WHITEPAPER

Videodaten als Beweismittel

Mit AXIS Camera Station die Integrität von Videodaten sichern

Juli 2021

AXIS COMMUNICATIONS

Inhalt

1 Zusammenfassung

Hochwertige, glaubwürdige und unverfälschte Videodaten können als Beweis herangezogen werden. Die Best Practices zum Umgang mit Videodaten als Beweis mithilfe von AXIS Camera Station:

- Planen, konfigurieren und validieren Sie Ihr System einwandfrei, um die Bildqualität, die Aufzeichnung und die Sicherheit zu erhalten, die Sie haben wollen
- Regelmäßige Wartung durchführen
- Mit jedem Beweis nach festgelegten Verfahren umgehen

2 Einführung

Überwachungsvideos sind praktisch maßgeschneidert für die Verwendung als Beweismittel vor Gericht. Ein sozusagen „auf Band festgehaltenes" Ereignis ist nicht zu leugnen, oder? Nun, ein Richter würde wahrscheinlich Videodaten akzeptieren, die hochwertig, glaubwürdig und unverfälscht sind.

Es gibt jedoch auch Fälle, in denen die Beweiskraft von Videos ungewollt abgeschwächt wird. Beispielsweise wird Überwachungsvideomaterial mit Zeitlücken, auf dem Personen oder Fahrzeuge plötzlich verschwinden oder im Bild „springen", unter Umständen nicht als hinreichend vertrauenswürdig erachtet, um als Beweis herangezogen zu werden. Das Video könnte auch in Zweifel gezogen werden, wenn seine Metadaten wie beispielsweise Zeitstempel oder die MAC-Adresse der Kamera keinen Sinn ergeben. Jeder Verdacht, ein Video könnte bearbeitet, teilweise gelöscht oder manipuliert worden sein, kann der Glaubwürdigkeit des Videoeigentümers schaden.

Dieses Whitepaper enthält Empfehlungen dazu, wie mit Videomaterial als Beweismittel umzugehen ist. Insbesondere wird die Rolle der Video Management Software (VMS) AXIS Camera Station in der Beweiskette sowie die Rolle des Videoeigentümers beschrieben.

Figure 1. Videoüberwachung an strategischen Stellen kann bei richtiger Einrichtung und Verwaltung wertvolle Beweise liefern

3 Best Practices im Umgang mit Videodaten als Beweis

Unternehmen und Organisationen, die Videoüberwachung einsetzen, müssen Prozesse und Verfahren eingeführt haben, die vorgeben, wie mit Videodaten umzugehen ist und wie sie zu speichern sind. Für eine umfassende Vorbereitung auf den Fall, dass eine Ihrer Kameras ein Ereignis erfasst, müssen Sie sicherstellen, dass das Video gegen Überschreiben, Manipulieren oder Diebstahl geschützt ist. Außerdem muss es möglich sein, das Filmmaterial sicher zu exportieren und es den Strafverfolgungsbehörden zu übergeben.

Aber die Produktion hochwertiger Videobeweise ist ein Prozess, der mit einer gezielten Planung Ihres Videosystems beginnt. Außerdem ist es von höchster Wichtigkeit, dass Sie Ihr System auf dem neuesten Stand halten und alle Unregelmäßigkeiten im Blick behalten. In diesem Abschnitt stellen wir die Schritte in diesem Prozess vor und erläutern, wie sie mit Hilfe von AXIS Camera Station und der zugehörigen Toolbox AXIS Camera Station Integrator Suite umgesetzt werden können.

Wenn Sie Überwachungsvideomaterial nach diesen Grundsätzen zur Systemplanung, Systemwartung und zum Umgang mit Ereignissen produzieren, wird es die aktuellen Cybersicherheitsanforderungen erfüllen und höchst wahrscheinlich Beweiskraft haben, falls das erforderlich sein sollte.

Figure 2. Die AXIS Camera Station VMS vereinfacht sowohl die Einrichtung und den täglichen Betrieb als auch die strategische Verwaltung eines Videosicherheitssystems.

3.1 Ihr System richtig planen...

Ein Videoüberwachungssystem ist sorgfältig zu planen. Sie müssen die Ausstattung nach Ihren Bedürfnissen auswählen und so einrichten, dass sie das von Ihnen gewünschte Bild, die gewünschte Aufzeichnungsart und die gewünschte Sicherheit bietet. AXIS Site Designer leistet wichtige Unterstützung zu diesen Zwecken.

