúng cách các thiết bị IoT.

Mục đích

Làm cho người dùng IoT nhận thức được các rủi ro bảo mật trong việc sử dụng các thiết bị IoT và để đảm bảo việc triển khai các biện pháp bảo mật.

Đối tượng: Nhà cung cấp dịch vụ IoT hoặc nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Các nhà phát triển dịch vụ IoT và các nhà cung cấp dịch vụ IoT có trách nhiệm về bảo mật tương ứng với vai trò của họ trong việc phát triển và cung cấp dịch vụ IoT. Trong việc sử dụng các thiết bị IoT, một số biện pháp bảo mật cần được thực hiện bởi người dùng IoT. Để hỗ trợ người dùng IoT, các nhà phát triển dịch vụ IoT và các nhà cung cấp dịch vụ IoT cần cung cấp thông tin về các rủi ro và hậu quả và hướng dẫn sử dụng đúng cách các thiết bị IoT.

Các rủi ro và các hành động cần thiết để giảm thiểu các rủi ro cần được thông báo cho người dùng IoT trước khi bắt đầu cung cấp dịch vụ.

Các rủi ro và các hành động cần thiết có thể bao gồm những điều liên quan đến:

a) các thiết bị IoT được hỗ trợ;
b) các phiên bản và mức độ tùy chỉnh được hỗ trợ của phần mềm;
c) các yêu cầu về thiết lập khởi tạo và đăng ký người dùng;
d) sử dụng an toàn hệ thống và dịch vụ IoT;
e) các rủi ro bảo mật gây ra bởi việc sử dụng không đúng cách hệ thống và thiết bị IoT và
f) điểm liên hệ của nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT có thể truy cập trong quá trình vận hành.

Đặc biệt, các thay đổi về các thiết lập và cấu hình do người dùng IoT thực hiện cần được hướng dẫn kèm theo thông tin hỗ trợ nhằm góp phần vào việc sử dụng thiết bị hoặc dịch vụ một cách an toàn.

Người dùng IoT cần được hướng dẫn để thay đổi mật khẩu khởi tạo. Việc thay đổi mật khẩu khởi tạo có thể được bắt buộc theo quy trình khi thích hợp.

Hướng dẫn có thể bao gồm:

g) các thiết bị và cấu hình đã được xác minh để sử dụng trong hệ thống và dịch vụ IoT;
h) các bản cập nhật bảo mật cần thiết cho phần mềm;
i) cài đặt (chẳng hạn như cho Wi-Fi) và cấu hình an toàn; và
j) tiêu chí cho mật khẩu hợp lệ.

Các rủi ro và hậu quả được cung cấp cho người dùng IoT có thể bao gồm nhưng không giới hạn ở:

k) lây nhiễm mã độc trên thiết bị IoT;
l) rò rỉ thông tin cá nhân của người dùng IoT;
m) rò rỉ thông tin kinh doanh; và
n) sử dụng thiết bị IoT nhiễm mã độc cho tấn công từ chối dịch vụ (DoS).

Thông tin bảo mật được cung cấp bởi nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT cần là một phần của hướng dẫn sử dụng/quản trị của sản phẩm hoặc dịch vụ.

7.1.2.21 Xác định vai trò bảo mật cho các bên liên quan

Biện pháp kiểm soát-21

Vai trò của nhà phát triển dịch vụ IoT, nhà cung cấp dịch vụ IoT và các bên liên quan khác trong bảo mật hệ thống và dịch vụ IoT cần được xác định và thống nhất giữa các bên liên quan.

Mục đích

Đảm bảo bảo mật của hệ thống và dịch vụ IoT có sự tham gia của các thực thể tham gia vào việc cung cấp và sử dụng hệ thống và dịch vụ IoT.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Vai trò của nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT trong bảo mật cần được xác định cùng với vai trò của họ trong việc cung cấp dịch vụ IoT.

Nhà phát triển dịch vụ IoT cần có vai trò bảo mật trong việc phát triển, triển khai, kiểm thử và tích hợp dịch vụ IoT. Nhà cung cấp dịch vụ IoT cần có vai trò bảo mật trong việc quản lý và vận hành dịch vụ IoT. Các vai trò phụ của nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT cần được phân công với các vai trò bảo mật khi cần thiết.

Các vai trò bảo mật cần được truyền thông/thông báo đến các bên liên quan bao gồm cả người dùng IoT.

Việc thông báo có thể dưới dạng:

a) thông số kỹ thuật dịch vụ được cung cấp cho người dùng IoT; hoặc
b) thỏa thuận giữa các bên trong chuỗi cung ứng cho dịch vụ IoT.

Vai trò bảo mật của người dùng IoT có thể được thực thi trong quy trình thiết lập ban đầu thông qua việc yêu cầu một hành động như là xác nhận vai trò bảo mật.

7.1.2.22 Quản lý các thiết bị dễ bị tấn công

Biên pháp kiểm soát-22

Các thiết bị IoT dễ bị tấn công cần được phát hiện, ghi lại và cần cung cấp cảnh báo cho người dùng IoT và quản trị viên của các thiết bị này.

Mục đích

Duy trì các thiết bị IoT an toàn.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý.

Hướng dẫn

Nhà cung cấp dịch vụ IoT cần phát triển và thiết lập các cơ chế để:

a) phát hiện và ghi lại các thiết bị IoT dễ bị tấn công; và
b) cung cấp cảnh báo cho người dùng IoT và quản trị viên của các thiết bị.

