Mẫu Phụ lục VI - Thông tư 13/2019/TT-BTTTT

**THUYẾT MINH DỰ THẢO QUY CHUẨN KỸ THUẬT QUỐC GIA**

**YÊU CẦU AN TOÀN THÔNG TIN CƠ BẢN CHO CAMERA GIÁM SÁT sử dụng giao thức InTERNET**

**1. Tên gọi và ký hiệu của QCVN**

Tên gọi: Quy chuẩn kỹ thuật quốc gia về yêu cầu an toàn thông tin cơ bản cho camera giám sát sử dụng giao thức Internet.

Ký hiệu: QCVN XXXX:2024/BTTTT.

**2. Đặt vấn đề**

*2.1. Tổng quan*

a) Giới thiệu camera sử dụng giao thức Internet (IP Camera)

IP Camera (Internet Protocol Camera) là một loại camera kỹ thuật số có khả năng gửi và nhận dữ liệu qua mạng Internet. Khác với camera analog truyền thống, IP camera không cần đầu ghi hình riêng biệt mà có thể hoạt động độc lập và truyền hình ảnh trực tiếp đến các thiết bị kết nối mạng như điện thoại, máy tính, hoặc máy chủ lưu trữ.

Một hệ thống IP camera bao gồm các thành phần sau:



IP Camera: Thiết bị ghi hình và gửi dữ liệu hình ảnh qua mạng.

Router: Thiết bị chuyển tiếp dữ liệu từ IP camera đến mạng Internet.

Switch: Thiết bị kết nối nhiều IP camera trong cùng một hệ thống mạng.

Máy chủ lưu trữ/NVR (Network Video Recorder): Thiết bị lưu trữ và quản lý dữ liệu video từ các IP camera.

Thiết bị xem (PC, smartphone): Thiết bị nhận và xem dữ liệu hình ảnh từ IP camera.

Một số vấn đề bảo mật phổ biến liên quan đến IP camera bao gồm:

* + Tấn công DoS (Denial of Service): Kẻ tấn công làm quá tải hệ thống, khiến camera ngừng hoạt động.
  + Tấn công Brute Force: Thử nhiều mật khẩu để chiếm quyền điều khiển camera.
  + Lỗ hổng phần mềm: Sử dụng lỗ hổng trong phần mềm camera để xâm nhập và kiểm soát hệ thống.
  + Nghe lén và đánh cắp dữ liệu: Xâm nhập vào mạng để nghe lén và đánh cắp dữ liệu video.
  + Thiết lập bảo mật yếu: Sử dụng mật khẩu mặc định, không mã hóa dữ liệu, và không cập nhật phần mềm thường xuyên.

b) Hiện trạng

Theo dự báo đến năm 2025, thế giới sẽ có hơn 75 tỷ thiết bị IoT kết nối Internet, trong đó có 1 tỷ camera giám sát được sử dụng. Theo thống kê của Tổng cục Hải quan, tại Việt Nam đã có trên 16 triệu thiết bị camera giám sát được nhập khẩu và triển khai, sử dụng trên thị trường trong 5 năm gần đây. Ước tính đến năm 2025, Việt Nam sẽ có hơn 20 triệu camera giám sát được sử dụng, bằng 1/5 dân số cả nước. Số lượng, chủng loại camera nhập khẩu mỗi năm[[1]](#footnote-1): Bao gồm 163 loại mặt hàng nhập khẩu camera giám sát và IP camera thuộc mã 8525.80 (được kết xuất theo tên hàng camera giám sát, quan sát, an ninh, ip camera). Trung bình mỗi năm nhập khẩu 3,2 triệu. Trong đó, Trung Quốc tỷ lệ 96,3%, Hàn Quốc 0,6%, Khác: 3,1%.

Các thiết bị camera giám sát là một trong những đối tượng được tin tặc nhắm tới trong các cuộc tấn công và tiềm ẩn nhiều rủi ro bị khai thác, xâm nhập và chiếm quyền điều khiển. Hậu quả là thông tin, dữ liệu của người dùng có thể bị thu thập trái phép, sau đó được sử dụng cho các mục đích lừa đảo và chiếm đoạt tài sản, gây ảnh hưởng đến uy tín, danh dự của cá nhân, tổ chức; thiết bị camera bị chiếm quyền điều khiển và sử dụng cho các cuộc tấn công mạng, phát tán các chương trình, phần mềm độc hại lây lan trong các hệ thống thông tin.

Hệ thống giám sát của Bộ Thông tin và Truyền thông đã phát hiện hơn 800 nghìn camera giám sát của Việt Nam đang bị chia sẻ dữ liệu hình ảnh công khai trên mạng Internet, trong số đó có 360 nghìn camera (chiếm 45%) có nguy cơ, điểm yếu, lỗ hổng dễ bị khai thác tấn công, chiếm quyền điều khiển. Hơn nữa, trên mạng xã hội, hàng trăm hội nhóm đã công khai rao bán hình ảnh và video lộ lọt từ camera giám sát, mỗi nhóm có hàng nghìn thành viên với các mức phí từ 200 nghìn đến 1 triệu đồng. Cũng theo thống kê của Bộ Thông tin và Truyền thông, trong năm 2021, trung bình hàng tháng có khoảng 1 triệu địa chỉ IP Việt Nam nằm trong các mạng IP botnet, trong đó có 48.690 địa chỉ IP liên quan trực tiếp đến các mã độc từ camera giám sát (chiếm khoảng 5%).

Ngoài ra, nhóm nguy cơ thứ hai đến từ việc phần lớn các hệ thống thông tin sử dụng camera giám sát chưa được triển khai công tác đảm bảo an toàn thông tin mạng theo cấp độ theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016. Khoảng 90% các hệ thống này chưa được kiểm tra, đánh giá an toàn thông tin mạng trước khi đưa vào vận hành khai thác cũng như đánh giá an toàn thông tin mạng định kỳ hàng năm.

*2.2. Tình hình tiêu chuẩn hóa*

Qua nghiên cứu, khảo sát kinh nghiệm của các quốc gia trong việc đảm bảo an toàn thông tin mạng cho camera giám sát, có thể thấy, cách tiếp cận phổ biến trên thế giới hiện nay đối với các thiết bị IoT nói chung và camera giám sát nói riêng là “an toàn từ khâu thiết kế”. Tức là thiết bị camera khi được cung cấp ra thị trường phải đảm bảo đáp ứng các tiêu chí, tiêu chuẩn về an toàn thông tin mạng. Việc thúc đẩy công bố áp dụng các tiêu chí, tiêu chuẩn an toàn thông tin mạng trong sản xuất thiết bị và quản lý an toàn thông tin mạng liên quan đến việc triển khai các thiết bị này đang được nhiều quốc gia triển khai dưới dạng các chương trình, sáng kiến mà Việt Nam có thể tham khảo.

a) Singapore

Vào tháng 3/2020, Cơ quan An toàn thông tin mạng Singapore (CSA) đã đưa Kế hoạch gán nhãn an toàn thông tin mạng (CLS) vào Kế hoạch tổng thể về an toàn không gian mạng của Singapore. CLS được khởi xướng như một chương trình tự nguyện và sử dụng cho các thiết bị tiêu dùng thông minh có kết nối internet hoặc thiết bị IoT tiêu dùng. Nhãn an toàn thông tin mạng cho biết mức độ an toàn trong các tính năng bảo mật của thiết bị thông minh, giúp người tiêu dùng đưa ra quyết định sáng suốt về thiết bị và hiểu rõ hơn về khả năng đối mặt với những rủi ro về an toàn thông tin mạng, đồng thời khuyến khích các nhà sản xuất phát triển các sản phẩm an toàn. CLS được thực hiện theo tiêu chuẩn Châu Âu ETSI EN 303 645 dựa trên những đánh giá và kiểm thử về: đáp ứng các yêu cầu an toàn cơ bản như bảo đảm mật khẩu mặc định duy nhất; tuân thủ nguyên tắc an toàn từ khâu thiết kế; không tồn tại lỗ hổng phần mềm phổ biến; có khả năng chống lại các kiểm thử xâm nhập cơ bản.

