BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 736 /QĐ-BTTTT	*Hà Nội, ngày 31 tháng 5 năm 2021*

QUYẾT ĐỊNH

Ban hành Danh mục yêu cầu cơ bản bảo đảm an toàn thông tin mạng cho thiết bị IoT tiêu dùng

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Danh mục yêu cầu cơ bản bảo đảm an toàn thông tin mạng cho thiết bị IoT tiêu dùng.

Điều 2. Khuyến nghị áp dụng Danh mục tại Điều 1 Quyết định này trong việc bảo đảm an toàn thông tin mạng cho thiết bị IoT tiêu dùng.

Điều 3. Cục An toàn thông tin chủ trì, phối hợp với các cơ quan, đơn vị liên quan hướng dẫn, kiểm tra, đánh giá việc áp dụng các yêu cầu theo Danh mục tại Điều 1 Quyết định này.

Điều 4. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 5. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, Thủ trưởng các đơn vị thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 5;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng Thông tin điện tử của Bộ;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Huy Dũng

DANH MỤC YÊU CẦU BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG CHO THIẾT BỊ IOT TIÊU DÙNG

(Ban hành kèm theo Quyết định số 736/QĐ-BTTTT ngày 31 tháng 5 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông)

STT	Tên yêu cầu	Quy định áp dụng
I	Yêu cầu về an toàn thông tin mạng cho thiết bị IoT tiêu dùng	
1	Không sử dụng mật khẩu mặc định dùng chung	Chấp thuận nguyên vẹn yêu cầu tại mục 5.1, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
2	Triển khai biện pháp quản lý báo cáo về các lỗ hổng bảo mật	Chấp thuận nguyên vẹn yêu cầu tại mục 5.2, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
3	Bảo đảm phần mềm trên thiết bị luôn được cập nhật	Chấp thuận nguyên vẹn yêu cầu tại mục 5.3, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.
4	Lưu trữ an toàn các tham số bảo mật nhạy cảm	Chấp thuận nguyên vẹn yêu cầu tại mục 5.4, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
5	Sử dụng các giao tiếp kết nối an toàn	Chấp thuận nguyên vẹn yêu cầu tại mục 5.5, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
6	Hạn chế tối thiểu các bề mặt cho phép tấn công, khai thác	Chấp thuận nguyên vẹn yêu cầu tại mục 5.6, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer

		Internet of Things: Baseline Requirements
7	Bảo đảm tính nguyên vẹn của phần mềm	Chấp thuận nguyên vẹn yêu cầu tại mục 5.7, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
8	Bảo đảm an toàn thông tin dữ liệu cá nhân	Chấp thuận nguyên vẹn yêu cầu tại mục 5.8, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
9	Khả năng tự khôi phục lại hệ thống bình thường sau sự cố	Chấp thuận nguyên vẹn yêu cầu tại mục 5.9, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
10	Cho phép kiểm tra, đánh giá dữ liệu hệ thống từ xa	Chấp thuận nguyên vẹn yêu cầu tại mục 5.10, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
11	Cho phép người dùng dễ dàng xóa dữ liệu cá nhân	Chấp thuận yêu cầu tại mục 5.11, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. Loại bỏ "including the GDPR" trong 5.11-2 do đây là Luật Bảo vệ dữ liệu chung áp dụng cho châu Âu.
12	Dễ dàng cài đặt và bảo trì thiết bị	Chấp thuận nguyên vẹn yêu cầu tại mục 5.12, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
13	Khả năng kiểm tra tính hợp lệ của dữ liệu đầu vào	Chấp thuận nguyên vẹn yêu cầu tại mục 5.13, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer

		Internet of Things: Baseline Requirements
II	Yêu cầu về bảo vệ dữ liệu cá nhân cho thiết bị IoT tiêu dùng	Chấp thuận nguyên vẹn yêu cầu tại mục 6, tiêu chuẩn ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

Phụ lục

CÁC THUẬT NGỮ, ĐỊNH NGHĨA

(Ban hành kèm theo Quyết định số 736 /QĐ-BTTTT ngày 31 tháng 5 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông)

1. Thiết bị IoT tiêu dùng

Thiết bị IoT tiêu dùng là thiết bị kết nối mạng (hoặc có thể kết nối mạng) có mối quan hệ với các dịch vụ liên kết và được người tiêu dùng sử dụng trong gia đình hoặc làm thiết bị đeo điện tử.