Trong quá trình vận hành, các thiết bị IoT cần được giám sát liên tục để phát hiện các hành vi bất thường. Khi bất kỳ hành vi đáng ngờ nào được phát hiện, hành vi đó cần được ghi lại và cảnh báo cần được thông báo cho người dùng IoT và quản trị viên.

Bao gồm các thiết bị IoT trong các quá trình quản lý lỗ hổng bảo mật để đảm bảo việc xác định và xử lý đầy đủ bất kỳ lỗ hổng bảo mật nào có trong các thiết bị.

7.1.2.23 Quản lý mối quan hệ với nhà cung cấp trong bảo mật IoT

Biện pháp kiểm soát-23

Các thông số kỹ thuật và các nghĩa vụ hỗ trợ của các nhà cung cấp đối với an toàn thông tin của thiết bị IoT và dịch vụ IoT cần được quản lý bởi tổ chức mua sắm dựa trên các hợp đồng với các nhà cung cấp.

Mục đích

Đảm bảo việc cung cấp liên tục thiết bị và dịch vụ IoT an toàn.

Đối tượng: Nhà cung cấp dịch vụ IoT hoặc nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Khi một nhà phát triển dịch vụ IoT hoặc một nhà cung cấp dịch vụ IoT mua sắm các thiết bị IoT và dịch vụ IoT, một cơ chế cần được thiết lập cho phép tổ chức mua sắm xác định các thông số kỹ thuật và các biện pháp kiểm soát bảo mật được triển khai bởi nhà cung cấp và các biện pháp kiểm soát bảo mật mà tổ chức mua sắm phải triển khai. Các thông số kỹ thuật và biện pháp kiểm soát bảo mật này cần bao gồm:

a) quản lý lỗ hổng bảo mật;
b) cập nhật phần sụn;
c) các thay đổi hệ thống do thay đổi thông số kỹ thuật của các thiết bị IoT; và
d) việc cung cấp thông tin liên quan cho người dùng IoT. Khi phát triển cơ chế này, việc quản lý phù hợp dựa trên các hợp đồng cần được tiến hành để thông tin cần thiết có thể được thu thập một cách đáng tin cậy từ các nhà cung cấp.

Khi một nhà phát triển thiết bị IoT tạm ngừng cung cấp các thiết bị IoT hoặc thay đổi đáng kể các thông số kỹ thuật của chúng, thông báo cần được cung cấp với thời gian đủ để các tổ chức mua sắm có thể đưa ra quyết định phù hợp.

7.1.2.24 Công bố một cách an toàn thông tin liên quan đến bảo mật của các thiết bị IoT

Biện pháp kiểm soát-24

Thông tin về thiết bị IoT liên quan đến bảo mật của các dịch vụ IoT cần được lập thành văn bản và chỉ được công bố cho các bên có nhu cầu.

Mục đích

Đảm bảo bảo mật của các dịch vụ IoT sử dụng thiết bị IoT.

Đối tượng: Nhà phát triển thiết bị IoT.

Miền IoT: Cảm biến và Điều khiển.

Hướng dẫn

Thông tin về thiết bị IoT liên quan đến bảo mật của các dịch vụ IoT cần được công bố cho các nhà phát triển dịch vụ IoT và các nhà cung cấp dịch vụ IoT có liên quan để hỗ trợ việc phát triển và triển khai các biện pháp kiểm soát bảo mật của các dịch vụ IoT.

Đối với việc lập kế hoạch và phát triển các dịch vụ IoT, thông tin sau đây về thiết bị IoT cần được công bố:

a) các thông số kỹ thuật bao gồm cả các chức năng bảo mật;
b) tính sẵn có của các bản cập nhật phần mềm hoặc phần sụn; và
c) thời gian bảo hành.

Để vận hành và bảo trì các dịch vụ IoT, thông tin sau đây về thiết bị IoT cần được công bố:

d) các lỗ hổng mới được phát hiện;
e) các bản nâng cấp của phần mềm hoặc phần sụn; và
f) chấm dứt sản xuất hoặc giao hàng.

Thông tin này cần được lập thành văn bản để có thể được chuyển giao một cách chính xác.

Thông tin cần được công bố theo một hợp đồng như thỏa thuận không tiết lộ để ngăn chặn việc rò rỉ thông tin cho các bên thứ ba có ý đồ xấu.

7.1.3 Các biện pháp kiểm soát bảo mật cho người dùng IoT

7.1.3.1 Liên hệ và dịch vụ hỗ trợ

Biện pháp kiểm soát-25

Người dùng IoT chỉ nên chọn các thiết bị IoT và dịch vụ IoT có cung cấp thông tin liên hệ cho dịch vụ hỗ trợ.

Mục đích

Đảm bảo bảo mật trong việc sử dụng thiết bị và dịch vụ IoT.

Đối tượng: Người dùng IoT.

Miền IoT: Người dùng.

Hướng dẫn

Người dùng IoT cần có thể truy cập các dịch vụ hỗ trợ cho thiết bị IoT và dịch vụ IoT cung cấp thông tin và trả lời các câu hỏi bao gồm cả những câu hỏi liên quan đến bảo mật (7.1.2.19, 7.1.2.20, 7.1.2.22).

Không nên chọn một thiết bị hoặc dịch vụ IoT nếu không có thông tin về nhà sản xuất hoặc điểm liên lạc cho dịch vụ hỗ trợ. Nhà cung cấp của thiết bị hoặc dịch vụ như vậy không nên được tin cậy để có khả năng loại trừ mã độc và duy trì bảo mật đầy đủ trong suốt vòng đời của thiết bị hoặc dịch vụ.

