Rahmenbedingungen und Praktiken für die Cybersicherheit bei Axis

Januar 2024, Version 1.1

AXIS COMMUNICATIONS

Inhaltsverzeichnis

1. Einführung

Kunden in der Informations-, Technologie- und Sicherheitsbranche benötigen die Gewissheit, dass die in ihrem Unternehmen implementierten Lösungen sicher und vertrauenswürdig sind. Die Zugänglichkeit von Systemen und Daten muss für vorgesehene Nutzer gewährt und auf diese beschränkt sein; Geräte müssen im Netzwerk ohne Eingriff oder unbeabsichtigte Gefährdung betrieben werden können. Die Lösung muss den beabsichtigten Zweck erfüllen; Integrität und ununterbrochene Funktionalität müssen gewährleistet sein.

Zugleich gilt es, ständig vorhandene Sicherheitsbedrohungen zu berücksichtigen. Diese entstehen ständig neu und ihr Charakter kann sich jederzeit ändern.

Axis Communications hat sich der Gewährleistung von Unternehmenssicherheit verschrieben und stellt Prozesse und Verfahren zur kontinuierlichen Eindämmung von Sicherheitsbedrohungen bereit. Alle Mitarbeiter erhalten Schulungen zum Thema Sicherheitsbewusstsein und Sorgfaltspflicht.

Mit diesem Dokument möchten wir Ihnen einen Einblick in unsere Rahmenbedingungen und Praktiken für Cybersicherheit geben, die einen systematischen Ansatz zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit unserer Vermögenswerte schaffen.

2. Rahmenbedingungen für die Cybersicherheit

Das Axis Information Security Management System (ISMS) ist die Grundlage der Rahmenbedingungen für Cybersicherheit. Das ISMS basiert auf den Anforderungen der Norm ISO 27001:2022 und ermöglicht eine kontinuierliche Verbesserung und Überwachung der Sicherheitssituation bei Axis. Das ISMS ist für den im Zertifikat definierten Umgang nach ISO 27001:2022 zertifiziert.

Als Teil des ISMS hat Axis Rahmenbedingungen für die Kontrolle der Cybersicherheit implementiert, die auf den Kontrollen laut ISO 27002 basieren. Sowohl das ISMS als auch die damit verbundenen Sicherheitskontrollen werden jährlich von einer externen akkreditierten Zertifizierungsstelle überprüft, um die Einhaltung der Norm ISO 27001 nachzuweisen. Darüber hinaus führt Axis interne Audits des ISMS gemäß einem jährlichen Auditplan durch, der intern von der Geschäftsleitung beschlossen wird.

2.1 Informationssicherheitspolitik

Die Informationssicherheitspolitik legt die Gesamtrichtung der Sicherheitsarbeit von Axis fest. Die Informationssicherheitspolitik ist für alle Mitarbeiter, Zeitarbeitskräfte und Berater sowie Mitglieder der Geschäftsführung und des Vorstands obligatorisch.

Die Informationssicherheitspolitik wird durch detailliertere unterstützende Dokumente wie Richtlinien, Routinen und die Sicherheitsrichtlinien von Axis ergänzt (mehr hierüber erfahren Sie in Kapitel 3). Die Informationssicherheitspolitik und die ihr zugrunde liegenden Dokumente werden jährlich überprüft und/oder im Falle von Änderungen der gesamten Geschäftsstrategie oder dem Umfeld von Axis aktualisiert.

2.2 Funktionen und Verantwortlichkeiten

Die kontinuierliche Verbesserung der Sicherheit im Unternehmen wird durch mehrere Funktionen gewährleistet. Axis fördert einen kollaborativen Sicherheitsansatz und betont, dass allen Mitarbeitern hierbei eine wichtige Rolle zukommt. Beispiele für Funktionen und Organisationen, die sich der Sicherheit widmen, sind unter anderem:

> Chief Information Officer (CIO)
- trägt die Gesamtverantwortung für Informationssicherheit und Datenschutz bei Axis
- ist Teil des Unternehmensführungsteams und informiert den Vorstand über sicherheitsrelevante Angelegenheiten

> ISMS-Management-Team
- hat die Aufsicht über das ISMS

> Datenschutz-Team
- Ansprechpartner für Datenschutzangelegenheiten im Unternehmen

> IT-Governance
- entwickelt kontinuierlich die Methodik und Struktur rund um das Axis-ISMS weiter

> Gruppe für Software-Sicherheit (Software Security Group, SSG)
- Die SSG ist die zentrale interne Anlaufstelle für Entwicklungsorganisationen in sicherheitsrelevanten Fragen.
- Sie ist für das Sicherheitsentwicklungsmodell von Axis (Axis Security Development Model, ASDM) zuständig, ein Rahmenwerk für die von Axis genutzten Aktivitäten zur Entwicklung sichererer Software.
- Das ASDM ist die Komponente, die für die sichere Entwicklung innerhalb des ISMS steht.

