

AXIS OS Hardening Guide

AXIS OS Hardening Guide

[AXIS OS Portal](#) | [Versionshinweise zu AXIS OS](#) | [AXIS OS Knowledge Base](#) | [AXIS OS YouTube Playlist](#) | [Sicherheitshinweise](#)

AXIS OS Hardening Guide

Einführung

Einführung

Axis Communications wendet beim Design, der Entwicklung und dem Test unserer Geräte bewährte Verfahren der Cybersicherheit an, um das Risiko von Schwachstellen zu minimieren, die bei einem Hackerangriff ausgenutzt werden könnten. Die gesamte Lieferkette des Anbieters und die Endbenutzer-Organisation müssen jedoch an der Sicherung des Netzwerks, der Geräte und der unterstützten Dienste beteiligt sein. Eine sichere Umgebung hängt von ihren Nutzern, den Prozessen und der Technologie ab. Dieser Leitfaden hilft Ihnen dabei, Ihr Netzwerk, Ihre Geräte und Dienste zu schützen.

Die größten Bedrohungen für ein Axis Gerät sind physische Sabotage, Vandalismus und Manipulation. Um ein Produkt vor diesen Bedrohungen zu schützen, ist es wichtig, ein vandalismusbeständiges Modell oder Gehäuse auszuwählen, es auf die empfohlene Weise zu montieren und die Kabel zu schützen.

Axis Geräte sind wie Computer und Mobiltelefone Netzwerkendpunkte. Viele von ihnen verfügen über eine Weboberfläche, die Sicherheitslücken in verbundenen Systemen aufweisen kann. In dieser Anleitung erklären wir, wie Sie diese Risiken verringern können.

Diese Anleitung enthält technische Tipps für das Bereitstellen von Axis Lösungen. Sie enthält eine empfohlene Basiskonfiguration sowie einen Hardening Guide, der die sich entwickelnde Bedrohungslage berücksichtigt. Weitere Informationen zur Konfiguration bestimmter Einstellungen finden Sie im Benutzerhandbuch des Produkts. Beachten Sie, dass Axis Geräte mit AXIS OS 7.10 und 10.9 eine Weboberflächen-Aktualisierung erhalten haben, mit der der Konfigurationspfad geändert wurde.

Konfiguration der Weboberfläche

Der Leitfaden bezieht sich auf das Konfigurieren der Geräteeinstellungen auf der Weboberfläche des Axis Geräts. Der Konfigurationspfad unterscheidet sich je nach der auf dem Gerät installierten AXIS OS Version:

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Wechseln Sie zu „Setup > System Options (Systemoptionen) > Security (Sicherheit) > IEEE 802.1X“.
7.10	Einstellungen > System > Sicherheit
≥ 10.9	System > Sicherheit

Bereich

Diese Anleitung gilt für alle auf AXIS OS basierenden Produkte mit AXIS OS (LTS oder Active Track) sowie für ältere Produkte mit 4.xx und 5.xx.

CIS-Schutzstufen

Wir befolgen die im Center for Internet Safety (CIS) Controls Version 8 beschriebenen Methoden, um unsere Empfehlungen für das Cybersicherheitsrahmenverfahren zu strukturieren. Die CIS Controls, früher als SANS Top 20 Critical Security Controls bezeichnet, bieten 18 Kategorien von kritischen Sicherheitskontrollen (Critical Security Controls, CSC), die sich auf die häufigsten Kategorien von Cybersicherheitsrisiken in Organisationen konzentrieren.

Diese Anleitung bezieht sich auf die kritischen Sicherheitskontrollen, indem die CSC-Nummer (CSC #) für jedes Sicherungsthema hinzugefügt wird. Weitere Informationen zu den CSC-Kategorien finden Sie in den *18 CIS Critical Security Controls* unter [cisecurity.org](https://www.cisecurity.org).

AXIS OS Hardening Guide

Standardschutz

Standardschutz

Die Standardschutzeinstellungen für Axis Geräte sind bereits vorhanden. Es gibt mehrere Sicherheitssteuerungen, die Sie nicht konfigurieren müssen. Diese Steuerelemente bieten einen grundlegenden Geräteschutz und bilden die Basis für ein umfangreicheres Härten.

Das Diagramm zur AXIS OS-Sicherheitsarchitektur zeigt die Cybersicherheitsfunktionen von AXIS OS auf verschiedenen Ebenen. Es bietet eine umfassende Übersicht über die Sicherheitsgrundlagen, die siliziumgestützte Sicherheit, das AXIS OS-Betriebssystem sowie die Anwendungs- und Zutrittskontrollenebene.

Access control	Access control management Local user device management with password complexity indicator Federated user device management through OpenID Connect (RFC6749, 1.3.1 Authorization Code) providing ADFS-integration that unlocks features such as password complexity enforcement, rotation, automatic account lock-out Multi-factor authentication (MFA), Microsoft AD entitlement functionality		Privacy Use of diagnostics data Minimalistic approach to how much customer-specific data should be stored
Application	Application security TLS-based application security (MQTT, SFTP, NTS, HTTPS, WebRTC) Encrypted video streaming (RTSPS/SRTP, HTTPS), Secure remote syslog		
Operating system	Encryption and data protection OpenSSL 1.1.1 and 3.0 X.509 certificate PKI and cryptography Transport layer security (TLS 1.2/TLS 1.3) SD card encryption (AES-XTS-Plain64 256bit) Encrypted file system (AES-XTS-Plain64 256bit), Signed video	Default security HTTPS enabled by default Brute-Force Delay Protection Host-based Firewall Network time security (NTS) Insecure TLS versions disabled UART/Debug port disabled	Enterprise network security IEEE 802.1X (network access control) IEEE 802.1AR (secure device identity) IEEE 802.1AE (MAC security, MACsec)
AXIS OS Operating System Common Linux-based operating system with more than 95% industry-standard open-source software components such as OpenSSL, Apache, Curl and others. Active track for feature growth and 5-year long-term support tracks (LTS) for 3rd party integration and backwards-compatibility use cases.			
Silicon assisted security (chip)	Hardware root-of-trust ARM-based system-on-chip (SoC) security Trusted Execution Environment (TEE/OP-TEE) Trusted platform module (TPM 2.0), Secure element		Secure key storage Tamper-protected storage and operation of cryptographic keys such as customer uploaded private keys, video signing keys and the Axis Device ID.
Security foundation	Axis Security Development Model Axis security development model (ASDM) 3rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)	Compliance Common Critical EAL FIPS 140 ETSI EN 303 645	Trusted device identity Axis Edge Vault cybersecurity platform Secure boot with Signed OS (code-signing) Axis Device ID (IEEE 802.1AR)

Klicken Sie mit der rechten Maustaste und öffnen Sie das Bild für eine bessere Darstellung in einer neuen Registerkarte.

In der Standardeinstellung deaktiviert

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

Das Axis Gerät wird nur betrieben, wenn das Administratorkennwort festgelegt wurde.

Nach dem Festlegen des Administratorkennworts ist der Zugriff auf Administratorfunktionen und/oder Videostreams nur über die Authentifizierung mittels gültiger Anmeldedaten für Benutzername und Kennwort möglich. Es wird nicht empfohlen, Funktionen zu verwenden, die den nicht autorisierten Zugriff ermöglichen, z. B. anonyme Ansicht und immer Multicast-Modus.

Informationen zum Konfigurieren des Gerätezugriffs finden Sie unter *Gerätezugriff* in der AXIS OS Knowledge Base.

AXIS OS Hardening Guide

Standardschutz

Edge Storage

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

Ab AXIS OS 12.0 wurde die Option noexec mount als Standardoption für eingehängte Netzwerkfreigaben hinzugefügt. Dadurch wird die direkte Ausführung von Binärdateien von der eingehängten Netzwerkfreigabe deaktiviert. Bei SD-Speicherkarten wurde diese Option bereits in früheren Versionen von AXIS OS hinzugefügt.

Netzwerkprotokolle

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

In der Standardeinstellung von Axis Geräten ist nur eine minimale Anzahl von Netzwerkprotokollen und -diensten aktiviert. In dieser Tabelle finden Sie Informationen dazu.

Protokoll	Port	Verkehrswesen	Anmerkungen
HTTP	80	TCP	Allgemeiner HTTP-Datenverkehr wie Weboberflächenzugriff, VAPIX- und ONVIF-API-Schnittstelle oder Edge-to-Edge-Kommunikation.*
HTTPS	443	TCP	Allgemeiner HTTPS-Datenverkehr wie Weboberflächenzugriff, VAPIX- und ONVIF-API-Schnittstelle oder Edge-to-Edge-Kommunikation.*
RTSP	554	TCP	Wird vom Axis Gerät für Video-/Audio-Streaming verwendet.
RTP	Ephemerer Port-Bereich*	UDP	Wird vom Axis Gerät für Video-/Audio-Streaming verwendet.
UPnP	49152	TCP	Wird von Anwendungen von Drittanbietern verwendet, um das Axis Gerät über das UPnP®-Erkennungsprotokoll zu erkennen. HINWEIS: Standardmäßig deaktiviert ab AXIS OS 12.0.
Bonjour	5353	UDP	Wird von Anwendungen von Drittanbietern verwendet, um das Axis Gerät über das mDNS-Erkennungsprotokoll (Bonjour) zu erkennen.

AXIS OS Hardening Guide

Standardschutz

Protokoll	Port	Verkehrswesen	Anmerkungen
SSDP	1900	UDP	Wird von Anwendungen von Drittanbietern verwendet, um das Axis Gerät über SSDP (UPnP®) zu entdecken. HINWEIS: Standardmäßig deaktiviert ab AXIS OS 12.0.
WS-Erkennung	3702	UDP	Wird von Anwendungen von Drittanbietern verwendet, um das Axis Gerät über das WS-Discovery-Erkennungsprotokoll (ONVIF) zu erkennen.

* Weitere Informationen zu Edge-to-Edge finden Sie im Whitepaper zur Edge-to-Edge-Technologie.

** Wird gemäß RFC 6056 automatisch innerhalb eines vordefinierten Portnummernbereichs zugewiesen. Weitere Informationen hierzu finden Sie im Wikipedia-Artikel „Ephemerer Port“.

Wir empfehlen, ungenutzte Netzwerkprotokolle und -dienste nach Möglichkeit zu deaktivieren. Eine vollständige Liste der Dienste, die standardmäßig verwendet werden oder je nach Konfiguration aktiviert werden können, finden Sie unter *Häufig verwendete Netzwerkports* in der AXIS OS Knowledge Base.

Beispielsweise müssen die Audioeingang/Audioausgang- und Mikrofonfunktionen von Axis Videosicherheitsprodukten wie Netzwerk-Kameras manuell aktiviert werden. In Axis Wechselsprechanlagen und Netzwerklautsprechern sind Audioeingang/Audioausgang- und Mikrofonfunktionen die wichtigsten Funktionen und daher standardmäßig aktiviert.