7.1.3.2 Cài đặt ban đầu của thiết bị và dịch vụ IoT

Biện pháp kiểm soát-26

Các cài đặt ban đầu của thiết bị và dịch vụ IoT cần được áp dụng chính xác.

Mục đích

Đảm bảo các cài đặt ban đầu an toàn của thiết bị và dịch vụ IoT.

Đối tượng: Người dùng IoT.

Miền IoT: Người dùng.

Hướng dẫn

Các thiết lập mặc định của thông tin xác thực như "ID do nhà máy thiết lập" và "mật khẩu mặc định" cho các thiết bị IoT được coi là công khai từ khi tài liệu hướng dẫn sử dụng được công bố rộng rãi. Thông tin xác thực mặc định cần được đặt lại bởi người dùng IoT.

Thiết lập mới không nên giống với cài đặt ban đầu, không nên dùng chung với thiết lập của thiết bị IoT khác và không nên dễ đoán và không nằm trong danh sách ID/mật khẩu phổ biến có sẵn trên internet.

7.1.3.3 Vô hiệu hóa các thiết bị không sử dụng

Biện pháp kiểm soát-27

Các thiết bị IoT cần được vô hiệu hóa và các thông tin xác thực cần được thu hồi khi chúng không còn được sử dụng.

Mục đích

Giảm thiểu các rủi ro bảo mật gây ra bởi thiết bị IoT không còn được sử dụng.

Đối tượng: Người dùng IoT.

Miền IoT: Người dùng.

Hướng dẫn

Các thiết bị IoT không còn được sử dụng nhưng vẫn được kết nối với mạng, có thể bị chiếm quyền kiểm soát và sử dụng mà không bị phát hiện qua mạng bởi các bên thứ ba trái phép. Để giảm thiểu rủi ro tiềm tàng của việc lạm dụng các thiết bị IoT, các thiết bị IoT không còn được sử dụng cần được vô hiệu hóa, ví dụ như tắt thiết bị.

Biện pháp kiểm soát này cần được áp dụng để triển khai đúng giai đoạn "Kết thúc" trong vòng đời của người dùng IoT được đưa ra trong 5.5.

7.1.3.4 Tiêu hủy hoặc tái sử dụng thiết bị IoT một cách an toàn

Biện pháp kiểm soát-28

Dữ liệu và phần mềm được cấp phép lưu trữ trong thiết bị IoT cần được gỡ bỏ hoặc ghi đè một cách an toàn trước khi tiêu hủy hoặc tái sử dụng.

Mục đích

Đảm bảo bảo vệ thông tin khi tiêu hủy hoặc tái sử dụng các thiết bị IoT.

Đối tượng: Người dùng IoT.

Miền IoT: Người dùng.

Hướng dẫn

Thông tin được thu thập và sử dụng trong quá trình vận hành dịch vụ IoT có thể được lưu trữ trong các thiết bị IoT. Để tránh rò rỉ thông tin cho người dùng khác và các bên thứ ba, thông tin được lưu trữ trong các thiết bị IoT cần được xóa, hoặc các thiết bị IoT cần được đặt lại về trạng thái mặc định của nhà sản xuất trước khi tiêu hủy hoặc tái sử dụng các thiết bị IoT.

7.2 Các biện pháp kiểm soát quyền riêng tư

7.2.1 Tổng quan

Các biện pháp kiểm soát quyền riêng tư được khuyến nghị ở đây nằm trong bối cảnh của IoT. Các biện pháp này dành cho nhà phát triển dịch vụ IoT, nhà cung cấp dịch vụ IoT và người dùng IoT. Các biện pháp kiểm soát này phù hợp với ISO/IEC 27701 về các biện pháp kiểm soát cơ bản về quản lý thông tin riêng tư và khác biệt đối với IoT từ các góc độ riêng tư theo thiết kế và riêng tư theo mặc định.

Để mô tả các biện pháp kiểm soát, một định dạng chung được sử dụng:

Biện pháp kiểm soát XX — Biện pháp kiểm soát được nêu, trong đó XX là số thứ tự, được đưa ra để dễ dàng tham chiếu đến biện pháp kiểm soát.

Mục đích - giải thích mục đích của các biện pháp kiểm soát.

Đối tượng - nêu tên các bên liên quan có tham gia và cần được thông báo về biện pháp kiểm soát. Tham khảo 5.3 để biết danh sách các bên liên quan.

Miền IoT - liệt kê các miền mà biện pháp kiểm soát liên quan đến, dựa trên mô hình tham chiếu dựa trên miền được giới thiệu trong 5.6.

Hướng dẫn - cung cấp thông tin hướng dẫn.

7.2.2 Các biện pháp kiểm soát quyền riêng tư cho nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT

7.2.2.1 Ngăn chặn các sự kiện xâm phạm quyền riêng tư

Biện pháp kiểm soát-29

Các tính năng nâng cao quyền riêng tư cần được tích hợp vào các thiết bị IoT và dịch vụ IoT.

Mục đích

Ngăn chặn các sự cố xâm phạm quyền riêng tư trong việc cung cấp và sử dụng các thiết bị IoT và dịch vụ IoT.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Xác định các thành phần dữ liệu nhạy cảm sớm ngay từ giai đoạn thiết kế. Tích hợp các tính năng nâng cao quyền riêng tư vào kiến trúc thiết bị IoT và thiết kế dịch vụ IoT để ngăn chặn các sự cố xâm phạm quyền riêng tư.