b) Phần Lan

Phần Lan bắt đầu thực hiện chương trình Gán nhãn an toàn thông tin mạng từ năm 2019. Đây là một chương trình tự nguyện với các yêu cầu dựa trên ETSI EN 303 645. Năm 2019, Phần Lan bắt đầu thí điểm Gán nhãn an toàn thông tin mạng do chuyên gia an toàn thông tin mạng của Cơ quan Quản lý viễn thông Phần Lan (Traficom) thực hiện. Từ năm 2020, khi chương trình này thu hút nhiều đơn đăng ký, quá trình kiểm định được thực hiện bởi các công ty an toàn thông tin mạng chuyên về kiểm định bảo mật và được Traficom phê chuẩn. Sau khi bên thứ 3 thực hiện kiểm định, Traficom sẽ đánh giá quá trình kiểm định và kết quả kiểm định trước khi cấp Nhãn, hiệu lực của Nhãn này được rà soát định kỳ hàng năm.

c) Vương quốc Anh

Bộ Văn hóa, Truyền thông và Thể thao số (DCMS) cùng với Trung tâm An toàn thông tin Quốc gia (NCSC) của Vương quốc Anh đã ban hành tài liệu cung cấp các hướng dẫn nhằm đảm bảo an toàn thông tin cho các sản phẩm IoT tiêu dùng. Tài liệu nhằm hỗ trợ các bên liên quan trong việc phát triển, sản xuất và bán lẻ các sản phẩm IoT tiêu dùng an toàn theo thiết kế. Các yêu cầu an toàn áp dụng cho các sản phẩm IoT tiêu dùng kết nối Internet và/hoặc mạng gia đình cùng với các dịch vụ liên quan như ứng dụng di động, lưu trữ đám mây và API của bên thứ ba. Tài liệu hướng dẫn 13 tiêu chí an toàn, đây cũng là các tiêu chí được Châu Âu tham khảo để xây dựng ETSI EN 303 645:

* Không sử dụng mật khẩu mặc định: Tất cả mật khẩu của thiết bị IoT phải là duy nhất và không được đặt lại về giá trị mặc định của nhà máy.
* Thực hiện chính sách tiết lộ lỗ hổng: Cung cấp điểm liên hệ công khai để báo cáo lỗ hổng bảo mật và xử lý chúng kịp thời.
* Cập nhật phần mềm: Phần mềm phải có khả năng cập nhật an toàn, và các bản cập nhật không được ảnh hưởng đến chức năng của thiết bị.
* Lưu trữ an toàn thông tin nhạy cảm: Thông tin nhạy cảm và thông tin xác thực phải được lưu trữ an toàn trên thiết bị và dịch vụ.
* Giao tiếp an toàn: Sử dụng các tiêu chuẩn internet mở và được đánh giá ngang hàng để bảo mật giao tiếp.
* Giảm thiểu bề mặt tấn công: Thiết bị và dịch vụ chỉ nên cung cấp các quyền truy cập cần thiết và hạn chế các cổng không cần thiết.
* Đảm bảo tính toàn vẹn của phần mềm: Phần mềm trên thiết bị IoT phải được xác minh bằng các cơ chế khởi động an toàn và báo cáo khi phát hiện thay đổi trái phép.
* Bảo vệ dữ liệu cá nhân: Xử lý dữ liệu cá nhân theo luật bảo vệ dữ liệu hiện hành, cung cấp thông tin minh bạch về việc sử dụng dữ liệu.
* Tăng cường tính bền vững của hệ thống: Thiết kế các hệ thống IoT để duy trì hoạt động trong trường hợp mất kết nối mạng hoặc điện, và khôi phục một cách có trật tự.
* Giám sát dữ liệu hệ thống: Thu thập và giám sát dữ liệu nhật ký để phát hiện các tình huống bất thường và giảm thiểu rủi ro.
* Dễ dàng xóa dữ liệu cá nhân: Cung cấp cơ chế cho phép người dùng xóa dữ liệu cá nhân khi thay đổi quyền sở hữu thiết bị hoặc khi không còn sử dụng.
* Dễ dàng cài đặt và bảo trì thiết bị: Đảm bảo quy trình cài đặt và bảo trì đơn giản, cung cấp hướng dẫn rõ ràng để người dùng có thể cấu hình thiết bị một cách an toàn.
* Xác thực dữ liệu đầu vào: Kiểm tra và xác thực dữ liệu đầu vào qua giao diện người dùng và API để ngăn chặn dữ liệu không hợp lệ.

d) Hoa Kỳ

Vào tháng 02/2022, Viện Tiêu chuẩn và công nghệ quốc gia đã ban hành tài liệu cung cấp các tiêu chí được khuyến nghị cho chương trình dán nhãn an toàn thông tin cho các sản phẩm IoT tiêu dùng (Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products) theo Sắc lệnh Hành pháp (EO) 14028 nhằm "Cải thiện An toàn thông tin của Quốc gia" ban hành ngày 12 tháng 5, 2021.

Mục tiêu nhằm đưa ra các tiêu chí cho nhãn sản phẩm IoT tiêu dùng, thiết kế nhãn, giáo dục người tiêu dùng và các cân nhắc đánh giá sự phù hợp. Tiêu chí được khuyến nghị cho sản phẩm IoT và nhà phát triển sản phẩm IoT, bao gồm:

* Nhận diện tài sản: Sản phẩm IoT phải có thể nhận diện duy nhất và duy trì danh sách các thành phần kết nối.
* Cấu hình sản phẩm: Cho phép thay đổi cấu hình và khôi phục cài đặt mặc định an toàn.
* Bảo vệ dữ liệu: Bảo vệ dữ liệu lưu trữ và truyền dẫn khỏi truy cập, tiết lộ và sửa đổi trái phép.
* Kiểm soát truy cập giao diện: Hạn chế truy cập logic đến các giao diện và dịch vụ chỉ cho các thực thể được ủy quyền.
* Cập nhật phần mềm: Có thể cập nhật phần mềm một cách an toàn.
* Nhận thức trạng thái an toàn thông tin: Hỗ trợ phát hiện các sự cố an toàn thông tin.
* Tài liệu: Tạo và lưu trữ thông tin liên quan đến an toàn thông tin trong suốt vòng đời phát triển sản phẩm.
* Tiếp nhận thông tin và truy vấn: Có khả năng tiếp nhận thông tin liên quan đến an toàn thông tin và trả lời các truy vấn từ khách hàng.
* Phát tán thông tin: Phát sóng và phân phối thông tin liên quan đến an toàn thông tin.
* Giáo dục và nâng cao nhận thức: Tạo ra nhận thức và giáo dục khách hàng về thông tin liên quan đến an toàn thông tin.

Cách tiếp cận nhãn: Khuyến nghị sử dụng nhãn nhị phân (chỉ định sản phẩm đã đáp ứng tiêu chuẩn cơ bản) kết hợp với mã QR hoặc URL để cung cấp thêm chi tiết trực tuyến.

*2.3. Một số tiêu chuẩn quốc tế liên quan*

a) ETSI EN 303 645: "Cyber Security for Consumer Internet of Things: Baseline Requirements"

TSI EN 303 645 là tiêu chuẩn do Viện Tiêu chuẩn Viễn thông Châu Âu (ETSI) phát triển, nhằm mục đích thiết lập các yêu cầu an toàn cho các thiết bị IoT tiêu dùng. Tiêu chuẩn này, được công bố vào tháng 6 năm 2020, nhằm đảm bảo rằng các thiết bị IoT tiêu dùng có mức an toàn cơ bản và bảo vệ quyền riêng tư của người dùng. Một số nội dung chính của ETSI EN 303 645:

- Quản lý mật khẩu: Các thiết bị không nên sử dụng mật khẩu mặc định và cố định mà tất cả các thiết bị đều giống nhau. Mật khẩu nên được quản lý một cách an toàn.

- Cập nhật phần mềm: Các thiết bị phải có khả năng cập nhật phần mềm để sửa lỗi bảo mật. Quá trình cập nhật phần mềm phải an toàn và được bảo vệ chống lại các cuộc tấn công.

- Bảo mật dữ liệu cá nhân: Các thiết bị phải bảo vệ dữ liệu cá nhân của người dùng và tuân thủ các quy định về bảo vệ dữ liệu. Dữ liệu cá nhân phải được mã hóa khi truyền tải và lưu trữ.

