Axis Hardening Guide

für IP-Kameras

Inhalt

1. Einführung

Axis wendet beim Design, der Entwicklung und dem Test seiner Geräte bewährte Verfahren der Cybersecurity an, um das Risiko von Schwachstellen zu minimieren, die bei einem Angriff ausgenutzt werden könnten. Die Sicherung eines IP-Netzwerks, seiner Geräte und der Services, die es unterstützt, erfordert jedoch die aktive Mitarbeit der gesamten Lieferkette sowie die des Endnutzers. Eine sichere Umgebung hängt von ihren Nutzern, den Prozessen und der Technologie ab. Daher haben wir diese Richtlinie erstellt, um Sie bei der Sicherung Ihres Netzwerks, Ihrer Geräte und Services zu unterstützen.

Dieses Dokument enthält technische Ratschläge für jeden, der am Einsatz von Axis-Videolösungen beteiligt ist. Es legt eine Basis-Konfiguration und eine Härtungsrichtlinie fest, die sich mit der entstehenden Bedrohungslandschaft befasst. Wie bei vielen Unternehmen aus dem Sicherheitsbereich verwendet auch die Axis-Baseline die CIS Controls - Version 6.1, siehe www.cisecurity.org/critical-controls.cfm. *Diese Controls waren bisher unter dem Namen SANS Top 20 Critical Security Controls bekannt.* Dieses Dokument bezieht sich auf diese CSC (Critical Security Control) durch die Kennzeichnung CSC#.

Für die Konfiguration bestimmter Einstellungen benötigen Sie unter Umständen das Benutzerhandbuch des Produkts. Axis stellt kostenfrei ACM (AXIS Camera Management) www.axis.com/products/axis-camera-management zur Verfügung, womit sich eine Reihe von Sicherheitseinstellungen effizienter durchführen lassen.

Hinweis: Dieses Dokument, Kontaktinformationen und Sicherheitsratschläge finden Sie unter
www.axis.com/support/product-security

1.1 IP-Kameras in einer Netzwerkumgebung

Die offensichtlichsten Bedrohungen für eine Netzwerk-Kamera sind physikalische Sabotage, Vandalismus und Manipulation. Um das Produkt vor diesen Bedrohungen zu schützen, ist es wichtig, ein vandalismusgeschütztes Modell oder Gehäuse auszuwählen, es auf die empfohlene Weise zu montieren und die Kabel zu schützen.

Aus IT-/Netzwerk-Perspektive ist die Kamera ein Netzwerk-Endpunkt ähnlich wie Laptops, Desktops und mobile Geräte in Unternehmen. Im Gegensatz zu einem Laptop in einem Unternehmen ist eine Netzwerk-Kamera nicht der häufigen Bedrohung durch Benutzer ausgesetzt, die eventuell schädliche Websites besuchen, gefährliche E-Mail-Anhänge öffnen oder nicht vertrauenswürdige Anwendungen installieren. Die Kamera ist jedoch ein Netzwerk-Gerät mit einer Schnittstelle, durch die das System Risiken ausgesetzt sein kann. Diese Richtlinie konzentriert sich darauf, den Einwirkungsbereich dieser Risiken zu reduzieren.

1.2 Freigabe im Internet begrenzen

Es wird nicht empfohlen, die Kamera als öffentlichen Webserver freizugeben und dadurch unbekannten Clients einen Netzwerkzugriff auf die Kamera zu ermöglichen. Einzelpersonen und kleinen Organisationen, die kein VMS (Video Management System) besitzen und einen Fernzugriff auf Videos benötigen, empfiehlt Axis die Verwendung von AXIS Companion. AXIS Companion ist eine kostenfreie Client-Software für Windows/IOS/Android, mit der auf einfache und sichere Weise auf Videos zugegriffen werden kann, ohne die Kamera im Internet freizugeben. Informationen über AXIS Companion sowie den Download finden Sie unter **www.axis.com/companion.** Große Organisationen, die ein VMS verwenden, sollten sich beim Anbieter des VMS nach einem Fernzugriff auf die Videos erkundigen.