3.1.1 Für das Bild, die Sie haben wollen

Die Bildqualität hängt von der Kamera und ihrer Platzierung ab. Die Bildauflösung und insbesondere die Pixeldichte in der Szene der Ereignisse lassen sich berechnen, wenn Sie das Kameramodell, das Objektiv sowie Abstand und Winkel der Kamera zur Szene kennen. Für angemessene Pixeldichte über dem Gesicht einer Person in der Szene müssen Sie möglicherweise mehr Kameras einsetzen oder Kameras mit höherer Auflösung verwenden. Sie müssen das Sichtfeld, den Beleuchtungsbedarf und weitere Parameter für spezifische Kameras an Ihrem speziellen Standort untersuchen. All das lässt sich in AXIS Site Designer reibungslos planen.

3.1.2 Für die Aufzeichnungen, die Sie haben wollen

Zum Aufzeichnen Ihres Videos sollten Sie leistungsstarke, validierte Hardware mit Redundanz verwenden. Für höhere Systemzuverlässigkeit unterstützt AXIS Camera Station die ausfallsichere Aufzeichnung durch vorübergehendes Speichern der Bilder auf der SD-Karte der Netzwerk-Kamera. Wenn Sie

VMD-Analysefunktionen (video motion detection, dt.: Videobasierte Bewegungserkennung) nutzen, achten Sie darauf, dass Aufzeichnungen lang genug sind, um bei der Überprüfung des gesamten Ereignisses von Wert zu sein. Eine nicht optimal kalibrierte Aufzeichnung der Bewegungserkennung kann Zeitlücken und unzusammenhängende Aufnahmen enthalten. In vielen Fällen kann kontinuierliches Aufzeichnen die bessere Alternative sein; es setzt jedoch viel mehr Speicher sowie die ständige Verfügbarkeit ausreichender Bandbreite voraus.

3.1.3 Für die Sicherheit, die Sie haben wollen

Sie sollten das System mit der physischen Sicherheit ausstatten, die nötig ist, um unbefugten Zugriff zu verhindern. Alle Hardwarekomponenten einschließlich Kameras, Netzwerkausstattung und -kabeln, Servern, Datenspeichern, strombetriebener Geräte und Kabeln sollten geschützt werden. Zu den Sicherheitsmaßnahmen könnte gehören, dass der Serverraum ein Bereich mit eingeschränktem Zugang ist, dass der Serverschrank verschlossen wird, dass der Server in einem Rack untergebracht wird, dass die physischen Anschlüsse des Servers deaktiviert werden und dass die Netzwerkkabel nicht offen liegen.

Sie sollten sich außerdem bemühen, für die nötige Cybersicherheit des Systems zu sorgen, um die Risiken von Datenmissbrauch, Datenmanipulationsversuchen und bösartigen Angriffen zu minimieren. So genanntes Härten kann teilweise durch Software Tools und Technologie erfolgen. Damit wird sichergestellt, dass das System aktuellen Sicherheitsstandards entspricht. Aber Härten setzt auch voraus, dass der Systemeigentümer von der Notwendigkeit der Cybersicherheit überzeugt ist und aktiv daran arbeitet, diese Überzeugung im Unternehmen zu verbreiten. Beispielsweise müssen alle Benutzer eines Systems wissen, wie wichtig es ist, starke, schwer zu erratende Kennwörter zu verwenden und darauf zu achten, sie nicht preiszugeben. Auch Benutzerzugriffe sollten auf ein Minimum beschränkt werden, ebenso wie Benutzerberechtigungen, indem das Konzept der Benutzer mit sehr eingeschränkten Rechten (Least-Privileged User Account [LUA]) zur Anwendung kommt. Es liegt in der Verantwortung des Systemeigentümers, seine Mitarbeiter über Best Practices zu unterrichten und dafür zu sorgen, dass diese erfolgreich implementiert werden. Ein autorisierter Integrator kann das System härten; einige Cybersicherheitsmaßnahmen können jedoch nur greifen, wenn die Systembenutzer aktiv mitwirken.