CHÚ THÍCH 1: Các thiết bị IoT tiêu dùng cũng thường được sử dụng trong kinh doanh. Các thiết bị này vẫn được phân loại là thiết bị IoT tiêu dùng.

CHÚ THÍCH 2: Các thiết bị IoT tiêu dùng thường được bày bán trong cửa hàng bán lẻ. Các thiết bị IoT tiêu dùng cũng có thể được vận hành và/hoặc cài đặt bằng dịch vụ chuyên nghiệp.

Một danh sách không đầy đủ về thiết bị IoT tiêu dùng bao gồm:

- Đồ chơi trẻ em và màn hình theo dõi, giám sát trẻ em được kết nối mạng;
- Đầu báo khói, khóa cửa và cảm biến cửa sổ được kết nối mạng;
- Cổng kết nối IoT, trạm gốc và trung tâm (hub) kết nối thiết bị;
- Máy ảnh, TV và loa thông minh;
- Thiết bị theo dõi sức khỏe dạng đeo;
- Hệ thống tự động hóa và báo động trong nhà được kết nối mạng, đặc biệt là các cổng và trung tâm kết nối;
- Thiết bị gia dụng được kết nối mạng, như máy giặt và tủ lạnh;
- Hệ thống hỗ trợ quản lý nhà thông minh.

2. Thiết bị hạn chế

Thiết bị hạn chế là thiết bị có giới hạn vật lý về khả năng xử lý dữ liệu, giao tiếp dữ liệu, lưu trữ dữ liệu hoặc tương tác với người dùng, do các hạn chế phát sinh từ mục đích sử dụng.

CHÚ THÍCH 1: Các giới hạn vật lý có thể do nguồn điện, tuổi thọ pin, năng lực xử lý, truy cập vật lý, chức năng giới hạn, bộ nhớ giới hạn hoặc băng thông mạng giới hạn. Những giới hạn này có thể yêu cầu thiết bị hạn chế phải được hỗ trợ bởi một thiết bị khác, chẳng hạn như trạm gốc hoặc thiết bị đi kèm.

VÍ DỤ 1: Người dùng không thể sạc hoặc thay pin của cảm biến cửa sổ; đây là một thiết bị hạn chế.

VÍ DỤ 2: Thiết bị không thể cập nhật phần mềm do giới hạn lưu trữ, dẫn đến thay thế phần cứng hoặc ngắt ra khỏi mạng là những lựa chọn duy nhất để quản lý lỗ hổng bảo mật.

VÍ DỤ 3: Một thiết bị năng lượng thấp sử dụng pin để có thể được triển khai ở nhiều vị trí. Thực hiện các hoạt động mật mã năng lượng cao sẽ nhanh chóng làm giảm tuổi thọ pin, vì vậy nó dựa vào trạm gốc hoặc thiết bị trung tâm (hub) để thực hiện xác nhận các bản cập nhật.

VÍ DỤ 4: Thiết bị không có màn hình hiển thị để xác thực mã ràng buộc cho ghép nối Bluetooth.

VÍ DỤ 5: Thiết bị không có khả năng nhập liệu, chẳng hạn như thông qua bàn phím, thông tin xác thực.

CHÚ THÍCH 2: Một thiết bị có nguồn điện dây, hỗ trợ các giao thức dựa trên IP và các mật mã nguyên thủy được sử dụng bởi các giao thức đó không phải là thiết bị hạn chế.

VÍ DỤ 6: Một thiết bị được cấp nguồn chính và giao tiếp chủ yếu bằng TLS (Bảo mật tầng giao vận).

3. Dịch vụ liên kết

Dịch vụ liên kết là dịch vụ kỹ thuật số, cùng với thiết bị, tạo nên một giải pháp IoT tổng thể và thường được yêu cầu để cung cấp chức năng dự kiến của sản phẩm.

VÍ DỤ 1: Các dịch vụ liên kết có thể bao gồm các ứng dụng di động, điện toán đám mây/lưu trữ và Giao diện lập trình ứng dụng (API) của bên thứ ba.

VÍ DỤ 2: Một thiết bị truyền dữ liệu kiểm tra, đánh giá từ xa đến dịch vụ của bên thứ ba do nhà sản xuất thiết bị chọn cũng là một dịch vụ liên kết.