WHITEPAPER

Februar 2024

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 Signierte Firmware, Sicheres Booten und Signiertes Video.

Wenn die Bilder live über AXIS Body Worn Live gestreamt werden, sind die Daten in Ruhe, während der Übertragung und im Webbrowser des Betrachters verschlüsselt. Außerdem sind sie mit dem Protokoll XChaCha20-Poly1305 End-to-End-verschlüsselt. Und noch dazu bestimmt der Administrator, wer den Livestream ansehen kann, bis hin zum einzelnen Computer, Webbrowser und Benutzerzugang.

Inhalt

1 Akronyme und Terminologie

BWC: Body Worn-Kamera

VMS: Video Management System

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 zeigen wir die verschiedenen Speichermedien und weitere Sicherheitsüberlegungen auf.

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.

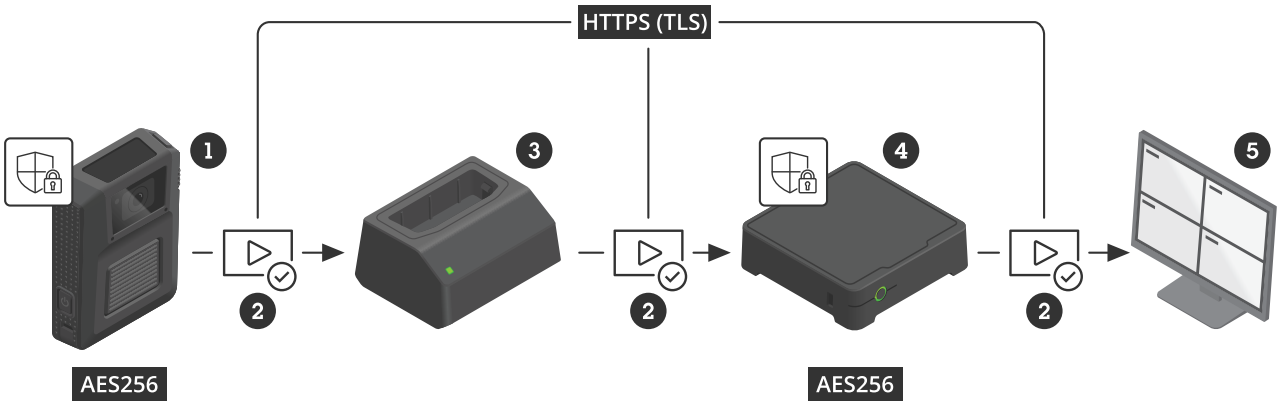
Der interne Speicher der BWC wird mit AES-256 verschlüsselt, um bei einem Verlust der Kamera unbefugten Zugriff auf die Daten zu verhindern.

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 länger als vier Wochen nicht angedockt und vom System getrennt sein, akzeptiert der Systemcontroller noch während einer Karenzzeit von acht Wochen ältere Zertifikate. Nach einer noch längeren Abwesenheit muss die Kamera über ein Master-Verschlüsselungskennwort manuell wieder in das System aufgenommen werden. 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 kurz im Systemcontroller gespeichert, und zwar in ihrem SSD-Speicher, der mit AES-256 verschlüsselt ist. Daraufhin überträgt der Systemcontroller die Daten per HTTPS zur Dateiablage.



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 Hochfahren* sorgt dafür, dass die Geräte nur mit autorisierter Firmware gestartet werden können. *Signierte Firmware* sorgt dafür, dass Firmware Upgrades abgelehnt wird, wenn die Firmware-Integrität beeinträchtigt ist. *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.

Unter *www.axis.com/de-de/developer-community/signed-video* finden Sie weitere Informationen über signiertes Video, und unter *www.axis.com/de-de/solutions/built-in-cybersecurity-features* erfahren Sie mehr über die Cybersicherheitsfunktionen von Axis.

