

TCVN XXXXX:2026

Xuất bản lần 1

AN NINH MẠNG -
THIẾT BỊ INTERNET VẠN VẬT (IOT) - YÊU CẦU CƠ BẢN

*Cyber security -
Internet of Things (IoT) - Baseline requirements*

Mục lục

Lời nói đầu	5
Lời giới thiệu	6
1 Phạm vi áp dụng	7
2 Tài liệu viện dẫn	7
3 Thuật ngữ, định nghĩa và chữ viết tắt	7
3.1 Thuật ngữ và định nghĩa	7
3.2 Chữ viết tắt	9
4 Phân loại mức bảo đảm an ninh	10
4.1 Khái quát	10
4.2 Mức 1 – Cơ bản	10
4.3 Mức 2 – Nâng cao	10
4.4 Mức 3 – Trọng yếu	11
4.5 Nguyên tắc xác định mức áp dụng	11
5 Yêu cầu kỹ thuật	11
5.1 Yêu cầu cơ bản	11
5.2 Yêu cầu kiểm soát truy cập	12
5.3 Yêu cầu mật mã và quản lý khóa	12
5.4 Yêu cầu gốc tin cậy và khởi động an toàn	13
5.5 Yêu cầu kênh truyền thông an toàn	13
5.6 Yêu cầu giảm thiểu bề mặt tấn công	14
5.7 Yêu cầu cập nhật phần mềm và phần sụn	14
5.8 Yêu cầu an toàn ứng dụng	15
5.9 Yêu cầu bảo vệ dữ liệu trên thiết bị	15
5.10 Yêu cầu ghi nhật ký và giám sát	16
5.11 Yêu cầu khả năng phục hồi	16
5.12 Yêu cầu kết nối mạng và phân vùng	17
5.13 Yêu cầu bảo vệ vật lý	17
5.14 Yêu cầu về quan hệ giữa an ninh mạng và an toàn vận hành	18

5.15 Yêu cầu về chính sách và tổ chức	18
5.16 Yêu cầu quản lý tài sản và thành phần phần mềm	18
5.17 Yêu cầu đánh giá rủi ro và mô hình hóa mối đe dọa	19
5.18 Yêu cầu phát triển an toàn	19
5.19 Yêu cầu quản lý chuỗi cung ứng	20
5.20 Yêu cầu quản lý lỗ hổng bảo mật	20
5.21 Yêu cầu kiểm thử và đánh giá	21
5.22 Yêu cầu quản lý sự cố an ninh mạng	21
5.23 Yêu cầu vận hành và kết thúc vòng đời	21
5.24 Yêu cầu về tài liệu hướng dẫn sử dụng	22
5.25 Yêu cầu bảo vệ dữ liệu cá nhân theo thiết kế và theo mặc định	22
5.26 Yêu cầu thông báo và sự đồng ý	22
5.27 Yêu cầu tối thiểu hóa dữ liệu thu thập	23
5.28 Yêu cầu ẩn danh hóa và hạn chế liên kết dữ liệu	23
5.29 Yêu cầu bảo đảm quyền của chủ thể dữ liệu	23
5.30 Yêu cầu lưu trữ và chuyển dữ liệu	23
5.31 Yêu cầu trách nhiệm giải trình	23

Lời nói đầu

TCVN XXXX:2026 An ninh mạng - Thiết bị Internet vạn vật - Yêu cầu kỹ thuật chung do Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao biên soạn, Bộ Công an 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

Tiêu chuẩn này quy định các yêu cầu kỹ thuật đối với thiết bị và hệ thống Internet vạn vật (IoT) nhằm bảo đảm an ninh mạng và bảo vệ dữ liệu cá nhân trong suốt vòng đời sản phẩm, từ thiết kế, sản xuất, triển khai, vận hành cho tới thanh lý.

Để đạt hiệu quả bảo vệ ở mức cao nhất, khuyến khích tổ chức, cá nhân sản xuất, cung cấp và sử dụng thiết bị IoT áp dụng đầy đủ các yêu cầu quy định trong tiêu chuẩn này ở mức bảo đảm phù hợp với rủi ro của thiết bị, kết hợp với các biện pháp quản lý, kỹ thuật và vận hành khác.

An ninh mạng - Internet vạn vật (IoT) - Yêu cầu kỹ thuật chung

Cyber security - Internet of Things (IoT) - General requirements

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu kỹ thuật chung về an ninh mạng đối với thiết bị IoT, hệ thống IoT và dịch vụ đi kèm, bao gồm nhưng không giới hạn các yêu cầu về định danh và xác thực, kiểm soát truy cập, mật mã, cập nhật phần mềm, ghi nhật ký, khả năng phục hồi, quản lý vòng đời, chuỗi cung ứng và bảo vệ dữ liệu cá nhân.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 14423:2026 An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản.

3 Thuật ngữ, định nghĩa và chữ viết tắt

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN 9801-1:2022 và các thuật ngữ sau.

3.1 Thuật ngữ và định nghĩa

3.1.1

Thiết bị IoT (IoT device)

Thực thể của hệ thống IoT tương tác và giao tiếp với thế giới vật lý thông qua cảm biến hoặc bộ chấp hành, có ít nhất một giao diện kết nối mạng.

3.1.2

Hệ thống IoT (IoT system)

Hệ thống cung cấp chức năng của Internet vạn vật, bao gồm thiết bị IoT, cổng kết nối, cảm biến, bộ chấp hành, ứng dụng và hạ tầng phía sau phục vụ giải pháp IoT.

3.1.3

Dịch vụ đi kèm (Associated service)

Dịch vụ đám mây, ứng dụng di động hoặc ứng dụng web mà nếu thiếu, thiết bị IoT không thực hiện được chức năng đã công bố.

3.1.4

Nhà phát triển thiết bị (Device developer)

Tổ chức, cá nhân thiết kế, sản xuất và cung cấp thiết bị IoT hoàn chỉnh.

3.1.5

Nhà phát triển dịch vụ (Service developer)

Tổ chức, cá nhân thiết kế, lập trình và tích hợp hệ thống, nền tảng và ứng dụng IoT.

3.1.6

Nhà cung cấp dịch vụ (Service provider)

Tổ chức, cá nhân triển khai, cấu hình, vận hành, bảo trì và ngừng vận hành hệ thống IoT được cung cấp cho người dùng.

3.1.7

Người dùng IoT (IoT user)

Cá nhân hoặc tổ chức mua sắm, thiết lập và sử dụng thiết bị, hệ thống hoặc dịch vụ IoT.

3.1.8

Tham số an toàn nhạy cảm (Sensitive security parameter)

Khóa mật mã, chứng thư số, thông tin xác thực, giá trị khởi tạo và tham số cấu hình mà việc để lộ hoặc sửa đổi làm mất hiệu lực của biện pháp bảo vệ.