1.3 Freigabe im lokalen Netzwerk begrenzen

In einer VMS-Umgebung greifen die Clients immer über den VMS-Server auf Live-Videos und Aufzeichnungen zu. Die Platzierung des VMS-Servers und der Kameras in einem isolierten Netzwerk, entweder durch physikalische oder durch virtuelle Isolation, ist eine übliche und empfohlene Maßnahme, um Gefahren und Risiken zu reduzieren.

2. Schutzstufen

Diese Richtlinie verwendet verschiedene Schutzstufen, die von der Systemgröße und den Anforderungen abhängig sind. Bei jeder Stufe wird angenommen, dass die Empfehlungen der vorherigen Stufe befolgt wurden.

Schutzstufe		Empfohlen für	Maßnahmen
0	Voreingestellter Schutz	Nur empfohlen für Demo-Zwecke und Test-Szenarien.	n. v.
1	Standardschutz	Empfohlene Mindest-Schutzstufe. Diese Stufe ist geeignet für kleine Unternehmen oder Büroinstallationen, in denen der Betreiber typischerweise auch der Administrator ist.	> Werkseitige Standardeinstellungen > Neueste Firmware verwenden > Master-Kennwort festlegen > Ein Video-Client-Konto erstellen > Netzwerkeinstellungen konfigurieren > Datum und Uhrzeit einstellen > Audio deaktivieren, sofern zutreffend > Edge-Storage-Verschlüsselung
2	Unternehmensschutz	Empfohlene Einstellungen für Unternehmen, die einen eigenen System-Administrator haben.	> HTTP Digest Authentication > Domain- und Host-Name > Nicht genutzte Services deaktivieren > IP-Adressfilter > HTTPS-Verschlüsselung
3	Managed Enterprise Protection (Gelenkter Unternehmensschutz)	Große Netzwerkinfrastruktur mit einer IT-/IS-Abteilung. Für Umgebungen, in denen Kameras in eine Unternehmens-Netzwerkinfrastruktur integriert werden müssen.	> Netzwerkzugriffskontrolle auf Basis von IEEE 802.1X > SNMP-Überwachung > Remote System Log

3. Voreingestellte Schutzstufen

Die Kameras werden mit vorinstallierten Standardeinstellungen und einem Standardkennwort ausgeliefert. Es wird nicht empfohlen, diese Einstellungen für den täglichen Betrieb zu verwenden.

4. Standardschutz

Die Standardschutzstufe ist die empfohlene Mindest-Schutzstufe. Diese Stufe ist geeignet für kleine Unternehmen und kleine Organisationen, in denen der Betreiber typischerweise auch der Administrator ist.

4.1 Werkseitige Standardeinstellungen

CSC #3: Sichere Konfiguration für Hard- und Software.

Bevor Sie beginnen, vergewissern Sie sich, dass sich das Produkt in einem bekannten Werkseinstellungszustand befindet. Wenn Sie sich in Bezug auf den Zustand unsicher sind, gehen Sie zu *System Options > Maintenance* und klicken Sie auf Default.

4.2 Neueste Firmware verwenden

CSC #2: Verzeichnis autorisierter und nicht autorisierter Software.

Wenn neue Schwachstellen entdeckt werden, sind die meisten entweder nicht kritisch oder es wäre sehr kostspielig, sie auszunutzen. Gelegentlich wird eine kritische Schwachstelle entdeckt, und Gerät, Computer und System-Services müssen gepatcht werden. Das Patchen von Software und Firmware ist ein wichtiger Prozess der Cybersecurity. Angreifer werden oft versuchen, übliche (bekannte) Schwachstellen auszunutzen. Wenn sie Netzwerkzugriff auf einen ungepatchten Service erhalten, können sie damit Erfolg haben. Stellen Sie sicher, dass Sie immer die neueste Firmware verwenden, da diese Sicherheitspatches für bekannte Schwachstellen enthalten kann. Die Versionshinweise für eine bestimmte Firmware erwähnen vielleicht ausdrücklich ein wichtiges Sicherheitsupdate, aber nicht alle allgemeinen Aktualisierungen.

Laden Sie die neueste Firmware-Datei auf Ihren Computer herunter. Die neueste Version ist immer kostenfrei verfügbar unter **www.axis.com/techsup/firmware.php.** Bevor Sie die Firmware aktualisieren, lesen Sie die Anweisungen im Benutzerhandbuch.