> Security Operations Center (SOC)
- Ständige Überwachung zur Erkennung und Eindämmung von Cyberbedrohungen

3. Axis-Sicherheitsrichtlinien

Die Sicherheitsrichtlinien von Axis sind die zentrale Referenz für alle Sicherheitsanforderungen bei Axis und ein wichtiger Bestandteil der Informationssicherheitspolitik von Axis.

Um eine Sicherheitsrichtlinie festzulegen, hat Axis mehrere Bereiche unter Einbeziehung weltweit anerkannter Sicherheitsrahmen wie ISO 27001/2, NIST SP 800-53 sowie regulatorischer Anforderungen wie der DSGVO definiert. Nachfolgend finden Sie eine allgemeine Beschreibung der jeweiligen Bereiche und angewandten Praktiken.

3.1 Vermögensverwaltung und Informationsklassifikation

Informationsressourcen sind für Axis als Organisation von großem Wert und müssen angemessen geschützt werden. Axis verwaltet seine Vermögenswerte durch die Führung von Vermögensbeständen und die Klassifizierung von Vermögenswerten nach ihrer Kritikalität. Zu den Leitlinien der Vermögensverwaltung gehört ein Vermögensklassifizierungsschema mit definierten Klassifizierungsstufen. Die Klassifizierung von Vermögenswerten ist eine Voraussetzung für den effizienten Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Vermögenswerte.

Den identifizierten Vermögenswerten wird geschäftliches und technisches Eigentum zugeordnet und im Vermögensbestand dokumentiert. Die kontinuierliche Arbeit mit den Vermögensbeständen und deren Klassifizierung wird von hierfür zugeteilten Eigentümern erledigt.

3.2 Sicherung und Wiederherstellung

Die Sicherungs- und Wiederherstellungsverfahren dienen dem Schutz vor Verlust und der ausreichenden Wiederherstellung von Daten. Die Sicherung erfolgt je nach Verfügbarkeitsanforderungen der Daten mindestens täglich. Alle Backups werden auf einem sekundären Sicherungsspeicher gesichert.

Mithilfe der vorhandenen technischen Lösungen und Tools werden in regelmäßigen Abständen Wiederherstellungstests von Backups durchgeführt.

3.3 Geschäftskontinuitätsmanagement (Business Continuity Management, BCM)

Das Business Continuity Management (BCM) ist ein integraler Bestandteil von Axis. Es werden verschiedene Maßnahmen umgesetzt, um die Geschäftskontinuität sicherzustellen. Die Daten werden in primären und sekundären Rechenzentren an verschiedenen geografischen Standorten gespeichert, um Redundanz zu gewährleisten. Assets werden in einem Anlagenregister mit Kritikalitätsklassifizierungen und Anforderungen an Recovery-Zeitvorgaben (Recovery Time Objectives, RTO) und Wiederherstellungspunkte (Recovery Point Objective, RPO) dokumentiert.

Es bestehen Kommunikationspläne für die interne Kommunikation bei Problemen mit potenziellen Auswirkungen auf die Geschäftskontinuität. Die externe Kommunikation wird über die Statusseite von Axis, status.axis.com, verwaltet.

3.4 Kryptographie, Schlüssel- und Zertifikatsmanagement

Es werden Anforderungen für die ordnungsgemäße und effektive Nutzung und Verwaltung kryptografischer Schlüssel und der zugehörigen Zertifikate definiert, um eine sichere Kommunikation und Speicherung von Informationen zu gewährleisten.