3.1.9

Gốc tin cậy (Root of trust)

Thành phần phần cứng hoặc phần mềm được tin cậy vô điều kiện, làm điểm neo cho chuỗi tin cậy của thiết bị.

3.1.10

Khởi động an toàn (Secure boot)

Cơ chế kiểm tra chữ ký số của bộ nạp khởi động và phần mềm trước khi thực thi, bảo đảm chỉ mã đã được xác thực mới được chạy trên thiết bị.

3.1.11

Thao tác có tác động lớn (Impactful operation)

Thao tác có khả năng thay đổi trạng thái an ninh, quyền truy cập, luồng dữ liệu hoặc gây hậu quả vật lý, bao gồm đặt lại thông tin xác thực, cập nhật phần sụn từ xa, thay đổi cấu hình lưu trữ dữ liệu và điều khiển bộ chấp hành.

3.1.12

Danh mục thành phần phần mềm (Software bill of materials)

Danh mục các thành phần phần mềm cấu thành một bản phát hành, ở định dạng máy đọc được, kèm phiên bản và quan hệ phụ thuộc.

3.1.13

Bảng thông tin triển khai kỹ thuật (Implementation information table)

Tài liệu do nhà phát triển hoặc nhà cung cấp khai báo, mô tả cách từng yêu cầu của tiêu chuẩn này được hiện thực hóa trên sản phẩm cụ thể, dùng làm căn cứ đánh giá sự phù hợp.

3.1.14

Dữ liệu cá nhân (Personal data)

Thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể, theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

3.1.15

Ẩn danh hóa (De-identification)

Quá trình xử lý dữ liệu cá nhân để không thể xác định trực tiếp một con người cụ thể nếu không sử dụng thêm thông tin khác.

3.1.16

Sự đồng ý (Consent)

Sự thể hiện ý chí rõ ràng, tự nguyện của chủ thể dữ liệu về việc cho phép xử lý dữ liệu cá nhân của mình.

3.2 Chữ viết tắt

ABAC	Attribute-Based Access Control	Kiểm soát truy cập theo thuộc tính
API	Application Programming Interface	Giao diện lập trình ứng dụng
CIA	Confidentiality, Integrity, Availability	Bí mật, toàn vẹn, sẵn sàng
CTI	Cyber Threat Intelligence	Tình báo mối đe dọa mạng
CVE	Common Vulnerabilities and Exposures	Danh mục lỗ hổng và điểm yếu công khai
DDoS	Distributed Denial of Service	Từ chối dịch vụ phân tán

DTLS	Datagram Transport Layer Security	Bảo mật tầng truyền tải cho gói dữ liệu
HSM	Hardware Security Module	Mô-đun bảo mật phần cứng
IOC	Indicator of Compromise	Chỉ dấu tấn công
IoT	Internet of Things	Internet vạn vật
IXIT	Implementation eXtra Information for Testing	Bảng thông tin triển khai phục vụ đánh giá
MFA	Multi-Factor Authentication	Xác thực đa yếu tố
MQTT	Message Queuing Telemetry Transport	Giao thức truyền thông điệp cho IoT
OTA	Over-The-Air	Cập nhật qua sóng vô tuyến
PII	Personally Identifiable Information	Thông tin định danh cá nhân
PKI	Public Key Infrastructure	Hạ tầng khóa công khai
RBAC	Role-Based Access Control	Kiểm soát truy cập theo vai trò
SBOM	Software Bill of Materials	Danh mục thành phần phần mềm
SIEM	Security Information and Event Management	Hệ thống quản lý thông tin và sự kiện bảo mật
TLS	Transport Layer Security	Bảo mật tầng truyền tải
TPM	Trusted Platform Module	Mô-đun nền tảng tin cậy
UART	Universal Asynchronous Receiver-Transmitter	Cổng truyền dữ liệu nối tiếp không đồng bộ
VLAN	Virtual Local Area Network	Mạng cục bộ ảo
VPN	Virtual Private Network	Mạng riêng ảo

4 Phân loại mức bảo đảm an ninh

4.1 Khái quát

Tiêu chuẩn này quy định ba mức bảo đảm an ninh, ký hiệu Mức 1, Mức 2 và Mức 3, áp dụng theo nguyên tắc tích lũy: một thiết bị đạt Mức 2 phải đáp ứng toàn bộ yêu cầu của Mức 1; một thiết bị đạt Mức 3 phải đáp ứng toàn bộ yêu cầu của Mức 1 và Mức 2.

Mức 1 - Cơ bản

- Mức 1 áp dụng cho mọi thiết bị IoT, không phân biệt chủng loại.

Mức 2 - Nâng cao

Mức 2 áp dụng cho thiết bị thuộc một trong các trường hợp sau:

- Thu thập hình ảnh, âm thanh, vị trí, dữ liệu sinh trắc học hoặc dữ liệu cá nhân khác;

- Điều khiển bộ chấp hành tác động tới không gian sinh hoạt hoặc làm việc của con người;
- Tham gia xử lý giao dịch có giá trị tiền tệ.

Mức 3 - Trọng yếu

- Mức 3 áp dụng cho thiết bị thuộc hệ thống thông tin quan trọng, thiết bị thuộc hạ tầng thiết yếu quốc gia, thiết bị y tế, giao thông, năng lượng, hệ thống điều khiển công nghiệp

4.2 Nguyên tắc xác định mức áp dụng

Tổ chức, cá nhân xác định mức áp dụng theo giá trị cao nhất trong ba tiêu chí quy định tại Bảng 1. Không được hạ mức áp dụng vì lý do chi phí; khi thiết bị không đáp ứng được yêu cầu của mức tương ứng, tổ chức, cá nhân phải thay đổi thiết kế hoặc thu hẹp phạm vi sử dụng đã công bố.

Bảng 1 - Tiêu chí xác định mức bảo đảm an ninh

Tiêu chí	Dẫn tới Mức 1	Dẫn tới Mức 2	Dẫn tới Mức 3
Hậu quả đối với con người	Không có tác động vật lý	Gây bất tiện hoặc thiệt hại tài sản có giới hạn	Có khả năng gây tổn hại sức khỏe hoặc tính mạng
Dữ liệu cá nhân được xử lý	Không xử lý dữ liệu cá nhân	Dữ liệu cá nhân cơ bản, hình ảnh, âm thanh, vị trí	Dữ liệu cá nhân nhạy cảm theo quy định pháp luật
Vai trò trong hệ thống	Thiết bị độc lập, không điều khiển	Thiết bị kết nối mạng doanh nghiệp hoặc điều khiển cục bộ	Thiết bị thuộc hạ tầng thiết yếu hoặc điều khiển quá trình công nghiệp

5 Yêu cầu kỹ thuật

5.1 Yêu cầu cơ bản

5.1.1 Định danh thiết bị

- Thiết bị phải có định danh duy nhất, không sửa đổi được và xác minh được, phân biệt được với mọi thiết bị khác kể cả thiết bị cùng model.
- (Mức 3) Thiết bị, cổng kết nối và nền tảng phải xác thực lẫn nhau trước khi thiết lập kết nối và định kỳ xác thực lại, dựa trên chứng thư thiết bị neo vào gốc tin cậy phần cứng.

