TCVN

TIÊU CHUẨN QUỐC GIA

DỰ THẢO

TCVN XXXXX:2026

ISO/IEC 27402:2023

Xuất bản lần 1

AN NINH MẠNG — BẢO MẬT VÀ QUYỀN RIÊNG TƯ IOT — CÁC YÊU CẦU CƠ BẢN VỀ THIẾT BỊ

Cybersecurity — IoT security and privacy — Device baseline requirements

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu

TCVN XXXXX:2026 hoàn toàn tương đương với ISO/IEC 27402:2023.

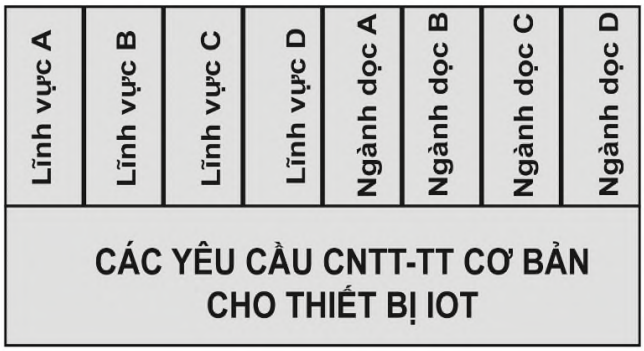
TCVN XXXXX:2026 do Ban Cơ yếu Chính phủ biên soạn, Bộ trưởng Bộ Quốc phòng đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Với số lượng thiết bị Internet vạn vật (IoT) ngày càng tăng và sự phụ thuộc ngày càng lớn vào các thiết bị này, các rủi ro về bảo mật và quyền riêng tư liên quan đến những "vật" đó dự kiến sẽ tiếp tục gia tăng. Việc triển khai rộng rãi chúng trong các mạng và hệ thống khiến chúng trở thành mục tiêu dễ bị tấn công và là đích nhắm hàng đầu của các cuộc tấn công mạng.

Tiêu chuẩn này cung cấp một bộ yêu cầu cơ bản về công nghệ thông tin và truyền thông (CNTT-TT) để các thiết bị IoT có thể hỗ trợ các biện pháp bảo mật và quyền riêng tư. Việc đánh giá rủi ro là yếu tố then chốt để xây dựng một kế hoạch xử lý rủi ro nhằm xác định các tính năng cần thiết của thiết bị IoT cũng như các biện pháp đối phó phù hợp. Việc quản lý các hệ thống sử dụng thiết bị IoT phụ thuộc vào khả năng của những thiết bị đó (cùng với các yếu tố khác).

Nói một cách khái quát, tiêu chuẩn này đề cập đến các yêu cầu CNTT-TT cho các thiết bị IoT được cung cấp ra thị trường. Các yêu cầu trong tiêu chuẩn này được xây dựng như một bộ yêu cầu cơ bản, trong đó các thị trường ngành dọc (như y tế, dịch vụ tài chính, công nghiệp, điện tử tiêu dùng và giao thông vận tải) có thể phát triển các yêu cầu bổ sung phù hợp với mục đích sử dụng dự kiến và các rủi ro của thiết bị IoT trong các ứng dụng của họ, như minh họa tại Hình 1. Bên cạnh tiêu chuẩn này, các lĩnh vực khác nhau (ví dụ: tư nhân/công nghiệp, công cộng, quốc phòng, an ninh quốc gia) và các thị trường ngành dọc có các yêu cầu đặc thù theo lĩnh vực hoặc theo ngành dọc, ví dụ như những yêu cầu được nêu trong ETSI EN 303 645 [11] đối với thiết bị tiêu dùng và loạt tiêu chuẩn IEC 62443 cho các thiết bị và hệ thống công nghiệp. Mặc dù tiêu chuẩn này có thể đưa ra các yêu cầu cho một chương trình đánh giá sự phù hợp, nhưng dự kiến các bên liên quan của các lĩnh vực và thị trường ngành dọc cụ thể sẽ đạt được sự đồng thuận về các yêu cầu đặc thù với bối cảnh của họ, xây dựng trên cơ sở ‘mở rộng’ từ tiêu chuẩn này. Tiếp theo, có thể xây dựng các chương trình đánh giá sự phù hợp cho các lĩnh vực và thị trường ngành dọc cụ thể đó. Tiêu chuẩn này sẽ được tích hợp hiệu quả vào các chương trình như vậy, đồng thời cung cấp một bộ các yêu cầu cơ bản.



CHÚ THÍCH: Các yêu cầu bổ sung có thể được phát triển hoặc yêu cầu bởi các lĩnh vực và thị trường ngành dọc cụ thể.

Hình 1 - Mối quan hệ giữa các yêu cầu cơ bản trong tiêu chuẩn này và các yêu cầu bổ sung tiềm năng

Khi bối cảnh công nghệ phức tạp của các thiết bị IoT tiếp tục phát triển, tiêu chuẩn này có thể hỗ trợ một cách tiếp cận có khả năng mở rộng được hài hòa hóa toàn cầu cho các yêu cầu cơ bản về bảo mật và quyền riêng tư, đồng thời cung cấp thông tin cho các sáng kiến về chính sách và quy định kỹ thuật.

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

An ninh mạng — Bảo mật và quyền riêng tư IoT — Các yêu cầu cơ bản về thiết bị

Cybersecurity — IoT security and privacy — Device baseline requirements

1. Phạm vi áp dụng

Tiêu chuẩn này cung cấp các yêu cầu CNTT-TT cơ bản cho các thiết bị IoT để hỗ trợ các biện pháp kiểm soát bảo mật và quyền riêng tư.

2. Tài liệu viện dẫn

Các tài liệu sau đây được viện dẫn trong văn bản theo cách mà một phần hoặc toàn bộ nội dung của chúng tạo thành yêu cầu của tiêu chuẩn này. Đối với các tài liệu viện dẫn có ghi năm ban hành, chỉ phiên bản được viện dẫn mới được áp dụng. Đối với các tài liệu viện dẫn không ghi năm ban hành, áp dụng phiên bản mới nhất của tài liệu được viện dẫn (bao gồm mọi sửa đổi, bổ sung).

TCVN ISO/IEC 27000:2019 (ISO/IEC 27000), Công nghệ thông tin — Các kỹ thuật an toàn — Hệ thống quản lý an toàn thông tin — Tổng quan và từ vựng

ISO/IEC 27400:2022, An ninh mạng — Bảo mật và quyền riêng tư IoT — Hướng dẫn

TCVN ISO 31000:2020 (ISO 31000:2018), Quản lý rủi ro — Hướng dẫn

3. Thuật ngữ, định nghĩa và thuật ngữ viết tắt

3.1 Thuật ngữ và định nghĩa

3.1.1

định danh (identifier)

thông tin phân biệt rõ ràng một thực thể này với một thực thể khác trong một bối cảnh nhận dạng nhất định.

[NGUỒN: ISO/IEC 23093-1:2022, 3.2.7]

3.1.2

giao diện người dùng (user interface)

tập hợp tất cả các thành phần của một hệ thống tương tác cung cấp thông tin và các điều khiển để người dùng thực hiện các tác vụ cụ thể trên hệ thống tương tác đó.