Axis folgt den FIPS 140-3 (IEC/ISO 19790:2012)-Empfehlungen für die Algorithmusauswahl so weit möglich mit den folgenden Präferenzen:

> Verschlüsselung von Daten in Bewegung (TLS / mTLS) - RSA 2048 und höher
> Verschlüsselung von Daten im Ruhezustand - AES 256
> Digitales Signieren - RSA 2048 und höher, ECDSA p256 und höher mit SHA256 und höher

3.5 Identitäts- und Zutrittsmanagement

Durch das Identitäts- und Zugriffsmanagement (IAM) wird der Zugriff auf physische und logische Ressourcen auf autorisierte Benutzer beschränkt. Axis hat zahlreiche Sicherheitskontrollen und -praktiken im Zusammenhang mit IAM implementiert, sowohl präventiv als auch aufdeckend. Beispiele für Sicherheitskontrollen sind unter anderem:

> Benutzerregistrierungs-/-abmeldeprozess mit definierten Genehmigungsworkflows
> Automatisierter Prozess zum Offboarding/Deaktivieren des Active-Directory-Kontos von Ausscheidern
> Anwendung des Least-Privilege-Prinzips
> Multi-Faktor-Authentifizierung (MFA)
> Regelmäßige Überprüfung des Benutzerzugriffs
> Protokollierung und Überwachung von Benutzerzugriffen und -aktivitäten
> Privilegierte Kontoverwaltung
> Einmalige Anmeldung
> Fernzugriffsverwaltung (einschließlich VPN mit MFA)
> Aufgabentrennung

3.6 Störfallmanagement

Das Störfallmanagement ist für die Geschäftskontinuität von entscheidender Bedeutung. Axis hat einen Störfallmanagementprozess definiert, um die potenziellen Auswirkungen auf das Unternehmen und die Beteiligten im Falle eines Störfalls zu minimieren. Dazu gehören die Erkennung, Kommunikation, Koordination, Schadensbegrenzung und Lösung des Störfalls sowie das Lernen aus vergangenen Störfällen, um eine kontinuierliche Verbesserung zu ermöglichen.

Axis überwacht Systeme und Dienste aktiv mithilfe automatisierter Tools, um Anomalien und andere Hinweise auf mögliche Störfälle zu erkennen. Um rund um die Uhr eine Reaktion auf Störfälle gewährleisten zu können, hat Axis ein Security Operations Center (SOC) eingerichtet. Das SOC ist für die kontinuierliche Überwachung von Sicherheitsproblemen verantwortlich und greift ein, sobald Anomalien, Alarme oder Zero-Day-Schwachstellen erkannt werden.

Störfälle werden anhand der potenziellen Geschäftsauswirkungen klassifiziert, entsprechend eskaliert und im Störfallmanagement-System bis zur Lösung verfolgt. Für alle größeren Störfälle wird ein Störfallbericht dokumentiert, um die Grundursache zu klären und eine kontinuierliche Verbesserung der Sicherheitslage zu ermöglichen.

Für datenschutzbezogene Störfälle und potenzielle Verstöße gilt eine Routine zur Abwicklung von Datenschutzverletzungen. Diese umfasst Kommunikationskanäle, Eskalationspfade, Bewertung und Dokumentation. Die Routine basiert auf relevanten Datenschutzgesetzen und -vorschriften, vor allem der DSGVO.

Externe Informationen zu Störfällen und zum Status der Axis-Dienste finden Sie unter status.axis.com.

3.7 IT-Betriebssicherheit

Die IT-Betriebssicherheit umfasst Prozesse, Verfahren und Kontrollen zum Schutz der betrieblichen IT-Umgebung hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit. Dazu gehört bei Axis beispielsweise die Verwaltung von Kunden und Servern, die Durchführung des Änderungsmanagements nach einem strukturierten und systematischen Prozess sowie die Durchführung des Konfigurationsmanagements nach Best Practices und Absicherungshandbüchern.

Auch das Patch-Management ist ein wesentlicher Bestandteil der IT-Betriebssicherheit und wird im Rahmen eines definierten Lifecycle-Management-Prozesses verwaltet.

3.8 Netzwerksicherheit

Zum Schutz der Netzwerkkommunikation wurden verschiedene Maßnahmen zur Gewährung der Zugangskontrolle und Betriebssicherheit eingeführt.