4.3 Master-Kennwort festlegen

CSC #5: Kontrollierte Verwendung von administrativen Privilegien.

Das Kennwort ist die wichtigste Schutzmaßnahme für eine Netzwerk-Kamera. Stellen Sie sicher, dass Sie ein starkes Kennwort verwenden, und halten Sie es geschützt. Bei einer Installation mit mehreren Kameras können die Kameras dasselbe Kennwort oder eigene Kennwörter haben. Die Verwendung desselben Kennworts vereinfacht die Verwaltung, erhöht aber das Risiko, wenn die Sicherheit einer Kamera gefährdet ist.

Erstellen Sie ein schwer zu erratendes Kennwort mit mindestens 8 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Verwenden Sie dazu am besten einen Kennwortgenerator.

4.4 Ein Video-Client-Konto erstellen

CSC #5: Kontrollierte Verwendung von administrativen Privilegien.
CSC #11: Einschränkung und Kontrolle von Netzwerk-Ports, Protokollen und Services.

Das standardmäßige Root-Konto hat volle Privilegien und sollte für administrative Aufgaben reserviert sein. Es wird empfohlen, für den täglichen Betrieb ein Client-Benutzerkonto mit eingeschränkten Privilegien zu erstellen. Dies reduziert die Verteilung des Administrator-Kennworts.

Gehen Sie zu *System Options > Security > Users* und erstellen Sie ein Konto für den täglichen Betrieb. Je nachdem, welche Kamera-Services der Client verwenden wird, müssen Sie Viewer oder Operator auswählen. Ein Video Management System (VMS) sollte normalerweise die Privilegiengruppe für Operator verwenden, kann in manchen Fällen jedoch auch Administrator-Privilegien erfordern. Fragen Sie beim Anbieter des VMS nach.

4.5 Netzwerkeinstellungen konfigurieren

CSC #3: Sichere Konfiguration für Hard- und Software.

Die IP-Konfiguration des Geräts hängt von der Netzwerkkonfiguration ab, also zum Beispiel von IPv4/IPv6, statischer oder dynamischer (DHCP) Netzwerkadresse, Subnetzmaske und Standardrouter.

Gehen Sie zu System Options > Network > TCP/IP > Basic/Advanced, um die Netzwerkeinstellungen zu konfigurieren.

4.6 Datum und Uhrzeit einstellen

CSC #3: Sichere Konfiguration für Hard- und Software.

Aus Sicherheitsperspektive ist es wichtig, dass Datum und Uhrzeit korrekt sind, damit zum Beispiel die Zeitstempel der System-Logs die richtigen Informationen haben.

Es wird empfohlen, die Uhr der Kamera mit einem Network Time Protocol (NTP) Server zu synchronisieren. Einzelpersonen und kleine Organisationen, die keinen lokalen NTP-Server haben, können einen öffentlichen NTP-Server verwenden. Fragen Sie bei Ihrem Internetdienstanbieter nach, oder verwenden Sie einen öffentlichen NTP-Server wie zum Beispiel pool.ntp.org.

Gehen Sie zu *System Options > Date & Time*, um die Zeiteinstellungen einschließlich Zeitzone und Sommerzeit zu konfigurieren.

4.7 Audio deaktivieren

CSC #11: Einschränkung und Kontrolle von Netzwerk-Ports, Protokollen und Services.
CSC #13: Datenschutz.

Audio hat im Vergleich zu Video aufgrund von Datenschutz und Integrität typischerweise eine höhere Datenklassifizierung. Es wird empfohlen, die örtlichen Vorschriften zu überprüfen, bevor das Audiostreaming zugelassen wird.

Gehen Sie zu *System Options > Security> Audio Support*, um zu verhindern, dass Clients Audio anfordern.

4.8 Edge-Storage-Verschlüsselung

CSC #13: Datenschutz.

