



BỘ CÔNG AN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: **167** /2026/TT-BCA

Hà Nội, ngày **30** tháng **9** năm 2026

THÔNG TƯ

**Ban hành Quy chuẩn kỹ thuật quốc gia về an ninh mạng cho
hệ thống camera giám sát trong cơ quan nhà nước**

CỤC THÔNG TIN VÀ TRUYỀN THÔNG CHÍNH PHỦ	
ĐẾN	Giờ: 5
	Ngày: 15/10/2026

Căn cứ Luật Tiêu chuẩn và quy chuẩn kỹ thuật số 68/2006/QH11 được sửa đổi, bổ sung bởi Luật số 35/2018/QH14 và Luật số 70/2025/QH15;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Căn cứ Nghị định số 22/2026/NĐ-CP quy định chi tiết một số điều và biện pháp để tổ chức, hướng dẫn thi hành Luật Tiêu chuẩn và quy chuẩn kỹ thuật;

Căn cứ Nghị định số 02/2025/NĐ-CP quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công an được sửa đổi, bổ sung bởi Nghị định số 11/2025/NĐ-CP và Nghị định số 10/2026/NĐ-CP;

Theo đề nghị của Cục trưởng Cục An ninh mạng;

Bộ trưởng Bộ Công an ban hành Thông tư ban hành Quy chuẩn kỹ thuật quốc gia về an ninh mạng cho hệ thống camera giám sát trong cơ quan nhà nước.

Điều 1. Ban hành kèm theo Thông tư này Quy chuẩn kỹ thuật quốc gia về an ninh mạng cho hệ thống camera giám sát trong cơ quan nhà nước - QCVN 14:2026/BCA.

Điều 2. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 6 năm 2027.

Điều 3. Điều khoản thi hành

1. Cục trưởng Cục An ninh mạng có trách nhiệm theo dõi, kiểm tra, đôn đốc việc thực hiện Thông tư này.

2. Thủ trưởng đơn vị thuộc cơ quan Bộ Công an, Giám đốc Công an tỉnh, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

Trong quá trình thực hiện Thông tư này, nếu có khó khăn, vướng mắc Công an các đơn vị, địa phương, tổ chức, cá nhân có liên quan phản ánh về Bộ Công an (qua Cục An ninh mạng) để kịp thời hướng dẫn. *la*

Nơi nhận:

- Các đồng chí Thứ trưởng Bộ Công an;
- Văn phòng Chính phủ;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố;
- Các đơn vị thuộc cơ quan Bộ Công an;
- Công an các tỉnh, thành phố;
- Công báo;
- Cổng TTĐT Chính phủ;
- Cổng TTĐT Bộ Công an;
- Lưu: VT, V03, A05.

BỘ TRƯỞNG



Almanu

Đại tướng Lương Tam Quang



CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN 14:2026/BCA

**QUY CHUẨN KỸ THUẬT QUỐC GIA
VỀ AN NINH MẠNG CHO HỆ THỐNG CAMERA GIÁM SÁT
TRONG CƠ QUAN NHÀ NƯỚC**

*National technical regulation
on Cybersecurity for Surveillance Camera System in State Agencies*

HÀ NỘI - 2026

Lời nói đầu

QCVN 14:2026/BCA do Cục An ninh mạng biên soạn, Cục Khoa học, chiến lược và lịch sử Công an trình duyệt, Bộ Khoa học và Công nghệ có ý kiến, Bộ trưởng Bộ Công an ban hành theo Thông tư số 167/2026/TT-BCA ngày 30 tháng 9 năm 2026.

Mục lục

Lời nói đầu	3
1. QUY ĐỊNH CHUNG	7
1.1. Phạm vi điều chỉnh	7
1.2. Đối tượng áp dụng	7
1.3. Tài liệu viện dẫn	7
1.4. Chữ viết tắt	7
1.5. Giải thích từ ngữ	8
2. QUY ĐỊNH KỸ THUẬT	10
2.1. Yêu cầu đối với thiết bị camera giám sát sử dụng giao thức Internet	10
2.2. Yêu cầu đối với thiết bị đầu ghi hình	10
2.2.1. Yêu cầu 2.2.1	10
2.2.2. Yêu cầu 2.2.2	10
2.2.3. Yêu cầu 2.2.3	10
2.2.4. Yêu cầu 2.2.4	10
2.2.5. Yêu cầu 2.2.5	10
2.2.6. Yêu cầu 2.2.6	10
2.2.7. Yêu cầu 2.2.7	10
2.2.8. Yêu cầu 2.2.8	10
2.3. Yêu cầu đối với hệ thống mạng	11
2.3.1. Yêu cầu 2.3.1	11
2.3.2. Yêu cầu 2.3.2	11
2.3.3. Yêu cầu 2.3.3	11
2.3.4. Yêu cầu 2.3.4	11
2.3.5. Yêu cầu 2.3.5	11
2.4. Yêu cầu đối với cấu phần lưu trữ	11
2.4.1. Yêu cầu 2.4.1	11
2.4.2. Yêu cầu 2.4.2	11
2.4.3. Yêu cầu 2.4.3	11
2.4.4. Yêu cầu 2.4.4	12
2.4.5. Yêu cầu 2.4.5	12
2.5. Yêu cầu đối với phần mềm quản lý video	12
2.5.1. Yêu cầu 2.5.1	12
2.5.2. Yêu cầu 2.5.2	12
2.5.3. Yêu cầu 2.5.3	12
2.5.4. Yêu cầu 2.5.4	12

2.5.5. Yêu cầu 2.5.5	12
2.5.6. Yêu cầu 2.5.6	12
2.5.7. Yêu cầu 2.5.7	12
2.5.8. Yêu cầu 2.5.8	13
2.5.9. Yêu cầu 2.5.9	13
2.5.10. Yêu cầu 2.5.10	13
2.6. Yêu cầu đối với thiết bị trung gian xử lý tại biên	13
2.6.1. Yêu cầu 2.6.1	13
2.6.2. Yêu cầu 2.6.2	13
2.6.3. Yêu cầu 2.6.3	13
2.6.4. Yêu cầu 2.6.4	13
2.6.5. Yêu cầu 2.6.5	13
2.6.6. Yêu cầu 2.6.6	13
3. PHƯƠNG PHÁP ĐO	14
3.1. Đối với thiết bị camera giám sát sử dụng giao thức Internet	14
3.2. Đối với thiết bị đầu ghi hình.....	14
3.2.1. Nhóm kiểm thử yêu cầu 2.2.1	14
3.2.2. Nhóm kiểm thử yêu cầu 2.2.2	14
3.2.3. Nhóm kiểm thử yêu cầu 2.2.3	15
3.2.4. Nhóm kiểm thử yêu cầu 2.2.4	15
3.2.5. Nhóm kiểm thử yêu cầu 2.2.5	16
3.2.6. Nhóm kiểm thử yêu cầu 2.2.6	17
3.2.7. Nhóm kiểm thử yêu cầu 2.2.7	17
3.2.8. Nhóm kiểm thử yêu cầu 2.2.8	18
3.3. Nhóm kiểm thử yêu cầu đối với hệ thống mạng	18
3.3.1. Nhóm kiểm thử yêu cầu 2.3.1	18
3.3.2. Nhóm kiểm thử yêu cầu 2.3.2	19
3.3.3. Nhóm kiểm thử yêu cầu 2.3.3	19
3.3.4. Nhóm kiểm thử yêu cầu 2.3.4	20
3.3.5. Nhóm kiểm thử yêu cầu 2.3.5	20
3.4. Nhóm kiểm thử yêu cầu đối với cấu phần lưu trữ.....	21
3.4.1. Nhóm kiểm thử yêu cầu 2.4.1	21
3.4.2. Nhóm kiểm thử yêu cầu 2.4.2	22
3.4.3. Nhóm kiểm thử yêu cầu 2.4.3	22
3.4.4. Nhóm kiểm thử yêu cầu 2.4.4	23
3.4.5. Nhóm kiểm thử yêu cầu 2.4.5	23

QCVN 14:2026/BCA

3.5. Nhóm kiểm thử yêu cầu đối với phần mềm quản lý video	24
3.5.1. Nhóm kiểm thử yêu cầu 2.5.1	24
3.5.2. Nhóm kiểm thử yêu cầu 2.5.2	24
3.5.3. Nhóm kiểm thử yêu cầu 2.5.3	25
3.5.4. Nhóm kiểm thử yêu cầu 2.5.4	26
3.5.5. Nhóm kiểm thử yêu cầu 2.5.5	26
3.5.6. Nhóm kiểm thử yêu cầu 2.5.6	27
3.5.7. Nhóm kiểm thử yêu cầu 2.5.7	27
3.5.8. Nhóm kiểm thử yêu cầu 2.5.8	28
3.5.9. Nhóm kiểm thử yêu cầu 2.5.9	28
3.5.10. Nhóm kiểm thử yêu cầu 2.5.10	29
3.6. Nhóm kiểm thử yêu cầu đối với thiết bị trung gian xử lý tại biên.....	30
3.6.1. Nhóm kiểm thử yêu cầu 2.6.1	30
3.6.2. Nhóm kiểm thử yêu cầu 2.6.2	30
3.6.3. Nhóm kiểm thử yêu cầu 2.6.3	31
3.6.4. Nhóm kiểm thử yêu cầu 2.6.4	31
3.6.5. Nhóm kiểm thử yêu cầu 2.6.5	32
3.6.6. Nhóm kiểm thử yêu cầu 2.6.6	32
4. QUY ĐỊNH VỀ QUẢN LÝ	34
5. TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN	34
6. TỔ CHỨC THỰC HIỆN	34

QUY CHUẨN KỸ THUẬT QUỐC GIA
VỀ AN NINH MẠNG CHO HỆ THỐNG CAMERA GIÁM SÁT
TRONG CƠ QUAN NHÀ NƯỚC
National technical regulation
on Cybersecurity for Surveillance Camera System in State Agencies

1. QUY ĐỊNH CHUNG

1.1. Phạm vi điều chỉnh

Quy chuẩn này quy định yêu cầu an ninh mạng cơ bản đối với các thành phần chính của hệ thống camera giám sát công trình quan trọng liên quan đến an ninh quốc gia, hệ thống camera giám sát của cơ quan, doanh nghiệp nhà nước phục vụ an ninh, trật tự và giám sát điều hành đô thị thông minh, hệ thống camera giám sát an ninh, trật tự, xử lý vi phạm và điều hành giao thông, bao gồm: ⁽¹⁾Thiết bị camera giám sát sử dụng giao thức Internet, ⁽²⁾Thiết bị đầu ghi hình, ⁽³⁾Hệ thống mạng, ⁽⁴⁾Cấu phần lưu trữ, ⁽⁵⁾Phần mềm quản lý video, ⁽⁶⁾Thiết bị trung gian xử lý tại biên.