[NGUỒN: ISO 9241-110:2020, 3.10]

3.1.3

internet vạn vật (internet of things - IoT)

cơ sở hạ tầng gồm các thực thể, con người, hệ thống và tài nguyên thông tin được kết nối với nhau, cùng với các dịch vụ xử lý và phản hồi thông tin từ thế giới thực và thế giới ảo.

[NGUỒN: ISO/IEC 20924:2021, 3.2.4]

3.1.4

hệ thống IoT (IoT system)

hệ thống cung cấp các chức năng của *internet vạn vật (IoT)* (3.1.3).

CHÚ THÍCH 1 của thuật ngữ: Một hệ thống IoT có thể bao gồm, nhưng không giới hạn ở, các *thiết bị IoT* (3.1.5), các *cổng IoT* (3.1.7), các cảm biến và các bộ truyền động.

CHÚ THÍCH 2 của thuật ngữ: Các thiết bị CNTT thông thường như các điện thoại thông minh và máy tính xách tay có thể tạo thành một phần của hệ thống IoT.

CHÚ THÍCH 3 của thuật ngữ: Các hệ thống IoT cũng bao gồm kết nối đám mây và mạng.

[NGUỒN: ISO/IEC 20924:2021, Điều 3.2.9, có chỉnh sửa — đã bổ sung CHÚ THÍCH 2 và 3 cho thuật ngữ.]

3.1.5

thiết bị IoT (IoT device)

thực thể của một *hệ thống internet vạn vật (IoT)* (3.1.4) tương tác và giao tiếp với thế giới vật lý thông qua cảm biến hoặc truyền động.

CHÚ THÍCH 1 của thuật ngữ: Một thiết bị IoT có thể là một cảm biến hoặc một bộ truyền động.

CHÚ THÍCH 2 của thuật ngữ: Một thiết bị IoT, trong bối cảnh này, là một thiết bị đã được lắp ráp có thể sử dụng cho các chức năng IoT dự kiến của nó mà không cần phải nhúng hoặc tích hợp vào bất kỳ sản phẩm nào khác.

CHÚ THÍCH 3 của thuật ngữ: Các thiết bị IoT thường tương tác qua các giao diện truyền thông.

[NGUỒN: ISO/IEC 20924:2021, Điều 3.2.6, có chỉnh sửa — đã bổ sung CHÚ THÍCH 1, 2 và 3 cho thuật ngữ.]

3.1.6

nhà phát triển thiết bị IoT (IoT device developer)

thực thể tạo ra một thiết bị IoT (3.1.5) đã được lắp ráp hoàn chỉnh.

CHÚ THÍCH 1 của thuật ngữ: "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.

[NGUỒN: ISO/IEC 27400:2022, 3.4]

3.1.7

cổng IoT (IoT gateway)

thực thể của một hệ thống IoT kết nối một hoặc nhiều mạng lân cận và các thiết bị IoT trên những mạng đó với nhau, đồng thời kết nối các thiết bị đó tới một hoặc nhiều mạng truy cập.

[NGUỒN: ISO/IEC 20924:2021, 3.2.8]

3.1.8

cơ sở tính toán đáng tin cậy (trusted computing base - TCB)

toàn bộ các cơ chế bảo vệ trong một hệ thống máy tính, bao gồm phần cứng, phần sụn và phần mềm, trong đó sự kết hợp của các thành phần này chịu trách nhiệm thực thi chính sách bảo mật.

3.1.9

mô-đun mật mã (cryptographic module)

tập hợp phần cứng, phần mềm, và/hoặc phần sụn thực hiện các chức năng bảo mật và được nằm trong ranh giới mật mã.

[NGUỒN: ISO/IEC 19790:2012, 3.25]

3.1.10

tham số bảo mật trọng yếu (critical security parameter - CSP)

thông tin liên quan đến bảo mật mà việc tiết lộ hoặc sửa đổi có thể làm suy yếu tính bảo mật của mô-đun mật mã (3.1.9).

CHÚ THÍCH 1 của thuật ngữ: Một CSP có thể là dạng bản rõ hoặc được mã hóa.

CHÚ THÍCH 2 của thuật ngữ: Trong ví dụ, "chứng thư" đề cập đến các khóa riêng khớp với các khóa công khai bên trong chứng thư.

VÍ DỤ 1: Các khóa mật mã bí mật và khóa riêng, dữ liệu xác thực như mật khẩu, PIN, chứng thư hoặc các neo tin cậy khác.

VÍ DỤ 2: Các cài đặt cấu hình cần thiết để khởi tạo.

[NGUỒN: ISO/IEC 19790:2012, Điều 3.18, có chỉnh sửa — đã bổ sung CHÚ THÍCH 2 cho thuật ngữ và ví dụ 2.]

3.1.11

tham số bảo mật nhạy cảm (sensitive security parameter - SSP)

các tham số bảo mật trọng yếu (3.1.10) và các tham số bảo mật công khai.

[NGUỒN: ISO/IEC 19790:2012, 3.110]

3.1.12

trạng thái mặc định của nhà sản xuất (factory default)

trạng thái của thiết bị sau khi khôi phục cài đặt gốc hoặc sau khi hoàn thành quá trình sản xuất/lắp ráp.

CHÚ THÍCH 1 của thuật ngữ: Điều này bao gồm thiết bị vật lý và phần mềm (bao gồm cả phần sụn) có trên thiết bị sau khi lắp ráp.

3.1.13

chế độ an toàn khi có lỗi (fail-safe mode)

thiết bị hoặc tính năng mà khi xảy ra lỗi sẽ phản ứng theo cách không gây hại hoặc giảm thiểu thiệt hại cho các thiết bị khác, và không gây nguy hiểm hoặc giảm thiểu nguy hiểm cho người vận hành.

[NGUỒN: ISO 25197:2020, 3.32]

3.2 Thuật ngữ viết tắt

API	Giao diện lập trình ứng dụng (application programming interface)
ASLR	Ngẫu nhiên hóa sắp xếp không gian địa chỉ (address space layout randomization)
CPU	Đơn vị xử lý trung tâm (central processing unit)
CSP	Tham số bảo mật trọng yếu (critical security parameter)
ICT	Công nghệ thông tin và truyền thông (information and communication technologies)
IoT	Internet vạn vật (internet of things)
PIN	Số nhận dạng cá nhân (personal identification number)
PSP	Tham số bảo mật công khai (public security parameter)
RoT	Gốc tin cậy (root of trust)
TCB	Cơ sở tính toán đáng tin cậy (trusted computing base)
SWID	Thẻ nhận dạng phần mềm (software identification)
XML	Ngôn ngữ đánh dấu mở rộng (extensible markup language)

4. Tổng quan

Các hệ thống IoT tiềm ẩn những rủi ro về bảo mật và quyền riêng tư; ISO/IEC 27400 cung cấp thông tin chung và hướng dẫn về các rủi ro và mối đe dọa đó. Để xử lý các rủi ro này, người dùng (các tổ chức và người tiêu dùng) cần triển khai các biện pháp kiểm soát phù hợp, vốn cũng được mô tả chi tiết trong ISO/IEC 27400. Các biện pháp kiểm soát này không thể được triển khai nếu các thiết bị IoT không có chức năng hỗ trợ tương ứng (các chính sách về quá trình, các khả năng, v.v.).