7.2.2.2 Quyền riêng tư IoT theo mặc định

Biện pháp kiểm soát-30

Các bên liên quan trong một hệ thống IoT cần đảm bảo rằng ngay cả khi không có bất kỳ sự tương tác hoặc can thiệp nào của người dùng IoT, các thiết lập quyền riêng tư nghiêm ngặt nhất sẽ được áp dụng theo mặc định.

Mục đích

Bảo vệ TTNDCN mà không cần sự tương tác hoặc can thiệp của người dùng.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý hoặc Ứng dụng và Dịch vụ.

Hướng dẫn

Cơ chế kiểm soát truy cập phù hợp cần được tích hợp sẵn trong thiết bị và dịch vụ. Trách nhiệm bảo vệ quyền riêng tư cần thuộc về các nhà phát triển dịch vụ IoT và các nhà cung cấp dịch vụ IoT. Một cài đặt quyền riêng tư mặc định nhằm mục đích bảo vệ TTNDCN mà không cần sự can thiệp của người dùng.

Dựa trên đánh giá tác động đến quyền riêng tư, TTNDCN được thu thập cần được xác định và xử lý một cách phù hợp. Dựa trên những kết quả này, các cơ chế kiểm soát cần được triển khai để bảo vệ TTNDCN theo mặc định và người dùng được tư vấn về những điều này trong một chính sách hoặc tuyên bố người dùng.

7.2.2.3 Cung cấp thông báo về quyền riêng tư

Biên pháp kiểm soát-31-1

Người dùng IoT cần được cung cấp một thông báo về quyền riêng tư mà trong đó nêu rõ dữ liệu cá nhân được thu thập bởi thiết bị IoT và dịch vụ IoT và mục đích sử dụng của dữ liệu đó.

Mục đích

Đảm bảo việc sử dụng dữ liệu cá nhân.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý hoặc Ứng dụng và Dịch vụ.

Hướng dẫn

Trước khi mua hàng, người dùng IoT cần được cung cấp chi tiết về tất cả các dữ liệu dự kiến được thu thập bởi các thiết bị và dịch vụ IoT, bao gồm cả TTNDCN. Điều này cho phép người dùng IoT cơ hội sử dụng sản phẩm / giải pháp một cách thích hợp dựa trên dữ liệu được cung cấp. Thông tin này có thể được cung cấp dưới dạng hợp đồng người dùng, chính sách quyền riêng tư hoặc cơ chế thông báo khác.

Biện pháp kiểm soát-31-2

Sự đồng ý của người dùng IoT đối với thông báo về quyền riêng tư cần được thu thập trước khi thu thập dữ liệu cá nhân hoặc thay đổi mục đích sử dụng.

Mục đích

Đảm bảo việc thu thập và sử dụng dữ liệu cá nhân có được sự đồng ý.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý hoặc Ứng dụng và Dịch vụ.

Hướng dẫn

Người dùng cuối cần được cung cấp một danh sách kiểm tra (checklist) trong đó nêu rõ mục đích, phương pháp và phạm vi thu thập, thời hạn, ai sẽ sử dụng dữ liệu này, cùng với các thông tin khác.

7.2.2.4 Xác minh chức năng IoT

Biện pháp kiểm soát-32

Việc xác minh độc lập đối với thiết bị IoT, các thành phần dữ liệu và dịch vụ IoT cần được cung cấp nhằm mang lại tính minh bạch và tin cậy cho tất cả các bên liên quan rằng thiết bị hoặc dịch vụ IoT đang hoạt động đúng theo các mục tiêu đã đề ra.

Mục đích

Đảm bảo giao diện/chức năng phản ánh chính xác hoạt động (What-You-See-Is-What-You-Get) của các chức năng cho các thiết bị và dịch vụ IoT.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Một phương pháp tiếp cận dựa trên việc xác minh để xây dựng niềm tin đối với các thiết bị và thành phần dữ liệu IoT là cần thiết nhằm đảm bảo tính minh bạch trong quá trình vận hành IoT. Việc cung cấp khả năng xác minh độc lập của thiết bị và dịch vụ IoT mang lại sự minh bạch và đảm bảo cho tất cả các bên liên quan rằng các chức năng IoT đang hoạt động theo các mục tiêu đã đề ra.

7.2.2.5 Xem xét người dùng IoT

Biện pháp kiểm soát-33

Các yêu cầu và mối quan ngại về quyền riêng tư của người dùng cuối cần được giải quyết trong việc thiết kế thiết bị và dịch vụ IoT.

Mục đích

Đảm bảo các yêu cầu và mối quan ngại về quyền riêng tư của người dùng IoT được giải quyết trong thiết bị và dịch vụ IoT đồng thời xây dựng lòng tin của người dùng IoT.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý, Ứng dụng và Dịch vụ, Truy cập và Trao đổi Tài nguyên hoặc Cảm biến và Điều khiển.

Hướng dẫn

Quyền riêng tư là một yêu cầu then chốt của người dùng cuối, một chiến lược 'người dùng là trên hết' trong việc thiết kế các thiết bị và dịch vụ IoT sẽ giúp xây dựng lòng tin và sự tự tin của người dùng để đảm bảo sự chấp nhận rộng rãi.

7.2.2.6 Quản lý các biện pháp kiểm soát quyền riêng tư IoT

Biện pháp kiểm soát-34

Tính hiệu quả của các biện pháp kiểm soát quyền riêng tư trong thiết bị và dịch vụ IoT cần được xem xét và các rủi ro mới về quyền riêng tư cần được nhận diện một cách liên tục dựa trên các nhu cầu quyền riêng tư ngày càng thay đổi của người dùng cuối và các yêu cầu pháp lý.