Các hệ thống camera giám sát đặc thù, bao gồm: hệ thống camera tác chiến, camera trinh sát; hệ thống camera giám sát buồng hỏi cung, trại giam, trại tạm giam, nhà tạm giữ không thuộc phạm vi điều chỉnh của Quy chuẩn này.

Hệ thống camera giám sát đã được phê duyệt cấp độ và triển khai đầy đủ phương án bảo đảm an ninh mạng theo cấp độ được phê duyệt thì không áp dụng quy định tại Quy chuẩn này.

1.2. Đối tượng áp dụng

Quy chuẩn này được áp dụng cho các cơ quan, tổ chức, doanh nghiệp nhà nước có hoạt động xây dựng, đầu tư, triển khai, vận hành hệ thống camera thuộc phạm vi điều chỉnh của Quy chuẩn này.

1.3. Tài liệu viện dẫn

QCVN 11:2026/BCA: Quy chuẩn kỹ thuật quốc gia về thiết bị camera giám sát sử dụng giao thức Internet - Các yêu cầu an ninh mạng cơ bản

1.4. Chữ viết tắt

API	Application Programming Interface	Giao diện lập trình ứng dụng
IP	Internet Protocol	Giao thức Internet
MAC	Media Access Control	Điều khiển truy cập môi trường
VMS	Video Management System	Phần mềm quản lý video
NVR	Network Video Recorder	Đầu ghi hình mạng
DVR	Digital Video Recorder	Đầu ghi hình kỹ thuật số

QCVN 14:2026/BCA

RAID	Redundant Array of Independent Disks	Mảng đĩa độc lập dự phòng
VPN	Virtual Private Network	Mạng riêng ảo
WORM	Write Once Read Many	Ghi một lần, đọc nhiều lần
eSATA	External Serial Advanced Technology Attachment	Chuẩn kết nối SATA được thiết kế chuyên biệt để kết nối các thiết bị lưu trữ gắn ngoài
USB	Universal Serial Bus	Chuẩn kết nối vật lý được dùng để liên kết các thiết bị điện tử
NTP	Network Time Protocol	Giao thức đồng bộ hóa thời gian mạng
OTA	Over The Air	Phương thức phân phối, cập nhật từ xa
TCP	Transmission Control Protocol	Giao thức điều khiển truyền vận
UDP	User Datagram Protocol	Giao thức gói dữ liệu người dùng
IPSec	Internet Protocol Security	Bảo mật giao thức Internet
SSH	Secure Shell	Kênh giao tiếp bảo mật
TLS	Transport Layer Security	Giao thức bảo mật tầng giao vận
ONVIF	Open Network Video Interface Forum	Diễn đàn giao diện video mạng mở
HTTPS	Hypertext Transfer Protocol Secure	Giao thức truyền tải siêu văn bản an toàn
CVSS	Common Vulnerability Scoring System	Hệ thống chấm điểm lỗ hổng bảo mật chung
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình động máy chủ
HTTP	Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản
WAN	Wide Area Network	Mạng diện rộng

1.5. Giải thích từ ngữ

Quy chuẩn này sử dụng các thuật ngữ và định nghĩa trong QCVN 11:2026/BCA và các thuật ngữ sau:

1.5.1. Hệ thống camera giám sát (Surveillance Camera System)

Hệ thống camera giám sát bao gồm tập hợp các thành phần nhằm bảo đảm quá trình thu, ghi, nhận, truyền dữ liệu camera giám sát đến nơi giám sát.

1.5.2. Đầu ghi hình mạng (Network video recorder)

Đầu ghi hình mạng là thiết bị chuyên dụng nhận, xử lý và lưu trữ các luồng video kỹ thuật số từ camera IP qua mạng cục bộ hoặc mạng diện rộng.

1.5.3. Đầu ghi hình kỹ thuật số (Digital video recorder)

Đầu ghi hình kỹ thuật số là thiết bị số hóa, xử lý và ghi lại tín hiệu video analog từ các hệ thống camera giám sát trực tiếp lên phương tiện lưu trữ cục bộ.

1.5.4. Phần mềm quản lý video (Video management system)

Phần mềm quản lý video là thành phần của hệ thống camera giám sát thu thập video từ camera và các nguồn khác, ghi lại video đó vào thiết bị lưu trữ và cung cấp giao diện để xem video trực tiếp cũng như truy cập ngẫu nhiên vào video đã ghi.

1.5.5. Hình mờ (Watermark)

Hình mờ là văn bản hoặc hình ảnh được làm mờ và chèn chìm lên các sản phẩm kỹ thuật số.

1.5.6. Ổ đĩa dự phòng nóng (Hot spare)

Ổ đĩa được cấu hình sẵn trong hệ thống lưu trữ để tự động thay thế ổ đĩa bị hỏng, bảo đảm độ tin cậy của hệ thống.

1.5.7. Thiết bị trung gian xử lý tại biên (Edge device)

Thiết bị đặt giữa camera và các thành phần xử lý trung tâm của hệ thống camera giám sát, có chức năng thu nhận dữ liệu từ camera để xử lý, phân tích, lưu đệm hoặc chuyển tiếp kết quả về hệ thống camera giám sát.

2. QUY ĐỊNH KỸ THUẬT

2.1. Yêu cầu đối với thiết bị camera giám sát sử dụng giao thức Internet

Thiết bị camera giám sát sử dụng giao thức Internet được sử dụng trong hệ thống camera thuộc phạm vi điều chỉnh của Quy chuẩn này phải đáp ứng QCVN 11:2026/BCA.

2.2. Yêu cầu đối với thiết bị đầu ghi hình

2.2.1. Yêu cầu 2.2.1

Thiết bị đầu ghi hình nếu có giao diện kết nối lưu trữ, sao lưu ngoại vi (như USB, eSATA) thì phải có khả năng ngăn chặn nạp tệp thực thi từ các thiết bị ngoại vi được kết nối, trừ bản cập nhật firmware đã được xác thực chữ ký số theo yêu cầu 2.2.8.

2.2.2. Yêu cầu 2.2.2

Thiết bị đầu ghi hình phải có chức năng cho phép kiểm soát, vô hiệu hóa các giao diện mạng và giao diện logic.

2.2.3. Yêu cầu 2.2.3

Thiết bị đầu ghi hình phải có cơ chế cho phép thiết lập ngưỡng cảnh báo và tự động phát ra các tín hiệu cảnh báo khi dung lượng lưu trữ khả dụng thấp hơn giá trị ngưỡng đã đặt.

2.2.4. Yêu cầu 2.2.4

Thiết bị đầu ghi hình phải có cơ chế chống can thiệp hoặc chống giả mạo, bảo đảm khả năng ngăn chặn hoặc phát hiện việc cắt ghép, sửa đổi cấu trúc tệp đối với tệp video được ghi nhận và lưu trữ trên thiết bị.

2.2.5. Yêu cầu 2.2.5

Thiết bị đầu ghi hình phải hỗ trợ mã hóa tệp video khi truyền tải, xuất ra hoặc sao lưu ngoại tuyến, sử dụng thuật toán mã hóa mạnh chưa bị công bố điểm yếu.

2.2.6. Yêu cầu 2.2.6

Thiết bị đầu ghi hình không được cho phép cài đặt, kích hoạt các tệp thực thi, ứng dụng bên thứ ba nếu các tệp, ứng dụng này chưa được xác thực tính toàn vẹn và hợp lệ.

2.2.7. Yêu cầu 2.2.7

Thiết bị đầu ghi hình phải được thiết lập lại tài khoản, mật khẩu quản trị trước khi đưa vào vận hành chính thức; không duy trì tài khoản, mật khẩu mặc định của nhà sản xuất ở trạng thái có thể sử dụng để đăng nhập.

2.2.8. Yêu cầu 2.2.8

Thiết bị đầu ghi hình phải hỗ trợ cơ chế cập nhật phần mềm, firmware (bao gồm cả cập nhật qua phương thức OTA nếu có) có xác thực chữ ký số nguồn gốc bản cập nhật; có khả năng phát hiện bản cập nhật không hợp lệ và khôi phục về phiên bản ổn định trong trường hợp cập nhật thất bại hoặc bị gián đoạn.

2.3. Yêu cầu đối với hệ thống mạng

2.3.1. Yêu cầu 2.3.1

Hệ thống mạng chỉ được mở các giao thức an toàn phục vụ cho việc truyền tải dữ liệu camera giám sát và quản trị các cấu phần của hệ thống camera giám sát; trường hợp sử dụng chuẩn ONVIF thì phải truyền qua HTTPS/TLS, hỗ trợ Profile G/T/M phù hợp với chức năng của từng thiết bị.

2.3.2. Yêu cầu 2.3.2

Hệ thống mạng phải bảo đảm phân tách vùng mạng camera giám sát và các vùng mạng còn lại. Các vùng mạng còn lại trong hệ thống chỉ được kết nối với vùng mạng camera giám sát theo chính sách kiểm soát truy cập đã thiết lập để phục vụ quản trị, vận hành, khai thác hệ thống.