Wenn die Kamera eine SD-Speicherkarte unterstützt und Video auf diesem Speichergerät aufgezeichnet wird, wird empfohlen, eine Verschlüsselung anzuwenden. Dies verhindert, dass nicht autorisierte Personen, die die SD-Speicherkarte entfernt haben könnten, das gespeicherte Video abspielen können. Wenn ein Network Attached Storage (NAS) als Aufzeichnungsgerät verwendet wird, sollte es in einem gesperrten Bereich geschützt werden, und seine Konten/Zugangsdaten müssen korrekt konfiguriert sein.

Gehen Sie zu *System Options > Storage > SD Card > Encrypt* und legen Sie eine Passphrase fest. Die verwendete Verschlüsselung ist AES-128.

5. Unternehmensschutz

Bei mittleren und großen Organisationen, die ein professionelles Videoüberwachungssystem einsetzen, wird empfohlen, eine Video Management System (VMS) Software oder NVR zu verwenden. Die Unternehmensschutzstufe umfasst die Risikominimierung durch Reduzierung des möglichen Angriffsbereichs der Netzwerk-Kamera. Es ist wichtig, die Empfehlungen des VMS-Herstellers zur Cybersecurity zu befolgen.

Einige der Einstellungen, die in diesem Abschnitt beschrieben werden, werden bereits im Werk voreingestellt. Stellen Sie sicher, dass sie korrekt sind, indem Sie die Anweisungen unten befolgen.

5.1 Offene Ports

Als Referenz haben die Kameras die folgenden offenen Ports vorkonfiguriert.

Port	Service
TCP-21	FTP-Server
TCP-80	HTTP-Server
TCP-554	RTSP-Server
TCP-49152	UPnP (Discovery Protocol)
TCP-1900	UPnP Simple Service Discovery Protocol (SSDP)
UDP-3702	Web Service Dynamic Discovery
UDP-4815	Bonjour Discovery Protocol (mDNS)
UDP-57143	Bonjour (mDNSResponderPosix)

5.2 HTTP Digest Authentication

CSC #3: Sichere Konfiguration für Hard- und Software.
CSC #13: Datenschutz.

Um zu verhindern, dass Clients Login-Kennwörter in Klartext über das Netzwerk versenden, wird empfohlen, nur Digest Authentication (verschlüsselte Kennwörter) zuzulassen.

Gehen Sie zu *System Options > Users > Allow Password type* und wählen Sie Encrypted Only aus. Wenn Sie einen Client haben, der keine Digest Authentication unterstützt, sollten Sie Encrypted & Unencrypted auswählen.

5.3 Domain- und Host-Name

CSC #1: Verzeichnis autorisierter und nicht autorisierter Geräte.

Wenn Ihre Netzwerkinfrastruktur ein lokales Domain Name System (DNS) unterstützt, wird empfohlen, dass auf Kameras unter Verwendung eines Fully Qualified Domain Name (FQDN) anstelle ihrer IP-Adresse zugegriffen wird. Dies erleichtert die Verwaltung und Nachverfolgung der Kameras.

Gehen Sie zu *System Options > Network > Advanced > Host Name configuration*, um das System mit Ihrer DNS-Infrastruktur auszurichten.

5.4 Nicht genutzte Services deaktivieren

Auch wenn nicht genutzte Services keine unmittelbare Sicherheitsbedrohung darstellen, sollten sie deaktiviert werden, um unnötige Risiken zu reduzieren. Nachstehend einige Services, die deaktiviert werden können, wenn sie nicht genutzt werden:

5.4.1 FTP-Server

Der FTP-Server ist standardmäßig aktiviert und wird normalerweise zur erweiterten Wartung und Fehlersuche verwendet. Der FTP-Server sollte nach dem Einsatz der Kamera deaktiviert werden.

Bitte beachten Sie, dass bei neuerer Kamera-Firmware dieser Service standardmäßig deaktiviert sein kann. Wir empfehlen Ihnen, die Einstellungen zu überprüfen.

Gehen Sie zu *System Options > Network > Advanced > FTP.*

5.4.2 SSH – Secure Shell

Die Schnittstelle der SSH-Befehlszeile ist standardmäßig deaktiviert. SSH kann bei erweiterter Wartung und Fehlersuche nützlich sein, während des normalen Betriebs sollte SSH deaktiviert sein. Wir empfehlen Ihnen, dies sicherzustellen.