5.1.2 Quản lý mật khẩu và thông tin xác thực

- Không sử dụng mật khẩu mặc định dùng chung cho nhiều thiết bị. Mật khẩu khởi tạo phải duy nhất theo từng thiết bị, hoặc thiết bị phải buộc người dùng đặt mật khẩu mới trong lần thiết lập đầu tiên trước khi cho phép sử dụng chức năng.
- Phần mềm và phần sụn không được chứa tài khoản ẩn, mật khẩu cứng, khóa dịch vụ dùng chung hoặc cơ chế truy cập kỹ thuật không được công bố.

- c) Thiết bị phải có cơ chế chống dò mật khẩu qua mạng, bao gồm giới hạn số lần thử liên tiếp, tăng dần độ trễ giữa các lần thử hoặc khóa tạm thời, kèm ghi nhật ký.
- d) Người dùng phải đổi được thông tin xác thực bằng cơ chế an toàn. Quy trình khôi phục và đặt lại mật khẩu không được tạo đường vòng qua cơ chế xác thực.
- e) (Mức 2) Chính sách mật khẩu phải yêu cầu tối thiểu 8 ký tự gồm chữ và số. Thiết bị phải từ chối mật khẩu nằm trong danh sách mật khẩu phổ biến công khai.
- f) (Mức 2) Xác thực đa yếu tố phải được hỗ trợ và bắt mặc định cho các thao tác có tác động lớn, bao gồm đặt lại thông tin xác thực, cập nhật phần sụn từ xa và truy cập quản trị từ xa.
- g) Thông tin xác thực phải được bảo vệ khỏi truy cập trái phép, không phân biệt được lưu trữ trên thiết bị, trên hệ thống hay đang trong quá trình truyền.

5.1.3 Cấu hình mặc định

- a) Cấu hình mặc định phải là cấu hình an toàn nhất trong các cấu hình được hỗ trợ.
- b) Mọi nói lỏng so với cấu hình mặc định chỉ được kích hoạt bởi hành động chủ động của người dùng, kèm cảnh báo mô tả hệ quả.

5.2 Yêu cầu kiểm soát truy cập

5.2.1 Quản lý phiên và phân quyền

- a) Áp dụng nguyên tắc đặc quyền tối thiểu. Vai trò người dùng thường và vai trò quản trị phải tách biệt, quyền của mỗi vai trò phải được công bố trong tài liệu kỹ thuật.
- b) Phiên làm việc phải có thời hạn, tự kết thúc khi không hoạt động và bị hủy khi người dùng đăng xuất, đổi mật khẩu hoặc bị thu hồi quyền.
- c) (Mức 2) Hệ thống phải hỗ trợ phân quyền theo vai trò hoặc theo thuộc tính, với mức chi tiết tới từng người dùng và từng ứng dụng kết nối.
- d) (Mức 3) Quản trị khóa mật mã và các thao tác tác động diện rộng phải áp dụng kiểm soát kép và tách nhiệm vụ, không để một cá nhân đơn lẻ thực hiện trọn vẹn.

5.2.2 Kiểm soát truy cập vật lý tới cổng dịch vụ

- a) (Mức 2) Truy cập vật lý tới cổng dịch vụ, bao gồm UART, JTAG, USB và khe thẻ nhớ, phải bị vô hiệu hóa, che chắn hoặc yêu cầu xác thực trước khi sử dụng.

5.3 Yêu cầu mật mã và quản lý khóa

5.3.1 Thuật toán và tham số mật mã

- a) Chỉ được sử dụng thuật toán, chế độ và độ dài khóa còn hiệu lực theo khuyến nghị hiện hành, bao gồm AES-128 hoặc AES-256 ở chế độ GCM, hàm băm từ SHA-256 trở lên, đường cong ECDSA hoặc ECDH từ P-256 trở lên, RSA từ 3072 bit.

- b) Không được sử dụng MD5, SHA-1, DES, 3DES, RC4 và chế độ mã hóa khối ECB.
- c) (Mức 2) Thiết bị phải cho phép cập nhật thuật toán và tham số mật mã qua bản cập nhật phần mềm, không phụ thuộc vào việc thay thế phần cứng.
- d) (Mức 3) Với khóa và chứng thư có vòng đời dự kiến trên 5 năm, phải công bố kế hoạch chuyển đổi sang thuật toán kháng tấn công lượng tử và bảo đảm thiết bị có khả năng nhận bản cập nhật thực hiện chuyển đổi đó.

5.3.2 Sinh số ngẫu nhiên và khóa

- a) Bộ sinh số ngẫu nhiên phải dựa trên nguồn entropy phần cứng hoặc nguồn entropy đã được đánh giá.
- b) Không được sinh khóa hoặc giá trị bí mật từ dữ liệu suy đoán được, bao gồm số sê-ri, địa chỉ MAC hoặc thời gian khởi động.
- c) Mỗi thiết bị phải sử dụng khóa và giá trị bí mật riêng biệt. Việc lộ khóa của một thiết bị không được ảnh hưởng tới các thiết bị còn lại trong cùng dòng sản phẩm.

5.3.3 Quản lý vòng đời khóa

(Mức 2) Phải quản lý trọn vòng đời khóa, bao gồm sinh, phân phối, lưu trữ, sử dụng, luân chuyển, thu hồi và hủy. Chu kỳ đổi khóa phải được xác định và ghi trong hồ sơ kỹ thuật.

5.4 Yêu cầu gốc tin cậy và khởi động an toàn

5.4.1 Lưu trữ tham số an toàn nhạy cảm

- a) Tham số an toàn nhạy cảm phải được lưu trữ ở vùng chống đọc và chống ghi trái phép.
- b) Không được lưu tham số an toàn nhạy cảm ở dạng rõ, không nhúng trong mã nguồn, tệp cấu hình hoặc ảnh phần sụn phân phối công khai.

5.4.2 Gốc tin cậy phần cứng

(Mức 2) Thiết bị phải thiết lập gốc tin cậy bằng phần cứng, bao gồm mô-đun bảo mật phần cứng, phần tử an toàn rời hoặc vùng thực thi tin cậy của vi mạch, hoặc bằng phần tử an toàn ảo đã qua đánh giá.