Mục đích

Chứng minh hiệu quả của các biện pháp kiểm soát quyền riêng tư trong các thiết bị và dịch vụ IoT.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý.

Hướng dẫn

Triển khai các biện pháp kiểm soát bảo mật và quyền riêng tư về mặt kỹ thuật và vận hành đi kèm với việc xác nhận và xác minh các biện pháp kiểm soát này một cách liên tục nhằm đảm bảo các biện pháp kiểm soát này phù hợp theo nhu cầu thực tế.

7.2.2.7 Định danh thiết bị duy nhất

Biện pháp kiểm soát-35-1

Các nhà phát triển hệ thống IoT (đặc biệt là các nhà phát triển thiết bị) cần sử dụng một phương pháp nhận dạng duy nhất cho mỗi thiết bị IoT để nâng cao quyền riêng tư trong việc xác định thiết bị IoT bị nghi ngờ có liên quan đến một sự cố mạng.

Mục đích

Cho phép nhận dạng thiết bị IoT bị nghi ngờ có liên quan đến một sự cố mạng.

Đối tượng: Nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và Quản lý.

Hướng dẫn

Việc nhà cung cấp dịch vụ IoT hoặc người dùng IoT có khả năng giám sát các thiết bị IoT để phát hiện các bất thường, nhân bản thiết bị hoặc đánh tráo thiết bị với ý đồ xấu là rất quan trọng.

Biện pháp kiểm soát-35-2

Các nhà cung cấp dịch vụ IoT nên sử dụng, nếu cần thiết, một phương pháp để cho phép một ánh xạ/liên kết (mapping) duy nhất giữa một thiết bị IoT cụ thể và một người dùng IoT để tăng cường quyền riêng tư trong việc xác định mối liên kết giữa thiết bị IoT và (các) người dùng IoT.

Mục đích

Nhận dạng duy nhất một ánh xạ giữa thiết bị IoT và (các) người dùng IoT.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý.

Hướng dẫn

Thiết bị IoT có thể được sử dụng bởi nhiều hơn một người trong nhiều trường hợp (ví dụ: một chiếc xe được kết nối, một bộ điều nhiệt độ gia đình) và cần phải rõ ràng rằng sự ưu tiên của người dùng nào được coi là hợp lệ khi thiết bị được truy cập.

Một tiêu chuẩn định danh thiết bị và các phương thức để ánh xạ định danh này với từng cá nhân cần được thiết lập. Ánh xạ này cần được duy trì theo cách có thể truy cập được cho những người dùng IoT cần truy cập.

7.2.2.8 Xác thực an toàn khi có lỗi (Fail-safe)

Biện pháp kiểm soát-36

Hệ thống cần đảm bảo rằng cơ chế xác thực đã được triển khai không thể bị vượt qua, can thiệp trái phép hoặc làm giả bằng bất kỳ phương pháp hợp lý nào.

Mục đích

Vì thiết bị (vật) thường không ở cùng với người dùng và hệ quả của việc một người dùng sai (wrong user) kết nối với thiết bị có thể gây ra tổn hại nghiêm trọng về mặt an toàn, tổn thất tài chính, nguy cơ

sức khỏe, v.v. Đối với dịch vụ xác thực truyền thống, kết quả của việc truy cập là hiển nhiên đối với người dùng vì người dùng có thể trực tiếp chứng kiến hệ quả từ hành động của mình.

Đối tượng: Nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý hoặc Ứng dụng và Dịch vụ.

Hướng dẫn

Mặc dù xác thực là một phần của bảo mật dữ liệu, trong trường hợp của IoT, cần thiết lập một cơ chế độc lập để xác nhận rằng thiết bị đúng đã được truy cập và hành động đã được hoàn thành.

7.2.2.9 Giảm thiểu thu thập dữ liệu gián tiếp

Biện pháp kiểm soát-37

Việc thu thập dữ liệu từ các nguồn gián tiếp cần được giảm thiểu hoặc hoàn toàn không thu thập.

Mục đích

Ngăn chặn việc thu thập dữ liệu mà không có sự tham gia và đồng ý của người dùng IoT.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý hoặc Truy cập và Trao đổi Tài nguyên.

Hướng dẫn

Bất kỳ dữ liệu gián tiếp nào được thu thập, được ghi lại mà không có sự tham gia của người dùng, cần được giảm thiểu đến mức tối thiểu cần thiết, trừ khi được người dùng đồng ý một cách rõ ràng.

Trong bối cảnh của một dịch vụ IoT, về mặt kỹ thuật, nhà cung cấp dịch vụ IoT có thể có quyền truy cập vào TTNDCN như địa chỉ IP, vị trí địa lý, nhiệt độ, thông tin ngữ cảnh và thông tin về sự hiện diện của các thiết bị khác trong vùng lân cận.

Nhà cung cấp dịch vụ IoT cần:

a) thiết kế và triển khai các hoạt động của dịch vụ IoT nhằm giới hạn dữ liệu, bao gồm cả TTNDCN, được thu thập trong phạm vi tương thích với mục đích sử dụng đã được thông báo;
b) thông báo cho người dùng IoT về dữ liệu nào được thu thập; và
c) lấy sự đồng ý của người dùng IoT đối với việc thu thập.

7.2.2.10 Thông báo các tùy chọn về quyền riêng tư

Biên pháp kiểm soát-38

Các tùy chọn của người dùng về các biện pháp kiểm soát quyền riêng tư chỉ nên được thêm vào, sửa đổi hoặc xóa khi người dùng được ủy quyền đã được xác thực vào hệ thống.