UART/Debug-Schnittstelle

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

Jedes Axis Gerät verfügt über eine so genannte physikalische UART-Schnittstelle (Universal Asynchronous Receiver Transmitter), die manchmal auch als "Debug-Port" oder "serielle Konsole" bezeichnet wird. Der Zugriff auf die Schnittstelle selbst ist nur möglich, wenn das Axis Gerät weitgehend zerlegt wird. Die UART/Debug-Schnittstelle wird nur für Produktentwicklungs- und Debugging-Zwecke bei internen F&E-Konstruktionsprojekten von Axis verwendet.

Die UART/Debug-Schnittstelle ist in der Standardeinstellung in Axis Geräten mit AXIS OS 10.10 und früheren Versionen aktiviert. Sie erfordert jedoch einen authentifizierten Zugriff und stellt bei nicht aktivierter Funktion keine empfindlichen Informationen offen. Ab AXIS OS 10.11 ist die UART/Debug-Schnittstelle in der Standardeinstellung deaktiviert. Die Schnittstelle kann nur über ein von Axis bereitgestelltes, einzigartiges, benutzerdefiniertes Zertifikat entsperrt werden.

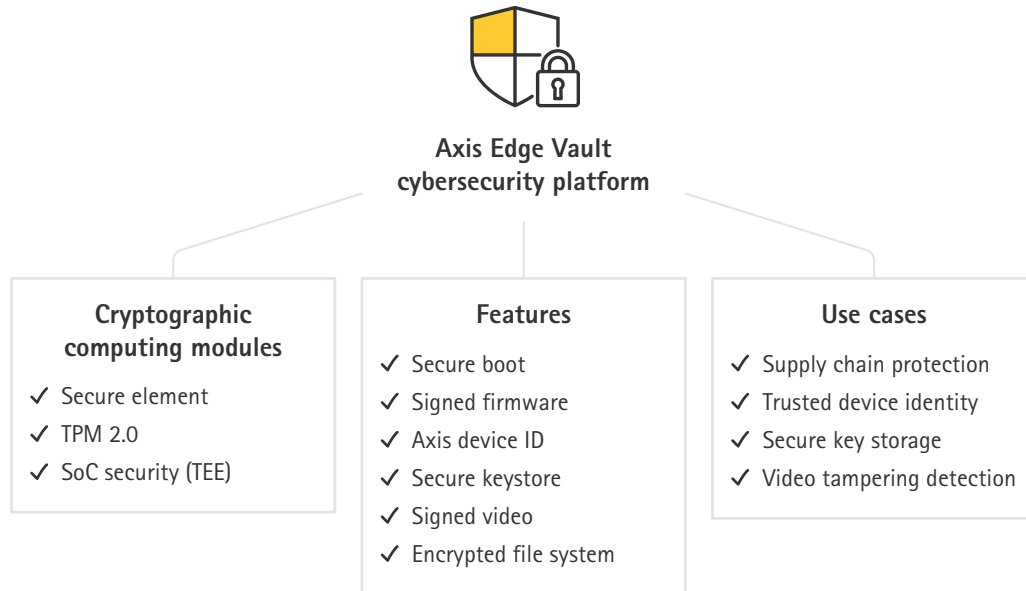
Axis Edge Vault

Axis Edge Vault stellt eine hardwarebasierte Cybersicherheitsplattform zum Schutz der Axis Geräte bereit. Es sorgt für eine starke Grundlage kryptografischer Berechnungsmodule (Sicherheitselement und TPM) und SoC-Sicherheit (TEE und Secure Boot), die wir mit Expertise in Edge-Gerätesicherheit kombinieren. Axis Edge Vault basiert auf einer soliden Vertrauensbasis, die durch sicheres Booten und signierte Firmware geschaffen wird. Diese Merkmale ermöglichen eine lückenlose Kette kryptografisch validierter Software für die Vertrauenskette, auf der sämtliche sicheren Operationen beruhen.

Axis Geräte mit Axis Edge Vault minimieren die Exposition der Kunden gegenüber Cybersicherheitsrisiken, indem sie Lauschangriffe und die böswillige Extraktion sensibler Informationen verhindern. Axis Edge Vault stellt zudem sicher, dass das Axis Gerät eine vertrauenswürdige und zuverlässige Einheit im Netzwerk des Kunden ist.

AXIS OS Hardening Guide

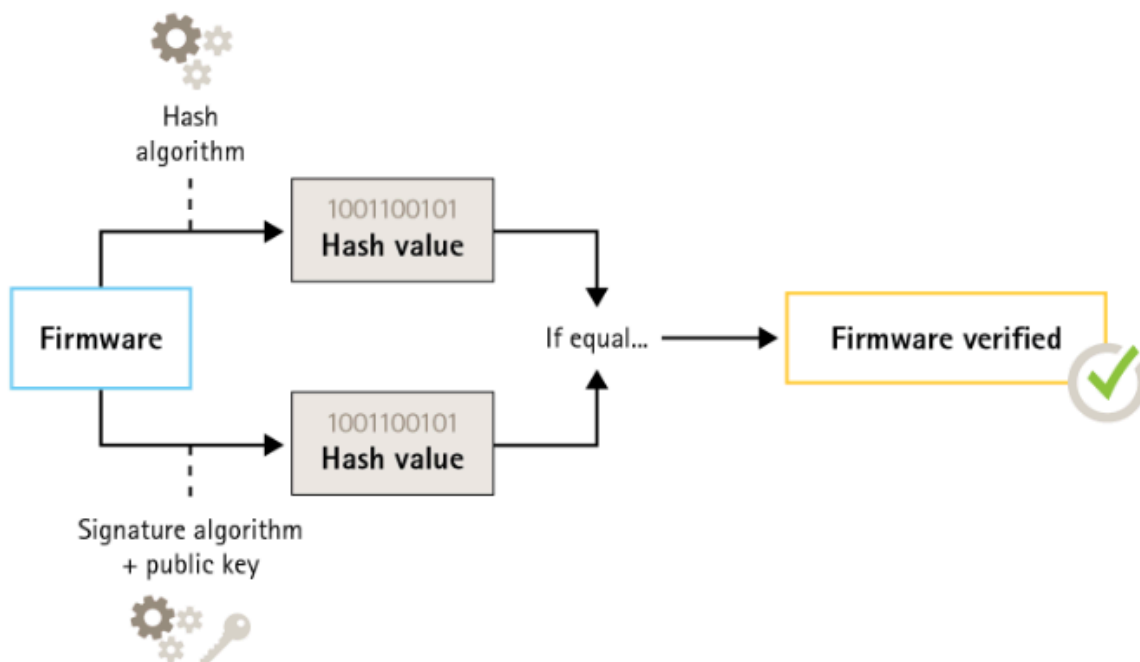
Standardschutz



Signierte Firmware

CSC Nr. 2: Inventar und Steuerung von Softwareressourcen

AXIS OS ist ab Version 9.20.1 signiert. Bei jeder Aktualisierung der AXIS OS Version auf dem Gerät kontrolliert das Gerät die Integrität der Aktualisierungsdateien mittels kryptografischer Signaturüberprüfung und weist manipulierte Dateien ab. Dadurch wird verhindert, dass Angreifer die Benutzer zur Installation kompromittierter Dateien verleiten.



AXIS OS Hardening Guide

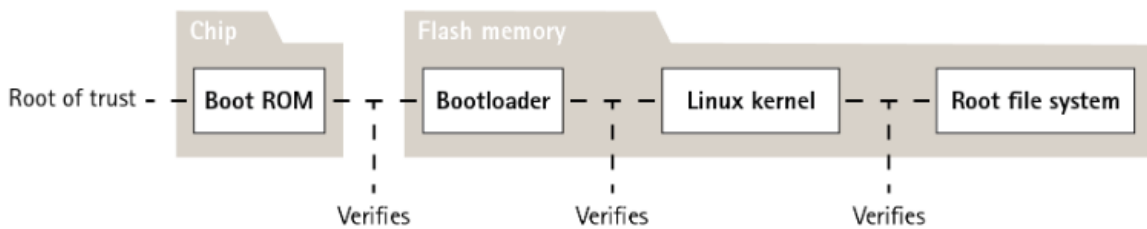
Standardschutz

Weitere Informationen finden Sie im Whitepaper *Axis Edge Vault*.

Sicheres Hochfahren

CSC Nr. 2: *Inventar und Steuerung von Softwareressourcen*

Die meisten Axis Geräte verfügen über eine sichere Bootsequenz, um die Integrität des Geräts zu gewährleisten. Sicheres Hochfahren verhindert das Bereitstellen manipulierter Axis Geräte.



Weitere Informationen finden Sie im Whitepaper *Axis Edge Vault*.

Sicherer Schlüsselspeicher

CSC Nr. 6: *Verwaltung der Zutrittskontrolle*

Der sichere Schlüsselspeicher speichert kryptografische Daten Hardware-basiert und manipulationsgeschützt. Es schützt die Axis Geräte-ID sowie kryptografische Informationen, die vom Kunden hochgeladen werden, verhindert jedoch im Fall einer Sicherheitsverletzung unbefugten Zugriff und böswilligen Zugriff. Je nach Sicherheitsanforderungen kann ein Axis Gerät über ein oder mehrere solcher Module verfügen, wie z. B. ein TPM 2.0 (Trusted Platform Module) oder ein sicheres Element, und/oder ein Trusted Execution Environment (TEE).



Weitere Informationen finden Sie im Whitepaper *Axis Edge Vault*.

Verschlüsseltes Dateisystem

CSC Nr. 3: *Datenschutz*

Ein böswilliger Kontrahent könnte versuchen, Informationen aus dem Dateisystem zu extrahieren, indem er versucht, den Flash-Speicher zu demontieren und mit einem Flash Reader-Gerät darauf zuzugreifen. Das Axis Gerät kann das Dateisystem jedoch vor unbefugtem Zugriff auf Daten und Konfigurationsmanipulationen schützen, falls jemand physischen Zugriff auf das Dateisystem bekommt oder es stiehlt. Wenn das Axis Gerät ausgeschaltet ist, sind die Informationen im Dateisystem AES-XTS-Plain64

AXIS OS Hardening Guide

Standardschutz

256bit verschlüsselt. Das Read-Write-Dateisystem wird während des sicheren Systemstarts entschlüsselt und dem Axis Gerät zur Verwendung bereitgestellt.

Weitere Informationen finden Sie im *Whitepaper Axis Edge Vault*.

HTTPS aktiviert

CSC Nr. 3: Datenschutz

Ab AXIS OS 7.20 wurde HTTPS standardmäßig mit einem eigensigniertem Zertifikat aktiviert, das eine sichere Einstellung des Gerätekennworts ermöglicht. Ab AXIS OS 10.10 wurde das eigensignierte Zertifikat durch das IEEE 802.1AR Zertifikat für sichere Geräte-ID ersetzt.