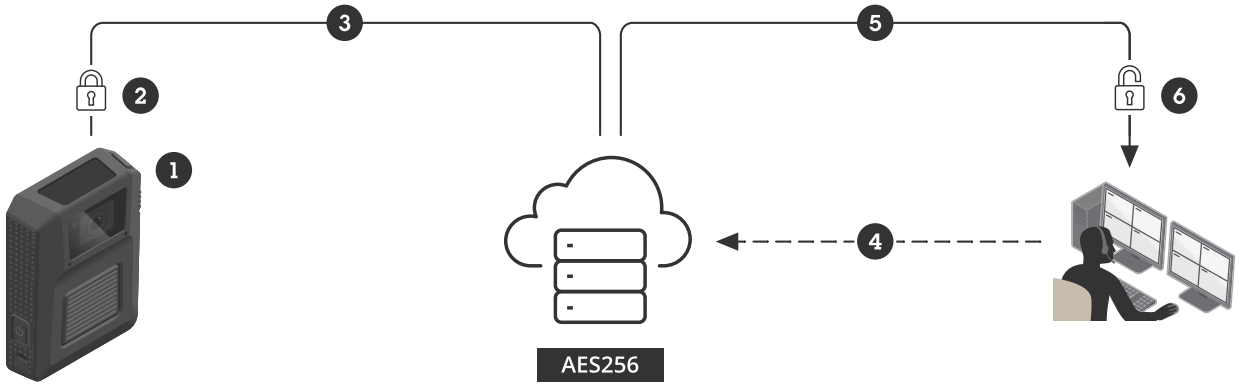
Der Kamerabenutzer kann aufgezeichnetes Video während des Einsatzes nur über die Anwendung AXIS Body Worn Assistant ansehen. Ist die App aktiviert, streamt die BWC Video direkt zur Anwendung, speichert aber kein Videomaterial für den späteren Zugriff im Cache oder im Speicher des Gerätes, auf dem die 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. AXIS Body Worn Live zeigt dem Benutzer einen Livestream von Video, Audio und andere Daten wie etwa Standortkoordinaten. Es wird zunächst als Cloud-basierter Service bereitgestellt.

Bei AXIS Body Worn Live sind die Daten nicht nur in Ruhe (im Speicher) und während der Übertragung geschützt, sondern zwischen der Kamera und dem Webbrowser des Betrachters auch vollständig End-to-End-verschlüsselt.

Alle in AXIS Body Worn Live gehosteten Daten und Dateien werden bei der Speicherung nach AES-256 verschlüsselt. Alle Kommunikationskanäle sind über HTTPS mit TLS gesichert, wobei von vertrauenswürdigen Zertifizierungsstellen signierte Zertifikate verwendet werden. AXIS Body Worn Live fügt außerdem mit dem Protokoll XChaCha20-Poly1305 eine weitere Ebene echter End-to-End-Verschlüsselung hinzu.



Sicheres Live Streaming mit End-to-End-Verschlüsselung in AXIS Body Worn Live

1 *Die BWC erhebt Live Video und weitere Daten.*
2 *Die Daten werden in der BCW verschlüsselt.*
3 *Die Daten werden von der BWC zu AXIS Body Worn Live übertragen.*
4 *Der Viewer fordert Daten von AXIS Body Worn Live an.*
5 *Die Daten werden von AXIS Body Worn Live zum Viewer übertragen.*
6 *Die Daten werden im Web Browser des Viewers entschlüsselt.*

Der Administrator des Body Worn-Kamerasystems hat die volle Kontrolle darüber, wer den Livestream sehen darf. Die Daten werden so verschlüsselt, dass nur die vom Administrator zugelassenen Personen das Video entschlüsseln und ansehen können, und der Administrator kann den Zugriff auch widerrufen. Der Betrachter muss dafür den richtigen Computer, den richtigen Webbrowser und die richtigen Zugangsdaten nutzen. Niemand sonst, nicht einmal Axis, kann auf den Livestream zugreifen. Axis hat keinen Zugriff auf die vom Benutzer erstellten End-to-end-Verschlüsselungscodes.

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 MitarbeiterInnen in über 50 Ländern und bietet mit Technologie- und Systemintegrationspartnern auf der ganzen Welt kundenspezifische Lösungen an. Der Hauptsitz ist in Lund, Schweden.