WHITEPAPER

Oktober 2026

Zusammenfassung

Obwohl es auf einer offenen Plattform basiert, bietet das Axis Body-Worn-System einen sehr hohen Grad an Systemsicherheit.

Zum Schutz für den Fall eines Verlustes basiert die Kamera auf einer minimierten Plattform ohne unnötige Softwarekomponenten. Weitere Funktionen sind stattdessen im Systemcontroller untergebracht, der meist weniger physischen Bedrohungen ausgesetzt ist. Außerdem ist der interne Speicher der Kamera nach AES-256 verschlüsselt, um unbefugten Zugriff auf die Daten zu verhindern. Die Kommunikation auf der Grundlage von IPv6 und Zertifikaten stellt sicher, dass die Kamera Daten nur in den spezifischen Systemcontroller oder das zugehörige System lädt.

Während der Datenübertragung von der Kamera zum Systemcontroller wird eine HTTPS-verschlüsselte Netzwerkverbindung verwendet. Die Daten werden nur kurz in der AES-256-verschlüsselten Speichervorrichtung des Systemcontrollers gespeichert, bevor sie über eine weitere HTTPS-verschlüsselte Verbindung in die Dateiablage übertragen werden.

Die Sicherheit und Integrität des Systemcontrollers wird weiter gestärkt durch ein FIPS 140-2-konformes TPM (Trusted Platform Module). Weitere Funktionen, die das Body Worn-System mit vielen anderen Axis Geräten teilt, sind Signiertes OS, Sicheres Booten und Signiertes Video.

Für das Live-Streaming von Bildmaterial über AXIS Body Worn Live können Organisationen zwischen einer von Axis gehosteten Lösung (Cloud) und einer selbst gehosteten Lösung (lokal) wählen. In beiden Fällen werden die Daten im Bereitschaftsmodus und während der Übertragung verschlüsselt und vollständig durchgehend verschlüsselt direkt zum Client des Viewers übertragen. Darüber hinaus hat der Administrator volle Kontrolle darüber, wer zur Anzeige des Livestreams berechtigt ist, einschließlich des jeweiligen Computers, des Clients und der Zugangsdaten des Benutzers.

Inhalt

1 Akronyme und Terminologie 4
2 Einführung 4
3 Sicherheit bei Kameraverlust 4
4 Sicherheit bei der Datenübertragung 4
5 Weitere Sicherheitsfunktionen 5
6 Sicherheit mit AXIS Body Worn Live 5
6.1 Von Axis gehostete Lösung 6
6.2 Selbst gehostete Lösung 6

1 Akronyme und Terminologie

BWC. Body Worn-Kamera

VMS. Videoverwaltungssystem

EMS. Evidence Management System

Dateiablage. Ein Speicherort für die Aufzeichnungen und Daten beispielsweise von Body Worn-Kameras. Beispiele für eine Dateiablage sind Video Management Systeme, Evidence Management Systeme und Medienserver.

2 Einführung

Das Axis Body Worn-System basiert auf einer offenen Plattform, so dass es leicht in externe Systeme für Video- und Beweismittelverwaltung integriert werden kann. Trotzdem ist das System sehr sicher, weil dies in jedem Schritt der Systementwicklung und Umsetzung einen hohen Stellenwert hatte.

Dieses Whitepaper beschreibt den Datenfluss zwischen den Komponenten im Axis Body Worn-System. Besonderer Schwerpunkt liegt auf den Maßnahmen zur Sicherung des Systems und seiner Daten, von der Aufzeichnung durch eine BWC bis hin zur Dateiablage. Außerdem wird erläutert, wie Livestreams mit AXIS Body Worn Live in beiden Lösungsmodellen verschlüsselt werden.

3 Sicherheit bei Kameraverlust

Während ihres alltäglichen Einsatzes ist eine Body Worn-Kamera (BWC) physikalisch der Gefahr von Diebstahl und Vandalismus ausgesetzt. Mehrere Systemdesignfunktionen wurden eingesetzt, um diese Bedrohungen einzudämmen, so dass die Sicherheit von System und Daten nicht gefährdet ist, auch wenn eine Kamera verloren geht.