In AXIS OS sind die gängigsten sicherheitsrelevanten HTTP(S)-Header standardmäßig aktiviert, um die Cybersicherheit in den Werkseinstellungen zu verbessern. Ab AXIS OS 9.80 können Sie die benutzerdefinierte HTTP-Header-VAPIX-API verwenden, um zusätzliche HTTP(S)-Header zu konfigurieren.

Weitere Informationen zur HTTP-Header-VAPIX-API finden Sie in der *VAPIX-Bibliothek*.

Weitere Informationen zu den Standard-HTTP(S) Headern finden Sie unter *Standard-HTTP(S) Header* in der AXIS OS Knowledge Base.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Security > HTTPS
7.10	Settings > System > Security > HTTP and HTTPS
≥ 10.9	System > Network > HTTP and HTTPS

Digest-Authentifizierung

CSC Nr. 3: Datenschutz

Clients, die auf das Gerät zugreifen, authentifizieren sich mit einem Kennwort, das beim Übertragen über das Netzwerk verschlüsselt werden muss. Daher wird empfohlen, die Digest-Authentifizierung anstelle von Basic oder Basic und Digest zu verwenden. Damit wird das Risiko verringert, dass Netzwerk-Sniffer an das Kennwort kommen.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Advanced > Plain Config > Network > Network HTTP Authentication policy
7.10	Settings > System > Plain config > Network > Network HTTP Authentication policy
≥ 10.9	System > Plain config > Network > Network HTTP Authentication policy

Angriffsschutz für ONVIF-Wiedergabe

CSC Nr. 3: Datenschutz

Der Angriffsschutz für Wiedergabe ist eine standardmäßig für Axis Geräte aktivierte Sicherheitsfunktion. Der Zweck besteht in der ausreichenden Sicherung der ONVIF-basierten Benutzerauthentifizierung durch Hinzufügen eines zusätzlichen Sicherheitsheaders, der UsernameToken, gültigen Zeitstempel, Nonce und Digest-Kennwort enthält. Das Digest-Kennwort wird aus dem Kennwort (das bereits im System gespeichert ist), Nonce und dem Zeitstempel berechnet. Mit dem Digest-Kennwort soll der Benutzer überprüft und Wiederholungsangriffen verhindert werden. Deshalb werden Digests zwischengespeichert. Es wird empfohlen, diese Einstellung aktiviert zu lassen.

AXIS OS Hardening Guide

Standardschutz

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Advanced > Plain Config > System > Enable Replay Attack Protection
7.10	Settings > System > Plain config > WebService > Enable Replay Attack Protection
≥ 10.9	System > Plain config > WebService > Enable Replay Attack Protection

Brute-Force-Angriffe verhindern

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

CSC Nr. 13: Netzwerküberwachung und -schutz

Axis Geräte verfügen über einen Vorbeugungsmechanismus zum Identifizieren und Verhindern von Brute-Force-Angriffen, beispielsweise durch Erraten des Kennworts. Die Funktion, der sogenannte *Schutz vor Brute-Force-Verzögerungen* ist in AXIS OS 7.30 und höher verfügbar.

Der Schutz vor Brute-Force-Verzögerung ist ab AXIS OS 11.5 standardmäßig aktiviert. Ausführliche Konfigurationsbeispiele und Empfehlungen finden Sie unter *Brute-Force-Verzögerungsschutz* in der AXIS OS Knowledge Base.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	n. v.
7.10	Settings > System > Plain config > System > PreventDosAttack
≥ 10.9	System > Security > Prevent brute-force attacks

Außerbetriebnahme

CSC Nr. 3: Datenschutz

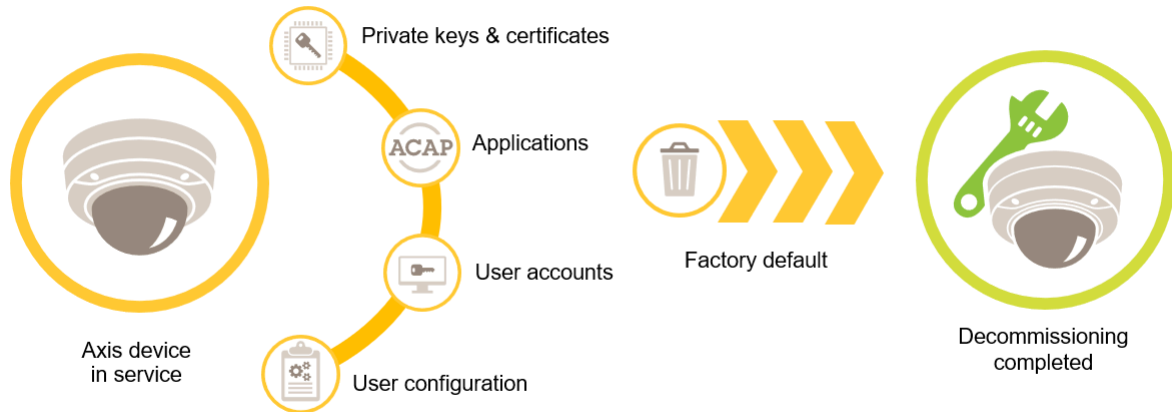
Axis Geräte verwenden sowohl flüchtigen als auch nicht flüchtigen Speicher. Während der flüchtige Speicher gelöscht wird, wenn Sie das Gerät von seiner Stromquelle trennen, bleiben die im nicht flüchtigen Speicher gespeicherten Informationen erhalten und werden beim Start erneut verfügbar gemacht. Wir vermeiden die gängige Praxis, die Datenmarker einfach zu entfernen, um die gespeicherten Daten für das Dateisystem unsichtbar zu machen. Deshalb ist ein Zurücksetzen auf die Werkseinstellungen erforderlich. Für NAND-Flash-Speicher wird die UBI-Funktion „Remove Volume“ (Volume entfernen) verwendet. Die gleiche Funktion wird für eMMC-Flash-Speicher verwendet, die signalisiert, dass Speicherblöcke nicht mehr verwendet werden. Der Speichercontroller löscht diese Speicherblöcke dann entsprechend.

Bei der Außerbetriebnahme eines Axis Geräts wird empfohlen, das Gerät auf die Werkseinstellungen zurückzusetzen, wodurch alle auf dem nichtflüchtigen Speicher des Geräts gespeicherten Daten gelöscht werden.

Bitte beachten Sie, dass ein Befehl zur werksseitigen Standardeinstellung die Daten nicht sofort löscht, sondern das Gerät neu startet und die Daten während des Systemstarts gelöscht werden. Daher reicht es nicht aus, die Werkseinstellungen wiederherzustellen, sondern das Gerät muss in der Lage sein, vor dem Ausschalten neu zu starten und den Bootvorgang abzuschließen, um sicherzustellen, dass die Daten vollständig gelöscht wurden.

AXIS OS Hardening Guide

Standardschutz



AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Maintenance > Default
7.10	Settings > System > Maintenance > Default
≥ 10.9	Maintenance > Default

Diese Tabelle enthält weitere Informationen zu im nicht flüchtigen Speicher gespeicherten Daten.

Informationen und Daten	Nach Werkseinstellungen gelöscht
VAPIX- und ONVIF-Benutzernamen und Kennwörter	Ja
Zertifikate und Privatschlüssel	Ja
Eigensigniertes Zertifikat	Ja
TPM und in Axis Edge Vault gespeicherte Informationen	Ja
WLAN-Einstellungen und Benutzer/Kennwörter	Ja
Benutzerdefinierte Zertifikate*	Nein
SD-Speicherkarten-Verschlüsselungsschlüssel	Ja
SD-Kartendaten**	Nein
Einstellungen für Netzwerk-Freigaben und Benutzer/Kennwörter	Ja
Netzwerk-Freigaben**	Nein
Benutzerkonfiguration***	Ja
Hochgeladene Anwendungen (ACAPs)****	Ja
Produktionsdaten und Lebenszeitstatistiken*****	Nein
Hochgeladene Grafiken und Overlays	Ja
RTC-Uhrendaten	Ja

* Der Prozess der signierten Firmware verwendet benutzerdefinierte Zertifikate, mit denen Benutzer (unter anderem) AXIS OS hochladen können.

AXIS OS Hardening Guide

Standardschutz

*** Aufzeichnungen und Bilder, die auf Edge Storage (SD-Speicherkarte, Netzwerkfreigabe) gespeichert sind, müssen vom Benutzer separat gelöscht werden. Weitere Informationen finden Sie unter Formatieren von Axis SD-Karten in der AXIS OS Knowledge Base.*

**** Alle vom Benutzer erstellten Konfigurationen, von der Kontenerstellung bis hin zu Netzwerk-, O3C-, Ereignis-, Bild-, PTZ- und Systemkonfigurationen.*

***** Das Gerät behält alle vorinstallierten Anwendungen bei, löscht aber alle vom Benutzer vorgenommenen Konfigurationen für diese Anwendungen.*

****** Produktionsdaten (Kalibrierung, 802.1AR-Produktionszertifikate) und Lebensdauerstatistiken enthalten nicht-sensible und nicht benutzerbezogene Informationen.*

Aufzeichnungsverschlüsselung exportieren

CSC Nr. 3: Datenschutz

Ab AXIS OS 10.10 unterstützen Axis Geräte den verschlüsselten Export von Edge-Aufzeichnungen. Es wird empfohlen, diese Funktion zu verwenden, um zu verhindern, dass unbefugte Personen exportiertes Videomaterial wieder abspielen können.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	n. v.
7.10	n. v.
≥ 10.9	Aufzeichnungen

AXIS OS Hardening Guide

Grundlegende Härtung

Grundlegende Härtung

Die grundlegende Härtung ist das für Axis Geräte empfohlene Mindestschutzniveau. Die grundlegenden Härtungsaspekte sind "on the edge" konfigurierbar. Dies bedeutet, dass sie direkt im Axis-Gerät konfiguriert werden können, ohne dass eine Abhängigkeit von der Netzwerkinfrastruktur, von Video- oder Beweisverwaltungssystemen (VMS, EMS), Geräten oder Anwendungen von Drittanbietern besteht.

Werkseitige Standardeinstellungen

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

Stellen Sie vor der Konfiguration des Geräts sicher, dass es sich in einer werkseitigen Standardeinstellung befindet. Außerdem ist es wichtig, das Gerät auf die Werkseinstellungen zurückzusetzen, wenn Benutzerdaten entfernt werden müssen oder es außer Betrieb genommen wird. Weitere Informationen finden Sie unter *Außerbetriebnahme auf Seite 10*.