Các nhà phát triển hệ thống IoT được kỳ vọng sẽ xây dựng các yêu cầu riêng và tìm kiếm các thiết bị IoT đáp ứng được các yêu cầu đó. Tiêu chuẩn này cung cấp các yêu cầu CNTT-TT cơ bản cho các thiết bị IoT. Trong nhiều trường hợp, các yêu cầu bổ sung sẽ được áp đặt hoặc được kỳ vọng nhằm giải quyết các rủi ro về bảo mật và quyền riêng tư của các thị trường ngành dọc cụ thể hoặc của các môi trường có mức rủi ro cao hơn.

5. Yêu cầu

5.1 Yêu cầu đối với chính sách và tài liệu của thiết bị IoT

5.1.1 Quản lý rủi ro

5.1.1.1 Yêu cầu

5.1.1.1.1 Các thiết bị IoT phải có tài liệu ghi lại kết quả của một quá trình đánh giá rủi ro được thực hiện ở cấp độ thiết bị IoT trong bối cảnh đánh giá rủi ro ở cấp độ hệ thống.

5.1.1.1.2 Quá trình đánh giá rủi ro phải xem xét các kết quả dự kiến cho trường hợp sử dụng dự kiến.

5.1.1.1.3 Quá trình đánh giá rủi ro cũng phải xem xét nhu cầu và kỳ vọng của các bên liên quan (ví dụ: các bên trên mạng mà thiết bị IoT được kết nối đến), bao gồm cả các tác động không mong muốn về mặt vật lý và logic.

CHÚ THÍCH 1: Các kỹ thuật đánh giá rủi ro có thể được tìm thấy trong IEC 31010 và ISO/IEC 27005.

CHÚ THÍCH 2: Các nhà phát triển thiết bị IoT thường thực hiện các đánh giá rủi ro và tạo ra các kế hoạch xử lý rủi ro.

5.1.1.1.4 Đánh giá rủi ro phải xem xét việc các thiết bị IoT có thể bị hạn chế (ví dụ: pin giới hạn, bộ nhớ ít, CPU "yếu"), điều này cung cấp thông tin cho quá trình xử lý rủi ro.

5.1.1.1.5 Các quá trình đánh giá và xử lý rủi ro phải được xác định và áp dụng như sau:

a) xác định xem các quá trình đánh giá và xử lý rủi ro riêng biệt có cần thiết cho các sản phẩm khác nhau hay không;

b) chọn các phương án xử lý rủi ro phù hợp, dựa trên kết quả đánh giá rủi ro;

CHÚ THÍCH 1: Các tiêu chuẩn cụ thể theo lĩnh vực hoặc thị trường ngành dọc có thể được sử dụng bổ sung cho tiêu chuẩn này. Một tiêu chuẩn như vậy có thể cung cấp một kế hoạch đánh giá rủi ro và/hoặc xử lý rủi ro cụ thể cho lĩnh vực hoặc thị trường ngành dọc đó. Việc tuân thủ các tiêu chuẩn đó có thể được sử dụng để đáp ứng các yêu cầu trong tiêu chuẩn này.

c) xác định tất cả các biện pháp kiểm soát cần thiết để triển khai (các) phương án xử lý rủi ro đã chọn;

d) xác định tất cả các tính năng bảo mật và quyền riêng tư của thiết bị IoT từ các biện pháp kiểm soát đã được xác định ở bước c) ở trên;

CHÚ THÍCH 2: Các nhà phát triển thiết bị IoT có thể thiết kế các tính năng theo yêu cầu hoặc xác định chúng từ bất kỳ nguồn thích hợp nào, chẳng hạn như một tiêu chuẩn ngành hoặc hướng dẫn của lĩnh vực.

e) so sánh các tính năng được xác định ở bước d) ở trên với các tính năng trong 5.2, và xác minh rằng không có tính năng cần thiết nào bị bỏ sót;

CHÚ THÍCH 3: 5.2 chứa một danh sách các tính năng cơ bản. Người sử dụng tiêu chuẩn này được hướng dẫn tham chiếu 5.2 để đảm bảo không bỏ sót yêu cầu nào.

CHÚ THÍCH 4: Danh sách các tính năng trong 5.2 không phải là danh sách đầy đủ. Các tính năng và biện pháp kiểm soát bổ sung có thể cần thiết tùy thuộc vào các phân khúc thị trường ngành dọc cụ thể hoặc để giải quyết các trường hợp sử dụng có rủi ro cao hơn.

f) lập ra một tuyên bố áp dụng bao gồm các tính năng cần thiết [xem các bước d) và e)] và lý do đưa vào và lý do loại trừ các tính năng trong 5.2;

g) nếu sử dụng các tiêu chuẩn khác liên quan đến các yêu cầu đối với thiết bị, thực hiện các yêu cầu của các tiêu chuẩn đó sau các bước từ a) đến f);

h) xây dựng một kế hoạch xử lý rủi ro;

i) thông báo cho chủ sở hữu rủi ro về kế hoạch xử lý rủi ro và các rủi ro còn lại, hoặc trong trường hợp có thể áp dụng, đạt được sự phê duyệt của họ đối với kế hoạch và sự chấp nhận các rủi ro còn lại.

5.1.1.1.6 Các thiết bị IoT phải thực hiện các tính năng và biện pháp kiểm soát được xác định là cần thiết trong tuyên bố áp dụng, cũng như các tính năng và biện pháp kiểm soát được xác định tại 5.1.1.1.5, bước g).

5.1.1.1.7 Tài liệu phải có sẵn trong suốt vòng đời được hỗ trợ của sản phẩm.

5.1.1.2 Khuyến nghị bổ sung

Các quá trình đánh giá và xử lý rủi ro cần tuân theo một phương pháp được chấp nhận rộng rãi như phương pháp được đưa ra trong ISO 31000. Để có hướng dẫn bổ sung về việc sử dụng ISO 31000, xem Phụ lục A.

5.1.1.3 Thông tin bổ sung

Các bên liên quan, chẳng hạn như nhà phát triển thiết bị IoT, nhà tích hợp hệ thống, nhà nhập khẩu, nhà bán lẻ hoặc các cơ quan quản lý, đều có thể thực hiện các đánh giá rủi ro như vậy.

Các thiết bị IoT có thể tích hợp các tính năng và biện pháp kiểm soát bảo mật và quyền riêng tư được xác định từ bất kỳ nguồn nào, chẳng hạn như các tiêu chuẩn đặc thù theo lĩnh vực hoặc thị trường ngành dọc, cũng như các tính năng và biện pháp kiểm soát được quy định trong tiêu chuẩn này. Các thiết bị IoT có thể tích hợp thêm các biện pháp kiểm soát bổ sung ngoài những biện pháp được xác định là cần thiết thông qua quá trình đánh giá rủi ro.

5.1.2 Công bố thông tin

5.1.2.1 Yêu cầu

5.1.2.1.1 Các thiết bị IoT phải có tài liệu người dùng liệt kê các tính năng mà thiết bị IoT cung cấp để hỗ trợ các biện pháp kiểm soát bảo mật và quyền riêng tư, trong đó làm rõ nếu có bất kỳ yêu cầu nào đối với thiết bị IoT tại 5.2 không được bao gồm.