Ein Beispiel hierfür ist, dass die BWC auf einer minimierten Softwareplattform basiert, aus der verglichen mit der anderer Axis Kameras alle unnötigen Softwarekomponenten entfernt wurden. Die Kamera und der Systemcontroller haben keine VAPIX-Unterstützung und unterstützen keine Protokolle wie FTP, SSH oder SNMP. Außerdem hat die Kamera keine Serverfunktion. Die Integration mit anderen Systemen wie VMS und EMS wird stattdessen vom Systemcontroller abgewickelt, der meist weniger physischen Bedrohungen ausgesetzt ist als die Kameras.

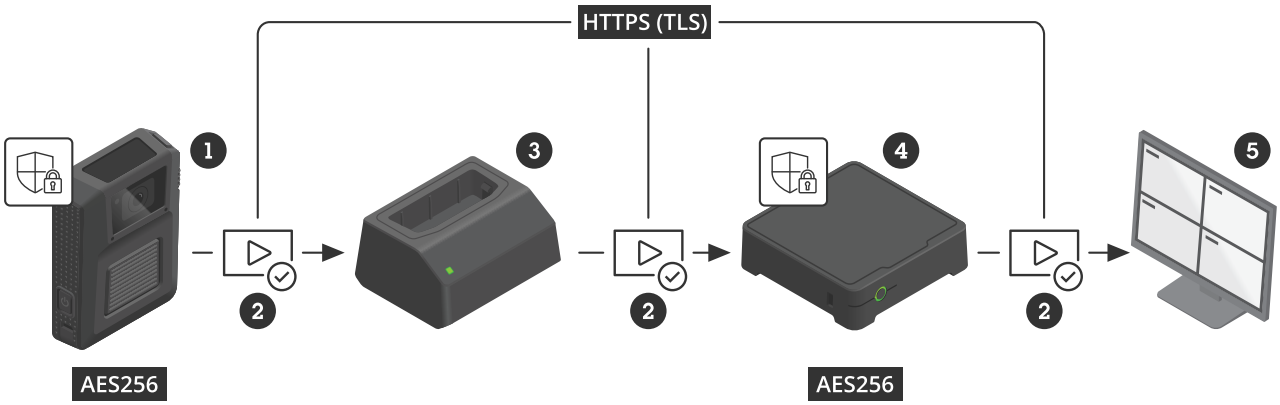
Der interne Speicher der BWC wird mit AES-256 verschlüsselt, um bei einem Verlust der Kamera unbefugten Zugriff auf die Daten zu verhindern.

Die Kamera lädt die Daten nur in den einen Systemcontroller bzw. das zugehörige System, denn die BWC und der Systemcontroller kommunizieren über IPv6 und nutzen Zertifikate. Die Zertifikate werden bei jedem Andocken der Kamera automatisch aktualisiert, so dass sie immer den aktuellen Zertifikaten des Systemcontrollers entsprechen.

Sollte eine Kamera acht Wochen lang vom System getrennt und nicht in dessen Nähe sein, wechselt sie aus Sicherheitsgründen in den Sicherheitsmodus und sperrt die Verbindung. Um wieder mit dem System verbunden werden zu können, ist eine manuelle Verifizierung mit der Hauptschlüssel-Passphrase erforderlich. So wird sichergestellt, dass eine verlorene oder längere Zeit abwesende Kamera nicht unbemerkt wieder hinzugefügt werden kann, da dies ein Sicherheitsrisiko bergen könnte.

4 Sicherheit bei der Datenübertragung

Beim typischen Einsatz wird die BWC nach einer vollen Schicht mitsamt der Videos und Metadaten angedockt. Alle Daten werden von der Dockingstation über eine mit HTTPS (HTTP mit TLS) verschlüsselte Netzwerkverbindung zum Systemcontroller heruntergeladen. Die Daten werden nur kurzzeitig auf dem AES-256-verschlüsselten SSD-Laufwerk des Systemcontrollers gespeichert. Der Systemcontroller überträgt die Daten anschließend über HTTPS an den Zielort.