Mục đích

Khác với các kịch bản truyền thống, nơi mà các tùy chọn quyền riêng tư được nắm rõ bởi tổ chức thu thập TTNDCN, trong trường hợp của IoT, điều tương tự là không thể bởi vì có nhiều thiết bị và dịch vụ cần truy cập dữ liệu.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý.

Hướng dẫn

Một giao thức kỹ thuật có khả năng tương tác cần được thiết lập để các tùy chọn về quyền riêng tư cho mỗi người dùng được lưu trữ an toàn trong thiết bị và được cung cấp cho các thiết bị hoặc dịch vụ được ủy quyền kết nối với nó. Bất kỳ thay đổi nào đối với các tùy chọn quyền riêng tư chỉ có thể thực hiện được thông qua xác thực bởi duy nhất người dùng đó mà không phải ai khác.

Nhà cung cấp dịch vụ IoT có thể tham khảo ISO/IEC 27556 để được hướng dẫn về cách quản lý các tùy chọn về quyền riêng tư.

7.2.2.11 Xác minh quyết định tự động

Biện pháp kiểm soát-39

Quyết định tự động được cung cấp bởi các dịch vụ IoT cần được xác minh.

Mục đích

Để tránh những thiệt hại không thể khắc phục gây ra bởi quyết định tự động sai lầm của một thiết bị hoặc hệ thống IoT.

Đối tượng: Nhà cung cấp dịch vụ IoT.

Miền IoT: Vận hành và Quản lý.

Hướng dẫn

Một xác minh độc lập thứ cấp cần là điều kiện tiên quyết đối với bất kỳ quyết định tự động nào của một thiết bị hoặc hệ thống IoT có thể dẫn đến thiệt hại không thể khắc phục cho người dùng IoT.

Khi thiệt hại có thể nghiêm trọng, một kiểm tra độc lập sẽ đảm bảo rằng quyết định tự động là chính xác và với đúng người. Ví dụ, nếu một thiết bị IoT đề nghị điều trị y tế bằng quyết định tự động dựa trên cảnh báo cảm biến, cần có một quá trình để xác minh quyết định đó, có tính đến các đầu vào từ các nguồn khác và lỗi tiềm ẩn của cảnh báo. Sự xâm nhập vào hệ thống IoT có thể khiến quyết định tự động đưa ra đề nghị không chính xác.

7.2.2.12 Trách nhiệm giải trình cho các bên liên quan

Biện pháp kiểm soát-40

Trách nhiệm giải trình cho các bên liên quan khác nhau cần được thiết lập.

Mục đích

Để xác định trách nhiệm giữa các bên liên quan của hệ thống IoT. Trong trường hợp xảy ra vi phạm dữ liệu hoặc yêu cầu của chủ thể dữ liệu, thực thể nào sẽ phản hồi, ai sẽ xử lý các yêu cầu tiết lộ dữ liệu, v.v.

Đối tượng: Nhà cung cấp dịch vụ IoT hoặc Nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và Quản lý.

Hướng dẫn

Một khung trách nhiệm giải trình cần được phát triển để xác định một cách nhất quán thực thể nào sẽ chịu trách nhiệm cho phần nào của vòng đời dữ liệu quyền riêng tư.

7.2.2.13 Tính không thể liên kết của TTNDCN (Unlinkability of PII)

Biện pháp kiểm soát-41

Hệ thống IoT cần đảm bảo rằng TTNDCN của người dùng sở hữu thiết bị không thể bị nhận dạng.

Mục đích

Ngăn chặn việc thu thập TTNDCN bằng cách giám sát một thiết bị IoT.

Đối tượng: Nhà cung cấp dịch vụ IoT hoặc Nhà phát triển dịch vụ IoT.

Miền IoT: Vận hành và quản lý hoặc ứng dụng và dịch vụ.

Hướng dẫn

Định danh duy nhất của thiết bị IoT có thể được biểu diễn bằng một biệt danh (pseudonym). Cách tiếp cận này đã được tiêu chuẩn hóa trong các hệ thống giao thông thông minh hợp tác (cooperative ITS). Các định danh duy nhất của phương tiện không thể bị nghe lén.

7.2.2.14 Chia sẻ thông tin về các biện pháp bảo vệ TTNDCN của các thiết bị IoT

Biện pháp kiểm soát-42

Các biện pháp bảo vệ TTNDCN liên quan đến rủi ro riêng tư trong các thiết bị IoT cần được quản lý một cách thích hợp và chỉ được tiết lộ cho các bên có nhu cầu.

Mục đích

Để đảm bảo việc bảo vệ TTNDCN của các dịch vụ IoT sử dụng thiết bị IoT.

Đối tượng: Nhà phát triển thiết bị IoT.

Miền IoT: Cảm biến và Điều khiển.

Hướng dẫn

Nhà phát triển thiết bị IoT cần đảm bảo rằng các đặc tả kỹ thuật và biện pháp kiểm soát bảo vệ TTNDCN liên quan đến rủi ro quyền riêng tư trong các thiết bị IoT được tiết lộ cho các nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT có liên quan. Nếu các đặc tả kỹ thuật và biện pháp kiểm soát này cần được bổ sung hoặc sửa đổi bởi các biện pháp kiểm soát do nhà phát triển dịch vụ IoT hoặc nhà cung cấp dịch vụ IoT triển khai thì tình huống đó cần được chia sẻ giữa các bên liên quan để vấn đề được xử lý một cách phù hợp. Các đặc tả kỹ thuật và biện pháp kiểm soát bảo vệ TTNDCN cho thiết bị IoT cần được tiết lộ một cách phù hợp cho các bên liên quan và được quản lý để ngăn chặn việc rò rỉ cho các bên thứ ba có ý đồ xấu.