5.4.3 Khởi động an toàn

- a) (Mức 2) Chữ ký của bộ nạp khởi động và ảnh phần sụn phải được kiểm tra trước khi thực thi.
- b) (Mức 2) Khi kiểm tra chữ ký thất bại, thiết bị phải dừng khởi động hoặc chuyển sang trạng thái an toàn có kiểm soát và ghi nhận sự kiện.
- c) (Mức 3) Với thiết bị lắp đặt ngoài khu vực được bảo vệ, phải có cơ chế chống can thiệp vật lý, bao gồm bằng chứng can thiệp, phát hiện mở vỏ và xóa khóa khi phát hiện can thiệp.

5.5 Yêu cầu kênh truyền thông an toàn

5.5.1 Mã hóa và toàn vẹn dữ liệu truyền

- a) Mọi dữ liệu nhạy cảm và mọi lệnh điều khiển truyền trên mạng phải được mã hóa và bảo vệ toàn vẹn.
- b) Phải sử dụng TLS từ phiên bản 1.2 trở lên cho tải TCP, DTLS cho tải UDP; giao thức MQTT phải chạy trên nền TLS.
- c) Phải vô hiệu hóa giao thức và bộ mã lỗi thời, bao gồm SSLv3, TLS 1.0, TLS 1.1, Telnet, FTP và giao diện quản trị chạy trên HTTP không mã hóa.
- d) (Mức 2) Kết nối tới dịch vụ đám mây của nhà phát triển phải ghi chứng thư hoặc ghi khóa công khai; bộ mã được chọn phải bảo đảm tính bí mật chuyển tiếp hoàn hảo.
- e) (Mức 3) Kênh quản trị phải tách biệt khỏi kênh dữ liệu và chỉ truy cập được từ mạng tin cậy, qua mạng riêng ảo hoặc qua điểm truy cập di động riêng của nhà mạng.

5.5.2 Xác thực đối tác kết nối

- a) Thiết bị phải xác thực đầy đủ chứng thư của đối tác kết nối, bao gồm chuỗi tin cậy, tên miền và hạn hiệu lực.
- b) Không được có tùy chọn bỏ qua lỗi chứng thư trong vận hành bình thường.
- c) (Mức 2) Mọi thủ tục ghép nối không dây và thiết lập ban đầu phải có xác thực. Không được sử dụng chế độ ghép nối không xác thực và chế độ thiết lập mở không giới hạn thời gian.

5.6 Yêu cầu giảm thiểu bề mặt tấn công

5.6.1 Vô hiệu hóa giao diện và dịch vụ không sử dụng

- a) Mọi giao diện mạng và giao diện logic không sử dụng phải bị vô hiệu hóa.
- b) Danh sách cổng mạng mở và dịch vụ đang chạy phải ở mức tối thiểu cần thiết và được công bố trong hồ sơ kỹ thuật.
- c) Giao diện gỡ lỗi phải bị vô hiệu hóa trong bản phát hành, hoặc tắt được bằng phần mềm và không truy cập được với cấu hình mặc định.

5.6.2 Làm cứng hệ thống

- a) Trước khi phát hành, phải loại bỏ cửa hậu, mã gỡ lỗi, tài khoản kỹ thuật và dịch vụ không cần thiết. Quy trình làm cứng phải có bằng chứng thực hiện.
- b) (Mức 2) Tiến trình phải chạy với đặc quyền tối thiểu và được cách ly lẫn nhau. Các biện pháp làm cứng nền tảng phải được bật, bao gồm ngẫu nhiên hóa không gian địa chỉ, chống thực thi trên vùng dữ liệu, bảo vệ ngăn xếp và hệ thống tệp gốc ở chế độ chỉ đọc khi khả thi.

5.7 Yêu cầu cập nhật phần mềm và phần sụn

5.7.1 Cơ chế cập nhật

- a) Thiết bị phải có cơ chế cập nhật phần mềm và phần sụn như một chức năng cơ bản, được thiết kế ngay từ giai đoạn phát triển.

- b) Cập nhật phải hoàn tất trọn vẹn hoặc thất bại theo cách khôi phục được. Khi thiết bị không xác minh được tính xác thực của bản cập nhật, thiết bị phải quay lui về cấu hình tốt gần nhất đã lưu.
- c) Phải có cơ chế ngăn hạ cấp trái phép về phiên bản cũ hơn trong vận hành bình thường. Thao tác hạ cấp có kiểm soát chỉ thực hiện được sau xác thực và phải được ghi nhật ký.
- d) Việc cập nhật không được làm giảm mức an toàn hiện có, không được khôi phục cấu hình mặc định kém an toàn và không được xóa thiết lập bảo mật do người dùng đặt.
- e) (Mức 2) Thiết bị phải thông báo cho người dùng khi có bản cập nhật bảo mật và khi cập nhật thất bại. Chức năng cập nhật tự động phải được hỗ trợ và bật theo mặc định đối với thiết bị tiêu dùng.

5.7.2 Bảo vệ gói cập nhật

- a) Gói cập nhật phải được ký số. Thiết bị phải kiểm tra chữ ký, chứng thư ký và chuỗi chứng thư trước khi bắt đầu quá trình cập nhật.
- b) Cập nhật qua sóng vô tuyến phải thực hiện trên kênh mã hóa.
- c) (Mức 3) Hạ tầng phát hành cập nhật phải áp dụng khóa ký lưu trong mô-đun bảo mật phần cứng, quy trình ký có kiểm soát kép, nhật ký ký số không thể chối bỏ và được lưu trữ độc lập.

5.7.3 Thông báo và công bố thời hạn hỗ trợ

Phải công bố công khai thời hạn hỗ trợ cập nhật bảo mật tối thiểu cho từng dòng sản phẩm, tính theo mốc thời gian xác định, và thông tin này phải nhìn thấy được trước khi mua.

5.8 Yêu cầu an toàn ứng dụng

5.8.1 Xác thực dữ liệu đầu vào

- a) Mọi dữ liệu đầu vào từ người dùng, cảm biến, giao diện lập trình, tệp cấu hình và mạng phải được kiểm tra về kiểu, độ dài, dải giá trị và bộ ký tự trước khi xử lý.
- b) Xử lý lỗi phải an toàn. Thông báo lỗi không được lộ dấu vết ngăn xếp, phiên bản thành phần, đường dẫn hệ thống hoặc nội dung tham số nhạy cảm.

5.8.2 Bảo vệ giao diện lập trình ứng dụng

- a) (Mức 2) Giao diện lập trình của thiết bị và dịch vụ đi kèm phải áp dụng xác thực và phân quyền cho từng lời gọi, giới hạn tần suất và danh sách phương thức được phép.
- b) (Mức 3) Trước mỗi bản phát hành lớn phải thực hiện phân tích mã tĩnh, phân tích tệp nhị phân và kiểm thử ngẫu nhiên hóa đầu vào với mọi giao diện nhận dữ liệu không tin cậy.