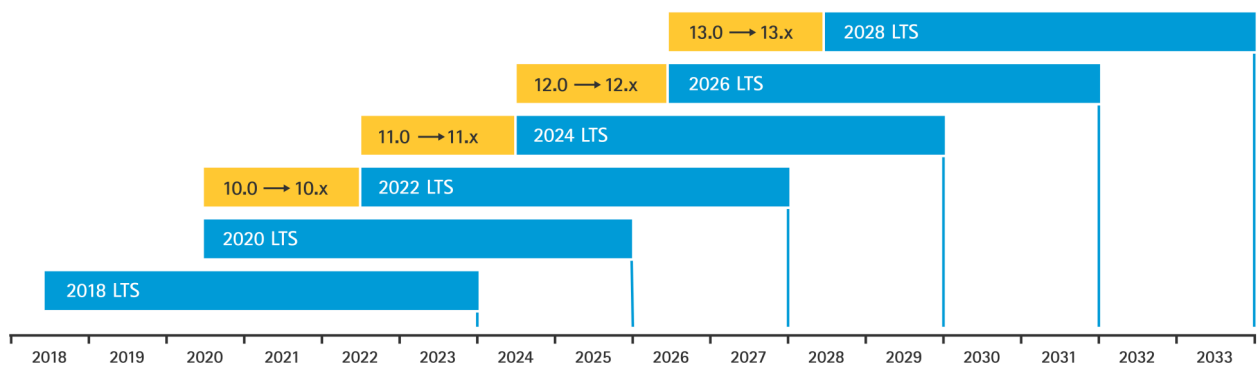
AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Maintenance > Default
7.10	Settings > System > Maintenance > Default
≥ 10.9	Maintenance > Default

Upgrade auf die aktuelle AXIS OS

CSC Nr. 2: Inventar und Steuerung von Softwareressourcen

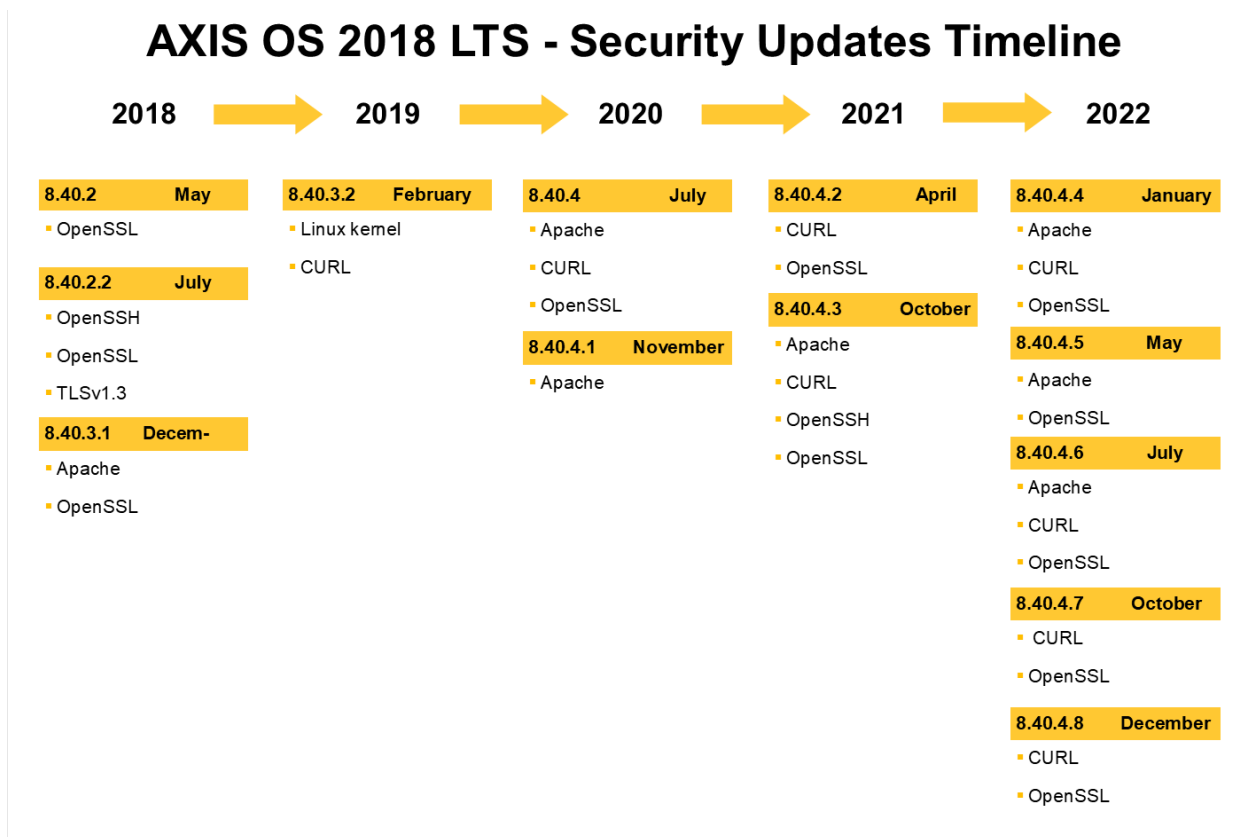
Patches für Software sind ein wichtiger Aspekt der Cybersicherheit. In der Regel versuchen Angreifer, Sicherheitslücken auszunutzen. Sie können erfolgreich sein, wenn sie Zugang zum Netzwerk über einen nicht aktualisierten Dienst erhalten. Stellen Sie sicher, dass Sie stets das aktuelle AXIS OS verwenden, da es möglicherweise Sicherheits-Patches für bekannte Sicherheitslücken enthält. In den Release-Notes für eine bestimmte Version wird möglicherweise ein kritisches Sicherheitsfix, aber nicht alle allgemeinen Fehlerbehebungen erwähnt.

Axis unterhält zwei Typen von AXIS OS-Tracks: den aktiven Track und die Tracks für den langfristigen Support (LTS). Beide Typen beinhalten die neuesten Patches für kritische Sicherheitslücken. Die LTS-Tracks enthalten jedoch keine neuen Funktionen, um das Risiko von Kompatibilitätsproblemen zu minimieren. Weitere Informationen finden Sie unter *AXIS OS Lifecycle* in *AXIS OS Information*.



Axis stellt eine Vorschau kommender Versionen mit Informationen zu wichtigen neuen Funktionen, Bugfixes und Sicherheits-Patches zur Verfügung. Weitere Informationen finden Sie unter *Anstehende Veröffentlichungen* in *AXIS OS Information*. Gehen Sie auf *Firmware* unter axis.com, um AXIS OS für Ihr Gerät herunterzuladen.

Diese Grafik illustriert, wie wichtig es ist, Axis Geräte auf dem neuesten Stand zu halten.



AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Maintenance > Upgrade Server
7.10	Settings > System > Maintenance > Firmware upgrade
≥ 10.9	Maintenance > Firmware upgrade

Dedizierte Konten erstellen

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

CSC Nr. 5: Kontenverwaltung

Für Axis Geräte gibt es zwei Kontotypen: ein Administratorkonto und ein Client-Benutzerkonto. Das Konto des Administrators ist das wichtigste Konto für die Verwaltung Ihres Geräts und sollte unbedingt nur administrativen Aufgaben vorbehalten sein. Bei der Einstellung Ihres Geräts müssen Sie einen Benutzernamen und ein Kennwort für das Konto des Administrators erstellen.

Erstellen Sie zusätzlich zum Administratorkonto ein Benutzerkonto mit eingeschränkten Rechten für den täglichen Betrieb. Auf diese Weise können Sie Ihr Gerät sicher verwalten und das Risiko verringern, dass das Kennwort des Geräteadministrators weitergegeben wird. Sie sollten das Client-Benutzerkonto für Aufgaben verwenden, die keine vollständigen Verwaltungsrechte erfordern.

Bei der Erstellung von Kennwörtern für beide Konten empfehlen wir Ihnen, Richtlinien wie die NIST- oder BSI-Kennwortempfehlungen zu befolgen, wonach neue Kennwörter ausreichend lang und komplex sein müssen. Axis Geräte unterstützen Kennwörter mit bis zu 64 Zeichen. Kennwörter, die kürzer als 8 Zeichen sind, gelten als schwach.

Weitere Informationen finden Sie im Abschnitt

„Identity and Access Management“ (Identität und Zugriffsverwaltung) der AXIS OS Knowledge Base.

AXIS OS Hardening Guide

Grundlegende Härtung

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > Grundeinstellungen > Benutzer
7.10	Einstellungen > System > Benutzer
≥ 10.9	System > Benutzer
≥ 11.6	System > Konten

Weboberflächenzugriff deaktivieren

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

CSC Nr. 5: Kontenverwaltung

Axis Geräte verfügen über einen Webserver, der über einen Standardwebbrowser Zugriff auf das Gerät ermöglicht. Die Weboberfläche ist für die Konfiguration, Wartung und Fehlerbehebung vorgesehen. Sie ist nicht für den täglichen Betrieb vorgesehen, z. B. als Client, um Videos anzusehen.

Die einzigen Clients, die während des täglichen Betriebs mit Axis Geräten interagieren sollten, sind Video Management Systeme (VMS) oder Geräteverwaltungs- und Verwaltungstools wie der AXIS Device Manager. Systembenutzer sollten niemals direkt auf Axis Geräte zugreifen dürfen.

Ab AXIS OS 9.50 kann die Weboberfläche eines Axis Geräts deaktiviert werden. Wenn Sie ein Axis Gerät in ein System einsetzen (oder es dem AXIS Device Manager hinzufügen), wird empfohlen, die Option für Personen innerhalb der Organisation, über einen Webbrowser auf das Gerät zuzugreifen, zu entfernen. Dies schafft eine zusätzliche Sicherheitsebene, wenn das Kennwort für das Gerätekonto innerhalb der Organisation geteilt wird. Die sicherere Option besteht in der ausschließlichen Einrichtung des Zugangs zu Axis Geräten mittels dedizierter Anwendungen, die eine moderne IAM (Identity Access Management)-Architektur, mehr Rückverfolgbarkeit und Sicherheitsmaßnahmen bieten, um Sicherheitslücken bei Konten zu verhindern.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	n. v.
7.10	Settings > System > Plain config > System > Web Interface Disabled
≥ 10.9	System > Plain config > System > Web Interface Disabled

Netzwerk, Datum und Uhrzeit konfigurieren

CSC Nr. 4: CSC Nr. 8: Verwaltung von Prüfprotokollen

CSC Nr. 12: Verwaltung der Netzwerk-Infrastruktur

Es ist wichtig, die Netzwerk-, Datums- und Zeiteinstellungen des Geräts richtig zu konfigurieren, damit Ihr Axis Gerät funktionsfähig und sicher bleibt. Diese Einstellungen wirken sich auf verschiedene Aspekte des Geräteverhaltens aus, einschließlich Netzwerkkommunikation, Protokollierung und Zertifikatsvalidierung.

