WHITEPAPER

NIS 2

Juni 2024

Inhalt

1 Einführung

1.1 Was ist NIS 2?

NIS 2 ist eine EU-Richtlinie, die bis zum 17. Oktober 2024 in der nationalen Gesetzgebung aller EU-Mitgliedstaaten Berücksichtigung finden muss. Ziel der NIS 2 ist es, ein hohes gemeinsames Cybersicherheitsniveau in der gesamten EU zu erreichen, um zur Sicherheit der Region und zum effektiven Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen. Sie verpflichtet Einrichtungen, die wesentliche und kritische Dienste in Schlüsselbereichen der Gesellschaft bereitstellen, zum Aufbau von Cybersicherheitskapazitäten, zur Eindämmung von Bedrohungen für Netz- und Informationssysteme, zur Gewährleistung der ununterbrochenen Verfügbarkeit dieser Dienste bei Sicherheitsvorfällen und zur Meldung von Sicherheitsvorfällen an die zuständigen Behörden. Mitgliedstaaten werden verpflichtet, nationale Cybersicherheitsstrategien zu verabschieden sowie Behörden beispielsweise für das Cyberkrisenmanagement sowie Computer-Notfallteams einzurichten. Die Richtlinie legt Maßnahmen zum Cybersicherheitsrisikomanagement und zur Durchsetzung der Vorschriften dar. Die Folgen der Nichteinhaltung von Vorschriften durch wesentliche und wichtige Einrichtungen können hohe Geldstrafen und rechtliche Konsequenzen für die Führungsebene sein.

Weitere Informationen finden Sie auf:
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 Wer ist von NIS 2 betroffen?

NIS 2 betrifft alle Einrichtungen, die **wesentliche** oder **wichtige** Dienste für die europäische Wirtschaft und Gesellschaft erbringen, einschließlich Unternehmen und Zulieferer.

1.2.1 Direkt betroffen

Wesentliche Einrichtungen – Energie, Verkehr, Banken/Finanzwesen, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, öffentliche Verwaltung, Raumfahrt

Wichtige Einrichtungen – Postdienste, Abfallwirtschaft, Chemikalien, Lebensmittel, Produktion (z. B. medizinische Geräte, elektrische Geräte und Transport), digitale Anbieter (z. B. Online-Marktplätze, Suchmaschinen, soziale Netzwerke), Forschungsorganisationen

Zuständige nationale Behörden – Die zuständigen nationalen Behörden werden von den EU-Mitgliedstaaten benannt, um die Umsetzung und Durchsetzung der NIS 2 in ihrem jeweiligen Land zu überwachen.

1.2.2 Indirekt betroffen

Anbieter und Lieferanten – Die NIS-2-Richtlinie betrifft indirekt auch Anbieter, Lieferanten und Drittdienstleister, die wesentliche Dienste oder digitale Dienste für wesentliche und wichtige Einrichtungen erbringen. Diese Unternehmen müssen die Sicherheit ihrer Produkte und Dienste gewährleisten und unterliegen möglicherweise vertraglichen Cybersicherheitsanforderungen seitens ihrer Kunden.

Benutzer wesentlicher Dienste und digitaler Dienste – Obwohl nicht direkt in der NIS 2 geregelt, profitieren Benutzer wesentlicher Dienste und digitaler Dienste von den in der Richtlinie geforderten, verbesserten Cybersicherheitspraktiken und Reaktionsmöglichkeiten bei Vorfällen. Dies erhöht indirekt auch die Sicherheit und Zuverlässigkeit der von ihnen genutzten Dienste.

2 Anforderungen von NIS 2

2.1 Für wesentliche und wichtige Einrichtungen

Sicherheitsmaßnahmen – Umsetzung geeigneter Sicherheitsmaßnahmen zur Kontrolle von Risiken und zur Gewährleistung der Sicherheit der Netz- und Informationssysteme dieser Einrichtungen. Diese Maßnahmen sollten sich auf Risikobewertungen und bewährte Verfahren stützen.

Meldung von Vorfällen – Meldung relevanter Vorfälle, die erhebliche Auswirkungen auf die Sicherheit der Netz- und Informationssysteme dieser Einrichtungen haben könnten, an die zuständigen Behörden. Die umgehende Meldung ist für die Koordinierung von Maßnahmen und die Minderung potenzieller Schäden unerlässlich.

Risikomanagement – Durchführung von Risikobewertungen zur Ermittlung potenzieller Bedrohungen und Schwachstellen und Ergreifung von Maßnahmen zur Risikominderung.

Zusammenarbeit mit den zuständigen Behörden – Zusammenarbeit mit den von den EU-Mitgliedstaaten benannten zuständigen Behörden. Dies umfasst die Bereitstellung der erforderlichen Informationen und des Zugangs zu Systemen für Zwecke der behördlichen Aufsicht und der Reaktion auf Vorfälle.