5.8.3 Ứng dụng di động và ứng dụng web đi kèm

(Mức 2) Ứng dụng di động và ứng dụng web đi kèm phải đáp ứng cùng mức yêu cầu như thiết bị. Không được lưu khóa, chứng thư hoặc thông tin xác thực trong mã nguồn hoặc tài nguyên của ứng dụng.

5.9 Yêu cầu bảo vệ dữ liệu trên thiết bị

5.9.1 Mã hóa dữ liệu lưu trữ

- a) Dữ liệu cá nhân và dữ liệu người dùng trao đổi giữa thiết bị, ứng dụng và dịch vụ đám mây phải được mã hóa và bảo vệ toàn vẹn.
- b) (Mức 2) Dữ liệu nhạy cảm lưu trên bộ nhớ trong và trên thẻ nhớ rời phải được mã hóa, với khóa gắn với thiết bị và không rút được bằng cách tháo thẻ nhớ.

5.9.2 Xóa dữ liệu

- a) Phải có chức năng cho phép người dùng xóa toàn bộ dữ liệu cá nhân và cấu hình trên thiết bị. Việc hoàn tất xóa phải được xác nhận rõ ràng cho người dùng.
- b) (Mức 2) Trước khi thanh lý, chuyển giao hoặc tái sử dụng, dữ liệu và phần mềm có bản quyền trên thiết bị phải được xóa hoặc ghi đè an toàn theo hướng dẫn đã công bố.

5.9.3 Công bố chức năng cảm biến

(Mức 2) Chức năng của từng cảm biến, bao gồm camera, micro, định vị và cảm biến sinh trắc học, phải được mô tả rõ trong tài liệu, và trạng thái đang hoạt động phải nhận biết được từ bên ngoài thiết bị.

5.10 Yêu cầu ghi nhật ký và giám sát

5.10.1 Sự kiện phải ghi nhật ký

- a) Phải ghi nhật ký tối thiểu các sự kiện sau: đăng nhập thành công và thất bại, thay đổi cấu hình và quyền, cập nhật phần sụn, kết nối mới, truy cập dữ liệu nhạy cảm, thao tác từ xa và thao tác có tác động lớn.
- b) Mỗi bản ghi phải có nhãn thời gian. Đồng hồ trong toàn hệ thống phải được đồng bộ để cho phép phân tích nhất quán.
- c) (Mức 2) Với thiết bị hạn chế tài nguyên không tự ghi nhật ký được, chức năng ghi nhật ký phải được thực hiện tại cổng kết nối hoặc tại máy chủ của hệ thống.

5.10.2 Bảo vệ nhật ký

- a) (Mức 2) Nhật ký phải được bảo vệ chống sửa đổi, xóa và lộ lọt, bao gồm chỉ đọc với mọi chủ thể trừ tiến trình hệ thống, cơ chế phát hiện thay đổi bằng giá trị băm và chuyển tập trung về hệ thống thu thập.

5.10.3 Phát hiện bất thường

- a) (Mức 3) Phải gửi cảnh báo qua kênh ngoài băng cho thao tác có tác động lớn và sự kiện an ninh nghiêm trọng.
- b) (Mức 2) Phải giám sát và cảnh báo sớm các dấu hiệu bất thường, bao gồm lưu lượng mạng bất thường, giá trị cảm biến vượt dải bình thường, dấu hiệu thao túng dữ liệu đo hoặc dữ liệu điều khiển, thay đổi vị trí thiết bị và mất kết nối kéo dài.

5.11 Yêu cầu khả năng phục hồi

5.11.1 Phục hồi sau mất điện, mất kết nối

- a) Thiết bị phải tự khôi phục hoạt động bình thường và giữ nguyên cấu hình sau khi mất điện hoặc mất kết nối mạng, không quay về trạng thái mặc định kém an toàn.
- b) Mất kết nối tới dịch vụ đám mây không được làm mất các chức năng an toàn cục bộ thiết yếu đã công bố.

5.11.2 Chống cạn kiệt tài nguyên

- a) (Mức 2) Phải có cơ chế chống cạn kiệt tài nguyên, bao gồm giới hạn số phiên đồng thời, giới hạn tần suất yêu cầu, kiểm soát phần mềm tiêu tốn tài nguyên, ngưỡng tiêu thụ năng lượng và dự phòng công suất.
- b) (Mức 3) Thiết bị phải tự kiểm tra tính toàn vẹn, phát hiện và sửa lỗi với các chức năng quan trọng, và chuyển về trạng thái an toàn khi phát hiện lỗi không sửa được.

5.11.3 Sao lưu và khôi phục

- a) (Mức 2) Dữ liệu và cấu hình hệ thống phải được sao lưu định kỳ. Khả năng khôi phục từ bản sao lưu phải được kiểm tra thực tế ít nhất mỗi 12 tháng.
- b) (Mức 3) Phải tổ chức diễn tập khôi phục sau thảm họa cho hệ thống IoT ít nhất mỗi 12 tháng.

5.12 Yêu cầu kết nối mạng và phân vùng

5.12.1 Kiểm soát kết nối ra ngoài

Thiết bị chỉ được khởi tạo kết nối ra ngoài tới các điểm đích cần thiết cho chức năng đã công bố. Danh sách tên miền và cổng đích phải được nêu trong hồ sơ kỹ thuật để người dùng cấu hình tường lửa.

5.12.2 Phân vùng mạng

- a) (Mức 2) Mạng IoT phải được tách khỏi mạng nghiệp vụ và mạng quản trị bằng mạng cục bộ ảo, tường lửa hoặc phân đoạn vi mô.
- b) (Mức 3) Khi thiết bị tham gia điều khiển quá trình công nghiệp, giữa vùng công nghệ vận hành và vùng công nghệ thông tin phải có cổng một chiều hoặc cách ly vật lý.

5.12.3 Kiểm soát thiết bị kết nối vào hệ thống

(Mức 2) Hệ thống phải kiểm soát thiết bị được phép kết nối bằng danh sách cho phép, bằng xác thực thiết bị, hoặc bằng cách lấy đặc tả thiết bị khi đàm phán kết nối rồi quyết định chấp nhận, từ chối hoặc giới hạn phạm vi chức năng được cấp.

5.13 Yêu cầu bảo vệ vật lý

5.13.1 Bảo vệ vỏ thiết bị

- a) Vỏ của cảm biến và bộ chấp hành đặt ở nơi công cộng phải chống được việc mở trái phép ở mức cơ bản.

b) Khi mức bảo vệ vật lý bị hạn chế, phải thông báo cho người sử dụng dữ liệu của thiết bị về mức độ tin cậy giới hạn đó.