Die IP-Konfiguration des Geräts hängt von der Netzwerkkonfiguration ab, z. B. von IPv4/IPv6, statischer oder dynamischer Netzwerkadresse (DHCP), Subnetzmaske und Standardrouter. Überprüfen Sie Ihre Netzwerktopologie, wenn Sie neue Komponenten hinzufügen. Es wird empfohlen, statische IP-Adressen zu konfigurieren, um die Erreichbarkeit des Netzwerks sicherzustellen und die Abhängigkeit von möglicherweise angreifbaren Netzwerkservers, wie z. B. DHCP-Servern, zu minimieren.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > Basic Setup > TCP/IP
7.10	Settings > System > TCP/IP
≥ 10.9	System > Network

AXIS OS Hardening Guide

Grundlegende Härtung

Eine genaue Zeitmessung ist unerlässlich, um Systemprotokolle zu führen, digitale Zertifikate zu validieren und Dienste wie HTTPS, IEEE und 802.1x zu aktivieren. Wir empfehlen, die Uhr Ihres Geräts mit Network Time Protocol (NTP) oder Network Time Security (NTS) Servern zu synchronisieren. Network Time Security (NTS), eine verschlüsselte und sichere Variante des Network Time Protocol (NTP), wurde in AXIS OS 11.1 hinzugefügt. Es wird empfohlen, mehrere Zeitserver zu konfigurieren, um die Genauigkeit zu erhöhen und mögliche Ausfälle zu berücksichtigen. Wenn Sie keine lokalen Zeitserver hosten können, sollten Sie öffentliche NTP- oder NTS-Server verwenden. Weitere Informationen zu NTP/NTS in Axis Geräten finden Sie unter *NTP und NTS* in der AXIS OS Knowledge Base.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > Basic Setup > Date & Time
7.10	Settings > System > Date and time
≥ 10.9	System > Date and time
≥ 11.6	System > Time and location

Edge Storage-Verschlüsselung

CSC Nr. 3: Datenschutz

SD-Karte

Wenn das Axis Gerät zum Speichern von Videoaufzeichnungen Secure Digital-Karten (SD) unterstützt und verwendet, wird eine Verschlüsselung empfohlen. Dadurch wird verhindert, dass unbefugte Personen das gespeicherte Video von einer entfernten SD-Karte wieder abspielen können.

Weitere Informationen zur SD-Karten-Verschlüsselung von Axis Geräten finden Sie unter *Unterstützung von SD-Karten* in der AXIS OS Knowledge Base.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Storage
7.10	Settings > System > Storage
≥ 10.9	System > Storage

Netzwerk-Freigabe (NAS)

Wenn Sie ein NAS (Network Attached Storage) als Aufnahmegerät verwenden, empfehlen wir, es in einem abgeschlossenen Bereich mit eingeschränktem Zugang aufzubewahren und die Festplattenverschlüsselung zu aktivieren. Axis Geräte verwenden SMB als Netzwerkprotokoll für den Anschluss an ein NAS zum Speichern von Videoaufzeichnungen. Da ältere Versionen von SMB (1.0 und 2.0) keine Sicherheit oder Verschlüsselung bieten, empfehlen wir spätere Versionen (2.1 und höher), spätere Versionen sollten daher während der Produktion verwendet werden.

Weitere Informationen zur ordnungsgemäßen SMB-Konfiguration beim Verbinden eines Axis Geräts mit einer Netzwerk-Freigabe finden Sie unter *Netzwerk-Freigabe* in der AXIS OS Knowledge Base.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Storage
7.10	Settings > System > Storage
≥ 10.9	System > Storage

Anwendungen (ACAPs)

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

Sie können Anwendungen auf das Axis Gerät hochladen, um die Funktionalität zu erweitern. Viele von ihnen verfügen über eine eigene Benutzeroberfläche für die Interaktion mit bestimmten Funktionen. Anwendungen können Sicherheitsfunktionen verwenden, die von AXIS OS bereitgestellt werden.

AXIS OS Hardening Guide

Grundlegende Härtung

Auf Axis Geräten sind mehrere Anwendungen vorinstalliert, die von Axis gemäß dem *Axis Security Development Model (ASDM)* entwickelt wurden. Weitere Informationen zu Axis Anwendungen finden Sie unter *Analysefunktionen* auf axis.com.

Bei Anwendungen von Drittanbietern empfehlen wir Ihnen, sich mit dem Anbieter in Verbindung zu setzen, um Nachweise für die Sicherheit der Anwendung in Bezug auf Betrieb und Tests zu erhalten und um zu erfahren, ob die Anwendung nach den gängigen Best-Practice-Sicherheitsentwicklungsmodellen entwickelt wurde. Sicherheitslücken in Anwendungen anderer Hersteller müssen direkt dem Drittanbieter mitgeteilt werden.

Es wird empfohlen, nur vertrauenswürdige Anwendungen zu betreiben und nicht verwendete Anwendungen von Axis Geräten zu entfernen.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > Applications
7.10	Settings > Apps
≥ 10.9	Apps

Nicht verwendete Dienste/Funktionen deaktivieren

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

Auch wenn nicht verwendete Dienste und Funktionen keine unmittelbare Sicherheitsgefahr darstellen, sollten ungenutzte Dienste und Funktionen deaktiviert werden, um unnötige Risiken zu verringern. Lesen Sie weiter, um mehr über Dienste und Funktionen zu erfahren, die Sie deaktivieren können, wenn sie nicht verwendet werden.

Nicht verwendete physische Netzwerkports

Ab AXIS OS 11.2 verfügen Geräte mit mehreren Netzwerkports wie AXIS S3008 über die Option, sowohl PoE als auch den Netzwerkverkehr ihrer Netzwerkports zu deaktivieren. Wenn ungenutzte Netzwerkports unbeaufsichtigt und aktiviert bleiben, besteht ein großes Sicherheitsrisiko.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	n. v.
7.10	n. v.
≥ 11.2	System > Power over Ethernet

Netzwerk-Erkennungsprotokolle

Erkennungsprotokolle wie Bonjour, UPnP®, ZeroConf und WS-Discovery und LLDP/CDP sind Supportdienste, mit denen sich Axis Geräte und deren Dienste im Netzwerk leichter finden lassen. Nachdem Sie das Gerät bereitgestellt und zum VMS hinzugefügt haben, wird empfohlen, das Erkennungsprotokoll zu deaktivieren, damit das Axis Gerät nicht mehr im Netzwerk angezeigt wird.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Advanced > Plain Config > Network > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled*
	n. v.
7.10	Settings > System > Plain config > Network > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled*
	Settings > System > Plain config > WebService > Discovery Mode

AXIS OS Hardening Guide

Grundlegende Härtung

AXIS OS Version	Konfigurationspfad für die Weboberfläche
≥ 10.9	Settings > Plain config > Network > Bonjour Enabled, UPnP Enabled, ZeroConf Enabled System > Plain config > WebService > DiscoveryMode > Enable WS-Discovery discoverable mode
≥ 11.11	System > Network > Network discovery protocols > LLDP and CDP**

* Funktion wurde von AXIS 10.12 entfernt und ist in späteren Versionen nicht verfügbar.

** Das Deaktivieren von LLDP und CDP kann sich auf das PoE-Leistungsmanagement auswirken.

Veraltete TLS-Versionen

Wir empfehlen, ältere, nicht abgesicherte und unsichere TLS-Versionen zu deaktivieren, bevor Sie Ihr Axis Gerät in Betrieb nehmen. In der Standardeinstellung sind veraltete TLS-Versionen in der Standardeinstellung deaktiviert. Sie können jedoch verwendet werden, um auf Axis Geräten Abwärtskompatibilität mit Anwendungen von Drittanbietern zu ermöglichen, die TLS 1.2 und TLS 1.3 noch nicht implementiert haben.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Advanced > Plain Config > HTTPS > Allow TLSv1.0 und/oder Allow TLSv1.1
7.10	Settings > System > Plain config > HTTPS > Allow TLSv1.0 und/oder Allow TLSv1.1
≥ 10.9	System > Plain config > HTTPS > Allow TLSv1.0 und/oder Allow TLSv1.1

Scripteditor-Umgebung

Es wird empfohlen, den Zugriff auf die Scripteditor-Umgebung zu deaktivieren. Der Scripteditor dient nur zur Fehlersuche und zum Debuggen.

Der Scripteditor wurde von AXIS OS 10.11 entfernt und ist in späteren Versionen nicht verfügbar.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	n. v.
7.10	Settings > System > Plain config > System > Enable the script editor (editcgi)
≥ 10.9	System > Plain config > System > Enable the script editor (editcgi)

HTTP(S)-Serverheader

Axis Geräte geben standardmäßig ihre aktuellen Apache- und OpenSSL-Versionen an, wenn sie über HTTP(S) mit Clients im Netzwerk verbunden sind. Diese Informationen sind bei der regelmäßigen Verwendung von Netzwerksicherheits-Scannern nützlich, da sie einen detaillierteren Bericht über die offenen Sicherheitslücken in einer bestimmten AXIS OS Version liefern.

Es ist möglich, die HTTP(S)-Server-Header zu deaktivieren, um die Preisgabe von Informationen bei HTTP(S)-Verbindungen zu reduzieren. Wir empfehlen jedoch, die Header nur zu deaktivieren, wenn Sie Ihr Gerät gemäß unseren Empfehlungen betreiben und stets auf dem neuesten Stand sind.

Die Option zum Deaktivieren der HTTP(S)-Server-Header ist ab AXIS OS 10.6 verfügbar.

AXIS OS Hardening Guide

Grundlegende Härtung

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	n. v.
7.10	Settings > System > Plain config > System > HTTP Server Header Comments
≥ 10.9	System > Plain config > System > HTTP Server Header Comments

Audio

Bei Videosicherheitsprodukten von Axis sind die Netzwerk-Kameras sowie Audioeingang/Audioausgang- und Mikrofonfunktionen in der Standardeinstellung deaktiviert. Wenn Sie Audiofunktionen benötigen, müssen diese vor der Verwendung aktiviert werden. Bei Axis Produkten, bei denen Audioeingang/Audioausgang- und Mikrofonfunktionen notwendig sind, wie z. B. bei Axis Wechselsprechanlagen und Netzwerklautsprechern sind die Audiofunktionen standardmäßig aktiviert.

Es wird empfohlen, die Audiofunktionen zu deaktivieren, wenn sie nicht verwendet werden.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Advanced > Plain Config > Audio > Audio A* > Enabled
7.10	Settings > Audio > Allow audio
≥ 10.9	Audio > Device settings

Einschub für SD-Speicherkarte(n)

Axis Geräte unterstützen in der Regel mindestens eine SD-Karte, um Videoaufzeichnungen lokal auf Edge Storage zu speichern. Es wird empfohlen, den Einschub für SD-Speicherkarten vollständig zu deaktivieren, wenn Sie keine SD-Karten verwenden. Die Option zum Deaktivieren des Einschubs für SD-Speicherkarten ist unter AXIS OS 9.80 verfügbar.