7.2.3 Các biện pháp kiểm soát quyền riêng tư cho người dùng IoT

7.2.3.1 Sự chấp thuận của người dùng

Biện pháp kiểm soát-43

Sự đồng ý cho việc sử dụng dữ liệu cá nhân cho thiết bị và dịch vụ IoT chỉ nên được cung cấp sau khi xem xét sự cần thiết và tác động có thể xảy ra nếu có sự vi phạm dữ liệu. Sự chấp thuận nên được thu hồi nếu đầu ra của IoT không còn cần thiết hoặc nếu có lo ngại về thiết bị hoặc dịch vụ IoT.

Mục đích

Để ngăn chặn việc sử dụng TTNDCN bởi thiết bị và dịch vụ IoT mà không có sự chấp thuận của người dùng.

Đối tượng: Người dùng IoT.

Miền IoT: Người dùng.

Hướng dẫn

Các nhà phát triển dịch vụ IoT có thể lập một danh sách những người dùng tiềm năng và phát triển cơ chế để có được sự chấp thuận cho việc sử dụng dữ liệu cá nhân.

Sự chấp thuận có thể bao gồm một trường "thời gian tồn tại" (time-to-live).

7.2.3.2 Sử dụng có mục đích để kết nối với các thiết bị và dịch vụ khác

Biên pháp kiểm soát-44

Việc kết nối thiết bị và dịch vụ IoT với các thiết bị hoặc dịch vụ khác chỉ nên được cho phép nếu có một nhu cầu chính đáng.

Mục đích

Để đảm bảo việc sử dụng có mục đích các thiết bị và dịch vụ IoT.

Đối tượng: Người dùng IoT, Nhà phát triển dịch vụ IoT, Nhà cung cấp dịch vụ IoT.

Miền IoT: Người dùng, Vận hành và Quản lý.

Hướng dẫn

Người dùng IoT cần sử dụng các thiết bị và dịch vụ IoT theo cách phù hợp với nhu cầu chính đáng.

Các nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT cần phát triển và thiết lập các cơ chế để phát hiện và cảnh báo mỗi khi có yêu cầu kết nối với thiết bị hoặc dịch vụ IoT khác mà không có lý do chính đáng (được chỉ ra bởi các thông số của dịch vụ hoặc một số kỹ thuật khác, được coi là phù hợp).

7.2.3.3 Chứng nhận/xác thực việc bảo vệ TTNDCN

Biện pháp kiểm soát-45

Chứng nhận hoặc xác thực các tính năng bảo vệ quyền riêng tư đối với thiết bị và dịch vụ IoT nên được tìm kiếm.

Mục đích

Để đảm bảo rằng các tính năng bảo vệ quyền riêng tư của thiết bị và dịch vụ IoT là đáng tin cậy.

Đối tương: Người dùng IoT.

Miền IoT: Người dùng.

Hướng dẫn

Người dùng IoT nên tìm kiếm chứng nhận hoặc xác thực các tính năng bảo vệ quyền riêng tư của thiết bị và dịch vụ IoT mà họ sẽ sử dụng.

Người dùng IoT cần đảm bảo rằng phạm vi của chứng nhận hoặc xác thực bao gồm các tính năng bảo vệ quyền riêng tư liên quan.

PHỤ LỤC A
(tham khảo)
Kịch bản rủi ro mẫu cho camera giám sát IoT

Kịch bản rủi ro mẫu của một hệ thống IoT được đưa ra trong Bảng A.1. Trong mẫu này, hệ thống IoT mô hình là một hệ thống camera giám sát mà:

- được triển khai trong một cơ sở, ví dụ: một cửa hàng, nhà máy hoặc trường học;
- có các camera kết nối mạng và các máy chủ lưu giữ hình ảnh camera.

Các nhà phát triển dịch vụ IoT và nhà cung cấp dịch vụ IoT có thể sử dụng mẫu này cho mục đích tham khảo trong việc phát triển các kịch bản rủi ro của riêng họ, trong đó sẽ có các yếu tố chi tiết về các nguồn rủi ro, sự kiện và hậu quả. Các kịch bản rủi ro khác nhau cần được cung cấp cho các quan điểm khác nhau để chỉ ra một cách rõ ràng chuỗi nguyên nhân và hậu quả. Ví dụ, kịch bản rủi ro thứ nhất có thể liên quan đến tính bảo mật của thông tin, kịch bản rủi ro thứ hai có thể liên quan đến tính toàn vẹn và tính khả dụng của thông tin và thiết bị và do đó liên quan đến tính liên tục kinh doanh của tổ chức và kịch bản rủi ro thứ ba có thể chứa các cuộc tấn công vào thiết bị của bên thứ ba như là các sự kiện và các tác động tiêu cực đối với chúng như là các hậu quả. Để làm cho kịch bản rủi ro mẫu trong Bảng A.1 trở nên ngắn gọn, nó bao gồm các yếu tố có thể được tách ra thành nhiều kịch bản rủi ro.

Bảng A.1 — Kịch bản rủi ro mẫu của một hệ thống camera giám sát

a) Nguồn rủi ro

1) Nguồn rủi ro liên quan đến cấu hình hệ thống và môi trường
   - Camera được kết nối với các máy chủ qua mạng.
   - Camera được đặt ở những nơi không được bảo vệ về mặt vật lý.
   - Camera được đặt ở những nơi mà các hiện tượng tự nhiên và điều kiện môi trường có thể ảnh hưởng đến hoạt động của camera.