5.1.2.1.2 Thông tin này phải được công bố công khai trong khoảng thời gian thiết bị IoT được hỗ trợ.

5.1.2.1.3 Các thiết bị IoT phải đi kèm với chính sách hỗ trợ bảo mật và các tài liệu hỗ trợ khác, trong đó người dùng được thông báo trước về thời điểm ngừng cung cấp các bản cập nhật bảo mật.

5.1.2.2 Khuyến nghị bổ sung

Thông tin theo các yêu cầu 5.1.2.1.1 đến 5.1.2.1.3 cần được cung cấp lần đầu tại thời điểm bán sản phẩm.

Hướng dẫn cần được cung cấp cho người dùng sau khi mua, có thể là một phần của quá trình cài đặt, nêu bật các sự kiện liên quan đến thiết bị IoT trong tương lai (chẳng hạn như cập nhật phần mềm) và cung cấp phương tiện để người dùng nhận các thông tin liên lạc trong tương lai.

Thời hạn hỗ trợ được cung cấp, như quy định trong tài liệu thiết bị IoT, cần phù hợp với các rủi ro và vòng đời dự kiến của sản phẩm. Nên tránh thay đổi các khoảng thời hạn hỗ trợ đã công bố vì điều này có thể gây gián đoạn các chu kỳ lập kế hoạch và vận hành của người dùng.

Tài liệu thiết bị cần bao gồm thông tin về cách người dùng có thể biết được thời hạn hỗ trợ có bị thay đổi sau khi công bố hay không.

Cần cung cấp thông tin rõ ràng, dễ hiểu về trách nhiệm của người dùng trong việc thiết lập và duy trì bảo mật và quyền riêng tư khi sử dụng thiết bị.

Tất cả các thỏa thuận cấp phép với người dùng cần xác định rõ phạm vi của các biện pháp kiểm soát bảo mật và quyền riêng tư cũng như các quyền trong suốt quá trình sử dụng sản phẩm, bao gồm cả dữ liệu được thu thập trong thời gian đó. Các thỏa thuận này cần được trình bày bằng ngôn ngữ rõ ràng và dễ hiểu.

Cần cung cấp thông tin về các thành phần phần mềm của bên thứ ba mà thiết bị IoT phụ thuộc có liên quan đến bảo mật của thiết bị IoT. Thông tin này có thể được cung cấp ở định dạng mà máy có thể đọc

được. Các thẻ nhận dạng phần mềm (SWID) (xem ISO/IEC 19770-2) có thể được sử dụng để nhận dạng các thành phần phần mềm đó.

5.1.2.3 Thông tin bổ sung

Thông tin dành cho người dùng có thể được cung cấp qua tài liệu tham khảo trực tuyến, ứng dụng di động, tài liệu in kèm thiết bị IoT và/hoặc nhãn trên bao bì. Có thể kết hợp sử dụng nhiều phương thức cùng lúc.

Nhiều người khác nhau có thể tương tác với, hoặc là đối tượng cảm biến của, một thiết bị IoT cụ thể. Cùng một người có thể tương tác với thiết bị IoT theo nhiều vai trò khác nhau, ví dụ: người mua, người cài đặt, người dùng chủ động và đối tượng bị cảm biến thụ động. Khi lập kế hoạch và thực hiện truyền thông với người dùng, phải đảm bảo rõ ràng và chính xác về đối tượng của từng thông tin, đồng thời tạo điều kiện để người dùng dễ dàng tiếp cận thông tin đó theo từng vai trò cụ thể cũng như theo góc nhìn tổng hợp tất cả các vai trò của một người.

Thông tin có thể bao gồm thời hạn hỗ trợ tối thiểu (ngoài thông báo bắt buộc về việc ngừng cung cấp cập nhật).

5.1.3 Quá trình công bố và xử lý lỗ hổng

5.1.3.1 Yêu cầu

5.1.3.1.1 Các thiết bị IoT phải có tài liệu quy định các quá trình công bố và xử lý lỗ hổng sẽ được áp dụng trong suốt vòng đời được hỗ trợ của thiết bị.

5.1.3.1.2 Các quá trình công bố và xử lý lỗ hổng phải bao gồm, ở mức tối thiểu, khả năng nhận báo cáo về các lỗ hổng tiềm ẩn từ công chúng.

5.1.3.2 Khuyến nghị bổ sung

Các yêu cầu 5.1.3.1.1 và 5.1.3.1.2 cần được thực hiện theo ISO/IEC 29147 (công bố lỗ hổng) và ISO/IEC 30111 (quá trình xử lý lỗ hổng).

5.2 Yêu cầu đối với khả năng và hoạt động của thiết bị IoT

5.2.1 Tổng quan

Điều này bao gồm các tính năng của thiết bị IoT được sử dụng cùng với quá trình đánh giá và xử lý rủi ro theo 5.1.1.

Các tính năng thiết bị IoT được yêu cầu trong tiêu chuẩn này được đưa vào vì chúng phù hợp với một tiêu chuẩn cơ bản. Mỗi yêu cầu trong 5.2 đều có phạm vi áp dụng rộng rãi, khả thi về mặt kỹ thuật, có tác động đáng kể và có thể đánh giá được.

5.2.2 Cấu hình

5.2.2.1 Yêu cầu

5.2.2.1.1 Nếu các thiết lập cấu hình của thiết bị IoT có thể được sửa đổi, chỉ các thực thể được ủy quyền mới được phép sửa đổi các thiết lập cấu hình của thiết bị IoT.

CHÚ THÍCH: Các thực thể được ủy quyền có thể là một người hoặc một thiết bị khác.

5.2.2.1.2 Nếu các thiết bị IoT có khả năng thay đổi cấu hình của các thiết bị IoT và các thiết bị khác, chúng chỉ được phép thực hiện các thay đổi đó khi được ủy quyền.

5.2.2.2 Khuyến nghị bổ sung

Quy trình cập nhật hoặc thay đổi thiết lập cấu hình cũng cần bao gồm:

a) phương thức để các thực thể được ủy quyền chuyển dữ liệu cấu hình đến thiết bị IoT và lưu trữ trên thiết bị theo cấu trúc dữ liệu và/hoặc định dạng dữ liệu đã được kiểm tra hợp lệ;

b) phương thức để xác minh tính toàn vẹn của các thiết lập cấu hình được truyền trước khi sử dụng;

c) phương thức để truyền tải an toàn các thiết lập, bao gồm xác thực nguồn của bản cập nhật;

d) phương thức xác nhận rằng các thiết lập đã được cập nhật thành công.

5.2.2.3 Thông tin bổ sung

Tùy thuộc vào các ràng buộc của thiết bị, việc cấp phép sửa đổi thiết lập cấu hình có thể được thực hiện theo nhiều cách khác nhau. Một số ví dụ minh họa bao gồm: có các vai trò người dùng riêng biệt như trong các hệ điều hành hiện đại; yêu cầu quyền truy cập vật lý vào thiết bị (ví dụ: nhấn nút "đặt lại"); yêu cầu thực hiện hành động cụ thể theo cách nhất định (ví dụ: phát một tín hiệu được điều chế đặc biệt đến thiết bị tại một tần số xác định). Các ví dụ trên chỉ mang tính minh họa và không mang tính liệt kê đầy đủ.