2.3.3. Yêu cầu 2.3.3

Hệ thống mạng phải có khả năng kiểm soát truy cập của các thiết bị kết nối vào hệ thống camera giám sát, tối thiểu bảo đảm kiểm soát truy cập thông qua địa chỉ MAC.

2.3.4. Yêu cầu 2.3.4

Hệ thống mạng phải bảo đảm các thiết bị trong hệ thống camera giám sát có khả năng đồng bộ thời gian qua máy chủ thời gian.

2.3.5. Yêu cầu 2.3.5

Hệ thống mạng bảo đảm việc truy cập, quản trị từ xa đối với các thiết bị trong hệ thống camera giám sát phải được thực hiện qua kênh kết nối mã hóa, xác thực hai chiều; không được phép mở trực tiếp cổng dịch vụ quản trị của camera, đầu ghi hình, thiết bị trung gian ra mạng Internet công cộng.

2.4. Yêu cầu đối với cấu phần lưu trữ

2.4.1. Yêu cầu 2.4.1

Cấu phần lưu trữ cục bộ có từ 02 ổ đĩa cứng trở lên phải có tính năng thiết lập cấu hình mảng đĩa độc lập dự phòng bảo đảm an toàn và chống mất, thất thoát dữ liệu do sự cố phần cứng.

2.4.2. Yêu cầu 2.4.2

Cấu phần lưu trữ cục bộ có từ 03 ổ đĩa cứng trở lên phải có chức năng hỗ trợ tự động thay thế và tiến hành tái tạo đồng bộ hóa dữ liệu thông qua ổ đĩa dự phòng nóng ngay khi phát hiện có sự cố hỏng đĩa.

2.4.3. Yêu cầu 2.4.3

Trong trường hợp lưu trữ trên đám mây, phải sử dụng kênh truyền mã hóa tối thiểu TLS 1.2 khi truyền qua mạng Internet công cộng hoặc sử dụng kênh truyền riêng có mã hóa (VPN Site-to-Site/IPSec).

2.4.4. Yêu cầu 2.4.4

Trong trường hợp lưu trữ trên đám mây, các thiết bị kết nối truyền tải dữ liệu lưu trữ lên đám mây chỉ được cấp quyền ghi, không được cấp quyền xem, sửa hoặc xóa dữ liệu.

2.4.5. Yêu cầu 2.4.5

Trong trường hợp lưu trữ trên đám mây, hệ thống lưu trữ đám mây phải có khả năng kích hoạt tính năng WORM, cho phép hệ thống tự động ghi đè hoặc xóa an toàn dữ liệu khi hết thời hạn lưu trữ.

2.5. Yêu cầu đối với phần mềm quản lý video

2.5.1. Yêu cầu 2.5.1

Phần mềm quản lý video phải có các cơ chế mã hóa kênh truyền cho toàn bộ dữ liệu hình ảnh, âm thanh và luồng lệnh điều khiển khi truyền tải giữa máy chủ, thiết bị đầu cuối và máy khách.

2.5.2. Yêu cầu 2.5.2

Phần mềm quản lý video phải có các biện pháp kỹ thuật xác minh nhằm bảo đảm tính toàn vẹn của dữ liệu, có khả năng tự động phát hiện và ngăn chặn việc chèn tệp, sửa đổi hoặc làm giả luồng dữ liệu truyền tải.

2.5.3. Yêu cầu 2.5.3

Phần mềm quản lý video phải thực hiện được việc xác thực, định danh người dùng và xác thực tính hợp lệ của thiết bị đầu cuối trước khi cho phép bất kỳ thiết bị hay tài khoản nào thiết lập kết nối trao đổi dữ liệu.

2.5.4. Yêu cầu 2.5.4

Phần mềm quản lý video phải phân quyền chức năng theo vai trò (như quản trị, vận hành, xem) cho từng tài khoản người dùng, không cho phép thực hiện thao tác vượt quá vai trò được gán.

2.5.5. Yêu cầu 2.5.5

Phần mềm quản lý video tại thời điểm đánh giá không được tồn tại lỗ hổng bảo mật đã được công bố ở mức nghiêm trọng hoặc cao và phải có khả năng ngăn chặn các hành vi tấn công dò mật khẩu tự động.

2.5.6. Yêu cầu 2.5.6

Phần mềm quản lý video phải có chức năng ghi nhật ký đối với mọi hoạt động của người sử dụng, tối thiểu bao gồm thông tin định danh người dùng, thời gian, thao tác thực hiện và đối tượng bị tác động.

2.5.7. Yêu cầu 2.5.7

Phần mềm quản lý video phải có tính năng phân quyền truy cập theo từng camera, đầu ghi hình cho từng tài khoản người dùng, không cho phép truy cập ngoài phạm vi được cấp.

2.5.8. Yêu cầu 2.5.8

Phần mềm quản lý video phải có chức năng nhúng hình mờ vào video camera giám sát.

2.5.9. Yêu cầu 2.5.9

Máy chủ triển khai phần mềm quản lý video chỉ được mở kết nối cho các cổng/giao thức phục vụ truyền phát, điều khiển video và quản trị, vận hành phần mềm, các dịch vụ hỗ trợ đã được khai báo trong hồ sơ thiết kế; các cổng/giao thức khác phải bị chặn.

2.5.10. Yêu cầu 2.5.10

Phần mềm quản lý video phải có tính năng hoặc giải pháp bảo vệ ứng dụng/API và thực hiện xác thực, phân quyền, kiểm soát phiên làm việc đối với từng yêu cầu kết nối.

2.6. Yêu cầu đối với thiết bị trung gian xử lý tại biên**2.6.1. Yêu cầu 2.6.1**

Thiết bị trung gian xử lý tại biên phải có định danh riêng bằng chứng thư số hoặc khóa mật mã riêng; không sử dụng chung tài khoản, mật khẩu hoặc chứng thư giữa nhiều thiết bị.

2.6.2. Yêu cầu 2.6.2

Thiết bị trung gian xử lý tại biên phải có tính năng khởi động an toàn và chỉ cho phép nạp, thực thi firmware, phần mềm đã được ký số hợp lệ.

2.6.3. Yêu cầu 2.6.3

Thiết bị trung gian xử lý tại biên chỉ được kết nối, truyền dữ liệu tới đúng địa chỉ, dịch vụ tiếp nhận; không được kết nối trực tiếp ra mạng Internet hoặc truy cập ngang sang camera, thiết bị khác ngoài phạm vi được cấp phép.

2.6.4. Yêu cầu 2.6.4

Dữ liệu hình ảnh, video, siêu dữ liệu lưu tạm hoặc lưu đệm cục bộ trên thiết bị trung gian xử lý tại biên phải được mã hóa và tự động xóa khi hết thời hạn lưu đã cấu hình.

2.6.5. Yêu cầu 2.6.5

Thiết bị trung gian xử lý tại biên phải có khả năng phát hiện hành vi can thiệp bất thường (như mở vỏ thiết bị, ngắt kết nối mô-đun, phát lại dữ liệu video cũ) trong hoạt động và tự động phát cảnh báo hoặc cách ly khỏi hệ thống khi phát hiện.

2.6.6. Yêu cầu 2.6.6

Thiết bị trung gian xử lý tại biên chỉ được mở các cổng, giao thức phục vụ đúng chức năng thu nhận dữ liệu từ camera, truyền kết quả về hệ thống camera giám sát và quản trị, bảo trì; mọi kết nối quản trị, bảo trì từ xa phải thực hiện qua kênh mã hóa, xác thực hai chiều.

3. PHƯƠNG PHÁP ĐO

3.1. Đối với thiết bị camera giám sát sử dụng giao thức Internet

Phương pháp đo kiểm, thử nghiệm và đánh giá sự tuân thủ đối với thiết bị camera giám sát sử dụng giao thức Internet được thực hiện theo các quy định và phương pháp đo quy định tại QCVN 11:2026/BCA.

3.2. Đối với thiết bị đầu ghi hình

3.2.1. Nhóm kiểm thử yêu cầu 2.2.1

3.2.1.1. Mục tiêu kiểm thử

Kiểm thử đầu ghi hình (NVR/DVR) đáp ứng hay không yêu cầu 2.2.1 Quy chuẩn này.

3.2.1.2. Đánh giá sự tuân thủ về thiết kế

3.2.1.2.1. Mục đích kiểm thử

Đánh giá NVR/DVR (nếu có cổng sao lưu vật lý) có ngăn chặn nạp tệp thực thi từ thiết bị ngoại vi hay không.

3.2.1.2.2. Phương pháp kiểm thử

1) Đánh giá đầu ghi hình có giao diện kết nối lưu trữ, sao lưu ngoại vi (như USB, eSATA) hay không; nếu không có thì bỏ qua các bước tiếp theo.

2) Kết nối một thiết bị lưu trữ ngoại vi có chứa tệp thực thi giả lập vào cổng sao lưu vật lý của đầu ghi hình.

3) Tiến hành nạp, thực thi tệp (qua chức năng cập nhật, khôi phục cấu hình hoặc tự động chạy) sau khi kết nối thành công vào đầu ghi hình.

4) Đánh giá phần mềm hệ thống của đầu ghi hình có khả năng ngăn chặn việc thực thi tệp từ thiết bị ngoại vi đó hay không.

3.2.1.2.3. Kết luận

1) Đáp ứng: Thiết bị không có cổng giao tiếp vật lý để kết nối thiết bị ngoại vi, hoặc nếu có cổng thì phát hiện và ngăn chặn thành công nạp tệp thực thi từ thiết bị ngoại vi.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.2.2. Nhóm kiểm thử yêu cầu 2.2.2

3.2.2.1. Mục tiêu kiểm thử

Kiểm thử đầu ghi hình (NVR/DVR) đáp ứng hay không yêu cầu 2.2.2 Quy chuẩn này.