Sichere Datenübertragung und -speicherung von der BWC (1) bis in die Dateiablage (5).

1 *BWC mit Axis Edge Vault*
2 *Signiertes Video (Cybersicherheitsmerkmal)*
3 *Docking Station*
4 *Systemcontroller mit Axis Edge Vault*
5 *Dateiablage*

Unterstützt wird auch ein Verschlüsselungscode von der Dateiablage zur Verschlüsselung der Daten in der BWC und im Systemcontroller, falls die Dateiablage einen öffentlichen Verschlüsselungscode bereitstellt. In diesem Fall haben die Daten eine weitere Verschlüsselungsschicht für die Übertragung an die Dateiablage.

5 Weitere Sicherheitsfunktionen

Die Sicherheit und Integrität des Systemcontrollers wird weiter gestärkt durch ein FIPS 140-2 konformes TPM (Trusted Platform Module).

Sowohl die BWC als auch der Systemcontroller ist mit Axis Edge Vault ausgestattet, einer Cybersicherheitsplattform auf Hardwarebasis, die alle Daten in den Geräten schützt und mehrere Sicherheitsmerkmale bietet. Beispielsweise ist das Dateisystem verschlüsselt, und der Schlüssel ist durch Axis Edge Vault geschützt. *Sicheres Booten* sorgt dafür, dass die Geräte nur mit autorisierter Gerätesoftware gestartet werden können. *Signiertes OS* sorgt dafür, dass Aktualisierungen abgelehnt wird, wenn die Integrität der Software beeinträchtigt wird. *Signiertes Video* sorgt für eine zusätzliche Sicherheitsebene, indem es eine kryptographische Prüfsumme in den Videostrom einfügt. Auf diese Weise kann das Video zuverlässig zu der Axis-Kamera zurückverfolgt werden, von der es stammt, und es wird sichergestellt, dass das Material nicht manipuliert wurde.

Weitere Informationen zu Signiertem Video und Axis Edge Vault finden Sie auf *developer.axis.com/video-streaming-and-recording/signed-video/* und *axis.com/solutions/edge-vault*

Der Kamerabenutzer kann aufgezeichnetes Video während des Einsatzes nur über die Anwendung AXIS Body Worn Assistant ansehen. Ist die App aktiviert, streamt die BWC Video direkt zur Anwendung, speichert aber kein Videomaterial für den späteren Zugriff im Cache oder im Speicher des Gerätes, auf dem die App ausgeführt wird. Außerdem hält ein Overlay im Videostream andere Aufzeichnungsgeräte von der Erfassung des Videos ab. Tun sie es trotzdem, kann der Videoclip über das Overlay zum BWC-Benutzer zurückverfolgt werden. Der USB-C-kompatible Anschluss der BWC kann nicht zum Ansehen, Löschen oder Herunterladen des Videos verwendet werden.

6 Sicherheit mit AXIS Body Worn Live

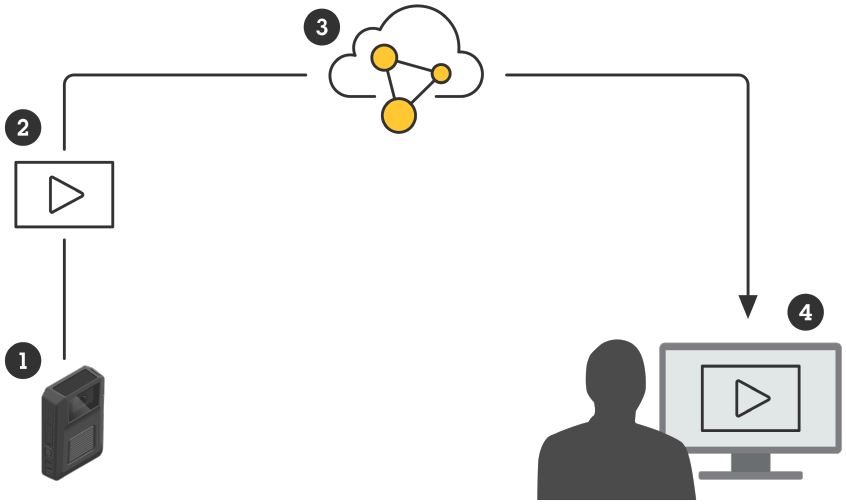
AXIS Body Worn Live ist eine App, die Zugriff auf Live-Daten von Axis Body Worn-Kameras erlaubt. Durch die Übertragung eines Livestreams mit Video, Audio und anderen Daten wie etwa Standortkoordinaten bietet AXIS Body Worn Live beispielloses Situationsbewusstsein bei Sicherheitsvorfällen. Um den unterschiedlichen