5.2.3 Đặt lại phần mềm

5.2.3.1 Yêu cầu

5.2.3.1.1 Nếu các thiết bị IoT có khả năng được đặt lại, quá trình đó phải an toàn.

5.2.3.1.2 Khả năng này chỉ được phép thực thi bởi một thực thể được ủy quyền.

5.2.3.2 Thông tin bổ sung

Đôi khi một lỗ hổng được khắc phục bằng cách thay đổi cấu hình; tuy nhiên, nếu sau đó thiết bị được khôi phục về trạng thái mặc định của nhà sản xuất, lỗ hổng có thể bị khai thác lại. Ví dụ điển hình là khi cấu hình hiện tại được thay đổi để ngăn thiết bị sử dụng các bộ mật mã không an toàn, trong khi trạng thái mặc định của nhà sản xuất lại cho phép tất cả bộ mật mã — do đó, việc khôi phục về trạng thái mặc định trong trường hợp này sẽ làm lộ các lỗ hổng một lần nữa.

Chức năng này đôi khi có thể được kết hợp với 5.2.4, sao cho việc đặt lại cấu hình và xóa dữ liệu người dùng có thể được thực hiện trong một thao tác duy nhất bởi thực thể được ủy quyền. Cấu hình thiết bị IoT và dữ liệu người dùng đôi khi được gộp chung hoặc khó tách biệt.

5.2.4 Xóa dữ liệu người dùng

5.2.4.1 Yêu cầu

5.2.4.1.1 Nếu thiết bị IoT lưu trữ dữ liệu người dùng, thiết bị phải cung cấp một chức năng để xóa dữ liệu người dùng thích hợp được lưu trữ trên thiết bị trong bất kỳ loại bộ nhớ nào.

5.2.4.1.2 Chức năng này phải được giới hạn chỉ cho các thực thể được ủy quyền.

5.2.4.2 Khuyến nghị bổ sung

Người dùng cần được cung cấp một thông báo rằng dữ liệu của họ đã được xóa một cách an toàn nếu thiết bị có thể làm như vậy.

5.2.4.3 Thông tin bổ sung

Dữ liệu người dùng có thể bao gồm dữ liệu cá nhân, dữ liệu cấu hình của người dùng và các tài liệu mật mã như khóa mật mã.

Một số thiết bị IoT có thể triển khai chức năng này bằng cách xóa tất cả dữ liệu của một nhóm người dùng (thậm chí toàn bộ dữ liệu của tất cả người dùng). Việc xóa nhiều hơn dữ liệu cần thiết của một người dùng cụ thể có thể là biện pháp chấp nhận được để đáp ứng yêu cầu này. Tuy nhiên, điều đó có thể dẫn đến việc dữ liệu người dùng bị lưu trữ lâu hơn mức cần thiết cho mục đích của nó. Do đó, cách làm này chỉ nên được thực hiện khi có lý do chính đáng.

Dữ liệu người dùng thường được lưu trữ ở các thành phần khác của hệ thống IoT (ví dụ: trong ứng dụng di động và đám mây), và người dùng kỳ vọng rằng việc xóa dữ liệu được áp dụng cho tất cả các thành phần của hệ thống IoT, không chỉ riêng thiết bị.

5.2.5 Bảo vệ dữ liệu

5.2.5.1 Yêu cầu

5.2.5.1.1 Các thiết bị IoT phải có khả năng bảo vệ dữ liệu được lưu trữ và truyền tải khỏi sự truy cập, sửa đổi và tiết lộ trái phép.

5.2.5.1.2 Điều này phải bao gồm các thiết lập cấu hình, dữ liệu nhận dạng, dữ liệu người dùng, nhật ký sự kiện và các tham số bảo mật nhạy cảm.

5.2.5.1.3 Các thiết bị IoT phải có khả năng bảo vệ phần mềm (bao gồm cả phần sụn) khỏi sự truy cập và sửa đổi trái phép.

5.2.5.1.4 Các thiết bị IoT phải sử dụng mật mã (ví dụ: mã hóa có xác thực, hàm băm mật mã, xác thực chữ ký số) để ngăn chặn việc xâm phạm tính bí mật và tính toàn vẹn của dữ liệu cần được bảo vệ.

CHÚ THÍCH: Các tiêu chuẩn quốc tế và các tiêu chuẩn được công nhận toàn cầu khác có thể được sử dụng cho các yêu cầu về mật mã.

5.2.5.2 Khuyến nghị bổ sung

5.2.5.2.1 Tổng quan

Khi các thiết bị IoT được khởi động, các thiết bị cần kiểm tra tính toàn vẹn và tính xác thực của phần mềm và/hoặc phần sụn và thực thi các biện pháp kiểm soát bảo mật. Nếu thiết bị IoT không vượt qua các kiểm tra này, thiết bị đó cần:

- thông báo cho người dùng về bất kỳ vi phạm nào,

- tự chuyển sang trạng thái không hoạt động (inoperable),

- hoạt động ở chế độ an toàn khi có lỗi (fail-safe mode) nhằm cung cấp sự bảo vệ về bảo mật, hoặc

- khởi động quá trình khôi phục thiết bị nếu các hành động khôi phục có thể được thực hiện một cách toàn vẹn.

Khi cài đặt lần đầu hoặc thực hiện bảo trì, các thiết bị IoT cần tự thiết lập về cấu hình mặc định an toàn. Các tùy chọn cấu hình dành cho người dùng cần ngăn chặn việc chọn cấu hình không an toàn hoặc phải đưa ra cảnh báo phù hợp.

Nếu có khả năng, các thiết bị IoT cần có khả năng cung cấp tính năng phân vùng.

Các thiết bị IoT cần sử dụng các mô-đun chức năng để hạn chế quyền truy cập vào các tài nguyên hệ thống, quyền này chỉ phải được cấp cho các thực thể được ủy quyền.

Cơ sở tính toán đáng tin cậy (TCB) cần được giữ nhỏ nhất có thể để giảm thiểu bề mặt bị phơi nhiễm trước những kẻ tấn công, đồng thời giảm xác suất một lỗi hoặc tính năng bị lợi dụng để vượt qua các biện pháp bảo vệ an toàn.

Các cơ chế bảo vệ bộ nhớ như ngôn ngữ an toàn bộ nhớ, kỹ thuật stack canaries, ngẫu nhiên hóa sắp xếp không gian địa chỉ (ASLR) và hạn chế quyền hoặc không cho quyền thực thi được khuyến nghị bất cứ đâu có thể áp dụng được.

5.2.5.2.2 Ghi nhật ký sự kiện

Nếu có khả năng, các thiết bị IoT cần ghi lại đủ chi tiết cho mỗi sự kiện để tạo điều kiện cho một thực thể được ủy quyền có khả năng xác định các sự kiện bất thường và phân tích dữ liệu liên quan một cách có ý nghĩa.

Các thiết bị IoT và nhật ký sự kiện cần được đồng bộ hóa với một hệ thống có thẩm quyền hoặc được chuyển đến các kho lưu trữ tập trung nếu dữ liệu đã được phi nhận dạng hóa một cách thích hợp.

5.2.5.2.3 Tham số bảo mật nhạy cảm

Kết quả của việc đánh giá rủi ro trong 5.1.1 cần giúp xác định xem một thiết bị IoT có thể bao gồm các tham số bảo mật nhạy cảm được lập trình cố định hoặc được chia sẻ hay không, với điều kiện các tham số đó là duy nhất cho mỗi thiết bị và không mang tính phổ quát.