5.13.2 Quản lý vị trí lắp đặt

(Mức 2) Vị trí lắp đặt của cảm biến và bộ chấp hành phải được kiểm kê và rà soát định kỳ trong hoạt động quản lý tài sản.

5.13.3 Điều kiện môi trường vận hành

(Mức 2) Thiết bị phải hoạt động ổn định trong dải điều kiện môi trường đã công bố và phải ghi nhận khi điều kiện môi trường vượt dải đó.

5.14 Yêu cầu về quan hệ giữa an ninh mạng và an toàn vận hành

5.14.1 Phân tích mối nguy an toàn phát sinh từ sự kiện an ninh

a) (Mức 2) Phải phân tích mối nguy mà sự kiện an ninh có thể gây ra cho chức năng an toàn, bao gồm dữ liệu điều khiển sai lệch gây hoạt động sai và tấn công làm chức năng an toàn mất tác dụng.

b) (Mức 2) Phải đánh giá tác động ngược của chính biện pháp an ninh lên hiệu năng và chức năng an toàn trước khi triển khai, và ghi lại kết luận trong hồ sơ thiết kế.

5.14.2 Xác minh quyết định tự động

a) (Mức 3) Quyết định tự động có khả năng gây hậu quả không đảo ngược cho con người phải qua một bước xác minh độc lập thứ hai, có tính tới dữ liệu từ nguồn khác và khả năng cảnh báo gốc bị sai.

5.15 Yêu cầu về chính sách và tổ chức

5.15.1 Chính sách an ninh mạng

Phải ban hành chính sách an ninh mạng cho IoT, được lãnh đạo phê duyệt, công bố, phổ biến tới nhân sự và các bên liên quan bên ngoài, rà soát theo định kỳ hoặc khi có thay đổi lớn.

5.15.2 Phân công trách nhiệm

a) Phải phân công và tài liệu hóa vai trò, trách nhiệm an ninh IoT cho quản lý rủi ro, thiết kế biện pháp bảo vệ, triển khai và vận hành, quản lý quan hệ nhà cung cấp, đào tạo nhận thức và quản lý sự cố.

b) Ranh giới trách nhiệm an ninh giữa nhà phát triển, nhà cung cấp dịch vụ và người dùng phải được thỏa thuận và truyền đạt bằng văn bản trước khi cung cấp dịch vụ.

5.15.3 Đào tạo nhận thức

(Mức 2) Phải tổ chức đào tạo nhận thức và kỹ năng an ninh định kỳ cho nhân sự tham gia phát triển, vận hành và hỗ trợ, có đánh giá kết quả.

5.16 Yêu cầu quản lý tài sản và thành phần phần mềm

5.16.1 Kiểm kê thiết bị

- a) Phải lập và duy trì danh mục thiết bị kết nối, phiên bản phần mềm và phần sụn, bản vá đã áp dụng. Danh mục phải chính xác, cập nhật và nhất quán trong suốt giai đoạn vận hành.
- b) Phải luôn biết được mỗi thiết bị IoT đang gắn với tài sản vật lý nào, đặt ở đâu và ai chịu trách nhiệm quản lý.

5.16.2 Danh mục thành phần phần mềm

(Mức 2) Phải lập và duy trì danh mục thành phần phần mềm cho mỗi bản phát hành ở định dạng máy đọc được, và cung cấp cho khách hàng tổ chức khi được yêu cầu.

5.16.3 Theo dõi lỗ hổng thành phần

(Mức 2) Phải theo dõi liên tục lỗ hổng của thành phần bên thứ ba và thành phần mã nguồn mở dựa trên danh mục thành phần, đối chiếu với cơ sở dữ liệu lỗ hổng công khai và danh mục lỗ hổng đang bị khai thác.

5.17 Yêu cầu đánh giá rủi ro và mô hình hóa mối đe dọa

5.17.1 Mô hình hóa mối đe dọa

- a) Phải thực hiện mô hình hóa mối đe dọa ngay từ đầu giai đoạn triển khai, bám theo môi trường vận hành dự kiến của thiết bị, xác định tài sản cần bảo vệ, bài toán an ninh, mục tiêu an ninh và yêu cầu an ninh tương ứng.
- b) Kết quả mô hình hóa mối đe dọa phải được lưu trong hồ sơ kỹ thuật.

5.17.2 Đánh giá rủi ro

- a) Phải nhận diện nguồn rủi ro liên quan tới cấu hình và môi trường, hạ tầng thiết yếu, chất lượng thành phần, chuỗi cung ứng, con người và các yếu tố bên ngoài hệ thống.
- b) (Mức 2) Phải thực hiện đánh giá rủi ro theo phương pháp đã được thừa nhận, và đánh giá tác động tới việc bảo vệ dữ liệu cá nhân khi hệ thống xử lý dữ liệu cá nhân.

5.17.3 Cập nhật kết quả đánh giá

(Mức 2) Phải cập nhật mô hình mối đe dọa và đánh giá rủi ro khi thay đổi kiến trúc, bổ sung tính năng, thay đổi nhà cung cấp thành phần hoặc sau mỗi sự cố an ninh.

5.18 Yêu cầu phát triển an toàn

5.18.1 Nguyên tắc kỹ thuật an toàn

Phải áp dụng và tài liệu hóa các nguyên tắc kỹ thuật an toàn cho phát triển hệ thống IoT, bao gồm an toàn mặc định, phòng thủ nhiều lớp, trách nhiệm giải trình và khả năng phục hồi.

5.18.2 Vòng đời phát triển phần mềm an toàn

Phải áp dụng vòng đời phát triển phần mềm an toàn với quy tắc lập trình an toàn, rà soát mã, kiểm soát phiên bản và tách biệt môi trường phát triển, kiểm thử và vận hành.

5.18.3 Môi trường phát triển

- a) (Mức 2) Phải đánh giá rủi ro cho môi trường phát triển, xét tới nhân sự, phương pháp và quy trình xử lý dữ liệu, sản phẩm và dịch vụ thuê ngoài, môi trường vật lý và mạng. Dữ liệu kiểm thử không được chứa dữ liệu cá nhân thật.
- b) (Mức 2) Quy trình sản xuất nạp phần sụn, khóa mật mã và chứng thư phải được kiểm soát, ghi nhận và có khả năng truy vết từng đơn vị sản phẩm.

5.19 Yêu cầu quản lý chuỗi cung ứng

5.19.1 Hợp đồng với nhà cung cấp

Hợp đồng với nhà cung cấp phải quy định rõ nghĩa vụ về quản lý lỗ hổng, cung cấp bản vá phần sụn, thông báo khi thay đổi đặc tả thiết bị và cung cấp thông tin liên quan cho người dùng cuối.