3.2.2.2. Đánh giá sự tuân thủ về thiết kế

3.2.2.2.1. Mục đích kiểm thử

Đánh giá khả năng của đầu ghi hình trong việc cho phép người quản trị kiểm soát, bật/tắt và vô hiệu hóa các giao diện mạng hoặc giao diện logic.

3.2.2.2.2. Phương pháp kiểm thử

1) Truy cập vào giao diện quản trị hệ thống của đầu ghi hình, tiến hành xác định danh sách các giao diện mạng hoặc giao diện logic đang hoạt động.

2) Thực hiện thao tác vô hiệu hóa một giao diện mạng cụ thể hoặc một cổng dịch vụ logic thông qua cấu hình hệ thống.

3) Sử dụng một thiết bị ngoại vi hoặc máy trạm thử kết nối trực tiếp vào giao diện vật lý, sử dụng công cụ quét mạng để cố gắng truy cập vào giao diện logic vừa bị vô hiệu hóa.

4) Đánh giá xem thiết bị có chặn hoàn toàn kết nối từ bên ngoài vào các giao diện đã bị đóng hay không.

3.2.2.2.3. Kết luận

1) Đáp ứng: Thiết bị cung cấp tính năng vô hiệu hóa giao diện rõ ràng và ngăn chặn thành công mọi truy cập vào các giao diện mạng/logic đã bị vô hiệu hóa.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.2.3. Nhóm kiểm thử yêu cầu 2.2.3

3.2.3.1. Mục tiêu kiểm thử

Kiểm thử đầu ghi hình (NVR/DVR) đáp ứng hay không yêu cầu 2.2.3 Quy chuẩn này.

3.2.3.2. Đánh giá sự tuân thủ về triển khai

3.2.3.2.1. Mục đích kiểm thử

Đánh giá tính năng thiết lập ngưỡng cảnh báo và cảnh báo khi sắp hết dung lượng lưu trữ của đầu ghi hình.

3.2.3.2.2. Phương pháp kiểm thử

1) Thiết lập ngưỡng cảnh báo dung lượng thấp trên cấu hình lưu trữ của thiết bị, đặt ở mức gần với dung lượng khả dụng hiện tại để rút ngắn thời gian thử nghiệm; tạm tắt chế độ ghi đè nếu có.

2) Tiến hành nạp dữ liệu liên tục vào hệ thống đĩa cho đến khi dung lượng khả dụng giảm xuống dưới mức ngưỡng cảnh báo.

3) Đánh giá thiết bị có phát ra các thông báo cảnh báo qua âm thanh, email, hoặc giao diện quản lý kịp thời hay không.

3.2.3.2.3. Kết luận

1) Đáp ứng: Đầu ghi hình cho phép thiết lập ngưỡng cảnh báo và hệ thống cảnh báo hoạt động chính xác khi dung lượng thực tế chạm ngưỡng cấu hình.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.2.4. Nhóm kiểm thử yêu cầu 2.2.4

3.2.4.1. Mục tiêu kiểm thử

QCVN 14:2026/BCA

Kiểm thử đầu ghi hình (NVR/DVR) đáp ứng hay không yêu cầu 2.2.4 Quy chuẩn này.

3.2.4.2. Đánh giá sự tuân thủ về triển khai

3.2.4.2.1. Mục đích kiểm thử

Đánh giá tính toàn vẹn và cơ chế cảnh báo chống can thiệp của tệp video được lưu trữ.

3.2.4.2.2. Phương pháp kiểm thử

1) Thực hiện ghi và trích xuất một tệp video hoàn chỉnh từ cấu phần lưu trữ của đầu ghi.

2) Sử dụng công cụ chỉnh sửa để can thiệp làm thay đổi một số bit dữ liệu trong tệp video đã trích xuất, sau đó kiểm tra tệp bằng chức năng xác minh của thiết bị hoặc công cụ xác minh của nhà sản xuất.

3) Đánh giá thiết bị hoặc công cụ xác minh có xác định được tệp đã bị chỉnh sửa và phát ra cảnh báo chống giả mạo hay không.

3.2.4.2.3. Kết luận

1) Đáp ứng: Thiết bị hoặc công cụ xác minh của nhà sản xuất có khả năng phát hiện tệp video bị thay đổi và từ chối xác nhận tính toàn vẹn của tệp.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.2.5. Nhóm kiểm thử yêu cầu 2.2.5

3.2.5.1. Mục tiêu kiểm thử

Kiểm thử đầu ghi hình (NVR/DVR) đáp ứng hay không yêu cầu 2.2.5 Quy chuẩn này.

3.2.5.2. Đánh giá sự tuân thủ về thiết kế

3.2.5.2.1. Mục đích kiểm thử

Đánh giá khả năng mã hóa dữ liệu của thiết bị đối với các tệp video khi truyền tải, xuất ra hoặc sao lưu ngoại tuyến.

3.2.5.2.2. Phương pháp kiểm thử

1) Thực hiện lệnh sao lưu/xuất tệp video ra thiết bị ngoại vi và kích hoạt chức năng mã hóa bảo mật dữ liệu trên đầu ghi.

2) Đánh giá thuật toán mã hóa áp dụng trên tệp xuất ra có tuân thủ các chuẩn mật mã mạnh chưa được các tổ chức quốc tế đưa ra điểm yếu (ví dụ: AES từ 128 bit trở lên) hay không.

3) Kiểm tra tệp xuất ra không thể giải mã và xem được nếu không cung cấp đúng khóa giải mã.

3.2.5.2.3. Kết luận

1) Đáp ứng: Tệp sao lưu được mã hóa theo thuật toán đạt chuẩn và không thể truy cập nếu thiếu khóa giải mã hợp lệ.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.2.6. Nhóm kiểm thử yêu cầu 2.2.6

3.2.6.1. Mục tiêu kiểm thử

Kiểm thử đầu ghi hình (NVR/DVR) đáp ứng hay không yêu cầu 2.2.6 Quy chuẩn này.

3.2.6.2. Đánh giá sự tuân thủ về thiết kế

3.2.6.2.1. Mục đích kiểm thử

Đánh giá khả năng chặn các tệp thực thi, các ứng dụng không hợp lệ trên thiết bị đầu ghi.

3.2.6.2.2. Phương pháp kiểm thử

1) Thông qua chức năng cài đặt ứng dụng hoặc cập nhật của đầu ghi, nạp một tệp ứng dụng chưa được ký số xác thực hoặc đã bị thay đổi nội dung.

2) Thực hiện lệnh kích hoạt tệp ứng dụng đó và đánh giá xem hệ điều hành của thiết bị có ngăn chặn, từ chối quyền thực thi hay không.

3.2.6.2.3. Kết luận

1) Đáp ứng: Thiết bị đầu ghi từ chối cấp quyền thực thi đối với các ứng dụng, phần mềm chưa được xác thực tính hợp lệ.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.2.7. Nhóm kiểm thử yêu cầu 2.2.7

3.2.7.1. Mục tiêu kiểm thử

Kiểm thử đầu ghi hình (NVR/DVR) đáp ứng hay không yêu cầu 2.2.7 Quy chuẩn này.

3.2.7.2. Đánh giá sự tuân thủ về thiết kế

3.2.7.2.1. Mục đích kiểm thử

Đánh giá việc thiết bị không còn tồn tại tài khoản, mật khẩu mặc định của nhà sản xuất ở trạng thái có thể đăng nhập.

3.2.7.2.2. Phương pháp kiểm thử

1) Tra cứu tài liệu kỹ thuật của nhà sản xuất hoặc cơ sở dữ liệu công khai để xác định danh sách tài khoản, mật khẩu mặc định theo model thiết bị.

2) Thử đăng nhập vào giao diện quản trị của thiết bị (Web, ứng dụng quản lý, giao diện dòng lệnh nếu có) bằng các tài khoản, mật khẩu mặc định đã xác định.

3) Đánh giá thiết bị có từ chối đăng nhập bằng tài khoản, mật khẩu mặc định hay có bắt buộc thiết lập lại tài khoản, mật khẩu ngay trong lần khởi tạo đầu tiên hay không.

3.2.7.2.3. Kết luận

1) Đáp ứng: Thiết bị từ chối việc đăng nhập bằng tài khoản, mật khẩu mặc định hoặc bắt buộc người dùng thiết lập lại tài khoản, mật khẩu khác tài khoản, mật khẩu mặc định trước khi cho phép sử dụng.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.2.8. Nhóm kiểm thử yêu cầu 2.2.8

3.2.8.1. Mục tiêu kiểm thử

Kiểm thử đầu ghi hình (NVR/DVR) đáp ứng hay không yêu cầu 2.2.8 Quy chuẩn này.

3.2.8.2. Đánh giá sự tuân thủ về thiết kế

3.2.8.2.1. Mục đích kiểm thử: Đánh giá thiết bị có cơ chế cập nhật phần mềm/firmware có xác thực chữ ký số nguồn gốc bản cập nhật, có khả năng phát hiện bản cập nhật không hợp lệ, có khả năng khôi phục về phiên bản ổn định khi cập nhật thất bại hoặc gián đoạn.

3.2.8.2.2. Phương pháp kiểm thử

1) Chuẩn bị gói cập nhật firmware giả lập chưa được ký số hợp lệ hoặc đã bị chỉnh sửa nội dung.

2) Thực hiện thao tác nạp gói cập nhật giả lập vào thiết bị qua kênh cập nhật thông thường (bao gồm cả kênh OTA nếu thiết bị hỗ trợ).

3) Đánh giá thiết bị có từ chối cài đặt gói cập nhật không hợp lệ hay không.

4) Trong một kịch bản riêng, chủ động ngắt nguồn hoặc ngắt kết nối trong khi thiết bị đang thực hiện một bản cập nhật hợp lệ, sau đó quan sát khả năng khôi phục của thiết bị.