Gehen Sie zu *System Options > Plain Config* und wählen Sie die Gruppe Network. Das Kontrollkästchen für SSH befindet sich nahe an der Unterseite.

5.4.3 Zuweisen der IP-Adresse per ARP/Ping

ARP/Ping ist eine Möglichkeit, mit dem ein Administrator eine statische IP-Adresse einstellen kann, indem er einen Kommandozeilen-Terminal verwendet, um eine Kombination aus ARP/Ping und Befehl zu senden. Der Service ist nach Neustart der Kamera nur insgesamt zwei Minuten lang verfügbar. Dieser Service wurde bei neuerer Firmware entfernt. Haben Sie jedoch eine ältere Firmware, sollten Sie den Service vollständig deaktivieren.

Gehen Sie zu *System Options > Network > Basic unter dem Abschnitt Services.*

5.4.4 AXIS Device Dispatcher – AVHS

AVHS (AXIS Video Hosting Systems) ist ein cloudbasierter Videoverwaltungsservice. Durch Drücken der Steuertaste an der Kamera wird die Kamera beim Hosting Service Dispatcher registriert. Der Dispatcher gestattet einem Benutzer, der Zugriff auf die Kamera hat und den korrekten OAK (Owner Authentication Key) vorlegt, den Anspruch auf die Kamera. Damit die Kamera sich nicht mit dem Dispatcher verbindet, wenn die physikalische Steuertaste gedrückt wird, gehen Sie zu *System Options > Network > Basic* und entfernen Sie das Häkchen bei Enable AVHS.

Bitte beachten Sie, dass manche VMS-Anbieter eventuell Axis Device Dispatcher unterstützen, wenn Kameras im System eingesetzt werden. Fragen Sie beim Anbieter des VMS nach.

Lesen Sie mehr über AVHS unter **www.axis.com/products/hosted-video**

5.4.5 Netzwerk-Erkennungsprotokolle

Erkennungsprotokolle sind Unterstützungs-Services, die das Auffinden der Kamera und ihrer Services im Netzwerk erleichtern. Nach dem Einsatz, sobald die Geräte-IP-Adresse der Kamera bekannt ist und die Kamera zum VMS hinzugefügt ist, wird empfohlen, dass Sie das Erkennungsprotokoll deaktivieren, damit die Kamera aufhört, ihre Präsenz im Netzwerk bekanntzugeben.

> UPnP (Universal Plug and Play)
Gehen Sie zu *System Options > Network > UPnP*

> Bonjour
Gehen Sie zu *System Options > Network > Bonjour*

> Link-local address (Zero Conf)
Gehen Sie zu *System Options > Network > Advanced Link-Local IPv4 Address*
Hinweis: Nach Deaktivierung des Erkennungsprotokolls ist die Kamera auch für Axis Tools nicht mehr auffindbar.

5.4.6 SOCKS

SOCKS ist standardmäßig deaktiviert und wird nur für spezielle Zwecke verwendet, damit die Kamera Netzwerk-Services (z. B. HTTP- oder FTP-Bilder-Upload) auf der anderen Seite einer Firewall/eines Proxy-Servers erreichen kann.

Gehen Sie zu *System Options > Network > SOCKS*

5.4.7 Always Multicast-Video

Always Multicast-Video ist standardmäßig deaktiviert. Dieser Service wird in bestimmten Umgebungen verwendet, um Video über ein lokales Netzwerk zu übertragen, ohne dass Clients Multicast-Video anfordern.

Gehen Sie zu *System Options > Network > RTP > Multicast*

5.4.8 QoS – Quality of Service

Wenn die Netzwerkinfrastruktur QoS nicht unterstützt, gehen Sie zu *System Options > Network > QoS* und stellen Sie alle DCSP-Einstellungen auf 0.

Gehen Sie zu *System Options > Network > QoS*

5.5 IP-Adressfilter (IP-Tabellen)

CSC #1: Verzeichnis autorisierter und nicht autorisierter Geräte
CSC #13: Datenschutz.
CSC #15: Zugriff beschränken auf notwendige Informationen.

Die Aktivierung der IP-Filterung nur für autorisierte Clients verhindert, dass die Kamera auf Netzwerktraffic anderer Clients antwortet. Stellen Sie sicher, dass Sie alle autorisierten Clients (VMS-Server und administrative Clients) zur Positivliste hinzufügen.