5.19.2 Thông tin an ninh của thiết bị

Thông tin an ninh của thiết bị phải được tài liệu hóa và cung cấp cho các bên cần biết theo thỏa thuận bảo mật, bao gồm đặc tả chức năng an ninh, khả năng cập nhật, thời hạn bảo hành, lỗ hổng mới phát hiện và thời điểm ngừng sản xuất.

5.19.3 Thông báo thay đổi và ngừng cung cấp

- a) (Mức 2) Khi ngừng cung cấp thiết bị hoặc thay đổi lớn đặc tả, phải thông báo trước với thời gian đủ để bên mua ra quyết định thay thế.
- b) (Mức 2) Phải xác minh nguồn gốc linh kiện và phần sụn. Chỉ được đưa vào sản phẩm thành phần không có lỗ hổng đã biết chưa được xử lý.

5.20 Yêu cầu quản lý lỗ hổng bảo mật

5.20.1 Chính sách công bố lỗ hổng

Phải công bố công khai chính sách tiếp nhận báo cáo lỗ hổng, bao gồm đầu mối liên hệ, cam kết thời gian phản hồi và khung thời gian xử lý.

5.20.2 Thu thập và phân tích thông tin lỗ hổng

- a) Phải thu thập thông tin lỗ hổng từ nhà cung cấp thành phần, trung tâm chia sẻ và phân tích thông tin, cơ quan điều phối ứng cứu sự cố, và phân tích tác động lên thiết bị, hệ thống và dịch vụ của mình.
- b) (Mức 2) Phải xây dựng cơ chế phát hiện, ghi nhận thiết bị đang vận hành có lỗ hổng hoặc có hành vi bất thường và gửi cảnh báo tới người dùng và quản trị viên của thiết bị đó.

5.20.3 Phát hành bản vá

Phải phát hành bản vá cho lỗ hổng nghiêm trọng trong khung thời gian đã công bố, thông báo cho người dùng và quản trị viên kèm mô tả rủi ro và biện pháp tạm thời.

5.20.4 Báo cáo lỗ hổng đang bị khai thác

(Mức 2) Phải thực hiện nghĩa vụ báo cáo lỗ hổng đang bị khai thác và sự cố nghiêm trọng theo quy định pháp luật hiện hành và cơ quan điều phối ứng cứu sự cố quốc gia.

5.21 Yêu cầu kiểm thử và đánh giá

5.21.1 Kiểm thử xác minh chức năng

Phải xác định thiết bị, chức năng và giao diện cần kiểm tra, lập kế hoạch kiểm thử xác minh và thực hiện trước khi đưa hệ thống vào vận hành. Kết quả kiểm thử phải được lưu.

5.21.2 Đánh giá lỗ hổng định kỳ

(Mức 2) Phải thực hiện đánh giá lỗ hổng định kỳ và trước mỗi bản phát hành lớn.

5.21.3 Kiểm thử xâm nhập

a) (Mức 3) Phải thực hiện kiểm thử xâm nhập có cấu trúc do bên thứ ba độc lập, tối thiểu mỗi 12 tháng và sau mỗi thay đổi kiến trúc lớn. Các phát hiện mức cao phải được khắc phục trước khi phát hành.

b) (Mức 3) Phải thực hiện phân tích tệp nhị phân phần mềm bởi tổ chức thử nghiệm được chỉ định, tập trung vào lỗ hổng đã biết và điểm yếu phần mềm phổ biến.

5.22 Yêu cầu quản lý sự cố an ninh mạng

5.22.1 Quy trình ứng phó sự cố

Phải xây dựng quy trình ứng phó sự cố có phân loại mức độ, đầu mối chịu trách nhiệm, thời hạn xử lý và kênh thông báo cho người dùng cùng cơ quan chức năng.

5.22.2 Rút kinh nghiệm sau sự cố

Sau khi khép lại mỗi sự cố, phải xác định nguyên nhân và hậu quả, sau đó cập nhật tương ứng đánh giá rủi ro, biện pháp kiểm soát đã áp dụng hoặc chỉnh quy trình quản lý sự cố.

5.22.3 Chia sẻ thông tin với cơ quan chức năng

(Mức 2) Phải tham gia cơ chế chia sẻ thông tin với cơ quan điều phối ứng cứu sự cố quốc gia và cộng đồng ngành, theo dõi cảnh báo do các cơ quan này phát hành.

5.23 Yêu cầu vận hành và kết thúc vòng đời

5.23.1 Bàn giao ở cấu hình an toàn

Thiết bị và dịch vụ phải được bàn giao ở cấu hình an toàn, với phiên bản phần mềm đã vá, cổng và dịch vụ mạng ở mức tối thiểu, quyền truy cập bị giới hạn. Mật khẩu khởi tạo phải được chuyển giao cho người dùng bằng cách an toàn.

5.23.2 Vô hiệu hóa thiết bị ngừng sử dụng

Thiết bị không còn sử dụng phải được vô hiệu hóa và thu hồi thông tin xác thực, không để tiếp tục kết nối mạng trong trạng thái không được quản lý.

5.23.3 Thanh lý và tái sử dụng

a) Trước khi thanh lý hoặc tái sử dụng, mọi thiết bị chứa phương tiện lưu trữ phải được kiểm tra để bảo đảm dữ liệu nhạy cảm và phần mềm có bản quyền đã được xóa hoặc ghi đè an toàn.

b) (Mức 2) Phải thông báo trước cho người dùng quy trình sẽ áp dụng khi chấm dứt hệ thống hoặc dịch vụ, bao gồm cách xử lý dữ liệu đang lưu và mức độ hoạt động còn lại của thiết bị sau khi dịch vụ dừng.

5.24 Yêu cầu về tài liệu hướng dẫn sử dụng

5.24.1 Nội dung tài liệu hướng dẫn

Phải cung cấp tài liệu hướng dẫn sử dụng an toàn bằng ngôn ngữ đơn giản, bao gồm thiết bị và cấu hình được hỗ trợ, phiên bản phần mềm được hỗ trợ, yêu cầu thiết lập ban đầu và đăng ký người dùng, cách đổi mật khẩu, cách cập nhật, cấu hình kết nối không dây an toàn và tiêu chí mật khẩu hợp lệ.

5.24.2 Thông tin về rủi ro sử dụng sai

Phải nêu rõ trong tài liệu các rủi ro và hậu quả khi sử dụng sai, tối thiểu bao gồm nhiễm mã độc, lộ thông tin cá nhân của người dùng, lộ thông tin kinh doanh và thiết bị bị lợi dụng cho tấn công từ chối dịch vụ.