Beispiele für Sicherheitskontrollen sind unter anderem:

> Rollenbasierter Netzwerkzugriff
> Für den Zugriff auf das Unternehmensnetzwerk ist ein Zertifikat (IEEE 802.1x) erforderlich.
> Netzwerksegmentierung
> Die Kommunikation zwischen Segmenten muss der Firewall-Richtlinie entsprechen.
> Kunden, die mit Produktionsnetzwerken verbunden sind, müssen über Endpunktschutz verfügen.
> Für den Remote-Netzwerkzugriff ist eine Verbindung über VPN mit Multi-Faktor-Authentifizierung erforderlich.
> Proaktive Überwachung des Netzwerkverkehrs und der Netzwerkausrüstung
> Netzwerkgeräte senden Protokolle an einen zentralen Datenspeicher.
> Änderungen an Netzwerkgeräten werden protokolliert.

3.9 Personalsicherheit

Bei der Personalsicherheit geht es darum, sicherzustellen, dass Mitarbeiter und externes Personal (Berater und Auftragnehmer) ihre Verantwortlichkeiten verstehen und für die ihnen zugedachten Funktionen geeignet sind.

Im Rekrutierungsprozess werden Richtlinien zur Sicherheit definiert. Dazu gehören Referenz- und Hintergrundüberprüfungen, abhängig von den regionalen Gesetzen und der Kritikalität der Funktion.

Der Prozess umfasst auch Sicherheitsmaßnahmen während und nach der Beschäftigung, wie z. B. Onboarding (Gewährung von physischem und logischem Zugriff), Geheimhaltungsvereinbarungen, Sensibilisierung und Schulung sowie Offboarding (Beendigung des physischen und logischen Zugriffs, wenn ein Benutzer das Unternehmen verlässt).

3.10 Physische Sicherheit

Spezielle Verfahren und Routinen sorgen für die Gewährleistung der physischen Sicherheit, die Schaffung einer sicheren Umgebung für alle, die auf dem Gelände von Axis arbeiten oder dieses besuchen und den Schutz der Vermögenswerte und Mitarbeiter von Axis.

Für den Zutritt zum Axis-Gelände sind eine Zugangskarte und ein PIN-Code erforderlich, und jeder, der sich auf dem Gelände aufhält, muss sichtbar einen Axis-Ausweis bei sich tragen. Jeder Zugang zum Gelände wird protokolliert. Die Protokolle werden an einen zentralen Datenspeicher gesendet. Auf dem gesamten Gelände sind Überwachungskameras installiert.

Besucher müssen sich stets an der Axis-Rezeption anmelden und dem Empfangs-/Serviceschalterpersonal ein offiziell anerkanntes Ausweisdokument vorlegen. Bei der Registrierung müssen Besucher stets sichtbar einen Besucherausweis bei sich tragen und dürfen das Axis-Gelände nur unter Begleitung betreten.

Das Axis-Gelände ist in verschiedene Sicherheitszonen unterteilt. Der Zugang zu Sperrbereichen ist auf autorisiertes Personal beschränkt.

3.11 Datenschutz

Axis stellt Schutzmaßnahmen und Mechanismen zum Schutz der personenbezogenen Daten von Mitarbeitern, Partnern und Kunden bereit. Im Mittelpunkt unserer Strategie stehen Vertrauen, unsere Stärke als Marke und transparente Beziehungen zu unseren Endkunden. Wir speichern die Daten unserer Endkunden, respektieren aber auch stets ihr Recht auf vollständige Kontrolle über ihre Daten im Einklang mit den geltenden Vorschriften und Verträgen.

Für die Erhebung und Verarbeitung personenbezogener Daten gelten folgende Grundprinzipien:

> fair und gesetzeskonform
> im nötigen Umfang
> für einen legitimen Zweck
> adäquat, relevant und für den Zweck notwendig

Weitere Informationen zu unseren Datenschutzverfahren unter www.axis.com/privacy

3.12 Fernarbeit

Axis hat Regeln und Sicherheitsprozesse zum Schutz von Geräten, die für Fernarbeit verwendet werden, beispielsweise auf Reisen oder bei der Arbeit im Homeoffice, definiert. Dies betrifft Systeme und Prozesse, die eine sichere und konforme Ausführung der Arbeit bei klarer Differenzierung zwischen geschäftlicher und nicht geschäftlicher Art gewährleisten.