3.2.8.2.3. Kết luận

1) Đáp ứng: Thiết bị từ chối cài đặt gói cập nhật không được ký số hợp lệ hoặc đã bị chỉnh sửa; khôi phục được về phiên bản ổn định khi quá trình cập nhật hợp lệ thất bại hoặc bị gián đoạn, không rơi vào trạng thái không thể khởi động.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.3. Nhóm kiểm thử yêu cầu đối với hệ thống mạng

3.3.1. Nhóm kiểm thử yêu cầu 2.3.1

3.3.1.1. Mục tiêu kiểm thử

Kiểm thử hệ thống mạng đáp ứng hay không yêu cầu 2.3.1 Quy chuẩn này.

3.3.1.2. Đánh giá sự tuân thủ về thiết kế

3.3.1.2.1. Mục đích kiểm thử

Đánh giá việc hệ thống mạng chỉ mở các giao thức an toàn phục vụ truyền tải và quản trị các cấu phần của hệ thống camera giám sát, chặn các giao thức không cần thiết.

3.3.1.2.2. Phương pháp kiểm thử

1) Sử dụng các công cụ rà quét cổng mạng từ một máy trạm nằm trong cùng vùng mạng và từ một máy trạm nằm ở vùng mạng khác (nếu có định tuyến).

2) Thực hiện quét toàn bộ các cổng TCP/UDP đối với các dải IP được quy hoạch cho camera giám sát và máy chủ quản lý (đối với hệ thống quy mô lớn, được phép quét theo mẫu đại diện cho từng chủng loại thiết bị).

3) Đối chiếu danh sách các cổng/giao thức đang mở với tài liệu thiết kế mạng. Kiểm tra sự tồn tại của các giao thức không mã hóa, kém an toàn (như Telnet, HTTP không mã hóa).

3.3.1.2.3. Kết luận

1) Đáp ứng: Hệ thống mạng chỉ phản hồi trên các cổng/giao thức an toàn đã được cấu hình; trường hợp sử dụng chuẩn ONVIF thì kết nối qua HTTPS/TLS với Profile phù hợp chức năng thiết bị; các giao thức không an toàn bị khóa hoàn toàn (trừ trường hợp ngoại lệ tại yêu cầu 2.3.1).

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.3.2. Nhóm kiểm thử yêu cầu 2.3.2

3.3.2.1. Mục tiêu kiểm thử

Kiểm thử hệ thống mạng đáp ứng hay không yêu cầu 2.3.2 Quy chuẩn này.

3.3.2.2. Đánh giá sự tuân thủ về thiết kế

3.3.2.2.1. Mục đích kiểm thử

Đánh giá khả năng phân tách độc lập giữa vùng mạng dành riêng cho camera giám sát và các vùng mạng khác.

3.3.2.2.2. Phương pháp kiểm thử

1) Kết nối một máy trạm vào vùng mạng người dùng nội bộ (không thuộc vùng mạng camera).

2) Thực hiện các lệnh kiểm tra kết nối (ping, traceroute...) và cố gắng truy cập thẳng vào dải IP tĩnh của các camera giám sát hoặc đầu ghi.

3) Đánh giá xem hệ thống tường lửa hoặc thiết bị chuyển mạch, tính năng phân tách mạng trên thiết bị đầu ghi có chặn truy cập chéo trái phép này hay không.

3.3.2.2.3. Kết luận

1) Đáp ứng: Không thể thiết lập kết nối từ các vùng mạng khác tới vùng mạng camera ngoài các kết nối phục vụ quản trị, vận hành, khai thác đã được cấu hình.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.3.3. Nhóm kiểm thử yêu cầu 2.3.3

3.3.3.1. Mục tiêu kiểm thử

Kiểm thử hệ thống mạng đáp ứng hay không yêu cầu 2.3.3 Quy chuẩn này.

3.3.3.2. Đánh giá sự tuân thủ về thiết kế

3.3.3.2.1. Mục đích kiểm thử

Đánh giá tính năng kiểm soát quyền truy cập của các thiết bị phần cứng khi cắm trực tiếp vào hệ thống camera giám sát thông qua địa chỉ MAC.

3.3.3.2.2. Phương pháp kiểm thử

- 1) Chuẩn bị một thiết bị máy tính giả mạo (không được đăng ký địa chỉ MAC hợp lệ).
- 2) Kết nối vật lý thiết bị này vào giao diện vật lý của hệ thống camera giám sát.
- 3) Kiểm tra xem thiết bị có được cấp phát địa chỉ IP (DHCP) hoặc (khi đặt địa chỉ IP tĩnh) có khả năng truyền nhận bản tin broadcast/multicast với các thiết bị khác trong mạng hay không.

3.3.3.2.3. Kết luận

- 1) Đáp ứng: Hệ thống camera giám sát từ chối cấp quyền truy cập, thiết bị ngoại lai không thể giao tiếp mạng.
- 2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.3.4. Nhóm kiểm thử yêu cầu 2.3.4

3.3.4.1. Mục tiêu kiểm thử

Kiểm thử hệ thống mạng đáp ứng hay không yêu cầu 2.3.4 Quy chuẩn này.

3.3.4.2. Đánh giá sự tuân thủ về thiết kế

3.3.4.2.1. Mục đích kiểm thử

Đánh giá khả năng đồng bộ thời gian của các thiết bị trong hệ thống với một máy chủ thời gian (NTP Server).

3.3.4.2.2. Phương pháp kiểm thử

- 1) Truy cập vào cấu hình của 01 camera IP và 01 thiết bị lưu trữ, thiết lập sai lệch thời gian hệ thống.
- 2) Cấu hình địa chỉ máy chủ NTP nội bộ (hoặc NTP được chỉ định) cho các thiết bị này và kích hoạt tính năng đồng bộ.
- 3) Kiểm tra lại thời gian trên các thiết bị, đối chiếu với thời gian thực tế của máy chủ NTP sau chu kỳ đồng bộ.

3.3.4.2.3. Kết luận

- 1) Đáp ứng: Thời gian trên các thiết bị tự động cập nhật và đồng bộ chính xác với máy chủ NTP.
- 2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.3.5. Nhóm kiểm thử yêu cầu 2.3.5

3.3.5.1. Mục tiêu kiểm thử

Kiểm thử hệ thống mạng đáp ứng hay không yêu cầu 2.3.5 Quy chuẩn này.

3.3.5.2. Đánh giá sự tuân thủ về thiết kế

3.3.5.2.1. Mục đích kiểm thử

Đánh giá việc truy cập, quản trị từ xa được thực hiện qua kênh mã hóa, xác thực hai chiều và cổng quản trị thiết bị không lộ ra Internet công cộng.

3.3.5.2.2. Phương pháp kiểm thử

1) Từ một máy trạm trên mạng Internet công cộng, thử dò quét và kết nối trực tiếp tới cổng dịch vụ quản trị (SSH, giao diện Web quản trị) của camera, đầu ghi hình, thiết bị trung gian theo địa chỉ IP công cộng (nếu có).

2) Thử thiết lập một phiên truy cập, quản trị từ xa hợp lệ và giám sát các thông số của phiên kết nối (giao thức, cơ chế xác thực...).

3.3.5.2.3. Kết luận

1) Đáp ứng: Không thể kết nối trực tiếp từ Internet công cộng tới cổng quản trị của thiết bị; phiên truy cập, quản trị từ xa hợp lệ chỉ được thiết lập qua kênh mã hóa, xác thực hai chiều.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.4. Nhóm kiểm thử yêu cầu đối với cấu phần lưu trữ

3.4.1. Nhóm kiểm thử yêu cầu 2.4.1

3.4.1.1. Mục tiêu kiểm thử

Kiểm thử cấu phần lưu trữ cục bộ đáp ứng hay không yêu cầu 2.4.1 Quy chuẩn này.

3.4.1.2. Đánh giá sự tuân thủ về thiết kế

3.4.1.2.1. Mục đích kiểm thử

Đánh giá khả năng cấu hình mảng đĩa độc lập dự phòng (RAID) bảo đảm an toàn, chống mất, thất thoát dữ liệu.

3.4.1.2.2. Phương pháp kiểm thử

1) Kiểm tra hồ sơ thiết kế và cấu hình thực tế của thiết bị lưu trữ, xác nhận hệ thống đã được thiết lập các chuẩn RAID có khả năng dự phòng (như RAID 1, RAID 5, RAID 6...).

2) Trong quá trình hệ thống đang ghi hình liên tục, tiến hành rút nóng ngẫu nhiên (hoặc ngắt kết nối bằng phần mềm) một ổ đĩa cứng thuộc cụm RAID.

3) Quan sát trạng thái hoạt động của hệ thống lưu trữ và trích xuất lại đoạn video vừa ghi.

3.4.1.2.3. Kết luận

1) Đáp ứng: Hệ thống duy trì hoạt động ghi hình bình thường, phát ra cảnh báo lỗi đĩa nhưng không làm gián đoạn hệ thống và không làm mất dữ liệu video.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.4.2. Nhóm kiểm thử yêu cầu 2.4.2

3.4.2.1. Mục tiêu kiểm thử

Kiểm thử cấu phần lưu trữ cục bộ đáp ứng hay không yêu cầu 2.4.2 Quy chuẩn này.

3.4.2.2. Đánh giá sự tuân thủ về thiết kế

3.4.2.2.1. Mục đích kiểm thử

Đánh giá cấu phần lưu trữ cục bộ có chức năng hỗ trợ tự động thay thế và tiến hành tái tạo đồng bộ hóa dữ liệu thông qua ổ đĩa dự phòng nóng ngay khi phát hiện có sự cố hỏng đĩa.

3.4.2.2.2. Phương pháp kiểm thử

1) Kiểm tra cấu hình thiết bị lưu trữ, bảo đảm đã gán ít nhất một ổ đĩa cứng ở trạng thái ổ đĩa dự phòng nóng (Hot spare).