5.2.5.3 Thông tin bổ sung

5.2.5.3.1 Tổng quan

Các giải pháp dựa trên phần cứng như bộ tăng tốc mật mã tích hợp và phần cứng chuyên dụng có thể tăng cường việc sử dụng các mô-đun mật mã và khả năng bảo vệ khóa mật mã để bảo vệ dữ liệu đang

lưu trữ và đang truyền tải nhằm đáp ứng các yêu cầu về hiệu năng. Các biện pháp đối phó vật lý có thể hỗ trợ chống lại các cuộc tấn công kênh kề. Các chức năng như vậy có thể bao gồm gốc tin cậy (Root of Trust - RoT) dựa trên phần cứng. RoT là một tính năng nền tảng để đem lại tính toàn vẹn cho nền tảng và đảm bảo một nền móng để phát triển và hỗ trợ chuỗi tin cậy của thiết bị. RoT lý tưởng nhất là dựa trên một quá trình khởi động được xác thực bằng phần cứng để đảm bảo hệ thống có thể được khởi động bằng mã lệnh từ một nguồn bất biến. Do đó, RoT là thiết yếu để cho phép chứng thực nền tảng bao gồm cả quá trình khởi động đã được xác minh. Khi được sử dụng để bảo vệ các bí mật và tính đúng đắn của thiết bị, phần cứng có thể hỗ trợ một gốc tin cậy nền tảng mà dựa vào đó, các chức năng phần mềm phong phú có thể được triển khai một cách bảo mật và an toàn hơn.

Các phân vùng độc lập được bảo vệ bởi các ranh giới do phần cứng thực thi để ngăn chặn một lỗi hoặc vi phạm trong một phân vùng phần mềm lan truyền sang các phân vùng phần mềm khác trong hệ thống. Sự phân vùng hóa tạo ra các ranh giới bảo vệ bổ sung bên trong cả ngăn xếp phần cứng và phần mềm để tạo thêm các lớp phòng thủ theo chiều sâu. Ví dụ, một kỹ thuật phổ biến là sử dụng các tiến trình hệ điều hành hoặc các máy ảo độc lập làm các phân vùng.

Việc kiểm tra tính toàn vẹn và các chế độ khôi phục có thể không phù hợp trong các ứng dụng trọng yếu về an toàn, nơi mà sự hoạt động liên tục là thiết yếu.

5.2.5.3.2 Nhật ký sự kiện

Việc triển khai ghi nhật ký sự kiện, bao gồm cả việc chỉnh sửa nhật ký, phụ thuộc vào khả năng lưu trữ của thiết bị. Các thiết bị IoT có thể hỗ trợ ghi nhật ký từ xa.

Mô-đun nền tảng tin cậy (Trusted Platform Modules - TPMs) là một ví dụ về gốc tin cậy phần cứng. TPMs có thể hỗ trợ nhận dạng thiết bị được ràng buộc bằng mật mã và truy cập giao diện, giúp ngăn chặn việc truy cập và sử dụng dữ liệu trái phép. Thông tin thêm về TPMs có thể tìm thấy trong ISO/IEC 11889-1.

5.2.6 Truy cập giao diện

5.2.6.1 Các yêu cầu

5.2.6.1.1 Các thiết bị IoT phải có các cơ chế để giới hạn quyền truy cập logic vào các giao diện của thiết bị, chỉ các thực thể được ủy quyền mới có thể truy cập.

5.2.6.1.2 Các thiết bị IoT phải sử dụng các cơ chế xác thực và kiểm soát truy cập thích hợp.

5.2.6.1.3 Các yêu cầu về bảo mật và quyền riêng tư phải được đánh giá khi thiết kế và triển khai các chức năng của các thiết bị IoT liên quan đến việc tạo và sử dụng các định danh.

5.2.6.1.4 Các thiết bị IoT phải đảm bảo rằng các giá trị chung cho các tham số bảo mật trọng yếu, chẳng hạn như các khóa riêng tư dùng chung hoặc mật khẩu tiêu chuẩn, được thay thế bằng các giá trị duy nhất cho mỗi thiết bị hoặc được xác định rõ ràng bởi một thực thể bên ngoài thích hợp trước khi các thiết bị IoT được đưa vào hoạt động.

CHÚ THÍCH: Đánh giá rủi ro là cơ sở của những gì là "thích hợp" trong bối cảnh này.

5.2.6.2 Khuyến nghị bổ sung

Thiết bị IoT cần có khả năng được nhận dạng một cách logic. Mặc dù các định danh có thể cho phép một loạt các biện pháp kiểm soát an ninh mạng (chẳng hạn như quản lý tài sản, tự động phát hiện thiết bị và cập nhật phần mềm), việc tạo hoặc sử dụng các định danh lâu dài (persistent) cần được tránh trừ khi việc sử dụng đó là không thể tránh khỏi. Khi những trường hợp sử dụng như vậy phát sinh, sự tồn tại của các định danh đó cần được làm rõ cho người dùng.

Các cơ chế giới hạn quyền truy cập logic (đối với các thực thể được ủy quyền) cần được áp dụng đối với:

a) khả năng kích hoạt hoặc vô hiệu hóa, thông qua các phương thức phần mềm hoặc phần cứng, bất kỳ giao diện nào (bao gồm cả giao diện cục bộ và mạng);

b) khả năng hạn chế quyền truy cập (ví dụ: thông qua xác thực) vào tất cả các giao diện từ xa;

c) khả năng xác định hoặc chặn các thiết bị không được hỗ trợ bởi một thiết bị IoT khi thiết bị đó cố gắng truy cập các giao diện.

Tất cả dữ liệu đầu vào và đầu ra cần được kiểm tra tính hợp lệ cho tất cả các loại giao diện. Dữ liệu cần được kiểm tra tính hợp lệ về độ dài, loại ký tự, các giá trị hoặc phạm vi chấp nhận được và định dạng thông điệp.

Các thiết bị IoT có giao diện từ xa có thể được dùng để thay đổi cấu hình hoặc hỗ trợ các chức năng quản trị cần triển khai các biện pháp ngăn chặn các loại tấn công phổ biến.

Các thực hành lập trình an toàn cần được tuân thủ, bao gồm việc sử dụng một ngôn ngữ an toàn về kiểu dữ liệu. Nếu điều này không thể thực hiện được, thiết bị IoT vẫn cần triển khai kiểm tra giới hạn, sử dụng định kiểu an toàn và các hàm xử lý chuỗi an toàn.

Các thiết bị IoT cần hỗ trợ một hoặc nhiều cơ chế để giới hạn quyền truy cập vào các giao diện dựa trên các kiểu người dùng hoặc nhóm người dùng.

Danh sách cho phép (gồm các ký tự hoặc loại thẻ token) nên được sử dụng thay vì danh sách từ chối khi lọc dữ liệu.

5.2.6.3 Thông tin bổ sung

5.2.6.3.1 Tổng quan

Ví dụ về giao diện người dùng bao gồm các bảng điều khiển quản trị, các trang web, các API hoặc các giao diện thiết bị IoT khác được phơi bày ra bên ngoài. Tấn công chèn mã (Injection), tấn công thực thể bên ngoài XML (XXE), tấn công mã lệnh chéo trang (XSS) và tấn công giải tuần tự không an toàn (insecure deserialization) là các ví dụ về các cuộc tấn công phổ biến vào giao diện từ xa.