Die Mitarbeiter werden in der Sicherheitsbewusstseinsschulung sowie durch die Richtlinien zur akzeptablen Nutzung in das Thema Fernarbeit eingewiesen. Um bei der Arbeit außerhalb des Büros auf interne Systeme und Ressourcen zugreifen zu können, muss sich jeder Benutzer über eine VPN-Verbindung mit Multi-Faktor-Authentifizierung authentifizieren.

Kunden und mobile Geräte sind verschlüsselt. Mobile Geräte werden über eine MDM-Lösung (Mobile Device Management) verwaltet, die bei Bedarf die Möglichkeit bietet, Daten aus der Ferne zu löschen.

3.13 Risikomanagement

Das Risikomanagement erfolgt gemäß einem jährlichen Risikomanagementzyklus, der von der Unternehmensführung gesteuert wird und sich über alle Geschäftsbereiche, einschließlich Sicherheit, erstreckt. Der Risikomanagementzyklus umfasst Risikobewertung, Risikoanalyse und Risikoverfolgung. Die Risikoanalyse wird dem Axis-Managementteam, dem Prüfungsausschuss und dem Vorstand vorgelegt.

Im Rahmen des unternehmensinternen Risikomanagementzyklus wird eine Richtlinie zur Risikobewertung der Informationssicherheit definiert und im ISMS angewendet. Dazu gehören kontinuierliche Risikobewertungen und Risikominderung durch Systembesitzer und Risikoverantwortliche im gesamten Unternehmen. Identifizierte Risiken werden bewertet und je nach Risikostufe entsprechend einer Risikobewertungsmatrix eskaliert. Der CIO trägt die Gesamtverantwortung für die Berichterstattung über Risiken an das Management und den Vorstand.

Der Ansatz, die Methodik und die Umsetzung des Informationssicherheitsrisikos werden jährlich im Rahmen des ISO-27001-Zertifizierungsprozesses extern geprüft.

3.14 Sichere Entwicklung

Um eine sichere Entwicklung unserer Produkte und Dienstleistungen zu ermöglichen, hat Axis das Axis Security Development Model (ASDM) definiert und implementiert. Die Hauptziele des ASDM sind:

> Integrierung der Softwaresicherheit in die Softwareentwicklung von Axis
> Reduzierung von sicherheitsrelevanten Geschäftsrisiken für Axis-Kunden
> Berücksichtigung des zunehmenden Bewusstseins von Kunden und Partnern für Sicherheitsaspekte
> Schaffung von Möglichkeiten zur Kostensenkung durch frühzeitige Erkennung und Lösung von Problemen

Das ASDM betrifft die gesamte Axis-Software aller Produkte und Lösungen von Axis. Weitere Informationen zum ASDM finden Sie unter help.axis.com/axis-security-development-model.

3.15 Sicherheitsbewusstsein und -training

Axis hat ein Sicherheitsbewusstseinsprogramm entwickelt, um unsere Mitarbeiter kontinuierlich darin zu schulen, Sicherheitsbedrohungen für das Unternehmen zu vermeiden und zu mindern.

Das Sensibilisierungsprogramm umfasst Sicherheitsbewusstseinsschulungen im Zusammenhang mit der Informationssicherheitsrichtlinie und gängigen Best Practices für die Sicherheit. Die Sensibilisierungsschulung ist für alle Axis-Vertreter obligatorisch.

Dazu gehört auch eine Sicherheitsschulung im Zusammenhang mit der physischen Sicherheit. Die Schulung ist für alle Mitarbeiter und Auftragnehmer, die das Gelände von Axis betreten, obligatorisch und muss durchgeführt werden, bevor der Person eine Zugangskarte für den Zutritt zum Gelände erteilt wird.

Abhängig von der Rolle und den Verantwortlichkeiten in der Organisation werden zusätzliche Sicherheitsschulungen durchgeführt, zum Beispiel ASDM für Entwickler (siehe Abschnitt 3.14 oben) und rollenspezifisches Bewusstsein für Systembesitzer.

3.16 Systembeschaffung und Lieferantenmanagement

Vor Vertragsabschluss wird eine Lieferantenprüfung durchgeführt. Dazu gehört die Bewertung des potenziellen Lieferanten anhand eines Bewertungsmodells, das eine rechtliche Prüfung, eine Sicherheitsbewertung und eine Datenschutzbewertung umfasst. Die Hauptverantwortung für die Überprüfung der Lieferanten obliegt den Vertragsmanagern und der Rechtsabteilung. Darüber hinaus werden verschiedene Experten innerhalb der Organisation hinzugezogen, beispielsweise Sicherheitsspezialisten.