Eine wichtige Möglichkeit, insgesamt höhere Cybersicherheit zu erreichen, besteht im Schutz Ihres Videomaterials durch verschlüsselten Datentransport. Beim Datentransport zwischen Client und Server nutzt die AXIS Camera Station AES-Verschlüsselung für Video-, Audio- und Metadaten sowie die TLS 1.2-Verschlüsselung für sonstige Daten. AXIS Camera Station kann mit HTTPS auch für die Verschlüsselung der Datenströme zwischen den Kameras und dem Server konfiguriert werden. Zu weiteren Best Practices zum Softwareschutz gehört die Deaktivierung aller nicht genutzten Dienste, die Anwendung von IP/MAC-Adressfiltern, die Aufnahme von IEEE 802.1X sowie SNMP-Überwachung, die richtige Einstellung von Datum und Zeit zusammen mit einem vertrauenswürdigen NTP-Server (damit die Präzision der Zeitstempel in Ihren Video-Metadaten gewährleistet ist) und die ausschließliche Verwendung von Axis Secure Remote Access für Fernverbindungen (anstelle von Port-Weiterleitung oder Remote Desktop). Einzelheiten zu Cybersicherheitsmaßnahmen und Empfehlungen finden Sie im Axis Hardening Guide.

3.1.4 Ihr System konfigurieren und validieren

Mit AXIS Site Designer können wichtige Teile des Systems bereits zum Zeitpunkt der Planung mit speziellen Kameranamen, Auflösungen und Speicherzeiten konfiguriert werden. Wenn Ihr System geplant und installiert ist, lassen sich in AXIS Site Designer vorgenommene Konfigurationen automatisch in AXIS Camera Station importieren, von wo aus Sie die Einstellungen bei Bedarf optimieren und anpassen können.

Nach Abschluss der eigentlichen Installation können Sie Ihr System mit AXIS Installation Verifier validieren, das ein Bestandteil der AXIS Camera Station Integrator Suite ist. AXIS Installation Verifier testet das System sowohl im Normal- als auch Nachtmodus um zu überprüfen, dass im Betrieb bei dunklen Lichtbedingungen, wenn das Bildrauschen höher ist und mehr Bandbreite benötigt wird, ausreichend Bandbreite vorhanden

ist. AXIS Installation Verifier führt dann einen Belastungstest durch, indem das im System generierte Datenvolumen stetig erhöht wird, bis der erste Engpass auftritt. So kann die Reservekapazität des Systems festgestellt und die Frage beantwortet werden, ob Systemverbesserungen erforderlich sind.

3.2 Regelmäßige Wartung durchführen

Wenn Ihr System in Betrieb ist, müssen Sie es laufend überwachen und aktualisieren.

Achten Sie darauf, dass sowohl die Hard- als auch Software weiterhin erwartungsgemäß funktionieren. Überprüfen Sie die Videoqualität, reinigen Sie regelmäßig das Kameraobjektiv, kontrollieren Sie, dass keine physische Manipulation stattgefunden hat und dass Sichtfeld und Ausrichtung der Kamera so geblieben sind, wie es sein soll. Untersuchen Sie regelmäßig die Systemprotokolle, denn sie liefern Informationen zu Anmeldungen, Verbindungen und Geräteproblemen. Die AXIS Camera Station VMS gibt Benachrichtigungen über festgestellte Unregelmäßigkeiten aus und verzeichnet sie in den Systemprotokollen. Leiten Sie Protokolle an einen entfernten Speicher mit Lesezugriff weiter, besonders nach dem Auftreten eines wichtigen Ereignisses. Axis bietet im Rahmen der AXIS Camera Station Integrator Suite auch Online-Überwachung des Systemzustands, damit Sie alle Ihre Installationen kontrollieren können, und gibt den Systemstatus aus, um Service und Wartung zu vereinfachen.

Sowohl die Hardware als auch die Software (Betriebssystem und VMS) sollte regelmäßig aktualisiert werden. Wenn Sie immer die neuesten Software- und Firmware-Versionen nutzen, profitiert Ihr System von den neuesten Sicherheits-Patches und Fehlerkorrekturen. Idealerweise findet die VMS alle Software- und Firmware-Aktualisierungen automatisch und fragt entweder, ob das Update installiert werden soll, oder aktualisiert einfach automatisch im Hintergrund. Jede Software, die Sie herunterladen, sollte aus vertrauenswürdigen Quellen stammen.

3.3 Behandeln Sie alle Beweismittel gemäß den festgelegten Verfahren

Wenn Sie die Grundsätze für die Entwicklung und Wartung Ihres Überwachungssystems richtig angewendet haben, sollte AXIS Camera Station in der Lage sein, glaubwürdige Beweise für alle von Ihren Kameras erfassten Vorfälle zu liefern. Dann müssen Sie Verfahren dafür eingeführt haben, wie weiter vorzugehen ist.

Sie müssen jeden Rat der Strafverfolgungsbehörden befolgen. Im Falle eines schweren Verbrechens ist die zuständige Strafverfolgungsbehörde berechtigt zu entscheiden, wie der Beweis geschützt werden sollte, und Sie müssen ihren Anweisungen Folge leisten.