2) Ngắt kết nối (hoặc rút vật lý) một ổ đĩa cứng đang chứa dữ liệu trong cụm RAID.

3) Giám sát quá trình phản hồi của bộ điều khiển lưu trữ.

3.4.2.2.3. Kết luận

1) Đáp ứng: Thiết bị tự động ghi nhận ổ đĩa hỏng, lập tức chuyển ổ đĩa dự phòng nóng vào cụm và bắt đầu quá trình tái tạo dữ liệu tự động.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.4.3. Nhóm kiểm thử yêu cầu 2.4.3

3.4.3.1. Mục tiêu kiểm thử

Kiểm thử cấu phần lưu trữ đám mây đáp ứng hay không yêu cầu 2.4.3 Quy chuẩn này.

3.4.3.2. Đánh giá sự tuân thủ về thiết kế

3.4.3.2.1. Mục đích kiểm thử

Đánh giá tính bảo mật của kênh truyền khi dữ liệu được đẩy từ hệ thống mạng cục bộ lên môi trường đám mây.

3.4.3.2.2. Phương pháp kiểm thử

1) Sử dụng công cụ phân tích gói tin mạng để theo dõi kết nối định tuyến đi ra Internet (WAN interface) hướng về địa chỉ máy chủ đám mây.

2) Phân tích cấu trúc các gói tin dữ liệu chứa video đang được truyền tải.

3) Kiểm tra giao thức trao đổi khóa mã hóa, xác minh xem kết nối có sử dụng TLS 1.2 trở lên hoặc sử dụng kênh truyền riêng có mã hóa (VPN Site-to-Site/IPSec) hay không.

3.4.3.2.3. Kết luận

1) Đáp ứng: Toàn bộ dữ liệu đẩy lên đám mây được mã hóa bằng TLS 1.2 trở lên hoặc thông qua kênh truyền riêng an toàn. Không thu được dữ liệu video ở dạng chưa mã hóa.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.4.4. Nhóm kiểm thử yêu cầu 2.4.4

3.4.4.1. Mục tiêu kiểm thử

Kiểm thử cấu phần lưu trữ đám mây đáp ứng hay không yêu cầu 2.4.4 Quy chuẩn này.

3.4.4.2. Đánh giá sự tuân thủ về thiết kế

3.4.4.2.1. Mục đích kiểm thử

Đánh giá cơ chế cấp quyền chỉ ghi, không cấp quyền xem, sửa, xóa cho các thiết bị truyền tải dữ liệu lên lưu trữ đám mây.

3.4.4.2.2. Phương pháp kiểm thử

1) Trích xuất thông tin xác thực (Access Key/Secret Key hoặc Token) được cấp phát cho một thiết bị camera/gateway đẩy dữ liệu lên đám mây.

2) Sử dụng bộ thông tin xác thực này trên một máy trạm trung gian, gửi lệnh yêu cầu API nhằm đọc, sửa tên hoặc xóa một tệp video đã tồn tại trên đám mây.

3.4.4.2.3. Kết luận

1) Đáp ứng: Đám mây chỉ chấp nhận các lệnh đẩy dữ liệu (chỉ ghi), trả về mã lỗi từ chối truy cập đối với mọi lệnh đọc, sửa hoặc xóa.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.4.5. Nhóm kiểm thử yêu cầu 2.4.5

3.4.5.1. Mục tiêu kiểm thử

Kiểm thử cấu phần lưu trữ đám mây đáp ứng hay không yêu cầu 2.4.5 Quy chuẩn này.

3.4.5.2. Đánh giá sự tuân thủ về thiết kế

3.4.5.2.1. Mục đích kiểm thử

Đánh giá tính năng WORM đối với dữ liệu trên nền tảng đám mây, cho phép tự động ghi đè hoặc xóa dữ liệu an toàn khi hết thời hạn lưu trữ.

3.4.5.2.2. Phương pháp kiểm thử

1) Thực hiện kiểm tra và kích hoạt tính năng khóa WORM trên thư mục lưu trữ đám mây với một thời gian lưu giữ ngắn (ví dụ 01 ngày).

2) Đẩy một tệp tin video lên thư mục này.

3) Sử dụng tài khoản có đặc quyền quản trị cao nhất (Root/Admin của hệ thống lưu trữ) thực thi lệnh xóa hoặc sửa đổi nội dung tệp video vừa tải lên (khi chưa hết thời hạn lưu trữ).

4) Sau khi hết thời hạn lưu giữ đã thiết lập, thực hiện đẩy tệp video ghi đè video có sẵn trong thư mục này.

3.4.5.2.3. Kết luận

1) Đáp ứng: Hệ thống đám mây từ chối mọi thao tác thay đổi hoặc xóa tệp tin, ngay cả với quyền quản trị viên, cho đến khi thời hạn WORM kết thúc; cho phép ghi đè video khi thời hạn WORM kết thúc.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.5. Nhóm kiểm thử yêu cầu đối với phần mềm quản lý video

3.5.1. Nhóm kiểm thử yêu cầu 2.5.1

3.5.1.1. Mục tiêu kiểm thử

Kiểm thử phần mềm quản lý video (VMS) đáp ứng hay không yêu cầu 2.5.1 Quy chuẩn này.

3.5.1.2. Đánh giá sự tuân thủ về thiết kế

3.5.1.2.1. Mục đích kiểm thử

Đánh giá cơ chế mã hóa dữ liệu hình ảnh, âm thanh và luồng lệnh điều khiển khi truyền tải giữa các thành phần của VMS.

3.5.1.2.2. Phương pháp kiểm thử

1) Thiết lập môi trường theo dõi gói tin mạng (ví dụ: packet sniffer) giữa máy khách, máy chủ VMS và thiết bị đầu cuối.

2) Giám sát quá trình truyền tải dữ liệu hình ảnh, âm thanh trực tiếp và các lệnh điều khiển cấu hình thiết bị.

3) Đánh giá các gói dữ liệu thu thập được có bị tiết lộ dưới dạng bản chưa được mã hóa hay không, xác minh hệ thống có sử dụng giao thức mã hóa, đường truyền an toàn.

3.5.1.2.3. Kết luận

1) Đáp ứng: Toàn bộ dữ liệu truyền tải được mã hóa, bảo đảm tính bảo mật cho hệ thống.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.5.2. Nhóm kiểm thử yêu cầu 2.5.2

3.5.2.1. Mục tiêu kiểm thử

Kiểm thử phần mềm quản lý video (VMS) đáp ứng hay không yêu cầu 2.5.2 Quy chuẩn này.

3.5.2.2. Đánh giá sự tuân thủ về thiết kế

3.5.2.2.1. Mục đích kiểm thử

Đánh giá tính năng bảo vệ toàn vẹn dữ liệu, tự động phát hiện, ngăn chặn chèn tệp, sửa đổi, làm giả luồng dữ liệu truyền tải.

3.5.2.2.2. Phương pháp kiểm thử

- 1) Triển khai thực thể trung gian, chặn bắt luồng truyền video thực tế.
- 2) Tiến hành chèn một đoạn video tĩnh hoặc gói tin điều khiển giả mạo vào luồng mạng và chuyển tiếp đến máy chủ VMS.
- 3) Đánh giá xem máy chủ VMS có cơ chế kiểm tra tính toàn vẹn (như mã băm, chữ ký số, chứng thư số) hoặc biện pháp ngăn chặn để phát hiện và từ chối gói tin giả mạo hay không.

3.5.2.2.3. Kết luận

1) Đáp ứng: VMS phát hiện luồng dữ liệu bị can thiệp, lập tức từ chối gói tin và ngắt kết nối không an toàn.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.5.3. Nhóm kiểm thử yêu cầu 2.5.3

3.5.3.1. Mục tiêu kiểm thử

Kiểm thử phần mềm quản lý video (VMS) đáp ứng hay không yêu cầu 2.5.3 Quy chuẩn này.

3.5.3.2. Đánh giá sự tuân thủ về thiết kế

3.5.3.2.1. Mục đích kiểm thử

Đánh giá cơ chế xác thực, định danh người dùng và xác thực tính hợp lệ của thiết bị đầu cuối trước khi cho phép bất kỳ thiết bị hay tài khoản nào thiết lập kết nối trao đổi dữ liệu.

3.5.3.2.2. Phương pháp kiểm thử

1) Kết nối một camera không có định danh hợp lệ vào hệ thống VMS. Đồng thời, thử nghiệm đăng nhập vào cổng quản trị máy chủ VMS bằng các phương thức xác thực và tài khoản không hợp lệ.

2) Đánh giá hệ thống có từ chối đăng nhập sai và từ chối thu thập dữ liệu từ thiết bị chưa xác thực danh tính hay không.

3) Đánh giá hệ thống có phương án kiểm soát các thiết bị kết nối vào hay không, có giao diện trên VMS để thực hiện khai báo kết nối hay không.

3.5.3.2.3. Kết luận

1) Đáp ứng: VMS yêu cầu và xác minh định danh của máy khách lần thiết bị, vô hiệu hóa mọi kết nối chưa xác thực.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.5.4. Nhóm kiểm thử yêu cầu 2.5.4

3.5.4.1. Mục tiêu kiểm thử

Kiểm thử phần mềm quản lý video (VMS) đáp ứng hay không yêu cầu 2.5.4 Quy chuẩn này.

3.5.4.2. Đánh giá sự tuân thủ về thiết kế

3.5.4.2.1. Mục đích kiểm thử

Đánh giá tính năng phân quyền chức năng theo vai trò đối với từng tài khoản người dùng của VMS.

3.5.4.2.2. Phương pháp kiểm thử

1) Đăng nhập vào VMS bằng tài khoản người dùng có quyền hạn giám sát thông thường (không có quyền quản trị).