- Bảo vệ giao tiếp: Giao tiếp giữa các thiết bị phải được bảo vệ để tránh việc bị đánh cắp hoặc sửa đổi thông tin. Các thiết bị phải sử dụng các giao thức bảo mật tiêu chuẩn.

- Quản lý và bảo vệ tài khoản người dùng: Các thiết bị phải cung cấp cơ chế quản lý và bảo vệ tài khoản người dùng. Phải có cơ chế đăng nhập an toàn và bảo vệ khỏi các cuộc tấn công brute-force.

- Xử lý các lỗ hổng bảo mật: Các nhà sản xuất phải có quy trình để báo cáo và xử lý các lỗ hổng bảo mật được phát hiện trong các thiết bị của họ. Các lỗ hổng bảo mật phải được vá kịp thời để bảo vệ người dùng.

ETSI EN 303 645 đã được công nhận rộng rãi và được coi là một bước tiến quan trọng trong việc nâng cao bảo mật của các thiết bị IoT tiêu dùng. Tiêu chuẩn này giúp các nhà sản xuất tạo ra các sản phẩm an toàn hơn và giúp người tiêu dùng yên tâm hơn khi sử dụng các thiết bị IoT.

b) TSI TS 103 701: "Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements"

ETSI TS 103 701 là tiêu chuẩn kỹ thuật do Viện Tiêu chuẩn Viễn thông Châu Âu (ETSI) phát triển, nhằm cung cấp các chỉ dẫn chi tiết về cách đo lường và đánh giá sự tuân thủ của các thiết bị IoT (Internet of Things) tiêu dùng theo tiêu chuẩn bảo mật ETSI EN 303 645. Một số nội dung chính của ETSI TS 103 701:

- Phạm vi áp dụng: Tiêu chuẩn này đưa ra các phương pháp và quy trình để đánh giá và kiểm tra sự tuân thủ của các thiết bị IoT tiêu dùng với ETSI EN 303 645. Nó tập trung vào các biện pháp bảo mật và các yêu cầu bảo mật cơ bản đã được xác định trong EN 303 645.

- Phương pháp đánh giá: ETSI TS 103 701 xác định các phương pháp kiểm tra, bao gồm kiểm tra chức năng, kiểm tra an toàn thông tin, và kiểm tra khả năng cập nhật phần mềm. Các bài kiểm tra bao gồm việc đánh giá việc quản lý mật khẩu, bảo mật cập nhật phần mềm, bảo vệ dữ liệu cá nhân, và các biện pháp bảo vệ giao tiếp.

- Quy trình kiểm tra: Tiêu chuẩn này cung cấp một quy trình kiểm tra chi tiết, từ việc chuẩn bị và lập kế hoạch kiểm tra, thực hiện kiểm tra, cho đến báo cáo kết quả kiểm tra. Quy trình kiểm tra bao gồm cả kiểm tra thủ công và tự động để đảm bảo độ chính xác và độ tin cậy.

- Yêu cầu đối với nhà sản xuất: Các nhà sản xuất thiết bị IoT tiêu dùng cần phải thực hiện các kiểm tra này để đảm bảo sản phẩm của họ tuân thủ các yêu cầu bảo mật cơ bản. Báo cáo kết quả kiểm tra phải được cung cấp để chứng minh sự tuân thủ.

- Bảo vệ quyền riêng tư: ETSI TS 103 701 cũng đặt ra các yêu cầu về việc bảo vệ quyền riêng tư của người dùng trong suốt quá trình kiểm tra và đánh giá. Dữ liệu cá nhân thu thập trong quá trình kiểm tra phải được xử lý và bảo vệ đúng quy định.

*2.4. Các tiêu chuẩn và yêu cầu kỹ thuật cơ bản trong nước*

a) Quyết định 736/QĐ-BTTTT ngày 31/5/2021 về Danh mục yêu cầu cơ bản bảo đảm an toàn thông tin mạng cho thiết bị IoT tiêu dùng.

Quyết định 736/QĐ-BTTTT do Bộ Thông tin và Truyền thông Việt Nam ban hành ngày 31 tháng 5 năm 2021, đưa ra Danh mục yêu cầu cơ bản bảo đảm an toàn thông tin mạng cho thiết bị IoT tiêu dùng. Quyết định này nhằm mục đích thiết lập các tiêu chuẩn an toàn thông tin mạng, đảm bảo rằng các thiết bị IoT tiêu dùng tại Việt Nam đáp ứng các yêu cầu cơ bản về bảo mật. Dưới đây là một số điểm chính trong Quyết định 736/QĐ-BTTTT:

- Quản lý mật khẩu: Thiết bị không được sử dụng mật khẩu mặc định và cố định. Người dùng phải có khả năng thay đổi mật khẩu mặc định.

- Cập nhật phần mềm: Thiết bị phải hỗ trợ khả năng cập nhật phần mềm để khắc phục lỗ hổng bảo mật. Quá trình cập nhật phải được thực hiện một cách an toàn.

- Bảo vệ dữ liệu cá nhân: Dữ liệu cá nhân của người dùng phải được bảo vệ, bao gồm mã hóa khi truyền tải và lưu trữ. Thiết bị phải tuân thủ các quy định về bảo vệ dữ liệu cá nhân. Cho phép người dùng dễ dàng xóa dữ liệu cá nhân

- Bảo vệ giao tiếp: Giao tiếp giữa các thiết bị IoT phải được bảo vệ để ngăn chặn việc đánh cắp hoặc thay đổi thông tin. Các giao thức bảo mật tiêu chuẩn phải được sử dụng.

- Quản lý và bảo vệ tài khoản người dùng: Thiết bị phải cung cấp các cơ chế quản lý và bảo vệ tài khoản người dùng. Các biện pháp bảo vệ khỏi các cuộc tấn công brute-force phải được triển khai.

- Xử lý các lỗ hổng bảo mật: Nhà sản xuất phải có quy trình để báo cáo và xử lý các lỗ hổng bảo mật phát hiện được. Các lỗ hổng bảo mật phải được vá kịp thời.

- Giám sát và kiểm tra: Thiết bị phải có khả năng cho phép kiểm tra, đánh giá dữ liệu hệ thống từ xa để đảm bảo tuân thủ các yêu cầu an toàn thông tin mạng. Báo cáo kết quả kiểm tra phải được cung cấp cho cơ quan quản lý khi cần thiết.

Quyết định 736/QĐ-BTTTT là một bước tiến quan trọng trong việc nâng cao bảo mật cho các thiết bị IoT tiêu dùng tại Việt Nam, giúp người tiêu dùng yên tâm hơn khi sử dụng các thiết bị này và đảm bảo rằng các nhà sản xuất tuân thủ các tiêu chuẩn an toàn thông tin mạng cần thiết.

b) Quyết định số 724/QĐ-BTTTT ngày 07/5/2024 ban hành Bộ tiêu chí về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát.

Quyết định số 724/QĐ-BTTTT ngày 07 tháng 5 năm 2024 được ban hành bởi Bộ Thông tin và Truyền thông Việt Nam, nhằm thiết lập Bộ tiêu chí về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát. Quyết định này đề ra các tiêu chuẩn bảo mật cần thiết để đảm bảo an toàn thông tin mạng cho các thiết bị camera giám sát, nhằm bảo vệ người dùng và dữ liệu của họ. Dưới đây là một số điểm chính của Quyết định số 724/QĐ-BTTTT:

- Phạm vi điều chỉnh: Đưa ra các yêu cầu kỹ thuật an toàn thông tin mạng cho thiết bị camera giám sát sử dụng giao thức mạng.

- Đối tượng áp dụng: Áp dụng cho các tổ chức, cá nhân Việt Nam và nước ngoài liên quan đến hoạt động nghiên cứu, phát triển, sản xuất, đánh giá, lựa chọn và sử dụng thiết bị camera.

- Yêu cầu về tài liệu: Phải có tài liệu hướng dẫn sử dụng sản phẩm.

- Quản lý xác thực, Phòng chống tấn công vét cạn: Thiết lập thời gian khóa và thông báo đăng nhập thất bại. Quản lý mật khẩu an toàn: Yêu cầu thay đổi mật khẩu mặc định, kiểm soát mật khẩu an toàn, sử dụng hàm băm SHA-256 hoặc cao hơn.