5.24.3 Đầu mối hỗ trợ

a) Phải cung cấp đầu mối hỗ trợ tiếp nhận câu hỏi liên quan tới an ninh trong quá trình vận hành. Người dùng chỉ lựa chọn thiết bị và dịch vụ IoT có thông tin nhà phát triển rõ ràng và có đầu mối hỗ trợ.

b) Người dùng phải đối thông tin xác thực mặc định ngay trong lần thiết lập đầu tiên. Thông tin xác thực mới không được trùng với giá trị cũ, không dùng chung với thiết bị khác, không dễ đoán và không nằm trong danh sách phổ biến trên Internet.

5.25 Yêu cầu bảo vệ dữ liệu cá nhân theo thiết kế và theo mặc định

a) Phải xác định các thành phần dữ liệu nhạy cảm ngay trong giai đoạn thiết kế và nhúng khả năng tăng cường bảo vệ dữ liệu cá nhân vào kiến trúc thiết bị và thiết kế dịch vụ.

b) Không cần bất kỳ tương tác nào của người dùng, thiết lập bảo vệ dữ liệu cá nhân nghiêm ngặt nhất phải được áp dụng theo mặc định. Cơ chế kiểm soát truy cập phù hợp phải được tích hợp sẵn trong thiết bị và dịch vụ.

5.26 Yêu cầu thông báo và sự đồng ý

a) Trước khi mua hoặc kích hoạt, người dùng phải được cung cấp thông báo về dữ liệu cá nhân mà thiết bị và dịch vụ thu thập cùng mục đích sử dụng.

b) Phải có sự đồng ý của người dùng trước khi thu thập dữ liệu cá nhân và trước khi thay đổi mục đích sử dụng. Người dùng phải được cung cấp thông tin về mục đích, phương thức, phạm vi thu thập, thời hạn lưu trữ và bên sẽ sử dụng dữ liệu. Cơ chế rút lại đồng ý phải dễ thực hiện không kém cơ chế cho đồng ý.

c) (Mức 2) Phải lưu vết việc cho đồng ý và rút lại đồng ý, bao gồm thời điểm, phạm vi và phiên bản thông báo đã hiển thị.

5.27 Yêu cầu tối thiểu hóa dữ liệu thu thập

- a) Phải thiết kế và vận hành dịch vụ sao cho phạm vi dữ liệu thu thập, kể cả dữ liệu cá nhân, giới hạn trong mức tương thích với mục đích đã thông báo.
- b) Dữ liệu thu thập gián tiếp, bao gồm địa chỉ IP, vị trí địa lý, nhiệt độ, thông tin ngữ cảnh và thông tin về sự hiện diện của thiết bị khác ở gần, phải được giảm tới mức tối thiểu cần thiết trừ khi người dùng đồng ý riêng.
- c) (Mức 2) Dữ liệu đo từ xa và dữ liệu chẩn đoán gửi về nhà phát triển phải là tùy chọn, tắt theo mặc định và có mô tả rõ nội dung được gửi.

5.28 Yêu cầu ẩn danh hóa và hạn chế liên kết dữ liệu

- a) (Mức 2) Định danh thiết bị dùng trong giao tiếp có thể bị nghe lén phải được biểu diễn bằng bí danh, sao cho không suy ra được dữ liệu cá nhân của chủ sở hữu thiết bị.
- b) (Mức 2) Ánh xạ giữa thiết bị và người dùng phục vụ vận hành phải được lưu tách biệt và chỉ truy cập được bởi những người dùng có nhu cầu hợp lệ.

5.29 Yêu cầu bảo đảm quyền của chủ thể dữ liệu

- a) Hệ thống phải hỗ trợ thực hiện các quyền của chủ thể dữ liệu, bao gồm quyền được biết, đồng ý, truy cập, chỉnh sửa, xóa, hạn chế xử lý và rút lại đồng ý, thực hiện được trực tiếp từ giao diện người dùng.
- b) (Mức 2) Tùy chọn bảo vệ dữ liệu cá nhân của từng người dùng phải được lưu an toàn trên thiết bị và chỉ cung cấp cho thiết bị hoặc dịch vụ đã được cấp quyền kết nối. Việc thêm, sửa hoặc xóa tùy chọn chỉ thực hiện được sau khi xác thực đúng người dùng đó.
- c) (Mức 2) Với thiết bị dùng chung nhiều người, phải xác định rõ tùy chọn của người dùng nào được áp dụng khi thiết bị được truy cập.

5.30 Yêu cầu lưu trữ và chuyển dữ liệu

- a) Phải công bố vị trí lưu trữ dữ liệu và các luồng chuyển dữ liệu ra ngoài lãnh thổ, bao gồm quốc gia đặt máy chủ và bên tiếp nhận.
- b) (Mức 2) Thiết bị phải có chức năng cho phép thiết lập cấu hình để dữ liệu chỉ được lưu trữ và xử lý trong lãnh thổ Việt Nam, chỉ kết nối tới máy chủ đặt tại Việt Nam.
- c) (Mức 2) Phải đánh giá tác động của việc chuyển dữ liệu cá nhân ra nước ngoài và lưu hồ sơ đánh giá theo quy định pháp luật hiện hành.

5.31 Yêu cầu trách nhiệm giải trình

- a) Phải xây dựng khung trách nhiệm giải trình xác định nhất quán bên nào chịu trách nhiệm cho phần nào của vòng đời dữ liệu, ai trả lời khi có vi phạm dữ liệu và ai xử lý yêu cầu công bố dữ liệu.
- b) (Mức 2) Phải rà soát liên tục hiệu lực của các biện pháp bảo vệ dữ liệu cá nhân và nhận diện rủi ro mới, có tính tới nhu cầu thay đổi của người dùng và yêu cầu pháp lý thay đổi.

Thư mục tài liệu tham khảo

- [1] ISO/IEC 27400:2022, Cybersecurity - IoT security and privacy - Guidelines.
 - [2] Info-communications Media Development Authority, IoT Cyber Security Guide, Version 1, Singapore, 2020.
 - [3] ETSI EN 303 645, Cyber Security for Consumer Internet of Things: Baseline Requirements.
 - [4] ETSI TS 103 701, Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements.
 - [5] NIST IR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers.
 - [6] NIST IR 8425, Profile of the IoT Core Baseline for Consumer IoT Products.
 - [7] EN 18031-1:2024, EN 18031-2:2024, EN 18031-3:2024, Common security requirements for radio equipment.
 - [8] IEC 62443 , Industrial communication networks - Network and system security.
 - [9] ISO/IEC 27005, Information security, cybersecurity and privacy protection - Guidance on managing information security risks.
 - [10] ISO/IEC 29134, Information technology - Security techniques - Guidelines for privacy impact assessment.
 - [11] ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, Information security and privacy information management systems.
 - [12] TCVN 9801-1:2022, Công nghệ thông tin - Các kỹ thuật an toàn - An toàn mạng - Phần 1: Tổng quan và khái niệm.
-