Các năng lực dựa trên phần cứng có thể tăng cường bảo vệ truy cập giao diện, chống lại các cuộc tấn công leo thang đặc quyền và tấn công luồng điều khiển.

5.2.6.3.2 Định danh

Các thiết bị IoT có thể sử dụng các định danh để hoạt động trong một hệ thống IoT. Các ví dụ về những định danh này bao gồm số sê-ri, khóa mật mã và chứng thư.

CHÚ THÍCH: Các định danh vật lý và logic có thể đại diện cho cùng một giá trị.

Gốc tin cậy dựa trên phần cứng (Hardware-based root of trust) có thể bảo vệ các định danh khỏi bị sửa đổi trái phép và có thể được dùng để tạo ra các định danh đặc thù cho từng thiết bị. Phần cứng có thể bao gồm các đặc tính quan trọng để hỗ trợ bảo mật thiết bị, chẳng hạn như một phần cứng chuyên dụng hỗ trợ ngăn chặn các hành động không mong muốn được thực hiện bởi các thực thể trái phép.

Các nhà phát triển thiết bị IoT có thể tăng cường một định danh logic duy nhất bằng cách thiết lập một định danh thiết bị bằng mật mã mạnh trong quá trình triển khai (hoặc sản xuất) hoặc sử dụng các cơ chế khác để xác thực thiết bị vật lý tham gia vào các hoạt động mạng chiều vào hoặc chiều ra cụ thể.

5.2.7 Cập nhật phần mềm và phần sụn

5.2.7.1 Yêu cầu

5.2.7.1.1 Nếu thiết bị IoT hỗ trợ cập nhật phần mềm, việc cập nhật phải được thực hiện bằng một quy trình an toàn.

5.2.7.1.2 Việc cập nhật chỉ được khởi tạo bởi các thực thể được ủy quyền.

CHÚ THÍCH: Phần sụn là một loại phần mềm cụ thể.

5.2.7.1.3 Khi một bản cập nhật bị gián đoạn đột ngột, thiết bị IoT phải được đưa về một trạng thái giảm thiểu tối đa các tác hại tiềm tàng, có cân nhắc đến các rủi ro phát sinh khi thiết bị không hoạt động như mong đợi.

5.2.7.2 Khuyến nghị bổ sung

Mỗi quy trình cập nhật cần bao gồm những điều sau:

a) một cách để xác nhận tính hợp lệ, tính xác thực và tính toàn vẹn của bất kỳ bản cập nhật nào trước khi cài đặt;

b) các tùy chọn cấu hình bao gồm:

1) việc cập nhật tự động được kích hoạt hay vô hiệu hóa;

2) đối với các quy trình cập nhật từ xa, việc tải xuống và cài đặt bản cập nhật được khởi tạo tự động hay thủ công;

3) đối với các quy trình cập nhật từ xa, một phương thức để lên lịch tải xuống và cài đặt tự động;

4) việc có thông báo xảy ra hay không khi có bản cập nhật (và ai hoặc cái gì được thông báo).

Các thiết bị IoT cần hỗ trợ cập nhật tự động (phù hợp với các yêu cầu từ 5.2.7.1.1 đến 5.2.7.1.3). Các thiết bị IoT cần có một quy trình cập nhật định kỳ kiểm tra xem có bản cập nhật bảo mật nào mới không, và nếu có, thông báo điều này cho người dùng.

Các thiết bị IoT cần đảm bảo rằng tính xác thực và tính toàn vẹn của các bản cập nhật phần mềm được xác minh trước khi cài đặt chúng. Điều này có thể được thực hiện bằng chữ ký số và hạ tầng khóa công khai (PKI). Hạ tầng cập nhật, đặc biệt là việc quản lý các khóa riêng, cần được bảo mật.

Cần xem xét việc tận dụng các khả năng dựa trên gốc tin cậy phần cứng để đo lường và xác minh tính hợp lệ của các bản cập nhật phần mềm và phần sụn.

Các bản cập nhật phần mềm không nên làm ảnh hưởng đến chức năng cơ bản của các thiết bị IoT, hoặc trong trường hợp không thể tránh khỏi, cần có thông báo rõ ràng cho người dùng khi một bản cập nhật sẽ làm gián đoạn chức năng của thiết bị.

Phần mềm trên các thiết bị IoT cần được xác minh bằng các cơ chế khởi động an toàn. Nếu phát hiện một thay đổi trái phép, thiết bị IoT cần cảnh báo cho người dùng hoặc hub cục bộ/cổng IoT về sự cố. Hơn nữa, thiết bị IoT cần chấm dứt mọi giao tiếp mạng ngoại trừ việc gửi cảnh báo hoặc khởi tạo quá trình khôi phục thiết bị.

Trong khuôn khổ của vòng đời phát triển an toàn hoặc tương tự, cần có một quá trình chính thức để đánh giá các thành phần mới, được thay thế hoặc sửa đổi, bao gồm cả các bản cập nhật phần sụn, đối với những thay đổi trọng yếu có thể làm phát sinh các rủi ro hoặc lỗ hổng mới.

5.2.7.3 Thông tin bổ sung

Các thiết bị IoT có thể có các chức năng liên quan đến an toàn, và việc mất các chức năng đó trong quá trình cập nhật có thể là một vấn đề đối với một số loại hệ thống nếu không được cân nhắc và quản lý. Việc hủy bỏ một bản cập nhật hoặc sử dụng một phiên bản cũ hơn có thể được dùng để khôi phục lại từ một bản cập nhật bị gián đoạn.

Quy trình cập nhật phần mềm có thể sử dụng các phương thức từ xa (ví dụ: tải xuống qua mạng) hoặc cục bộ (ví dụ: phương tiện lưu trữ di động hoặc thay thế linh kiện phần cứng).

Nếu thiết bị IoT không thể giao tiếp trực tiếp với máy chủ từ xa, chức năng này có thể được cung cấp bởi hub cục bộ/cổng IoT. Hub cục bộ có thể được cấu hình để định kỳ kiểm tra sự tồn tại của bản cập nhật mới và tải xuống nếu có.

Việc thay thế phần cứng là một cách chính đáng và có thể chấp nhận được để thực hiện một bản cập nhật.

5.2.8 Thông báo cho người dùng

5.2.8.1 Thông tin

Việc các thiết bị IoT thông báo cho người dùng về nhiều tình huống khác nhau có thể là cần thiết hoặc hữu ích. Một số khuyến nghị trong tiêu chuẩn này mô tả các tình huống như vậy. Điều này nhằm cung cấp thông tin để hỗ trợ việc thông báo cho người dùng thiết bị IoT về các sự kiện hoặc tình trạng bất lợi.

Một số thiết bị IoT không có khả năng chủ động thông báo cho người dùng (ví dụ: hiển thị một thông báo trên màn hình, phát ra âm thanh hoặc ánh sáng), nhưng chúng có thể phản hồi bằng một thông điệp khi được truy vấn hoặc truy cập từ xa. Các thiết bị IoT không có khả năng trực tiếp thông báo cho người dùng có thể gửi thông báo và cảnh báo thông qua một hub cục bộ. Một truy vấn của người dùng có thể đơn giản là việc cố gắng truy cập thiết bị bằng trình duyệt, ứng dụng di động, hoặc một cách phức tạp

hơn. Thay vào đó, các thiết bị IoT có thể gửi một thông điệp đến một thiết bị báo động, giám sát hoặc ghi nhật ký trong hệ thống IoT.