- Quản lý lỗ hổng bảo mật: Nhà sản xuất phải có hệ thống quản lý lỗ hổng và công bố thông tin về lỗ hổng.

- Quản lý và thực hiện cập nhật: Hệ thống quản lý cập nhật, thông tin phiên bản cập nhật, chức năng cập nhật qua Internet.

- Quản lý phiên an toàn: Quản lý phiên đăng nhập và tạo khóa phiên an toàn.

- Quản lý kênh giao tiếp: Yêu cầu đối với các giao tiếp kết nối an toàn và truy cập cấu hình thiết bị an toàn.

- Quản lý giao diện: Bảo mật thông tin xác thực, quản lý giao diện logic và mạng, giao diện gỡ lỗi, và giao diện vật lý.

- Bảo đảm an toàn thông tin dữ liệu người sử dụng: Bảo vệ dữ liệu cá nhân, cảm biến thu thập dữ liệu, thông báo bảo vệ dữ liệu cá nhân, và xóa dữ liệu.

- An toàn ứng dụng: Kiểm tra tính hợp lệ của dữ liệu đầu vào và ngăn chặn các dạng tấn công vào giao diện của thiết bị.

- Khả năng tự khôi phục lại hệ thống: Thiết bị phải đảm bảo hoạt động bình thường sau khi khởi động lại do lỗi phát sinh (ngoại trừ lỗi phần cứng).

*2.5. Căn cứ, mục đích*

a) Về căn cứ

Vấn đề an toàn, bảo mật liên quan đến thiết bị camera giám sát đang trở thành một vấn đề nhức nhối trong xã hội. Thực tế trong thời gian vừa qua tại Việt Nam đã xảy ra nhiều vụ lộ lọt thông tin cá nhân, dữ liệu hình ảnh camera riêng tư bị thu thập trái phép và tung lên mạng xã hội gây bất an cho người sử dụng và làm ảnh hưởng không nhỏ đến an toàn, an ninh xã hội. Hơn nữa, đến nay, trên cả nước đã có 41 trên 63 tỉnh, thành phố trực thuộc trung ương đã hoặc đang triển khai xây dựng đề án về đô thị thông minh. Trong đó, camera giám sát thông minh chính là các thiết bị nền tảng, chiếm đa số các hạng mục triển khai và phát triển đô thị thông minh. Trong thời gian tới sẽ có thêm hàng chục triệu camera giám sát được triển khai và đưa vào sử dụng tại Việt Nam.

Tỷ trọng sản phẩm camera giám sát được sản xuất trong nước hiện nay còn rất khiêm tốn, chiếm ưu thế là các sản phẩm đến từ các thương hiệu nước ngoài. Hơn nữa, tất cả các sản phẩm này đều chưa được kiểm tra, đánh giá an toàn thông tin mạng. Điều này đặt ra yêu cầu cấp bách cần kiểm soát, đánh giá an toàn thông tin mạng cho các thiết bị này khi nhập khẩu, trước khi đưa vào sử dụng và trong quá trình triển khai, vận hành. Đồng thời thúc đẩy sản xuất sản phẩm camera giám sát “Make in Việt Nam” đảm bảo yêu cầu an toàn thông tin mạng nhằm đáp ứng thị trường trong nước. Vấn đề này cũng được Chính phủ đặc biệt quan tâm và đã được Thủ tướng Chính phủ chỉ đạo tại Chỉ thị 23/CT-TTg năm 2022 về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát.

Căn cứ điểm a Khoản 2 Điều 52 Luật An toàn thông tin mạng, Bộ Thông tin và Truyền thông có trách nhiệm xây dựng, ban hành quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng.

Camera giám sát (mã HS 852589) thuộc nhóm 8525 (Thiết bị phát dùng cho phát thanh sóng vô tuyến hoặc truyền hình, có hoặc không gắn với thiết bị thu hoặc ghi hoặc tái tạo âm thanh; camera truyền hình, camera kỹ thuật số và camera ghi hình ảnh) theo quy định tại Thông tư 31/2022/TT-BTC, là nhóm sản phẩm thuộc thẩm quyền quản lý nhà nước của Bộ Thông tin và Truyền thông. Căn cứ về thẩm quyền ban hành QCVN về an toàn thông tin cho camera giám sát, các quy định về quản lý an toàn thông tin đối với thiết bị CNTT nói chung và camera giám sát nói riêng.

Do vậy, việc xây dựng, ban hành quy chuẩn kỹ thuật quốc gia về yêu cầu an toàn thông tin cơ bản cho camera giám sát sử dụng giao thức Internet là đúng thẩm quyền quản lý nhà nước của Bộ Thông tin và Truyền thông.

b) Về mục đích, đối tượng

Quy chuẩn kỹ thuật quốc gia về yêu cầu an toàn thông tin cơ bản cho camera giám sát sử dụng giao thức Internet được xây dựng và ban hành nhằm mục đích quản lý, tăng cường bảo đảm an toàn cho hệ thống IP Camera:

- Quy chuẩn kỹ thuật đảm bảo các biện pháp an ninh như quản lý mật khẩu an toàn, cập nhật phần mềm định kỳ, và bảo vệ giao tiếp dữ liệu để ngăn chặn tấn công từ chối dịch vụ (DoS) và các mối đe dọa bảo mật khác.

- Thiết lập các quy tắc mã hóa dữ liệu và quản lý quyền truy cập để đảm bảo an toàn thông tin cá nhân. Quy chuẩn này giúp ngăn chặn việc đánh cắp dữ liệu và lạm dụng thông tin cá nhân từ hệ thống camera giám sát qua đó bảo vệ dữ liệu cá nhân và quyền riêng tư.

- Đảm bảo tính minh bạch và độ tin cậy: Tạo điều kiện cho các nhà sản xuất và người dùng cuối yên tâm về tính an toàn của sản phẩm. Các quy định về giám sát, kiểm tra định kỳ, và quản lý lỗ hổng bảo mật giúp duy trì độ tin cậy của hệ thống camera giám sát.

Đối tượng áp dụng của quy chuẩn là tất cả các loại hình IP Camera được nhập khẩu, sản xuất, phân phối, sử dụng tại Việt Nam.

**3. Sở cứ xây dựng các yêu cầu kỹ thuật**

*3.1. Căn cứ lựa chọn tài liệu tham chiếu*

a) Tiêu Chuẩn của EU ETSI EN 303 645 V2.1.1 (2020-06)

ETSI EN 303 645 V2.1.1 (2020-06) là tiêu chuẩn do Viện Tiêu chuẩn Viễn thông Châu Âu (ETSI) phát triển nhằm thiết lập các yêu cầu an toàn thông tin cơ bản cho các thiết bị IoT tiêu dùng. Tiêu chuẩn này bao gồm các quy định về quản lý mật khẩu, bảo vệ dữ liệu, cập nhật phần mềm, và bảo mật giao tiếp.

Lý do lựa chọn: Tiêu chuẩn ETSI EN 303 645 V2.1.1 (2020-06) được công nhận rộng rãi và đã được nhiều quốc gia áp dụng. Tại Singapore, tiêu chuẩn này đã được triển khai thực tế trong Kế hoạch gán nhãn an toàn thông tin mạng (Cybersecurity Labelling Scheme - CLS) từ năm 2020. Việc áp dụng tiêu chuẩn này giúp đảm bảo rằng các thiết bị IP camera tại Việt Nam đáp ứng được các yêu cầu an toàn thông tin cơ bản và bảo vệ quyền riêng tư của người dùng.

b) Tiêu Chuẩn của EU ETSI TS 103 701 v1.1.1 (2021-08)

ETSI TS 103 701 v1.1.1 (2021-08) là tiêu chuẩn kỹ thuật được phát triển để cung cấp các hướng dẫn chi tiết về cách đo lường và đánh giá sự tuân thủ của các thiết bị IoT tiêu dùng theo tiêu chuẩn ETSI EN 303 645. Tiêu chuẩn này xác định các phương pháp kiểm tra bao gồm kiểm tra chức năng, kiểm tra an toàn thông tin, và kiểm tra khả năng cập nhật phần mềm.