2) Thực hiện các thao tác vượt giới hạn phân quyền (như thay đổi cấu hình mạng camera, xem lại tệp ghi hình, xóa nhật ký đăng nhập...).

3) Đánh giá xem VMS có ngăn chặn và từ chối thao tác dựa trên hệ thống phân quyền theo vai trò đã thiết lập hay không.

4) Đánh giá xem VMS có giao diện phân quyền cho người dùng hay không.

3.5.4.2.3. Kết luận

1) Đáp ứng: VMS có giao diện phân quyền, phân tách rõ ràng quyền hạn và chặn thành công mọi truy cập, thao tác vượt quyền được cấp.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.5.5. Nhóm kiểm thử yêu cầu 2.5.5

3.5.5.1. Mục tiêu kiểm thử

Kiểm thử phần mềm quản lý video (VMS) đáp ứng hay không yêu cầu 2.5.5 Quy chuẩn này.

3.5.5.2. Đánh giá sự tuân thủ về thiết kế

3.5.5.2.1. Mục đích kiểm thử

Đánh giá phần mềm VMS không tồn tại các lỗ hổng bảo mật ở mức nghiêm trọng hoặc cao và có khả năng ngăn chặn các hành vi tấn công dò mật khẩu tự động.

3.5.5.2.2. Phương pháp kiểm thử

1) Thiết lập các cuộc tấn công mạng mô phỏng, bao gồm các cuộc tấn công phổ biến, tấn công vét cạn tài khoản đăng nhập nhắm vào cổng dịch vụ của máy chủ VMS.

2) Đánh giá phần mềm VMS có tồn tại lỗ hổng bảo mật ở mức nghiêm trọng và mức cao theo thang điểm CVSS hay không; đồng thời đánh giá VMS có tự động khóa tài khoản, giới hạn lượt đăng nhập sau một số lần đăng nhập sai hay không.

3.5.5.2.3. Kết luận

1) Đáp ứng: VMS không tồn tại các lỗ hổng bảo mật ở mức nghiêm trọng và mức cao theo thang điểm CVSS, vô hiệu hóa cuộc tấn công vét cạn.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.5.6. Nhóm kiểm thử yêu cầu 2.5.6

3.5.6.1. Mục tiêu kiểm thử

Kiểm thử phần mềm quản lý video (VMS) đáp ứng hay không yêu cầu 2.5.6 Quy chuẩn này.

3.5.6.2. Đánh giá sự tuân thủ về thiết kế

3.5.6.2.1. Mục đích kiểm thử

Đánh giá khả năng ghi nhận nhật ký hoạt động đối với mọi hoạt động của người dùng trên VMS.

3.5.6.2.2. Phương pháp kiểm thử

1) Sử dụng tài khoản người dùng để thực hiện các thao tác: xem luồng video trực tiếp, phát lại video, thay đổi cấu hình thiết bị và xóa tệp video.

2) Trích xuất tệp nhật ký hệ thống của VMS và kiểm tra xem các hành động trên có được ghi lại đầy đủ thông tin (tài khoản định danh người dùng, thời gian, thao tác, đối tượng bị tác động...) hay không.

3.5.6.2.3. Kết luận

1) Đáp ứng: VMS ghi nhận đầy đủ, chính xác các thao tác của người dùng trong tệp nhật ký giám sát.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.5.7. Nhóm kiểm thử yêu cầu 2.5.7

3.5.7.1. Mục tiêu kiểm thử

Kiểm thử phần mềm quản lý video (VMS) đáp ứng hay không yêu cầu 2.5.7 Quy chuẩn này.

3.5.7.2. Đánh giá sự tuân thủ về thiết kế

3.5.7.2.1. Mục đích kiểm thử

Đánh giá tính hiệu quả của cơ chế phân quyền truy cập theo từng camera, đầu ghi hình đối với từng tài khoản người dùng.

3.5.7.2.2. Phương pháp kiểm thử

1) Thiết lập ít nhất hai tài khoản người dùng (A và B). Tài khoản A chỉ được cấp quyền truy cập Camera 1 và NVR 1; Tài khoản B chỉ được cấp quyền truy cập Camera 2 và NVR 2.

2) Sử dụng Tài khoản A đăng nhập và xem luồng video từ Camera 2, kết nối, trích xuất dữ liệu từ NVR 2. Thực hiện thao tác vượt quyền tương tự với Tài khoản B đối với Camera 1 và NVR 1.

3) Đánh giá xem VMS có chặn các thao tác vượt quyền và hiển thị thông báo từ chối truy cập tương ứng hay không.

3.5.7.2.3. Kết luận

1) Đáp ứng: VMS kiểm soát và giới hạn thành công quyền truy cập, người dùng không thể xem camera hay kết nối với NVR/DVR nằm ngoài cấu hình phân quyền.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.5.8. Nhóm kiểm thử yêu cầu 2.5.8

3.5.8.1. Mục tiêu kiểm thử

Kiểm thử phần mềm quản lý video (VMS) đáp ứng hay không yêu cầu 2.5.8 Quy chuẩn này.

3.5.8.2. Đánh giá sự tuân thủ về thiết kế

3.5.8.2.1. Mục đích kiểm thử

Đánh giá khả năng nhúng hình mờ vào video camera giám sát của VMS.

3.5.8.2.2. Phương pháp kiểm thử

1) Truy cập vào giao diện quản lý/cấu hình của VMS, tiến hành kích hoạt và thiết lập tính năng nhúng hình mờ lên video.

2) Đăng nhập vào phần mềm bằng tài khoản kiểm thử và mở màn hình xem trực tiếp hoặc tiến hành trích xuất một đoạn video từ hệ thống.

3) Quan sát màn hình hiển thị hoặc tệp tin video thu được nhằm xác định sự xuất hiện của hình mờ (đối với hình mờ ẩn, sử dụng công cụ của nhà sản xuất để trích xuất).

3.5.8.2.3. Kết luận

1) Đáp ứng: VMS có chức năng nhúng hình mờ vào video camera giám sát.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.5.9. Nhóm kiểm thử yêu cầu 2.5.9

3.5.9.1. Mục tiêu kiểm thử

Kiểm thử phần mềm quản lý video đáp ứng hay không yêu cầu 2.5.9 Quy chuẩn này.

3.5.9.2. Đánh giá sự tuân thủ về thiết kế

3.5.9.2.1. Mục đích kiểm thử

Đánh giá việc máy chủ cài đặt VMS chỉ cho phép hoạt động các cổng dịch vụ phục vụ truyền phát, điều khiển video và quản trị, vận hành phần mềm; chặn hoàn toàn các cổng/giao thức khác.

3.5.9.2.2. Phương pháp kiểm thử

1) Sử dụng một máy chủ/máy trạm độc lập nằm ở vùng mạng được phép tương tác với máy chủ VMS.

2) Sử dụng các công cụ rà quét cổng mạng chuyên dụng để thực hiện quét TCP và UDP trên địa chỉ IP của máy chủ VMS.

3) Đối chiếu kết quả các cổng/giao thức mạng đang mở trên hệ thống với tài liệu thiết kế mạng, tài liệu mô tả kỹ thuật của nhà sản xuất hoặc hồ sơ khai báo hệ thống.

4) Kiểm tra trạng thái của các giao thức không an toàn hoặc không phục vụ mục đích truyền phát và điều khiển hệ thống quản lý video để bảo đảm chúng không được phép kết nối.

3.5.9.2.3. Kết luận

1) Đáp ứng: Kết quả rà quét cho thấy hệ thống chỉ mở và phản hồi đối với các cổng, giao thức truyền phát, điều khiển video và quản trị, vận hành của VMS và các dịch vụ hỗ trợ đã được khai báo; các cổng/giao thức khác ở trạng thái đóng.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.5.10. Nhóm kiểm thử yêu cầu 2.5.10

3.5.10.1. Mục tiêu kiểm thử: Kiểm thử phần mềm quản lý video (VMS) đáp ứng hay không yêu cầu 2.5.10 Quy chuẩn này.

3.5.10.2. Đánh giá sự tuân thủ về thiết kế

3.5.10.2.1. Mục đích kiểm thử

Đánh giá hiệu quả của tính năng bảo vệ ứng dụng/API và xác thực, phân quyền, kiểm soát phiên làm việc đối với từng yêu cầu kết nối của VMS.

3.5.10.2.2. Phương pháp kiểm thử

1) Xác định danh sách API, Web Portal do VMS cung cấp phục vụ kết nối với hệ thống bên ngoài.

2) Thực hiện các kỹ thuật kiểm thử tấn công ứng dụng Web/API phổ biến (như SQL Injection, Cross-Site Scripting, gửi yêu cầu không xác thực...) nhằm vào các API, Web Portal đã xác định.

3) Đánh giá khả năng phát hiện, ngăn chặn của giải pháp bảo vệ ứng dụng/API đối với các kỹ thuật tấn công nêu trên; kiểm tra cơ chế xác thực, phân quyền và kiểm soát phiên đối với từng yêu cầu API.

3.5.10.2.3. Kết luận

1) Đáp ứng: Giải pháp bảo vệ ứng dụng/API phát hiện và ngăn chặn thành công các kỹ thuật tấn công thử nghiệm; mọi yêu cầu API đều được xác thực, phân quyền và kiểm soát phiên làm việc.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.6. Nhóm kiểm thử yêu cầu đối với thiết bị trung gian xử lý tại biên

3.6.1. Nhóm kiểm thử yêu cầu 2.6.1

3.6.1.1. Mục tiêu kiểm thử

Kiểm thử thiết bị trung gian xử lý tại biên đáp ứng hay không yêu cầu 2.6.1 Quy chuẩn này.

3.6.1.2. Đánh giá sự tuân thủ về thiết kế

3.6.1.2.1. Mục đích kiểm thử

Đánh giá việc mỗi thiết bị trung gian xử lý tại biên có chứng thư số, khóa mật mã riêng, không dùng chung giữa nhiều thiết bị.