Gehen Sie zu *System Options > Security > IP Address Filter*

5.6 HTTPS-Verschlüsselung

CSC #13: Datenschutz.

HTTPS verschlüsselt den Datenaustausch zwischen dem Client und der Kamera. Es wird empfohlen, HTTPS für alle administrativen Aufgaben an der Kamera zu verwenden. Bitte beachten Sie, dass die Aktivierung von HTTPS nicht automatisch Video verschlüsselt, das über RTP/RTSP gesendet wird. Wenn Video als beschränkt zugänglich klassifiziert wird und durch Verschlüsselung geschützt werden soll, muss der Video-Client RTP/RTSP-Video anfordern, das über HTTPS getunnelt wird. Dies wird vom Video-Client/VMS gesteuert.

Ein selbstsigniertes Zertifikat bietet eine angemessene Verschlüsselung, schützt aber nicht vor einem Man-in-the-Middle-Angriff. Clients (z. B. Webbrowser) werden davor warnen, dass das Zertifikat nicht vertrauenswürdig ist.

Ein CA-signiertes Zertifikat (privater oder öffentlicher CA) wird benötigt, damit der Client authentifiziert, dass er auf die korrekte Kamera zugreift. Dadurch wird das Risiko gemindert, dass ein angreifender Computer sich als Kamera ausgibt.

6. Managed Enterprise Protection (Gelenkter Unternehmensschutz)

Managed Enterprise Networks sind Systeme, die zusätzliche Tools und Services für die Ausrichtung der Kamera bieten.

6.1 Netzwerkzugriffskontrolle auf Basis von IEEE 802.1X

CSC #1: Verzeichnis autorisierter und nicht autorisierter Geräte.
CSC #13: Datenschutz.

Um in einer Netzwerkinfrastruktur akzeptiert zu werden, die durch IEEE 802.1X geschützt wird, müssen die Kameras geeignete Zertifikate und Einstellungen haben.

Gehen Sie zu *System Options > Security > Certificates* um Zertifikate zu verwalten und das CA-Root-Zertifikat zu installieren.
Gehen Sie zu System Options > Security > IEEE 802.1X

6.2 SNMP-Überwachung

CSC #14: Wartung, Überwachung und Analyse von Audit-Logs.

Axis-Kameras unterstützen die folgenden SNMP-Protokolle:

> SNMP v1: Wird nur wegen Abwärtskompatibilität unterstützt und sollte nicht mehr verwendet werden.

> SNMP v2c: Kann in einem geschützten Netzwerksegment verwendet werden.

> SNMP v3: Empfohlen für Überwachungszwecke.

Die Kameras unterstützen MIB-II und Axis Video MIB. Axis Video MIB kann heruntergeladen werden unter
www.axis.com/support/downloads/axis-video-mib

Weitere Informationen über SNMP finden Sie in der Bedienungsanleitung.

6.3 Remote System Log

CSC #4: Kontinuierliche Bewertung und Beseitigung von Schwachstellen.
CSC #6: Wartung, Überwachung und Analyse von Audit-Logs.
CSC #16: Kontoüberwachung und -kontrolle.
CSC #18: Reaktion auf und Verwaltung von Ereignissen.

Ein Syslog-Server sammelt alle Log-Meldungen der Kameras. Dies vereinfacht Audits und verhindert, dass Log-Meldungen in der Kamera verloren gehen, entweder absichtlich/heimtückisch oder unbeabsichtigt (durch einen Neustart der Kamera, der durch das Erreichen der maximalen Log-Größe verursacht wird).

Um Remote Syslog zu aktivieren, muss eine Kamera-Konfigurationsdatei bearbeitet werden.*Gehen Sie zu System Options > Advanced > Scripting > Open Script Editor und editieren Sie je nach Firmware-Version die folgende Datei:*

Kamera-Firmware bis Version 5.70
Wählen Sie mit dem eingebauten Script-Editor die Datei /etc/rsyslog.conf aus, und fügen Sie unten eine Zeile hinzu, die die IP-Adresse des Syslog-Servers enthält (z. B. *.*@10.2.0.2).