Lý do lựa chọn: ETSI TS 103 701 v1.1.1 (2021-08) cung cấp các tiêu chí cụ thể để làm rõ và chi tiết hóa các yêu cầu an toàn đã đề cập trong ETSI EN 303 645. Bộ Thông tin và Truyền thông Việt Nam đã ban hành Quyết định 736/QĐ-BTTTT ngày 31/5/2021 về danh mục yêu cầu cơ bản đảm bảo an toàn thông tin mạng cho thiết bị IoT tiêu dùng dựa trên tiêu chuẩn này. Quyết định số 724/QĐ-BTTTT ngày 07/5/2024 cũng dựa trên các tiêu chuẩn này để thiết lập bộ tiêu chí về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát. Việc áp dụng tiêu chuẩn này giúp đánh giá mức độ rủi ro và khả năng bị tấn công của thiết bị, xác minh và chứng nhận tính bảo mật của phần mềm và phần cứng.

*3.2. Phương án lựa chọn tiêu chí phù hợp*

Trên cơ sở mục đích xây dựng quy chuẩn và các kinh nghiệm của các nước, đơn vị soạn thảo nhận thấy các yêu cầu trong tiêu chuẩn ETSI EN 303 645, ETSI TS 103 701 và Kế hoạch gán nhãn an toàn thông tin mạng (CLS) của Singapore là phù hợp với thực trạng tại Việt Nam. Cụ thể các tiêu chuẩn/tài liệu lựa chọn làm tài liệu tham chiếu chính để xây dựng QCVN gồm:

- ETSI EN 303 645: Chọn các yêu cầu cơ bản tối thiểu bắt buộc để đảm bảo tính bảo mật nền tảng. Các yêu cầu này bao gồm quản lý mật khẩu mặc định, bảo vệ giao tiếp dữ liệu, và cập nhật phần mềm an toàn và bảo mật.

- ETSI TS 103 701: Lựa chọn một số tiêu chí cụ thể để làm rõ và chi tiết hóa các yêu cầu an toàn đã đề cập trong ETSI EN 303 645, bao gồm đánh giá mức độ rủi ro và khả năng bị tấn công của thiết bị, xác minh và chứng nhận tính bảo mật của phần mềm và phần cứng, và các biện pháp bảo vệ dữ liệu cá nhân và đảm bảo quyền riêng tư của người dùng.

- CLS của Singapore: Tham khảo mức 2 và lựa chọn các yêu cầu bắt buộc ở mức 3 trong 4 mức độ an toàn của tài liệu này. Các tiêu chí được lựa chọn phải đảm bảo tính phù hợp khi áp dụng cho các thiết bị camera giám sát, bao gồm cơ chế phát hiện và ngăn chặn tấn công mạng, bảo mật truyền thông dữ liệu, xác thực mạnh mẽ, và cơ chế khôi phục dữ liệu và hệ thống trong trường hợp bị tấn công.

- Các yêu cầu kỹ thuật liên quan tại Quyết định 736/QĐ-BTTTT ngày 31/5/2021 về Danh mục yêu cầu cơ bản bảo đảm an toàn thông tin mạng cho thiết bị IoT tiêu dùng và Quyết định số 724/QĐ-BTTTT ngày 07/5/2024 ban hành Bộ tiêu chí về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát.

**4. Giải thích nội dung QCVN**

**4.1. Quy định chung**

Phần này bao gồm các quy định cơ bản về phạm vi điều chỉnh, đối tượng áp dụng, tài liệu viện dẫn, chữ viết tắt và giải thích từ ngữ liên quan.

* **Phạm vi điều chỉnh**:

Quy chuẩn này đề ra các yêu cầu kỹ thuật về an toàn thông tin mạng cơ bản đối với các thiết bị camera giám sát sử dụng giao thức mạng Internet. Các yêu cầu này tập trung vào việc bảo đảm an toàn thông tin cho các thiết bị, bảo vệ dữ liệu người dùng và đảm bảo an toàn trong các giao dịch thông tin qua mạng.

* **Đối tượng áp dụng**:

Quy chuẩn áp dụng cho các tổ chức, cá nhân Việt Nam và nước ngoài liên quan đến hoạt động đánh giá, nghiên cứu phát triển, đánh giá lựa chọn và sử dụng các thiết bị thuộc phạm vi điều chỉnh của quy chuẩn trên lãnh thổ Việt Nam.

* **Tài liệu viện dẫn**:

ETSI EN 303 645 v2.1.1 (2020-06) “Cyber; Cybersecurity for Consumer Internet of Things: Baseline Requirements”.

ETSI TS 103 701 v1.1.1 (2021-08) “Cyber; Cybersecurity for Consumer Internet of Things: Conformance Assessment of Baseline Requirements”; Cybersecurity for Consumer Internet of Things: Conformance Asses.

**4.2. Quy định kỹ thuật**

Đây là phần cốt lõi của quy chuẩn, đưa ra các yêu cầu kỹ thuật cụ thể để đảm bảo an toàn thông tin cho thiết bị camera giám sát.

* **Khởi tạo mật khẩu mặc định duy nhất**:
  + Mật khẩu mặc định phải được khởi tạo duy nhất trên mỗi thiết bị và phải đáp ứng yêu cầu về độ phức tạp (ví dụ, tối thiểu 8 ký tự, bao gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt). Mật khẩu không được chứa thông tin công khai như địa chỉ MAC, SSID Wifi, tên sản phẩm, loại sản phẩm.
* **Quản lý lỗ hổng bảo mật**:
  + Nhà sản xuất phải có hệ thống trực tuyến để tiếp nhận và công bố thông tin về lỗ hổng bảo mật của thiết bị. Chính sách này phải bao gồm thông tin liên hệ để tiếp nhận thông tin, thời gian tối thiểu để xác nhận lỗ hổng, và cập nhật trạng thái xử lý lỗ hổng.
* **Quản lý cập nhật phần mềm**:
  + Thiết bị camera phải có chức năng kiểm tra tính hợp lệ của bản tải cập nhật bằng chữ ký số trước khi thực hiện cập nhật. Nhà sản xuất phải công bố bản cập nhật trong vòng 3 ngày đối với lỗ hổng bảo mật và 5 ngày đối với lỗi phần mềm hệ thống. Việc cập nhật qua mạng phải sử dụng kết nối an toàn được mã hóa.
* **Lưu trữ các thông số bí mật an toàn**:
  + Các tham số bảo mật bí mật phải được mã hóa và lưu trữ an toàn trên bộ nhớ của thiết bị. Các thông số này không được lưu trữ trực tiếp trên mã nguồn phần mềm và phải có độ phức tạp đảm bảo an toàn.
* **Quản lý kênh giao tiếp an toàn**:
  + Các kênh giao tiếp phải sử dụng phương pháp mã hóa dựa trên các tiêu chuẩn hiện hành của Việt Nam hoặc quốc tế. Chỉ cho phép cấu hình thiết bị khi người sử dụng xác thực thành công, và các thông số bảo mật phải được truyền qua kênh mã hóa an toàn.
* **Phòng chống tấn công thông qua các giao diện của thiết bị**:
  + Tất cả các giao diện mạng và logic không sử dụng phải được vô hiệu hóa. Giao diện quản trị phải bảo vệ thông tin liên quan đến các thông số bảo mật bí mật và nhạy cảm.
* **Bảo vệ dữ liệu người sử dụng**:
  + Dữ liệu cá nhân phải được truyền qua kênh kết nối mã hóa an toàn. Thiết bị phải có chức năng cho phép người dùng xóa dữ liệu lưu trữ trên các dịch vụ liên kết và thiết lập thời gian xóa dữ liệu tự động.
* **Khả năng tự khôi phục lại hoạt động bình thường sau sự cố**:
  + Thiết bị camera phải đảm bảo hoạt động bình thường sau khi khởi động lại do sự cố, và phải khôi phục kết nối mạng đến các dịch vụ liên kết khi mạng được khôi phục.
* **Xóa dữ liệu trên thiết bị camera**:
  + Thiết bị phải có chức năng cho phép người dùng xóa dữ liệu cá nhân và cấu hình hệ thống lưu trữ trên thiết bị.
* **Xác thực dữ liệu đầu vào**:
  + Thiết bị phải kiểm tra tính hợp lệ của dữ liệu đầu vào trước khi xử lý.