Phụ lục A

(tham khảo)

Hướng dẫn quản lý rủi ro

A.1 Tổng quan

Áp dụng hướng dẫn trong TCVN ISO 31000:2020 (ISO 31000:2018), 6.4.1. Các rủi ro về bảo mật và quyền riêng tư của IoT cần được nhận dạng, định lượng hoặc mô tả định tính, và được sắp xếp thứ tự ưu tiên theo các tiêu chí đánh giá rủi ro và các mục tiêu liên quan của tổ chức.

A.2 Nhận dạng rủi ro

Đánh giá rủi ro bao gồm nhận dạng rủi ro, phân tích rủi ro và định mức rủi ro. Áp dụng hướng dẫn trong TCVN ISO 31000:2020 (ISO 31000:2018), 6.4.2. Khi nhận dạng các rủi ro về bảo mật và quyền riêng tư của các thiết bị IoT, cần xem xét các nguồn rủi ro khác nhau. Các nguồn rủi ro này phụ thuộc vào bản chất của thiết bị IoT và các ứng dụng của nó.

A.3 Phân tích rủi ro

Áp dụng hướng dẫn trong TCVN ISO 31000:2020 (ISO 31000:2018), 6.4.3. Phân tích rủi ro có thể được thực hiện ở các mức độ chi tiết khác nhau, tùy thuộc vào mức độ quan trọng của các giá trị hoặc tài sản đã được xác định của tổ chức, phạm vi của các tác động tiêu cực và tích cực đã biết, và các kiến thức hoặc kinh nghiệm đã tích lũy, bao gồm cả lịch sử sự cố liên quan đến tổ chức.

A.4 Đánh giá rủi ro

Áp dụng hướng dẫn trong TCVN ISO 31000:2020 (ISO 31000:2018), 6.4.4. Sau khi các rủi ro đã được xác định và được gán giá trị về khả năng xảy ra và mức độ nghiêm trọng của hậu quả, các tổ chức cần áp dụng tiêu chí chấp nhận rủi ro của mình để xác định rủi ro nào là có thể chấp nhận. Các rủi ro không thể chấp nhận cần được sắp xếp thứ tự ưu tiên để xử lý.

A.5 Xử lý rủi ro

Áp dụng hướng dẫn trong TCVN ISO 31000:2020 (ISO 31000:2018), 6.5.1 và 6.5.2. Các phương án xử lý rủi ro do tổ chức xác định cần cân nhắc các mục tiêu của tổ chức, các yêu cầu hợp đồng, pháp lý và quy định, cũng như quan điểm của các bên liên quan. Các phương án xử lý rủi ro có thể bao gồm:

- tránh rủi ro bằng cách quyết định không bắt đầu hoặc tiếp tục với hoạt động gây ra rủi ro;

- thực hiện phân tích sâu hơn để hiểu rõ hơn về rủi ro;

- xem xét lại các mục tiêu;

- loại bỏ nguồn rủi ro;

- chia sẻ rủi ro (ví dụ: thông qua hợp đồng, mua bảo hiểm);

- chấp nhận rủi ro bằng quyết định có đầy đủ thông tin.

A.6 Giám sát và xem xét

Áp dụng hướng dẫn trong TCVN ISO 31000:2020 (ISO 31000:2018), 6.6. Cần có các hoạt động phối hợp để chỉ đạo và kiểm soát tổ chức trong công tác quản lý rủi ro.

A.7 Ghi nhận và báo cáo

Áp dụng hướng dẫn trong TCVN ISO 31000:2020 (ISO 31000:2018), 6.7. Tổ chức cần thiết lập, ghi lại và duy trì một hệ thống thu thập và xác minh thông tin về các thiết bị IoT, đồng thời thu thập và xem xét các thông tin công khai sẵn có về các sản phẩm tương tự trên thị trường. Sau đó, thông tin này cần được đánh giá về mức độ liên quan có thể có đối với độ tin cậy của thiết bị IoT.

Thư mục tài liệu tham khảo

[1] NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers

[2] NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline

[3] Broadband Internet Technical Advisory Group (BITAG). (2016) Internet of Things (IoT) Security and Privacy Recommendations. (Broadband Internet Technical Advisory Group (BITAG), Denver, CO). Available at: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[4] CTIA, 2018, CTIA Cybersecurity Certification Test Plan for IoT devices, Version1.0.1. CTIA,Washington, DC

[5] European Union Agency for Network and Information Security (ENISA). (2017) Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. (European Union Agency for Network and Information Security (ENISA), Athens, Greece). recommendations-for-iot

[6] Groupe Spéciale Mobile Association (GSMA). (2017) GSMA IoT Security Assessment. (Groupe Spéciale Mobile Association (GSMA), London, UK). Available at: https://www.gsma.com/iot/iot-security-assessment/

[7] Industrial Internet Consortium (IIC). (2016) Industrial Internet of Things Volume G4: Security Framework. (Industrial Internet Consortium (IIC), Needham, MA).

[8] IoT Security Foundation (IoTSF). (2017) IoT Security Compliance Framework, Release 1.1. (IoT Security Foundation (IoTSF), Livingston, Scotland). Available at: https://www.iotsecurity foundation.org/best-practice-guidelines/

[9] Cloud Security Alliance (CSA) IoT Working Group. (2015) Identity and Access Management for the Internet of Things. (Cloud Security Alliance (CSA)).

[10] AgeLight Digital Trust Advisory Group. (2019) IoT Safety Architecture & Risk Toolkit (IoTSA) v3.1. (AgeLight Advisory & Research Group, Bellevue, WA).

[11] European Telecommunications Standards Institute (ETSI) European Norm. (EN) (2020- 06) Cyber; Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI Technical Specification 303 645 V2.1.1. (European Telecommunications Standards Institute (ETSI), Sophia Antipolis Cedex, France). Available at: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[12] IEC 62443-4-1, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

[13] IEC 62443-4-2, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

[14] C2 Consensus on IoT Device Security Baseline Capabilities, Convene the Conveners Project, Available at: https://csde.org/wpcontent/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[15] ISO/IEC 19770-2, Information technology — IT asset management — Part 2: Software identification tag

[16] Security Specification Version O.C.F., 2.1.2, Available at: https://openconnectivity.org/specs/OCF_Security_Specification_v2.1.2.pdf

[17] ISO/IEC 29147, Information technology — Security techniques — Vulnerability disclosure

[18] ISO/IEC 30111, Information technology — Security techniques — Vulnerability handling processes

[19] ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

[20] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[21] IEC 31010, *Risk management — Risk assessment techniques*

[22] ISO/IEC 23093-1, *Information technology — Internet of media things — Part 1: Architecture*

[23] ISO 25197, *Small craft — Electrical/electronic control systems for steering, shift and throttle*

[24] ISO/IEC 20924:2021, *Information technology — Internet of Things (IoT) — Vocabulary*

[25] ISO/IEC 11889-1, *Information technology — Trusted platform module library — Part 1: Architecture*

[26] ISO 9241-110:2020, *Ergonomics of human-system interaction — Part 110: Interaction principles*