Kamera-Firmware 5.80 und höher
Eine Textdatei mit einer Zeile, die die IP-Adresse des Syslog-Servers enthält (z. B. *.*@10.2.0.2) muss unter /etc/rsyslog.d/40-remote-log.conf hinzugefügt werden.

Über dieses Dokument

Diese Richtlinie dient zum Härten von Axis Netzwerk-Kameras. Sie kann außerdem Einsatz-Teams, die sich mit lokalen Netzwerk-Strategien, Konfigurationen und Spezifikationen beschäftigen, als zusätzliche Sicherheit dienen.

Alle Einstellungen, die in diesem Dokument beschrieben werden, sind auf der Website des Produkts verfügbar. Die entsprechende Webadresse finden Sie im Benutzerhandbuch des jeweiligen Produkts.

Dieses Dokument wurde sorgfältig erstellt. Wenn Sie Unrichtigkeiten oder Auslassungen feststellen, informieren Sie bitte Ihre nächstgelegene Axis-Niederlassung. Axis Communications AB übernimmt keinerlei Haftung für technische oder typographische Fehler in diesem Dokument und behält sich das Recht vor, jederzeit ohne vorherige Ankündigung Änderungen am Produkt und an den Handbüchern vorzunehmen.

Axis Communications AB übernimmt keinerlei Garantie für den Inhalt dieses Dokuments. Dies gilt auch für die eingeschlossene Gewähr bezüglich der Handelsfähigkeit und Zweckdienlichkeit, ist aber nicht darauf beschränkt.

Axis Communications AB ist nicht für direkte oder indirekte Folgeschäden haftbar oder verantwortlich, die in Verbindung mit der Ausstattung, der Leistung und dem Einsatz dieses Produkts entstehen. Dieses Produkt darf nur für seinen vorgesehenen Zweck verwendet werden.

Schutz- und Urheberrechte

Kontaktinformationen

Axis Communications AB
Emdalavägen 14
223 69 Lund
Schweden
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30

www.axis.com

Support

Wenn Sie technische Unterstützung benötigen, wenden Sie sich bitte an Ihren Axis Händler. Wenn Ihre Fragen nicht sofort beantwortet werden können, leitet Ihr Händler Ihre Anfragen an die entsprechenden Stellen weiter, damit Sie umgehend Unterstützung erhalten.

Wenn Sie mit dem Internet verbunden sind, können Sie:

> Benutzerdokumentationen und Software-Aktualisierungen herunterladen.

> Antworten auf bereits gelöste Probleme in der FAQ-Datenbank finden. Sie können eine Suche auf der Grundlage eines Produkts, einer Kategorie oder eines Ausdrucks durchführen.

> Axis-Supportmitarbeiter über Probleme informieren, indem Sie sich in Ihrem persönlichen Supportbereich anmelden.

> mit Axis Supportmitarbeitern chatten.

> den Axis-Support unter **www.axis.com/techsup** besuchen.

70425/DE/R1/1705

Informationen zu Axis Communications

Axis bietet intelligente Sicherheitslösungen für den Schutz und die Sicherheit von Menschen, Unternehmen und Institutionen. Ziel von Axis ist es, zu einer sicheren, stabilen Welt beizutragen. Als Marktführer im Bereich Netzwerk-Video sorgt Axis durch die kontinuierliche Entwicklung innovativer Netzwerkprodukte für den technischen Fortschritt in der Branche. Die Axis-Produkte basieren allesamt auf einer offenen Plattform. Axis legt größten Wert auf die langfristigen Beziehungen mit seinen weltweiten Partnern und versorgt diese mit wegweisenden Netzwerkprodukten und technischem Know how für etablierte und neue Märkte. Die Kunden profitieren von diesem globalen Partnernetzwerk.

Axis beschäftigt über 2.700 engagierte Mitarbeiter in mehr als 50 Ländern und arbeitet mit über 90.000 Partnern zusammen. Das 1984 gegründete schwedische Unternehmen ist an der NASDAQ Stockholm unter dem Tickersymbol AXIS notiert.

Weitere Informationen über Axis finden Sie unter www.axis.com.

AXIS® COMMUNICATIONS