**4.3. Phương pháp đo và đánh giá kết quả**

Phần này cung cấp các phương pháp và kịch bản kiểm thử chi tiết để đánh giá sự tuân thủ của các thiết bị camera theo các yêu cầu kỹ thuật đã nêu trong phần 2.

* **Nhóm kiểm thử về mật khẩu**:
  + Các nhóm kiểm thử này đánh giá chức năng của mật khẩu mặc định, cơ chế tạo mật khẩu, và khả năng thay đổi mật khẩu qua giao diện đồ họa.
* **Nhóm kiểm thử về quản lý lỗ hổng bảo mật**:
  + Đánh giá sự hiện diện và hiệu quả của chính sách công bố lỗ hổng bảo mật và hệ thống trực tuyến của nhà sản xuất.
* **Nhóm kiểm thử về quản lý cập nhật**:
  + Kiểm thử khả năng ngăn chặn việc lợi dụng cơ chế cập nhật, tính đơn giản trong việc áp dụng cập nhật phần mềm, và sự phù hợp của các cơ chế mã hóa được sử dụng.
* **Nhóm kiểm thử về bảo vệ dữ liệu**:
  + Đánh giá khả năng bảo vệ dữ liệu người dùng, bao gồm việc mã hóa các thông số bảo mật, khả năng chống giả mạo và tính toàn vẹn của dữ liệu.

**4.4. Quy định về quản lý**

Thiết bị camera giám sát sử dụng giao thức mạng thuộc phạm vi điều chỉnh của Quy chuẩn này phải được chứng nhận hợp quy, công bố hợp quy theo quy định.

Phòng thử nghiệm phục vụ hoạt động đánh giá hợp quy phải được Bộ Thông tin và Truyền thông chỉ định hoặc cơ quan có thẩm quyền chỉ định theo quy định.

**4.5. Trách nhiệm của tổ chức, cá nhân**

Cơ quan, tổ chức có liên quan đến hoạt động sản xuất, nhập khẩu thiết bị camera thuộc pháp vi điều chỉnh của Quy chuẩn này thực hiện đánh giá hợp quy theo quy định.

Khuyến khích cơ quan, tổ chức sử dụng sản phẩm camera được công bố hợp chuẩn hợp quy theo quy định tại Quy chuẩn này để bảo đảm an toàn thông tin trong quá trình sử dụng.

**4.6. Tổ chức thực hiện**

Cục An toàn thông tin có trách nhiệm quản lý, tổ chức triển khai, hướng dẫn, đôn đốc, kiểm tra, thanh tra hoạt động đánh giá hợp quy cho camera sử dụng giao thức mạng theo quy định của pháp luật và quy định tại Quy chuẩn này.

Trong trường hợp các quy định tại Quy chuẩn này có sự thay đổi, bổ sung hoặc được thay thế thì thực hiện theo quy định tại văn bản mới.

**4.7. Phụ lục**

Tài liệu cũng bao gồm các phụ lục chi tiết, cung cấp danh mục thông tin cần thiết cho quá trình đánh giá thiết bị, các kịch bản kiểm thử cụ thể, và các tiêu chí kỹ thuật chi tiết để đảm bảo an toàn thông tin cho các thiết bị camera giám sát.

**5. Bảng đối chiếu nội dung QCVN với các tài liệu tham khảo**

|  |  |  |
| --- | --- | --- |
| **Tên QCVN/TCVN** | **Tài liệu tham khảo** | **Phương án xây dựng** |
| 1. Quy định chung |  | Tự xây dựng |
| 1.1. Phạm vi điều chỉnh |  | Tự xây dựng |
| 1.2. Đối tượng áp dụng |  | Tự xây dựng |
| 1.3. Tài liệu viện dẫn |  | Tự xây dựng |
| 1.4. Chữ viết tắt |  | Tham khảo ETSI EN 303 645 |
| 1.5. Giải thích từ ngữ |  | Tham khảo ETSI EN 303 645 |
| 2. Quy định kỹ thuật |  | Tự xây dựng |
| **2.1. Khởi tạo mật khẩu mặc định duy nhất** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.1-1 | Provision 5.1-1 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.1-2 | Provision 5.1-2 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.1-3 | Provision 5.1-3 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.1-4 | Provision 5.1-4 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.1-5 | Provision 5.1-5 | Tham khảo ETSI EN 303 645 |
| **2.2. Quản lý lỗ hổng bảo mật** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.2-1 | Provision 5.2-1 | Tham khảo ETSI EN 303 645 |
| **2.3. Quản lý cập nhật** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.3-1 | Provision 5.3-2 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.3-2 | Provision 5.3-3 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.3-3 | Provision 5.3-7 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.3-4 | Provision 5.3-8 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.3-5 | Provision 5.3-10 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.3-6 | Provision 5.3-13 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.3-7 | Provision 5.3-16 | Tham khảo ETSI EN 303 645 |
| **2.4. Lưu trữ các tham số nhạy cảm an toàn** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.4-1 | Provision 5.4-1 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.4-2 | Provision 5.4-2 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.4-3 | Provision 5.4-3 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.4-4 | Provision 5.4-4 | Tham khảo ETSI EN 303 645 |
| **2.5. Quản lý kênh giao tiếp an toàn** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.5-1 | Provision 5.5-1 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.5-2 | Provision 5.5-5 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.5-3 | Provision 5.5-7 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.5-4 | Provision 5.5-8 | Tham khảo ETSI EN 303 645 |
| **2.6. Phòng chống tấn công thông qua các giao diện của thiết bị** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.6-1 | Provision 5.6-1 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.6-2 | Provision 5.6-2 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.6-3 | Provision 5.6-4 | Tham khảo ETSI EN 303 645 |
| **2.7. Bảo vệ dữ liệu người sử dụng** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.7-1 | Provision 5.8-2 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.7-2 | Provision 5.8-3 | Tham khảo ETSI EN 303 645 |
| **2.8. Khả năng tự khôi phục lại hoạt động bình thường sau sự cố** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.8-1 | Provision 5.9-1 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.8-2 | Provision 5.9-2 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.8-3 | Provision 5.9-3 | Tham khảo ETSI EN 303 645 |
| **2.9. Xóa dữ liệu trên thiết bị camera** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.9-1 | Provision 5.11-1 | Tham khảo ETSI EN 303 645 |
| **2.10. Xác thực dữ liệu đầu vào** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.10-1 | Provision 5.13-1 | Tham khảo ETSI EN 303 645 |
| **2.11. Bảo vệ dữ liệu trên thiết bị camera** | **ETSI EN 303 645** | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.11-1 | Provision 6-1 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.11-2 | Provision 6-2 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.11-3 | Provision 6-3 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.11-4 | Provision 6-4 | Tham khảo ETSI EN 303 645 |
| Yêu cầu 2.11-5 | Provision 6-5 | Tham khảo ETSI EN 303 64, điều chỉnh phù hợp quy định pháp luật Việt Nam |