Weitere Informationen finden Sie unter *Deaktivieren der SD-Karte* in der AXIS OS Knowledge Base.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	n. v.
7.10	Settings > System > Plain config > Storage > SD Disk Enabled
≥ 10.9	System > Plain config > Storage > SD Disk Enabled

FTP-Zugriff

FTP ist ein unsicheres Kommunikationsprotokoll, das nur zu Zwecken der Fehlersuche und -behebung verwendet wird. Der FTP-Zugriff wurde aus AXIS OS 11.1 entfernt und ist in späteren Versionen nicht mehr verfügbar. Es wird empfohlen, den FTP-Zugriff zu deaktivieren und für die Fehlerbehebung einen sicheren SSH-Zugriff zu verwenden.

Weitere Informationen zu SSH finden Sie unter *SSH-Zugriff* im AXIS OS Portal. Informationen zu Debugging-Optionen mit FTP, siehe *FTP-Zugriff* im AXIS OS Portal.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Plain Config > Network > FTP Enabled
7.10	Settings > System > Plain config > Network > FTP Enabled
≥ 10.9	System > Plain config > Network > FTP Enabled

AXIS OS Hardening Guide

Grundlegende Härtung

SSH-Zugriff

SSH ist ein sicheres Kommunikationsprotokoll, das nur zur Fehlersuche und zum Debuggen verwendet wird. Es wird von Axis Geräten ab AXIS OS 5.50 unterstützt. Wir empfehlen, den SSH-Zugriff zu deaktivieren.

Weitere Informationen zu Debugging-Optionen mit SSH finden Sie unter *SSH-Zugriff* in der AXIS OS Knowledge Base.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Plain Config > Network > SSH Enabled
7.10	Settings > System > Plain config > Network > SSH Enabled
≥ 10.9	System > Plain config > Network > SSH Enabled

Telnet-Zugriff

Telnet ist ein unsicheres Kommunikationsprotokoll, das nur zur Fehlersuche und zum Debuggen verwendet wird. Es wird von Axis Geräten früherer Versionen als AXIS OS 5.50 unterstützt. Wir empfehlen, den Telnet-Zugriff zu deaktivieren.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 5.50	Anweisungen finden Sie unter <i>Gerätezugriff</i> in der AXIS OS Knowledge Base.
< 7.10	n. v.
7.10	n. v.
≥ 10.9	n. v.

ARP/Ping

ARP/Ping war eine Methode zum Einstellen der IP-Adresse des Axis Geräts mit Tools wie AXIS IP Utility. Die Funktion wurde von AXIS OS 7.10 entfernt und ist in späteren Versionen nicht verfügbar. Es wird empfohlen, die Funktion auf Axis Geräten mit AXIS OS 7.10 und früheren Versionen zu deaktivieren.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Advanced > Plain Config > Network > ARP/Ping
7.10	n. v.
≥ 10.9	n. v.

USB

Ab AXIS OS 12.1 verfügt der AXIS D1110 über die Möglichkeit, den USB Port zu deaktivieren. Wenn ungenutzte USB-Ports unbeaufsichtigt und aktiviert bleiben, besteht ein großes Sicherheitsrisiko.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	n. v.
7.10	n. v.
≥ 12.1	System > > Zubehör > USB Konfiguration

AXIS OS Hardening Guide

Grundlegende Härtung

Hostbasierte Firewall

CSC Nr. 1: Inventar und Steuerung von Unternehmensressourcen
CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software
CSC Nr. 13: Netzwerküberwachung und -schutz

Die in AXIS OS 11.9 eingeführte hostbasierte Firewall ist eine Sicherheitsfunktion, mit der Sie Regeln für den Datenaustausch nach IP-Adresse und/oder TCP/UDP Port-Nummern erstellen können. Dies hilft, unbefugten Zugriff auf das Gerät oder seine Dienste zu verhindern.

Wenn Sie die Standardrichtlinie auf „Deny“ (Verweigern) festlegen, stellen Sie sicher, dass alle autorisierten Clients (VMS und Verwaltungsclients) und/oder Ports zu Ihrer Liste hinzugefügt werden.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
≥ 11.9	Setup > Security > Firewall (Setup > Sicherheit > Firewall)

IP-Adressfilter

Geräte mit AXIS OS 11.8 und früheren Versionen verwenden IP-Adressen-Filterung, um den Zugriff von nicht autorisierten Clients zu verhindern. Wir empfehlen Ihnen, Ihr Gerät so zu konfigurieren, dass Sie entweder IP-Adressen von autorisierten Netzwerk-Hosts zulassen oder nicht autorisierte Adressen ablehnen.

Wenn Sie IP-Adressen zulassen, stellen Sie sicher, dass alle autorisierten Clients, einschließlich VMS-Servern und Verwaltungsclients, zu Ihrer Liste hinzugefügt werden.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Security > IP Address Filter
7.10	Settings > System > TCP/IP > IP address filter
10.9 – 11.8	Settings > Security > IP address filter

Hinweis

Sie können detailliertere Protokolle der Zugriffsversuche auf das Netzwerk aktivieren, um unerwünschte Zugriffsversuche von anderen Netzwerkhosts zu erkennen. Rufen Sie dazu **System > Plain config > Netzwerk** und das Netzwerkfilterprotokoll auf.

HTTPS

CSC Nr. 3: Datenschutz

HTTP und HTTPS sind in Axis Geräten ab AXIS OS 7.20 standardmäßig aktiviert. Während der HTTP-Zugriff ohne jegliche Verschlüsselung unsicher ist, verschlüsselt HTTPS den Datenaustausch zwischen dem Client und dem Axis Gerät. Es wird empfohlen, HTTPS für alle Verwaltungsaufgaben auf dem Axis Gerät zu verwenden.

Konfigurationsanweisungen finden Sie unter *Nur HTTPS auf Seite 21* und *HTTPS-Verschlüsselungen auf Seite 22*.

Nur HTTPS

Es wird empfohlen, das Axis Gerät so zu konfigurieren, dass es nur HTTPS verwendet (kein HTTP-Zugriff möglich). So wird HSTS (HTTP Strict Transport Security) automatisch aktiviert, wodurch sich die Sicherheit des Geräts weiter verbessert.

Ab AXIS OS 7.20 besitzen Axis Geräte ein eigensigniertes Zertifikat. Ein eigensigniertes Zertifikat ist zwar grundsätzlich nicht vertrauenswürdig, reicht aber aus, um bei der Erstkonfiguration und wenn keine Public Key Infrastructure (PKI) verfügbar ist, sicher auf das Axis Gerät zuzugreifen. Falls vorhanden, sollte das eigensignierte Zertifikat entfernt und durch ordnungsgemäß signierte Clientzertifikate ersetzt werden, die von einer PKI-Zertifizierungsstelle ihrer Wahl ausgegeben wurden. Ab AXIS OS 10.10 wurde das eigensignierte Zertifikat durch das IEEE 802.1AR Zertifikat für sichere Geräte-ID ersetzt.

AXIS OS Hardening Guide

Grundlegende Härtung

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Security > HTTPS
7.10	Settings > System > Security > HTTP and HTTPS
≥ 10.9	System > Network > HTTP and HTTPS

HTTPS-Verschlüsselungen

Axis Geräte unterstützen Verschlüsselungssuiten TLS 1.2 und TLS 1.3, um HTTPS-Verbindungen sicher zu verschlüsseln. Die verwendete TLS-Version und Verschlüsselungssuite hängt vom Client ab, der mit dem Axis Gerät verbunden ist, und wird dementsprechend verhandelt. Während der AXIS OS-Aktualisierung wird die Liste der verfügbaren Verschlüsselungen des Axis Gerät möglicherweise aktualisiert, ohne dass die Verschlüsselungskonfiguration geändert wird. Eine Änderung der Verschlüsselungskonfiguration muss vom Benutzer veranlasst werden, entweder durch eine Werkseinstellung des Axis Geräts oder durch eine manuelle Benutzerkonfiguration. Ab AXIS OS 10.8 wird die Liste der Verschlüsselungen automatisch aktualisiert, wenn der Benutzer eine AXIS OS-Aktualisierung durchführt.

TLS 1.2 und niedriger

Wenn Sie TLS 1.2 oder niedriger verwenden, können Sie die HTTPS-Chiffren angeben, die vom Axis Gerät nach dem Neustart verwendet werden sollen. Es gibt keine Einschränkungen bei der Auswahl der Verschlüsselungen, aber wir empfehlen, dass Sie eine oder alle der folgenden starken Verschlüsselungen auswählen:

ECDHE-ECDSA-AES128-GCM-SHA256 : ECDHE-RSA-AES128-GCM-SHA256 : ECDHE-ECDSA-AES256-GCM-SHA384 : ECDHE-RSA-AES256-GCM-SHA384 : ECDHE-ECDSA-CHACHA20-POLY1305 : ECDHE-RSA-CHACHA20-POLY1305

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Advanced > Plain Config > HTTPS > Ciphers
7.10	Settings > System > Plain config > HTTPS > Ciphers
≥ 10.9	System > Plain config > HTTPS > Ciphers

TLS 1.3

Standardmäßig sind nur starke Verschlüsselungssuites gemäß den Spezifikationen von TLS 1.3 verfügbar:

TLS_AES_128_GCM_SHA256 : TLS_CHACHA20_POLY1305_SHA256 : TLS_AES_256_GCM_SHA384

Diese Suiten können vom Benutzer nicht konfiguriert werden.

Zugangsprotokoll

CSC Nr. 1: Inventar und Steuerung von Unternehmensressourcen

CSC Nr. 8: Verwaltung von Prüfprotokollen

Das Zugriffsprotokoll enthält detaillierte Protokolle der Benutzer, die auf das Axis Gerät zugreifen, was sowohl Audits als auch das Zutrittskontrollmanagement vereinfacht. Es wird empfohlen, diese Funktion zu aktivieren und mit einem Remote-Syslog-Server zu kombinieren, damit das Axis Gerät seine Protokolle an eine zentrale Protokollierungsumgebung senden kann. Dies vereinfacht das Speichern von Protokollmeldungen und deren Aufbewahrungszeit.

Weitere Informationen finden Sie unter *Gerätezugriffsprotokollierung* in der AXIS OS Knowledge Base.