3.6.1.2.2. Phương pháp kiểm thử

1) Kiểm tra chứng thư số hoặc khóa mật mã được cấp cho tối thiểu hai thiết bị trung gian cùng model trong hệ thống.

2) Đối chiếu, so sánh thông tin định danh (số serial chứng thư, khóa công khai) giữa hai thiết bị.

3) Sử dụng một chứng thư/ khóa không được đăng ký để giả lập kết nối thay cho một thiết bị đã đăng ký.

3.6.1.2.3. Kết luận

1) Đáp ứng: Mỗi thiết bị có chứng thư/ khóa mật mã duy nhất, không trùng lặp; hệ thống từ chối kết nối khi phát hiện thiết bị sử dụng danh tính không đúng với thiết bị đã đăng ký.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.6.2. Nhóm kiểm thử yêu cầu 2.6.2

3.6.2.1. Mục tiêu kiểm thử

Kiểm thử thiết bị trung gian xử lý tại biên đáp ứng hay không yêu cầu 2.6.2 Quy chuẩn này.

3.6.2.2. Đánh giá sự tuân thủ về thiết kế

3.6.2.2.1. Mục đích kiểm thử

Đánh giá tính năng khởi động an toàn và chỉ cho phép nạp, thực thi firmware, phần mềm đã được ký số hợp lệ của thiết bị trung gian xử lý tại biên.

3.6.2.2.2. Phương pháp kiểm thử

1) Chuẩn bị bản firmware giả lập không có chữ ký số hợp lệ.

2) Thực hiện nạp bản firmware nêu trên vào thiết bị.

3) Quan sát quá trình khởi động của thiết bị và kết quả xác thực chữ ký số.

3.6.2.2.3. Kết luận

1) Đáp ứng: Thiết bị từ chối khởi động hoặc từ chối nạp firmware không có chữ ký số hợp lệ.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.6.3. Nhóm kiểm thử yêu cầu 2.6.3**3.6.3.1. Mục tiêu kiểm thử**

Kiểm thử thiết bị trung gian xử lý tại biên đáp ứng hay không yêu cầu 2.6.3 Quy chuẩn này.

3.6.3.2. Đánh giá sự tuân thủ về thiết kế**3.6.3.2.1. Mục đích kiểm thử**

Đánh giá việc thiết bị trung gian xử lý tại biên chỉ kết nối tới dịch vụ được cấp phép, không truy cập trực tiếp Internet hoặc truy cập ngang camera, thiết bị khác ngoài phạm vi cấp phép.

3.6.3.2.2. Phương pháp kiểm thử

1) Giám sát lưu lượng mạng phát sinh từ thiết bị trong điều kiện vận hành bình thường.

2) Thử cấu hình một địa chỉ đích ngoài danh sách được cấp phép (ví dụ một máy chủ ngoài Internet công cộng hoặc một camera khác trong hệ thống) và quan sát phản ứng của thiết bị, hạ tầng mạng.

3) Đối chiếu danh sách kết nối thực tế với danh mục dịch vụ đã được cấp phép trong hồ sơ thiết kế.

3.6.3.2.3. Kết luận

1) Đáp ứng: Thiết bị chỉ phát sinh kết nối tới các địa chỉ, dịch vụ đã được cấp phép; mọi kết nối ngoài danh mục đều bị hạ tầng mạng ngăn chặn.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.6.4. Nhóm kiểm thử yêu cầu 2.6.4**3.6.4.1. Mục tiêu kiểm thử**

Kiểm thử thiết bị trung gian xử lý tại biên đáp ứng hay không yêu cầu 2.6.4 Quy chuẩn này.

3.6.4.2. Đánh giá sự tuân thủ về thiết kế**3.6.4.2.1. Mục đích kiểm thử**

Đánh giá cơ chế mã hóa, giới hạn thời hạn lưu tạm hoặc lưu đệm cục bộ trên thiết bị trung gian xử lý tại biên.

3.6.4.2.2. Phương pháp kiểm thử

1) Trích xuất trực tiếp bộ nhớ lưu trữ cục bộ (thẻ nhớ, ổ lưu trữ gắn trong) của thiết bị sau một chu kỳ hoạt động có phát sinh dữ liệu đệm.

2) Sử dụng công cụ đọc dữ liệu thô để kiểm tra dữ liệu trích xuất được có ở dạng bản chưa được mã hóa hay đã được mã hóa.

3) Chờ hết thời hạn lưu đã cấu hình, sau đó kiểm tra lại dữ liệu lưu tạm còn tồn tại trên thiết bị.

3.6.4.2.3. Kết luận

1) Đáp ứng: Dữ liệu lưu tạm hoặc lưu đệm cục bộ được mã hóa; hết thời hạn lưu trữ dữ liệu lưu tạm không còn tồn tại trên thiết bị.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.6.5. Nhóm kiểm thử yêu cầu 2.6.5

3.6.5.1. Mục tiêu kiểm thử

Kiểm thử thiết bị trung gian xử lý tại biên đáp ứng hay không yêu cầu 2.6.5 Quy chuẩn này.

3.6.5.2. Đánh giá sự tuân thủ về thiết kế

3.6.5.2.1. Mục đích kiểm thử

Đánh giá khả năng phát hiện hành vi can thiệp bất thường và tự động cảnh báo hoặc cách ly của thiết bị trung gian xử lý tại biên.

3.6.5.2.2. Phương pháp kiểm thử

1) Thực hiện mở vỏ thiết bị hoặc ngắt kết nối một cảm biến/mô-đun của thiết bị trong điều kiện thiết bị đang hoạt động.

2) Trường hợp thiết bị có hỗ trợ, sử dụng công cụ chuyên dụng để phát lại một đoạn luồng video cũ vào đầu vào xử lý của thiết bị.

3) Quan sát phản ứng của thiết bị và hệ thống giám sát trung tâm sau các thao tác nêu trên.

3.6.5.2.3. Kết luận

1) Đáp ứng: Thiết bị hoặc hệ thống giám sát trung tâm phát hiện và phát cảnh báo về hành vi can thiệp bất thường; thiết bị bị cách ly hoặc dữ liệu từ thiết bị bị đánh dấu không tin cậy.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.6.6. Nhóm kiểm thử yêu cầu 2.6.6

3.6.6.1. Mục tiêu kiểm thử

Kiểm thử thiết bị trung gian xử lý tại biên đáp ứng hay không yêu cầu 2.6.6 Quy chuẩn này.

3.6.6.2. Đánh giá sự tuân thủ về thiết kế

3.6.6.2.1. Mục đích kiểm thử

Đánh giá việc thiết bị chỉ mở các cổng, giao thức phục vụ chức năng thu nhận dữ liệu từ camera và truyền kết quả về hệ thống camera giám sát; mọi kết nối quản trị, bảo trì từ xa phải thực hiện qua kênh mã hóa, xác thực hai chiều.

3.6.6.2.2. Phương pháp kiểm thử

1) Sử dụng công cụ rà quét cổng mạng để quét toàn diện dải cổng TCP/UDP trên địa chỉ IP của thiết bị.

2) Đối chiếu kết quả các cổng/giao thức đang mở với tài liệu thiết kế, mô tả kỹ thuật của nhà sản xuất.

3) Thiết lập kết nối quản trị từ một máy trạm không có chứng thư/khóa xác thực hợp lệ và quan sát phản ứng của thiết bị.

3.6.6.2.3. Kết luận

1) Đáp ứng: Thiết bị chỉ mở các cổng, giao thức phục vụ đúng chức năng thu nhận dữ liệu từ camera và truyền kết quả về hệ thống camera giám sát; từ chối thiết lập kết nối quản trị, bảo trì khi thiếu chứng thư/khóa xác thực hợp lệ.

2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

4. QUY ĐỊNH VỀ QUẢN LÝ

Việc quản lý hệ thống camera giám sát thuộc phạm vi điều chỉnh phải tuân thủ các yêu cầu tại Quy chuẩn này và các quy định của pháp luật khác có liên quan.

5. TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN

5.1. Cơ quan, tổ chức, cá nhân liên quan có trách nhiệm thực hiện các quy định của Quy chuẩn này và chịu sự kiểm tra của cơ quan quản lý nhà nước theo các quy định pháp luật.

5.2. Cục An ninh mạng, Công an các tỉnh, thành phố có trách nhiệm tổ chức triển khai, hướng dẫn cho các đơn vị triển khai hệ thống camera giám sát theo Quy chuẩn này.

5.3. Cục Khoa học, chiến lược và lịch sử Công an chịu trách nhiệm tổ chức phổ biến Quy chuẩn này cho tổ chức, cá nhân có liên quan theo quy định của pháp luật.

6. TỔ CHỨC THỰC HIỆN

6.1. Hệ thống camera giám sát thuộc phạm vi điều chỉnh của Quy chuẩn này đã được xây dựng, đưa vào sử dụng theo đúng quy định của pháp luật trước ngày Quy chuẩn này có hiệu lực vẫn được phép hoạt động bình thường; chậm nhất 24 tháng kể từ ngày Quy chuẩn này có hiệu lực, các hệ thống camera giám sát thuộc phạm vi điều chỉnh phải đáp ứng các quy định tại Quy chuẩn này.

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

6.3. Trong quá trình triển khai thực hiện Quy chuẩn này, nếu có vấn đề phát sinh, vướng mắc, các tổ chức và cá nhân có liên quan phản ánh bằng văn bản về Bộ Công an (qua Cục An ninh mạng) để được hướng dẫn, giải quyết.

Thư mục tài liệu tham khảo

- [1] Recommendation ITU-T F.743.23 (10/2023): Security requirements for video surveillance systems.
- [2] Recommendation ITU-T X.1453 (01/2022): Security threats and requirements for video management systems.
- [3] TAICS TS-0014 & TS-0015 Series (2019): Cybersecurity Standard for Video Surveillance System.