**Phương pháp đo kiểm**

|  |  |  |
| --- | --- | --- |
| **Dự thảo QCVN** | **ETSI TS 107 301** | **Phương án xây dựng** |
|
| **3.1. Khởi tạo mật khẩu mặc định duy nhất** | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301 |
| 3.1.1 Nhóm kiểm thử 2.1-1 | Test group 5.1-1 | Tham khảo ETSI TS 107 301 |
| 3.1.2 Nhóm kiểm thử 2.1-2 | Test group 5.1-2 | Tham khảo ETSI TS 107 301 |
| 3.1.3 Nhóm kiểm thử 2.1-3 | Test group 5.1-3 | Tham khảo ETSI TS 107 301 |
| 3.1.4 Nhóm kiểm thử 2.1-4 | Test group 5.1-4 | Tham khảo ETSI TS 107 301 |
| 3.1.5 Nhóm kiểm thử 2.1-5 | Test group 5.1-5 | Tham khảo ETSI TS 107 301 |
| 3.2. Quản lý lỗ hổng bảo mật | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301 |
| 3.2.1 Nhóm kiểm thử 2.2-1 | Test group 5.2-1 | Tham khảo ETSI TS 107 301 |
| **3.3. Quản lý cập nhật** | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301 |
| 3.3.1. Nhóm kiểm thử 2.3-1 | Test group 5.3-2 | Tham khảo ETSI TS 107 301 |
| 3.3.2. Nhóm kiểm thử 2.3-2 | Test group 5.3-3 | Tham khảo ETSI TS 107 301 |
| 3.3.3. Nhóm kiểm thử 2.3-3 | Test group 5.3-7 | Tham khảo ETSI TS 107 301 |
| 3.3.4. Nhóm kiểm thử 2.3-4 | Test group 5.3-8 | Tham khảo ETSI TS 107 301 |
| 3.3.5. Nhóm kiểm thử 2.3-5 | Test group 5.3-10 | Tham khảo ETSI TS 107 301 |
| 3.3.6. Nhóm kiểm thử 2.3-6 | Test group 5.3-13 | Tham khảo ETSI TS 107 301 |
| 3.3.7. Nhóm kiểm thử 2.3-7 | Test group 5.3-16 | Tham khảo ETSI TS 107 301 |
| **3.4. Quản lý phiên an toàn** | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301 |
| 3.4.1. Nhóm kiểm thử 2.4-1 | Test group 5.4-1 | Tham khảo ETSI TS 107 301 |
| 3.4.2. Nhóm kiểm thử 2.4-2 | Test group 5.4-2 | Tham khảo ETSI TS 107 301 |
| 3.4.3. Nhóm kiểm thử 2.4-3 | Test group 5.4-3 | Tham khảo ETSI TS 107 301 |
| 3.4.4. Nhóm kiểm thử 2.4-4 | Test group 5.4-4 | Tham khảo ETSI TS 107 301 |
| **3.5. Quản lý kênh giao tiếp** | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301 |
| 3.5.1. Nhóm kiểm thử 2.5-1 | Test group 5.5-1 | Tham khảo ETSI TS 107 301 |
| 3.5.2. Nhóm kiểm thử 2.5-2 | Test group 5.5-5 | Tham khảo ETSI TS 107 301 |
| 3.5.3. Nhóm kiểm thử 2.5-3 | Test group 5.5-7 | Tham khảo ETSI TS 107 301 |
| 3.5.4. Nhóm kiểm thử 2.5-4 | Test group 5.5-8 | Tham khảo ETSI TS 107 301 |
| **3.6. Quản lý giao diện** | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301 |
| 3.6.1. Nhóm kiểm thử 2.6-1 | Test group 5.6-1 | Tham khảo ETSI TS 107 301 |
| 3.6.2. Nhóm kiểm thử 2.6-2 | Test group 5.6-2 | Tham khảo ETSI TS 107 301 |
| 3.6.3. Nhóm kiểm thử 2.6-3 | Test group 5.6-4 | Tham khảo ETSI TS 107 301 |
| **3.7. Bảo đảm an toàn thông tin dữ liệu người sử dụng** | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301 |
| 3.7.1. Nhóm kiểm thử 2.7-1 | Test group 5.8-2 | Tham khảo ETSI TS 107 301 |
| 3.7.1. Nhóm kiểm thử 2.7-1 | Test group 5.8-3 | Tham khảo ETSI TS 107 301 |
| **3.8. Khả năng tự khôi phục lại hệ thống bình thường sau sự cố** | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301 |
| 3.8.1. Nhóm kiểm thử 2.8-1 | Test group 5.9-1 | Tham khảo ETSI TS 107 301 |
| 3.8.2. Nhóm kiểm thử 2.8-2 | Test group 5.9-2 | Tham khảo ETSI TS 107 301 |
| 3.8.3. Nhóm kiểm thử 2.8-3 | Test group 5.9-3 | Tham khảo ETSI TS 107 301 |
| **3.9. Xoá dữ liệu trên thiết bị camera** | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301 |
| 3.9.1. Nhóm kiểm thử 2.9-1 | Test group 5.11-1 | Tham khảo ETSI TS 107 301 |
| **3.10. Xác thực dữ liệu đầu vào** | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301 |
| 3.10.1. Nhóm kiểm thử 2.10-1 | Test group 5.13-1 | Tham khảo ETSI TS 107 301 |
| **3.11. Quy định bảo vệ dữ liệu trên thiết bị camera** | **ETSI TS 107 301** | Tham khảo ETSI TS 107 301, điều chỉnh phù hợp quy định pháp luật Việt Nam |
| 3.11.1. Nhóm kiểm thử 2.11-1 | Test group 6-1 | Tham khảo ETSI TS 107 301, điều chỉnh phù hợp quy định pháp luật Việt Nam |
| 3.11.2. Nhóm kiểm thử 2.11-2 | Test group 6-2 | Tham khảo ETSI TS 107 301, điều chỉnh phù hợp quy định pháp luật Việt Nam |
| 3.11.3. Nhóm kiểm thử 2.11-3 | Test group 6-3 | Tham khảo ETSI TS 107 301, điều chỉnh phù hợp quy định pháp luật Việt Nam |
| 3.11.4. Nhóm kiểm thử 2.11-4 | Test group 6-4 | Tham khảo ETSI TS 107 301, điều chỉnh phù hợp quy định pháp luật Việt Nam |
| 4. Quy định về quản lý |  | Tự xây dựng |
| 5. Trách nhiệm của tổ chức, cá nhân |  | Tự xây dựng |
| 6. Tổ chức thực hiện |  | Tự xây dựng |
| Phụ lục A (Quy định) Danh mục thông tin phục vụ đánh giá | A.4 Implementation eXtra Information for Testing (IXIT)  pro forma | Tham khảo ETSI TS 107 301 |
| Phụ lục B (Tham khảo) Danh mục ví dụ thông tin phục vụ đánh giá | Annex C (informative):  Sample IXIT | Tham khảo ETSI TS 107 301 |
| Phụ lục C (Quy định) Mã HS thiết bị camera giám sát sử dụng giao thức Internet |  | Tự xây dựng |

**6. Đánh giá tác động áp dụng QCVN**

Việc triển khai áp dụng QCVN đối với camera giám sát là vấn đề cấp thiết, liên quan trực tiếp đến công tác bảo đảm an toàn thông tin mạng, bảo vệ quyền riêng tư và lợi ích của người sử dụng. Quy chuẩn này áp dụng đối với các tổ chức, cá nhân Việt Nam và nước ngoài có liên quan đến hoạt động đánh giá, nghiên cứu, phát triển; đánh giá, lựa chọn và sử dụng các thiết bị thuộc phạm vi điều chỉnh của quy chuẩn này trên lãnh thổ Việt Nam.

Các đối tượng chịu tác động khi QCVN được ban hành:

- Doanh nghiệp sản xuất/nhập khẩu: phải đảm bảo đáp ứng QCVN và phải chứng nhận, công bố hợp quy khi kinh doanh sản phẩm tại thị trường Việt Nam.

- Người sử dụng (cơ quan, tổ chức, người tiêu dùng): Mức độ ảnh hưởng thấp do là đối tượng thụ hưởng cuối cùng. Các yếu tố an toàn được đảm bảo, bảo vệ lợi ích của người dùng cuối.

*6.1. Tác động đến thị trường sản phẩm camera*

Số lượng, chủng loại camera nhập khẩu mỗi năm: Bao gồm 163 loại mặt hàng nhập khẩu camera giám sát và IP camera thuộc mã 8525.80 (được kết xuất theo tên hàng camera giám sát, quan sát, an ninh, ip camera). Như vậy số lượng chủng loại IP Camera là dưới 163 loại.

Trung bình mỗi năm nhập khẩu 3,2 triệu. Trong đó, Trung Quốc tỷ lệ 96,3%, Hàn Quốc 0,6%, Khác: 3,1%.

Các chủng loại phổ biến: HIKVISION, EZVIZ, Dahua, KBVISION, Imou, Xiaomi…

- Số lượng, chủng loại camera sản xuất trong nước: (Không đủ thông tin chính thức), theo khảo sát đến tháng 4/2022 có 2 chủng loại: Viettel sản xuất camera Q83910-B (100 bộ), BKAV camera AI View S201

Phương án đánh giá, đo kiểm dự kiến theo loại sản phẩm đại điện cho mỗi mặt hàng, do vậy, số lượng IP Camera phải đo là không lớn.