AXIS OS Hardening Guide

Grundlegende Härtung

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Advanced > Plain Config > System > Access log
7.10	Settings > System > Plain config > System > Access log
≥ 10.9	System > Plain config > System > Access log

Physisches Zubehör zum Schutz vor Manipulation

CSC Nr. 1: Inventar und Steuerung von Unternehmensressourcen

CSC Nr. 12: Verwaltung der Netzwerk-Infrastruktur

Axis bietet physische Eindring- und/oder Manipulationsschalter als optionales Zubehör an, um den physischen Schutz von Axis Geräten zu verbessern. Diese Schalter können einen Alarm auslösen, der es Axis Geräten ermöglicht, eine Benachrichtigung oder einen Alarm an ausgewählte Clients zu senden.

Weitere Informationen über verfügbares Manipulationsschutzzubehör finden Sie unter:

- *AXIS TA8501 Physical Tampering Switch*
- *AXIS Dome Intrusion Switch C*
- *AXIS-Türschalter A*

AXIS OS Hardening Guide

Erweitertes Härten

Erweitertes Härten

Die Anweisungen zum erweiterten Härten bauen auf den unter *Standardschutz auf Seite 4* und *Grundlegende Härtung auf Seite 13* beschriebenen Härtethemen auf. Sie können die Standard- und grundlegenden Härteanweisungen direkt auf Ihr Axis Gerät anwenden. Für das erweiterte Härten ist jedoch eine aktive Teilnahme der gesamten Lieferkette des Anbieters, der Endbenutzer-Organisation sowie der IT- und/oder Netzwerkinfrastruktur erforderlich.

Begrenzung von Internet- und Netzwerkeexposition

CSC Nr. 12: Verwaltung der Netzwerk-Infrastruktur

Es wird nicht empfohlen, ein Axis Gerät als öffentlichen Webserver darzustellen oder unbekanntem Clients in irgendeiner Weise Netzwerkzugriff auf das Gerät zu geben. Für kleine Organisationen und Einzelpersonen, die keine Video Management Software (VMS) verwenden oder auf Videos von entfernten Einsatzorten zugreifen müssen, ist AXIS Camera Station Edge eine gute Option.

Die AXIS Camera Station Edge ist für Windows, iOS und Android kostenlos erhältlich und bietet eine einfache Möglichkeit, sicher auf Videos zuzugreifen, ohne dass Ihr Gerät dem Internet ausgesetzt ist. Weitere Informationen finden Sie auf axis.com/products/axis-camera-station-edge.

Hinweis

Wenn Ihre Organisation ein VMS verwendet, fragen Sie Ihren VMS-Anbieter nach bewährten Verfahren für den Fernzugriff auf Videos.

Die Isolierung von Netzwerk-Geräten sowie von zugehörigen Infrastruktur und Anwendungen verringert das Risiko der Netzwerkeexposition.

Wir empfehlen, Ihre Axis Geräte und die damit verbundene Infrastruktur und Anwendungen in einem lokalen Netzwerk zu isolieren. Dieses Netzwerk sollte von Ihrem Produktions- und Unternehmensnetzwerk getrennt sein.

Um eine grundlegende Härtung zu gewährleisten, müssen das lokale Netzwerk und seine Infrastruktur (Router, Switches) durch verschiedene Netzwerksicherheitsmechanismen vor unbefugtem Zugriff geschützt werden. Dazu können VLAN-Segmentierung, begrenzte Routing-Funktionen, VPN für den Standort-zu-Standort- oder WAN-Zugriff, Firewall der Netzwerkschicht 2/3 und Zutrittskontrolllisten (ACL) gehören.

Um die grundlegende Härtung zu erweitern, sollten Sie fortgeschrittene Netzwerkinspektionstechniken wie Deep Packet Inspection und Intrusion Detection anwenden. Dadurch wird der Schutz vor Bedrohungen innerhalb des Netzwerks verbessert. Bitte beachten Sie, dass für eine erweiterte Härtung des Netzwerks in der Regel spezielle Software und/oder Hardware erforderlich ist.

Suche nach Schwachstellen im Netzwerk

CSC Nr. 1: Inventar und Steuerung von Unternehmensressourcen

CSC Nr. 12: Verwaltung der Netzwerk-Infrastruktur

Mithilfe von Netzwerksicherheits-Scannern können Sie Schwachstellen Ihrer Netzwerkgeräte finden. Der Zweck einer Vulnerabilitätsbewertung besteht in der gezielten Überprüfung potenzieller Sicherheitslücken und Falschkonfigurationen.

Wir empfehlen Ihnen, Ihre Axis Geräte und deren zugehörige Infrastruktur regelmäßig auf Sicherheitslücken zu überprüfen. Stellen Sie vor dem Scannen sicher, dass Ihre Axis Geräte auf die neueste verfügbare AXIS OS Version aktualisiert wurden, entweder auf LTS oder dem aktiven Track.

Außerdem wird empfohlen, den Scanbericht zu überprüfen und für Axis Geräte erhaltene Fehlalarme herausfiltern zu lassen. Dies finden Sie im *Axis OS Vulnerability Scanner Guide*. Senden Sie den Bericht und weitere Informationen in einem Helpdesk-Ticket an den *Axis Support* unter axis.com.

Vertrauenswürdige Infrastruktur für öffentliche Schlüssel (PKI)

CSC Nr. 3: Datenschutz

CSC Nr. 12: Verwaltung der Netzwerk-Infrastruktur

AXIS OS Hardening Guide

Erweitertes Härten

Es wird empfohlen, Webserver- und Clientzertifikate für Ihre Axis Geräte bereitzustellen, die vertrauenswürdig und von einer öffentlichen oder privaten Zertifizierungsstelle (CA) unterzeichnet sind. Ein CA-Zertifikat mit einer validierten Vertrauenskette hilft, die Warnungen vor Browser-Zertifikaten zu entfernen, wenn Sie eine Verbindung über HTTPS herstellen. Ein CA-Zertifikat stellt auch die Authentizität des Axis Geräts sicher, wenn Sie eine Lösung für die Zutrittskontrolle im Netzwerk (NAC) einsetzen. Dies verringert das Risiko von Angriffen durch einen Computer mit der Identität eines Axis Geräts.

Mit dem AXIS Device Manager, der mit einem integrierten CA-Dienst kombiniert ist, können Axis Geräte signierte Zertifikate ausgeben.

Netzwerkzugriffskontrolle auf Basis von IEEE 802.1X

CSC Nr. 6: Verwaltung der Zutrittskontrolle

CSC Nr. 13: Netzwerküberwachung und -schutz

Axis Geräte unterstützen die portbasierte Netzwerk-Zugriffskontrolle nach IEEE 802.1X über die EAP-TLS-Methode. Für einen optimalen Schutz wird empfohlen, bei der Authentifizierung Ihres Axis Geräts von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) signierte Clientzertifikate zu verwenden.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Wechseln Sie zu „Setup > System Options (Systemoptionen) > Security (Sicherheit) > IEEE 802.1X“.
7.10	Einstellungen > System > Sicherheit > IEEE 802.1X
≥ 10.9	System > Sicherheit > IEEE 802.1X

IEEE 802.1AE MACsec

CSC Nr. 3: Datenschutz

CSC Nr. 6: Verwaltung der Zutrittskontrolle

Axis Geräte unterstützen IEEE 802.1AE MACsec. Dies ist ein genau definiertes Netzwerkprotokoll, das Punkt-zu-Punkt-Ethernet-Verbindungen auf Netzwerkschicht 2 kryptografisch sichert. Es gewährleistet die Vertraulichkeit und Integrität der Datenübertragungen zwischen zwei Hosts. MACsec arbeitet auf der unteren Ebene 2 des Netzwerk-Stacks und bietet daher zusätzliche Sicherheit für Netzwerkprotokolle, die keine nativen Verschlüsselungsfunktionen bieten (ARP, NTP, DHCP, LLDP, CDP usw.) sowie für Protokolle, die native Verschlüsselung bieten (HTTPS, TLS).

Der IEEE 802.1AE MACsec-Standard beschreibt zwei Betriebsmodi: einen manuell konfigurierbaren Pre-Shared Key (PSK)/Static CAK-Modus und einen automatischen Master Session/Dynamic CAK-Modus mit IEEE 802.1X EAP-TLS-Sitzungen. Das Axis Gerät unterstützt beide Modi.

Weitere Informationen zu 802.1AE MACsec und zur Konfiguration auf AXIS OS-Geräten finden Sie unter *IEEE 802.1AE* in der AXIS OS-Wissensdatenbank.

IEEE 802.1AR sichere Identität des Geräts

CSC Nr.1: Inventar und Steuerung von Unternehmensressourcen

CSC Nr. 13: Netzwerküberwachung und -schutz

Axis Geräte mit Axis Edge Vault unterstützen den Netzwerkstandard IEEE 802.1AR. Dies ermöglicht ein automatisches und sicheres Onboarding von Axis Geräten in das Netzwerk durch die Axis Geräte-ID, ein eindeutiges Zertifikat, das während der Produktion im Gerät installiert wird. Ein Beispiel für sicheres Geräte-Onboarding finden Sie unter *Sichere Integration von Axis Geräten in Aruba-Netzwerke*.

Weitere Informationen finden Sie im Whitepaper *Axis Edge Vault*. Informationen zum Herunterladen der Zertifikatskette der Axis Geräte-ID zum Validieren der Geräteidentität von Axis Geräten finden Sie im *Public Key Infrastructure Repository* auf axis.com.

Remote-Syslog

CSC Nr. 8: Verwaltung von Prüfprotokollen

AXIS OS Hardening Guide

Erweitertes Härten

Sie können ein Axis Gerät so konfigurieren, dass es alle Protokollmeldungen verschlüsselt an einen zentralen Syslog-Server sendet. Dies vereinfacht die Überprüfung und verhindert das vorsätzliche oder unbeabsichtigte Löschen von Protokollmeldungen auf dem Axis Gerät. Je nach Unternehmensrichtlinie kann die Aufbewahrungszeit von Geräteprotokollen ebenfalls verlängert werden.

Weitere Informationen zur Aktivierung des Remote-Syslog-Servers in verschiedenen AXIS OS Versionen finden Sie unter *Syslog* in der AXIS OS Knowledge Base.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Anweisungen finden Sie unter <i>Syslog</i> im AXIS OS Portal.
7.10	Settings > System > TCP/IP
≥ 10.9	System > Logs

Sicheres Videostreaming (SRTP/RTSPS)

CSC Nr. 3: Datenschutz

Ab AXIS OS 7.40 unterstützen Axis Geräte sicheres Video-Streaming über RTP, auch SRTP/RTSPS genannt. SRTP/RTSPS nutzt ein sicheres, durchgehend verschlüsseltes Datenübertragungsverfahren, um sicherzustellen, dass nur autorisierte Clients den Videostream vom Axis Gerät empfangen. Es wird empfohlen, SRTP/RTSPS zu aktivieren, wenn Ihr Video Management System (VMS) dies unterstützt. Verwenden Sie, falls verfügbar, anstelle des unverschlüsselten RTP-Videostreamings SRTP.