2) Nguồn rủi ro liên quan đến cơ sở hạ tầng thiết yếu
   - Hoạt động của hệ thống phụ thuộc vào nguồn cung cấp điện.
   - Hoạt động của hệ thống phụ thuộc vào các dịch vụ mạng.

3) Nguồn rủi ro liên quan đến chất lượng và chức năng của hệ thống và các thành phần
   - Các camera, các thành phần khác của hệ thống hoặc cấu hình hệ thống có các lỗ hổng bảo mật.
   - Các camera chấp nhận mật khẩu yếu.
   - Các bản cập nhật phần mềm không được áp dụng cho các camera hoặc các thành phần khác.
   - Cấu hình mạng cho phép người không được ủy quyền truy cập vào các camera và các thành phần khác.

4) Nguồn rủi ro liên quan đến nhà cung cấp và chuỗi cung ứng CNTT
   - Các nhà phát triển camera và hệ thống thiếu kiến thức và kỹ năng cần thiết để phát triển hệ thống và ứng dụng an toàn.
   - Các nhà phát triển camera và hệ thống không áp dụng các phương pháp phát triển đã được thiết lập.
   - Hệ thống và các thành phần của nó được sản xuất trong chuỗi cung ứng CNTT.
   - Người dùng không được thông báo đầy đủ về các yêu cầu để sử dụng hệ thống một cách an toàn.

5) Nguồn rủi ro liên quan đến những người tham gia vào việc sử dụng và cung cấp hệ thống
   - Người dùng không có kiến thức và kỹ năng cần thiết để sử dụng và bảo trì hệ thống một cách an toàn.
   - Có thể có lỗi do con người trong quá trình sử dụng hệ thống.

6) Nguồn rủi ro liên quan đến những người có ý đồ xấu

- Có những người có ý đồ xấu nhằm tấn công hoặc lạm dụng hệ thống thông qua mạng.

b) Sự kiện

1) Các sự kiện có nguồn gốc từ bên ngoài

- Nguồn điện gặp sự cố khi đang vận hành.
- Dịch vụ mạng gặp sự cố khi đang vận hành.
- Hệ thống bị tấn công.
- Hệ thống bị xâm nhập.

2) Các sự kiện liên quan đến camera và hệ thống

- Các camera bị hư hỏng do điều kiện thời tiết xấu.
- Các camera bị phá hủy hoặc bị đánh cắp.
- Các camera và hệ thống bị nhiễm phần mềm độc hại (mã độc).
- Hệ thống ngừng hoạt động.
- Các camera không thể hoạt động.
- Hình ảnh camera bị rò rỉ cho những người không được ủy quyền.
- Hình ảnh camera bị công khai trên trang web.
- Hình ảnh camera không hiển thị trên màn hình giám sát.

3) Các sự kiện ảnh hưởng đến các bên bên ngoài

- Các camera gửi các gói tin quét hoặc tấn công thiết bị của bên thứ ba.
- Thiết bị của bên thứ ba bị nhiễm phần mềm độc hại.
- Các camera được sử dụng cho tấn công DDoS vào hạ tầng thiết yếu của một quốc gia hoặc các tổ chức khác.

c) Hậu quả

1) Hậu quả liên quan đến tổ chức

- Quá trình kinh doanh sử dụng hình ảnh camera không thể vận hành.
- Bảo mật vật lý của cơ sở bị suy yếu.
- Chức năng giám sát an toàn trong nhà máy không thể hoạt động.
- Tổ chức chịu tổn thất về tài chính.
- Tổ chức chịu thiệt hại về danh tiếng.

2) Hậu quả liên quan đến các bên bên ngoài

- Quyền riêng tư của những người có trong hình ảnh camera bị xâm phạm.
- Hoạt động của một cơ sở hạ tầng quan trọng của một quốc gia bị tổn hại.

Thư mục tài liệu tham khảo

[1] ISO/IEC 20924, Information technology — Internet of Things (IoT) — Vocabulary

[2] ISO/IEC 30141:2018, Internet of Things (IoT) — Reference Architecture

[3] ISO/IEC TR 22417:2017, Information technology — Internet of things (IoT) use cases

[4] ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[5] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[6] ISO/IEC 27002, Information security, cybersecurity and privacy protection — Information security controls

[7] ISO 31000:2018, Risk management — Guidelines

[8] ISO/IEC 27701, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

[9] ISO/IEC 29100, Information technology — Security techniques — Privacy framework

[10] ISO/IEC 29134, Information technology — Security techniques — Guidelines for privacy impact assessment

[11] ISO/IEC 27035 (all parts), Information technology — Security techniques — Information security incident management

[12] ISO/IEC 27036-1, Cybersecurity — Supplier relationships — Part 1: Overview and concepts

[13] ISO/IEC 27036-2, Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements

[14] ISO/IEC 27036-3, Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security

[15] ISO/IEC 27036-4, Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services

[16] TR 64:2018, (ICS 35.030) — Guidelines for IoT security for smart nation. Singapore Standards Council

[17] IEC 62443 (all parts), Industrial communication networks — Network and system security series of standards

[18] Recommendation ITU-T Y.3500 | ISO/IEC 17788

[19] ISO/IEC TS 27570:2021, Privacy protection — Privacy guidelines for smart cities

[20] ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[21] ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[22] ISO/IEC 27005 Information technology — Security techniques — Information security risk management