Anforderungen von Unternehmen an Infrastruktur und Datenhoheit gerecht zu werden, ist die Lösung in zwei Lösungsvarianten verfügbar: von Axis gehostet und selbst gehostet.

Unabhängig von der gewählten Lösung hat der Administrator des Body Worn-Kamerasystems die volle Kontrolle darüber, wer den Livestream sehen darf. Die Daten werden so verschlüsselt, dass ausschließlich die vom Administrator zugelassenen Viewer das Video entschlüsseln und anzeigen können. Außerdem kann der Administrator den Zugriff rollenbasiert widerrufen, um die Integrität der Daten zu gewährleisten. Bei von Axis gehosteten Lösungen benötigt der Viewer Zugriff auf den autorisierten Webbrowser und das VMS sowie die richtigen Zugangsdaten. Bei selbst gehosteten Lösungen muss der Viewer Zugriff auf das lokale Netzwerk sowie die richtigen Zugangsdaten besitzen. Darüber hinaus erhält niemand anderes, nicht einmal Axis, Zugriff auf den Livestream. Außerdem kann Axis auch nicht auf von Benutzern erstellte End-to-End-Verschlüsselungsschlüssel zugreifen.

6.1 Von Axis gehostete Lösung

Bei Nutzung als cloudbasierter Dienst werden alle in AXIS Body Worn Live gehosteten Daten und Dateien im Bereitschaftsmodus per AES-256 verschlüsselt. Alle Kommunikationskanäle sind über HTTPS mit TLS gesichert, wobei von vertrauenswürdigen Zertifizierungsstellen signierte Zertifikate verwendet werden. Neben der Transportverschlüsselung nutzt AXIS Body Worn Live die Verschlüsselungssuite XChaCha20-Poly1305, um die Daten zusätzlich mit einer echten End-to-End-Verschlüsselung zu versehen.



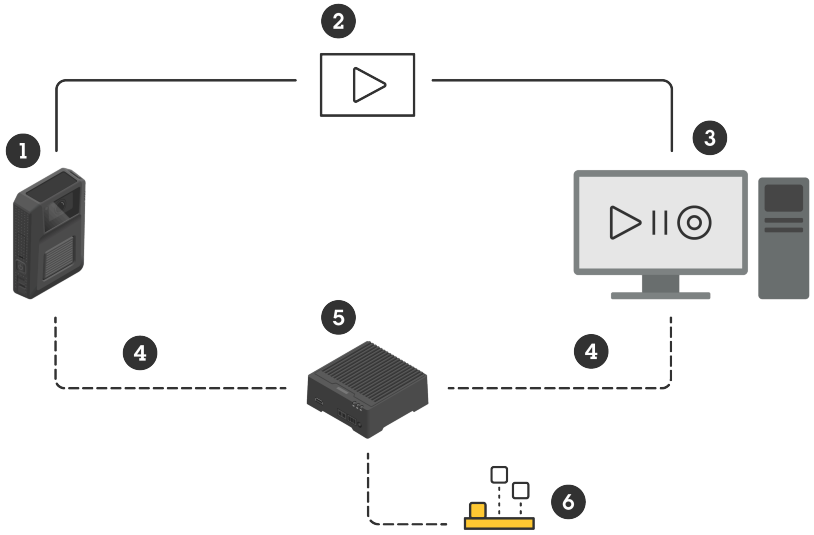
Sicherer Livestream mit End-to-End-Verschlüsselung bei einer von Axis gehosteten Lösung