Hinweis

SRTP/RTSPS verschlüsselt nur die Videostreamdaten. Für Verwaltungsaufgaben wird empfohlen, HTTPS nur zum Verschlüsseln dieses Kommunikationstyps zu aktivieren.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	Setup > System Options > Advanced > Plain Config > Network > RTSPS
7.10	Settings > System > Plain config > Network > RTSPS
≥ 10.9	System > Plain config > Network > RTSPS

Signiertes Video

CSC Nr. 3: Datenschutz

Ab AXIS OS 10.11 unterstützen Axis Geräte mit Axis Edge Vault signierte Videos. Mit signierten Videos können Axis Geräte ihrem Videostream eine Signatur hinzufügen, um sicherzustellen, dass das Video intakt ist, und um seine Herkunft zu überprüfen, indem es zu dem Gerät zurückverfolgt wird, das es produziert hat. Das Video Management System (VMS) oder das Evidence Management System (CNC) kann auch die Authentizität des von einem Axis Gerät bereitgestellten Videos überprüfen.

Weitere Informationen finden Sie im Whitepaper *Axis Edge Vault*. Informationen zum Suchen der Root-Zertifikate von Axis zur Validierung der Authentizität signierter Videos finden Sie unter *Gerätezugriff* in der AXIS OS Knowledge Base.

AXIS OS Version	Konfigurationspfad für die Weboberfläche
< 7.10	n. v.
7.10	n. v.
≥ 10.9	System > Plain config > Image > SignedVideo

AXIS OS Hardening Guide

Kurzanleitung

Kurzanleitung

Die Schnellstartanleitung bietet eine kurze Übersicht über die Einstellungen, die beim Härten von Axis Geräten mit AXIS OS 5.51 oder höher konfiguriert werden sollten. Es deckt die Härtungsthemen ab, die Sie in *Grundlegende Härtung auf Seite 13* nachlesen können, jedoch nicht die Themen in *Erweitertes Härten auf Seite 24*, da diese eine umfangreiche und kundenspezifische Konfiguration auf einer Fall-zu-Fall-Basis erfordern.

Es wird empfohlen, den AXIS Device Manager zu verwenden, um mehrere Axis Geräte schnell und kostengünstig zu härten. Wenn Sie eine andere Anwendung für die Gerätekonfiguration verwenden müssen oder nur einige Axis Geräte härten müssen, wird die Verwendung der VAPIX-API empfohlen.

Häufige Konfigurationsfehler

Im Internet dargestellte Geräte

CSC Nr. 12: Verwaltung der Netzwerk-Infrastruktur

Es wird nicht empfohlen, Axis Geräte als öffentlichen Webserver zu nutzen oder unbekanntem Clients in irgendeiner Weise Netzwerkzugriff auf das Gerät zu geben. Weitere Informationen finden Sie unter *Außerbetriebnahme auf Seite 10*.

Gemeinsames Kennwort

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

CSC Nr. 5: Kontenverwaltung

Wir empfehlen Ihnen dringend, für jedes Gerät ein eindeutiges Kennwort anstelle eines allgemeinen Kennworts für alle Geräte zu verwenden. Anweisungen finden Sie unter *Dedizierte Konten erstellen auf Seite 14*.

Anonymer Zugriff

CSC Nr. 4: Sichere Konfiguration von Unternehmensressourcen und Software

CSC Nr. 5: Kontenverwaltung

Es wird nicht empfohlen, anonymen Benutzern den Zugriff auf Video- und Konfigurationseinstellungen auf dem Gerät zu ermöglichen, ohne Anmeldeinformationen angeben zu müssen. Weitere Informationen finden Sie unter *Außerbetriebnahme auf Seite 10*.

Sichere Kommunikation deaktiviert

CSC Nr. 3: Datenschutz

Es wird nicht empfohlen, das Gerät mit unsicheren Kommunikationsmethoden und Zugriffsmethoden wie HTTP oder einer einfachen Authentifizierung zu betreiben, bei der Kennwörter verschlüsselungsfrei übertragen werden. Weitere Informationen finden Sie unter *Außerbetriebnahme auf Seite 10*. Empfehlungen für die Konfiguration siehe *Digest-Authentifizierung auf Seite 9*.

Veraltete AXIS OS Version

CSC Nr. 2: Inventar und Steuerung von Softwareressourcen

Wir empfehlen Ihnen dringend, das Axis Gerät mit der neuesten verfügbaren AXIS OS Version zu betreiben, entweder auf der LTS oder dem aktiven Track. Beide Tracks bieten die neuesten Sicherheits-Patches und Bugfixes. Weitere Informationen finden Sie unter *Außerbetriebnahme auf Seite 10*.

Grundlegendes Härten über VAPIX API

Verwenden Sie die VAPIX-API, um Ihre Axis Geräte anhand der in *Grundlegende Härtung auf Seite 13* behandelten Themen zu härten. In dieser Tabelle finden Sie alle grundlegenden Härtekonfigurationseinstellungen unabhängig von der AXIS OS Version Ihres Axis Geräts.

Es ist möglich, dass in der AXIS OS Version Ihres Geräts einige Konfigurationseinstellungen nicht mehr verfügbar sind, da einige Funktionen im Laufe der Zeit entfernt wurden, um die Sicherheit zu erhöhen. Wenn bei der Ausgabe des VAPIX-Anrufs ein Fehler auftritt, kann dies ein Hinweis darauf sein, dass die Funktion in der AXIS OS Version nicht mehr verfügbar ist.

AXIS OS Hardening Guide

Kurzanleitung

Zweck	VAPIX-API-Anruf
<i>POE an ungenutzten Netzwerkports deaktivieren*</i>	<code>http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no</code>
<i>Netzwerkverkehr an nicht genutzten Netzwerkports deaktivieren**</i>	<code>http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }</code>
<i>Bonjour-Erkennungsprotokoll deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update &Network.Bonjour.Enabled=no</code>
<i>UPnP®-Erkennungsprotokoll deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update &Network.UPnP.Enabled=no https://ip-address/axis-cgi/param.cgi?action=update &Network.UPnP.NATTraversal.Enabled=no</code>
<i>WebService-Erkennungsprotokoll deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update &WebService.DiscoveryMode.Discoverable=no</code>
<i>Cloud-Anbindung mit einem Klick (O3C) deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update &RemoteService.Enabled=no</code>
<i>Gerätezugriff auf SSH-Wartung deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update &Network.SSH.Enabled=no</code>
<i>Gerätezugriff auf FTP-Wartung deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update &Network.FTP.Enabled=no</code>
<i>ARP-Ping-IP-Adresskonfiguration deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update &Network.ARPPingIPAddress.Enabled=no</code>
<i>Zero-Conf-IP-Adresskonfiguration deaktivieren</i>	<code>http://ip-address/axis-cgi/param.cgi?action=update &Network.ZeroConf.Enabled=no</code>
<i>Nur HTTPS aktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update &System.BoaGroupPolicy.admin=https https://ip-address/axis-cgi/param.cgi?action=update &System.BoaGroupPolicy.operator=https https://ip-address/axis-cgi/param.cgi?action=update &System.BoaGroupPolicy.viewer=https</code>
<i>Nur TLS 1.2 und TLS 1.3 aktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update &HTTPS.AllowTLS1=no https://ip-address/axis-cgi/param.cgi?action=update &HTTPS.AllowTLS11=no</code>

AXIS OS Hardening Guide

Kurzanleitung

Zweck	VAPIX-API-Anruf
<i>Sichere Verschlüsselungskonfiguration für TLS 1.2</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.Ciphers=ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384</code>
<i>Schutz vor Brute-Force-Angriffen aktivieren***</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10 https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20 https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1 https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20 https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1</code>
<i>Skript-Editor-Umgebung deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no</code>
<i>Verbesserte Benutzerzugriffsprotokollierung aktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On</code>
<i>ONVIF-Wiedergabe-Angriffsschutz aktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes</code>
<i>Zugriff auf Geräte-Weboberfläche deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes</code>
<i>HTTP/OpenSSL-Server-Header deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no</code>
<i>Anonyme Anzeige und PTZ-Zugriff deaktivieren</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password https://ip-address/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password</code>

AXIS OS Hardening Guide

Kurzanleitung

Zweck	VAPIX-API-Anruf
Installation von Root-Rechten verhindern, für die ACAP-Anwendungen erforderlich sind	<code>http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowRoot&value=false</code>
Installation unsignierter ACAP-Anwendungen verhindern	<code>http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false</code>

* Ersetzen Sie "X" durch die tatsächliche Port-Nummer in "port=X". Beispiele: "port=1" deaktiviert Port 1 und "port=2" deaktiviert Port 2.

** Ersetzen Sie "1" durch die tatsächliche Port-Nummer in "eth1.1". Beispiele: "eth1.1" deaktiviert Port 1 und "eth1.2" deaktiviert Port 2.

*** Nach 20 fehlgeschlagenen Anmeldeversuchen innerhalb einer Sekunde wird die IP-Adresse des Clients für 10 Sekunden gesperrt.

Jede folgende fehlgeschlagene Anforderung innerhalb von 30 Sekunden führt dazu, dass die DoS-Sperrzeit um weitere 10 Sekunden verlängert wird.

Grundlegendes Härten über den AXIS Device Manager (Extend)

Mit dem AXIS Device Manager und dem AXIS Device Manager Extend können Sie Ihre Axis Geräte anhand der in *Grundlegende Härtung auf Seite 13* behandelten Themen härten. Verwenden Sie *diese Konfigurationsdatei*, die aus denselben Konfigurationseinstellungen besteht, die in *Grundlegendes Härten über VAPIX API auf Seite 27* aufgeführt sind.

Es ist möglich, dass in der AXIS OS Version Ihres Geräts einige Konfigurationseinstellungen nicht mehr verfügbar sind, da einige Funktionen im Laufe der Zeit entfernt wurden, um die Sicherheit zu erhöhen. AXIS Device Manager und AXIS Device Manager Extend werden diese Einstellungen automatisch aus der Härtekonfiguration entfernen.

Hinweis

Nach dem Hochladen der Konfigurationsdatei wird das Axis Gerät nur auf HTTPS konfiguriert und die Weboberfläche wird deaktiviert. Sie können die Konfigurationsdatei ihren Anforderungen entsprechend ändern, z. B. durch Entfernen oder Hinzufügen von Parametern.

Sicherheitsbenachrichtigungen

Wir empfehlen, den *Sicherheitsbenachrichtigungsdienst von Axis* zu abonnieren, um Informationen über neu entdeckte Sicherheitslücken in Axis Produkten, Lösungen und Diensten sowie über den Schutz Ihrer Axis Geräte zu erhalten.