**Về năng lực đo kiểm**

- Phương án tổ chức xây dựng phòng đo kiểm, chấp nhận kết quả đo kiểm:

+ Trung tâm VNCERT/CC và Trung tâm NCSC của Cục An toàn thông tin có khả năng đo kiểm các yêu cầu kỹ thuật tại dự thảo QCVN. Các đơn vị sẽ hoàn thiện hệ thống kỹ thuật, quy trình, nhân sự để đáp ứng quy định về công tác đo kiểm ngay sau khi hoặc đồng thời với việc xây dựng/ban hành QCVN.

+ Khi QCVN được ban hành, Bộ Thông tin và Truyền thông (Vụ Khoa học và Công nghệ) thông báo tới đầu mối MRA để các phòng đo có đủ năng lực nộp hồ sơ để Bộ thừa nhận; làm việc với các nhà sản xuất để trao đổi với phòng đo sẵn sàng tham gia theo MRA.

+ Cục An toàn thông tin trao đổi với 57 doanh nghiệp đang được cấp phép cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng để các Doanh nghiệp xem xét đo kiểm QCVN này khi QCVN được ban hành.

- Phòng đo kiểm: Một số hãng sản xuất IP Camera đã công bố tuân thủ ETSI EN 303 645. Danh sách một số phòng đo kiểm đủ năng lực đo kiểm thiết bị theo ETSI EN 303 645:

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên phòng đo** | **Quốc gia** |
| 1 | Deutsche Telekom Security GmbH Prüfstelle für IT Sicherheit | Bonner Talweg 100, 53113 Bonn, Germany |
| 2 | Riscure BV | Delftechpark 49, 2628 XJ Delft, The Netherlands |
| 3 | SGS Brightsight Singapore | 30, Boon Lay Way, #03-01, Singapore |
| 4 | TUV Informationstechnik GmbH | Am TÜV 1, 45307 Essen, Germany |
| 5 | T-Systems Singapore Pte. Ltd. | 15 Changi Business Park Crescent #06-01, Singapore |
| 6 | Setsco-An Security Pte Ltd | 531 Bukit Batok Street 23 Singapore |

\* Tác động tích cực:

- Người sử dụng cuối (đối tượng áp dụng): Tăng cảm giác an tâm và tin tưởng khi sử dụng các thiết bị camera giám sát đã được chứng nhận an toàn. Bảo vệ quyền riêng tư và dữ liệu cá nhân của họ trước các rủi ro mất an toàn thông tin. Giảm thiểu rủi ro mất dữ liệu quan trọng và thông tin nhạy cảm. Tăng khả năng đáp ứng các yêu cầu về bảo vệ dữ liệu và quyền riêng tư từ phía khách hàng và cơ quan quản lý. Tạo điều kiện cho một môi trường an toàn hơn và tăng cảm giác an toàn cho cộng đồng. Tăng cảm giác an toàn và hỗ trợ cho việc xây dựng một môi trường sống và làm việc an toàn hơn.

- Nhà sản xuất thiết bị camera giám sát: Nâng cao uy tín và niềm tin của khách hàng thông qua việc cung cấp các sản phẩm được chứng nhận an toàn. Góp phần vào việc thúc đẩy tiêu chuẩn an toàn trong ngành công nghiệp camera giám sát.

- Nhà phân phối và bán lẻ: Có thể sử dụng việc chứng nhận an toàn như một điểm bán hàng để thu hút khách hàng và tăng doanh số bán hàng. Tăng cơ hội hợp tác với các nhà sản xuất uy tín có sản phẩm được chứng nhận an toàn.

- Cơ quan quản lý và tổ chức chứng nhận: Góp phần vào việc nâng cao an toàn và quản lý rủi ro trong lĩnh vực camera giám sát. Tăng tính minh bạch và độ tin cậy của ngành công nghiệp. Cung cấp công cụ và dữ liệu hữu ích để hỗ trợ các hoạt động giám sát, điều tra và truy cứu trách nhiệm trong trường hợp xảy ra mất an toàn.

\* Tác động không tích cực:

- Tăng chi phí: Quá trình đạt được chứng nhận an toàn có thể đòi hỏi đầu tư lớn vào việc nâng cấp và thay đổi công nghệ, làm tăng chi phí sản xuất và phân phối thiết bị camera giám sát.

- Phức tạp hóa quy trình sản xuất: Việc tuân thủ các tiêu chuẩn an toàn có thể đòi hỏi các quy trình và thủ tục phức tạp trong quá trình sản xuất, làm tăng chi phí và thời gian sản xuất.

- Giảm hiệu suất sản xuất: Các biện pháp an toàn có thể làm giảm hiệu suất sản xuất do tăng thời gian kiểm tra và thử nghiệm, cũng như việc áp dụng các quy trình kiểm soát chất lượng nghiêm ngặt hơn.

- Cản trở sự linh hoạt và sử dụng: Việc tuân thủ các yêu cầu chứng nhận an toàn có thể làm giảm sự linh hoạt trong việc sử dụng và cấu hình thiết bị camera giám sát, làm hạn chế tính tùy chỉnh và khả năng tích hợp với các hệ thống khác.

- Tăng thời gian tiến hành kiểm định và cấp phát chứng nhận: Quá trình đạt được chứng nhận an toàn có thể đòi hỏi thời gian dài và tốn kém để thực hiện kiểm định và cấp phát chứng nhận, làm trì hoãn việc tung ra thị trường và làm chậm quá trình phát triển sản phẩm mới.

- Khó khăn trong việc tuân thủ các yêu cầu giữa các quốc gia: Các yêu cầu chứng nhận an toàn có thể không phù hợp hoặc khó tuân thủ đối với các khu vực hoặc quốc gia cụ thể, làm giảm khả năng tiếp cận thị trường và tạo ra rủi ro pháp lý.

a) Đối với sản phẩm sản xuất trong nước:

- Tích cực: Các sản phẩm trong nước được sản xuất đáp ứng các yếu tố cơ bản về an toàn thông tin mạng, quản lý, mã hóa dữ liệu tại Việt Nam sẽ có khả năng đáp ứng cao đối với các quy định về đảm bảo an toàn thông tin mạng tại QCVN.

- Tiêu cực: Phát sinh hoạt động chứng nhận hợp quy và công bố hợp quy, gia tăng chi phí cho doanh nghiệp trong hoạt động sản xuất, thương mại.

b) Đối với sản phẩm nhập khẩu:

- Tích cực: Các sản phẩm nhập khẩu phải đảm bảo đáp ứng các yêu cầu của QCVN, những doanh nghiệp sản xuất sản phẩm chất lượng cao sẽ có cơ hội tiếp cận thị trường Việt Nam tốt hơn.

- Tiêu cực: Các sản phẩm nhập khẩu phải được chứng nhận hợp quy và công bố hợp quy theo QCVN của Việt Nam, không sử dụng được các chứng nhận quốc tế đã đáp ứng (nếu có), phát sinh chi phí thương mại tại thị trường Việt Nam.

*6.2. Tác động đến cơ quan, tổ chức*

- Đối với cơ quan quản lý nhà nước chuyên ngành: cần hoàn thiện hành lang pháp lý, đưa camera giám sát vào các danh mục bắt buộc thực hiện các quy định về hợp quy; cần hoàn thiện năng lực đo kiểm, đánh giá để thực hiện công tác chứng nhận hợp quy cho doanh nghiệp.

- Đối với cơ quan, tổ chức là đơn vị sử dụng sản phẩm: cần rà soát lại hệ thống thông tin, nâng cấp thiết bị để đảm bảo an toàn thông tin mạng theo yêu cầu tại Chỉ thị 23/CT-TTg năm 2023 của Thủ tướng Chính phủ.

*6.3. Tác động đến người sử dụng đầu cuối*

- Người sử dụng đầu cuối là đối tượng được thụ hưởng tích cực khi sản phẩm được quản lý, bảo mật, đáp ứng các quy định của QCVN./.

1. Theo số liệu thống kê của Tổng cục Hải quan [↑](#footnote-ref-1)