In anderen Fällen ist der wichtigste Vorgang der sichere Export des Beweises. Das bedeutet, er muss außerhalb Ihres Systems in der gleichen unbearbeiteten Form und mit unveränderter Glaubwürdigkeit wie innerhalb des Systems erbracht werden können.

Der Export sollte von einem dafür bestimmten Anwender durchgeführt werden, vorzugsweise zusammen mit einem Zeugen. Dieser Anwender könnte ein externer Fachmann sein, der allein zum Zweck der Durchführung und Dokumentation eines glaubwürdigen Exports herangezogen wird. Es könnte das Risiko für den Eigentümer des Videos minimieren, der Beweismanipulation verdächtigt zu werden, wenn für den Export eine dritte, unabhängige Partei eingesetzt wird. Der Anwender muss dafür sorgen, dass das exportierte Video das tatsächliche Ereignis zeigt, jedoch auch genügend Informationen zu allen Vorgängen vermittelt, die dazu geführt haben, sowie zu möglichen Folgen.

Die ausgewählten Videoclips können auf schreibgeschützte Medien wie etwa CD-R, DVD-R oder Blu-ray (-R) exportiert werden, die anschließend der Strafverfolgungsbehörde übergeben werden können. Eine Alternative ist der Export der Videoclips in Zip-Dateien mit Verschlüsselung und Kennwortschutz. Die Dateien können digital mit einer Unterschrift signiert werden, die mit dem Kennwort des Benutzers

verschlüsselt (sog. Hashfunktion) wird. Zur Hash-Bestätigung und zum Abgleich mit dem derzeitigen Hash der Datei muss die Unterschrift in den AXIS File Player eingegeben werden. Wenn die Hashes übereinstimmen, wurden in dieser Datei keine Daten geändert.

Axis bietet außerdem den AXIS Camera Station Incident Report, der Anwendern als modernes Tool zum Export dient. Das Tool muss vorher von einem Administrator eingerichtet werden, der Daten wie beispielsweise Ereignis-Tags und den Zielort des Exports angibt. Der Incident Report automatisiert dann den Export, wobei die Videos nach Ereignissen organisiert und mit Tags als Ordnernamen exportiert werden können. Als Ort könnte eine lokale Ressource festgesetzt werden, beispielsweise der Network-Attached Storage (NAS) oder eine entfernte Ressource wie etwa ein Cloud-Speicher, wenn dieser über das SMB-Protokoll zugänglich ist. Der Bericht besteht aus Videodateien, Momentaufnahmen im JPG-Format (vom Anwender bei der Ausstellung des Berichts in AXIS Camera Station manuell erstellt), Lesezeichen im TXT-Format und allen Informationen, die in einem Bericht im PDF-Format zusammengestellt werden.

4 Ressourcen der Cybersicherheit

Axis wendet Cyber Hardening beim Design, der Entwicklung und dem Testen von Geräten an, um das Risiko von Fehlern zu minimieren, die bei einem Angriff ausgenutzt werden könnten. Bei der Cybersicherheit halten wir uns an die Best Practices der Branche, beispielsweise im Hinblick auf den Umgang mit Sicherheitsschwachstellen, die Anforderungen für sichere Datenübertragung und -speicherung sowie Verschlüsselung. Wir sind bestrebt, die Anwendung geeigneter Sicherheitskontrollen einfach und kosteneffizient zu gestalten. Zusätzlich unterstützen unsere Geräte das Verschlüsselungs- und Sicherheitsmanagement.

Während Axis als Hersteller und Systemanbieter alles daran setzt, die umfassendsten und sichersten Systeme und Lösungen anzubieten, tragen Sie als Endanwender große Verantwortung, die gängigen Best Practices der Sicherheitswelt anzuwenden. Axis bietet verschiedene Tools, Anleitungen und Selbstlerneinheiten zu Ihrer Unterstützung. Auf www.axis.com/cybersecurity finden Sie beispielsweise den Hardening Guide und Informationen zur Sicherheitsverwaltung. In unserem Blog „Secure Insights" finden Sie spannende Beiträge zum Thema Cybersicherheit.

T10169774/DE/M1.2/2107

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerk-Lösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für die Videoüberwachung/-analyse und Zutrittskontrolle sowie Sprechanlagen und Audiosysteme. Das 1984 gegründete schwedische Unternehmen beschäftigt mehr als 3.800 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an.

Weitere Informationen zu Axis bietet Ihnen unsere Webseite *axis.com*.

AXIS COMMUNICATIONS