1. *Die Body Worn-Kamera zeichnet Live-Video und andere Daten auf. Die Daten werden bereits in der Kamera verschlüsselt.*
2. *Livestream (Ende-zu-Ende-verschlüsselt).*
3. *Von Axis gehostete Cloud. Die Daten und Dateien werden per AES-256 verschlüsselt.*
4. *Webclient. Die Daten werden im Web Browser des Viewers entschlüsselt.*

6.2 Selbst gehostete Lösung

Organisationen mit strengen Sicherheitsrichtlinien bezüglich des vollständigen Verbleibs von Infrastruktur in ihren eigenen, kontrollierten Netzwerkumgebungen können die Serveranwendung AXIS Body Worn Live, Self Hosted lokal auf einem Gerät installieren. Bei diesem Servergerät kann es sich entweder um das AXIS W401 Body Worn Activation Kit oder den AXIS D3110 Mk II Connectivity Hub handeln. Auf dem lokalen Servergerät werden im Bereitschaftsmodus zu keinem Zeitpunkt Videos oder sensible Daten gespeichert; es dient ausschließlich zur Aufrechterhaltung der Verbindung. Der Kanal zur Übertragung von Medien zwischen Kameras und eingebundenen Komponenten wird mittels DTLS 1.0 oder höher gesichert. Die Sicherung des Kanals zur Übertragung von Signalen und Ereignissen zwischen dem Server und eingebundenen Komponenten erfolgt über HTTPS mit vom Kunden bereitgestellten Zertifikaten und TLS 1.2 oder höher.

Wenn Daten über die selbst gehostete Version gestreamt werden, stellt der lokale Server eine sichere WebRTC-Meldeverbindung mit zertifikatsbasierter Authentifizierung zwischen Server und BWC her. Sobald die Meldung erfolgt ist, wird eine verschlüsselte Peer-to-Peer-Verbindung direkt zwischen der BWC und dem WebRTC-Client des Viewers (z. B. einem VMS) aufgebaut. Da der Videostream ohne Zwischenspeicherung direkt über diese verschlüsselte Verbindung übertragen wird, kann dieser nicht unbefugt abgefangen werden. Das System ist für den Betrieb in geschlossenen, segmentierten Netzwerken ausgelegt, die keinen Internetzugang erfordern, was die Angriffsfläche für externe Bedrohungen minimiert.



Sicherer Livestream bei einer selbst gehosteten Lösung

1 *Die Body Worn-Kamera zeichnet Live-Video und andere Daten auf. Die Daten werden bereits in der Kamera verschlüsselt.*
2 *Peer-to-Peer-Videostream (verschlüsselt).*
3 *WebRTC-Client des Viewers.*
4 *WebRTC-Signalisierung.*
5 *Servergerät mit AXIS Body Worn Live, Self Hosted.*
6 *Serveranwendung AXIS Body Worn Live, Self Hosted. Diese dient zur Herstellung der WebRTC-Meldeverbindung.*

Über Axis Communications

Axis ermöglicht eine smartere und sichere Welt durch die Verbesserung von Sicherheit, Schutz, betrieblicher Effizienz und Geschäftsanalytik. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Videosicherheits-, Zutrittskontroll-, Intercom- und Audiolösungen. Die branchenweit anerkannten Schulungen der Axis Communications Academy vermitteln fundiertes Expertenwissen zu den neuesten Technologien.

Das 1984 gegründete schwedische Unternehmen beschäftigt etwa 5.000 engagierte Mitarbeiter in über 50 Ländern und bietet mit Technologie- und Systemintegrationspartnern auf der ganzen Welt kundenspezifische Lösungen an. Der Hauptsitz ist in Lund, Schweden.

© 2020 – 2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC und VAPIX sind in verschiedenen Jurisdiktionen eingetragene Marken von Axis AB. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.Wir behalten uns das Recht auf Änderungen ohne Vorankündigung vor.