Jeder Lieferant hat einen Vertragsinhaber, der die Gesamtverantwortung für die Überwachung der Lieferantenlieferung, die Erfüllung der Vertragsanforderungen und die regelmäßige Bewertung der Lieferantensicherheit trägt.

Beschaffte oder zu beschaffende Systeme und Dienstleistungen werden einer Bewertung unterzogen, um sicherzustellen, dass sie den Anforderungen von Axis entsprechen und Axis oder unseren Partner keinem inakzeptablen Risiko aussetzen. Diese Anforderungen sind in den Systembeschaffungsrichtlinien definiert und müssen vor Anschaffung eines neuen Systems oder einer neuen Dienstleistung berücksichtigt werden.

3.17 Threat Intelligence (Bedrohungsaufklärung)

Threat Intelligence ist die Sammlung von Informationen über das Auftreten und die Bewertung sowohl digitaler als auch physischer Bedrohungen und Bedrohungsakteure, um potenziellen Angriffen und schädlichen Ereignissen im Cyberspace entgegenzuwirken.

Es werden fortlaufend und über mehrere verschiedene Quellen Intelligence-Analysen und Bedrohungsinformationen durchgeführt.

Axis führt Bedrohungsanalysen im Zusammenhang mit der Überwachung von Zero-Day-Schwachstellen sowie bei der proaktiven Bereitstellung von Bedrohungsinformationen, beispielsweise durch die Teilnahme an Sicherheitsgemeinschaften, durch.

3.18 Schwachstellen-Management und Schadprogrammschutz

Verfahren zum Schwachstellenmanagement und zum Schutz vor Malware sorgen für die Anwendung geeigneter Tools und Methoden zur Bewertung und Eindämmung von Schwachstellen und Schadcodes in Systemen oder Anwendungen. Axis nutzt verschiedene Scan-Tools, um kontinuierlich interne und externe Schwachstellenscans unserer IT-Umgebung durchzuführen. Schwachstellen werden nach dem Common Vulnerability Scoring System (CVSS) klassifiziert und anhand ihrer Kritikalität priorisiert.

Mit dem Produktionsnetzwerk verbundene Geräte werden durch eine branchenführende Lösung zur Endpunkterkennung und -reaktion geschützt und überwacht.

In Bezug auf das Schwachstellenmanagement für unsere Produkte wendet Axis das Axis Security Development Model (siehe Abschnitt 3.14 oben) auf Software für den Lebenszyklus eines Produkts an. Axis ist eine autorisierte Common Vulnerability and Exposures (CVE) Numbering Authority (CNA) und legt Schwachstellen gemäß dem etablierten Rahmen des CVE-Programms auf transparente Weise offen. Weitere Einzelheiten zur Produktsicherheit und zum Schwachstellenmanagement finden Sie unter www.axis.com/support/cybersecurity/vulnerability-management und help.axis.com/axis-vulnerability-management-policy.

4. Zertifizierungen und Konformität

Axis erfüllt eine Vielzahl regulatorischer Anforderungen sowie strategisch ausgewählte Rahmenregelungen und Standards. Hierdurch beweisen wir unser Engagement für Informationssicherheit, Datenschutz und andere Bereiche, die sowohl für Axis als auch für unsere Partner wichtig sind.

Eine aktuelle Übersicht über entsprechende Zertifizierungen und Compliance finden Sie unter www.axis.com/compliance

Über Axis Communications

Axis ermöglicht eine smartere und sichere Welt durch die Entwicklung von Lösungen zur Verbesserung von Sicherheit und Geschäftsperformance. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte für die Videosicherheit und Zutrittskontrolle sowie Intercoms, Audiosysteme und intelligente Analyseanwendungen. Die branchenweit anerkannten Schulungen der Axis Communications Academy vermitteln fundiertes Expertenwissen zu den neuesten Technologien.

Das 1984 gegründete schwedische Unternehmen beschäftigt etwa 4.000 engagierte Mitarbeiterinnen in über 50 Ländern und bietet mit Technologie- und Systemintegrationspartnern auf der ganzen Welt kundenspezifische Lösungen an. Der Hauptsitz ist in Lund, Schweden.

Weitere Informationen über Axis finden Sie unter www.axis.com/de-de