Planung der Reaktion auf Vorfälle – Entwicklung und Pflege von Notfallplänen zur wirksamen Reaktion auf Cybersicherheitsvorfälle. In diesen Plänen sollten Verfahren zur Erkennung, Meldung und Eindämmung von Vorfällen beschrieben werden.

Sicherheit von Lieferketten – Sicherheit über die gesamte Lieferkette, einschließlich Drittanbieter und Zulieferer, um die allgemeine Widerstandsfähigkeit von Netzwerk und Informationssystemen zu gewährleisten.

Ständige Überwachung – Implementierung einer ständigen Überwachung und Prüfung von Netz- und Informationssystemen, um Bedrohungen und Schwachstellen in Echtzeit zu erkennen und darauf zu reagieren.

3 Auswirkungen auf die Lieferanten

Lieferanten können von NIS 2 betroffene Unternehmen unterstützen, indem sie die folgenden Anforderungen erfüllen:

Security by Design – Die Hersteller von IoT-Geräten sollten bereits in der Projektierungsphase Sicherheitsfunktionen in ihre Geräte integrieren und so dafür Sorge tragen, dass Sicherheit ein integraler Bestandteil des Produkts ist.

Regelmäßige Updates und Patches – Hersteller sollten regelmäßig Sicherheitsupdates und Patches bereitstellen, um Schwachstellen in ihren IoT-Geräten zu beheben.

Authentifizierung und Autorisierung – IoT-Geräte sollten starke Authentifizierungsmechanismen und angemessene Autorisierungskontrollen verwenden, um unbefugten Zugriff zu verhindern.

Datenverschlüsselung – Die Übertragung und Speicherung von Daten durch IoT-Geräte sollte verschlüsselt erfolgen, um sensible Informationen vor dem Abfangen oder dem Zugriff durch Unbefugte zu schützen.

Meldung von Vorfällen – Hersteller sollten den zuständigen Behörden sowie gegebenenfalls Verbrauchern oder Kunden alle relevanten Sicherheitsvorfälle oder -verstöße im Zusammenhang mit ihren IoT-Geräten melden.

Überlegungen zum Datenschutz – IoT-Geräte, die personenbezogene Daten verarbeiten, müssen neben den Datenschutzvorgaben von NIS 2 auch die DSGVO (Datenschutz-Grundverordnung) erfüllen.

Sicherheit der Lieferkette – Die Sicherheit muss über die gesamte Lieferkette von den Zulieferern bis zu den Kunden gewährleistet sein, um zu verhindern, dass an irgendeiner Stelle des Produktionsprozesses Schwachstellen eingebracht werden.

4 Die Antwort von Axis

Im Folgenden wird erläutert, wie Axis als Lieferant die Anforderungen für von der NIS-2-Richtlinie betroffene Unternehmen erfüllt:

4.1 Security by Design

Das Prinzip „Security by Design" soll sicherstellen, dass Sicherheitsüberlegungen und -praktiken bereits integraler Bestandteil der Projektierung und Entwicklung von Produkten sind, um das Risiko von Schwachstellen zu verringern und zu gewährleisten, dass Produkte standardmäßig robuste Sicherheitskonfigurationen nutzen. Bei Axis gilt das Security-by-Design-Prinzip für Soft- und Hardware gleichermaßen und wird durch die folgenden Hauptelemente abgedeckt:

- *Axis Security Development Model (ASDM)*: ASDM ist ein Rahmenwerk aus definierten Prozessen und Tools, die sicherstellen, dass Sicherheitsaspekte ein integraler Bestandteil der Softwareentwicklung sind. Zu den Praktiken gehören die Bewertung von Risiken, die Erstellung von Bedrohungsmodellen, Penetrationstests, Schwachstellenscans, das Vorfallmanagement sowie ein Bug-Bounty-Programm. Die Softwareentwickler von Axis gewährleisten mit ASDM, dass Sicherheit bereits in die Grundstruktur einer Software integriert wird, um die Gefahr der Veröffentlichung von Software mit Schwachstellen zu verringern.
- *Bug-Bounty-Programm*: Axis unterstützt ein privates Bug-Bounty-Programm ergänzend zu den eigenen Bemühungen um eine proaktive Identifizierung sowie das Patchen und Aufdecken von Schwachstellen in AXIS OS, dem Linux-basierten Betriebssystem, auf dem die meisten Axis Produkte laufen. Es stärkt das Engagement von Axis, professionelle Beziehungen zu externen Sicherheitsforschern und ethischen Hackern aufzubauen.
- *Software-Bestandsliste (SBOM)*: Axis bietet eine SBOM für AXIS OS, das Linux-basierte Betriebssystem, das in den meisten Axis Geräten verwendet wird. Sie bietet Sicherheitsforschern, Behörden und Kunden Einblicke in die Softwarekomponenten von AXIS OS. Dabei hilft sie besonders all denjenigen, die sich auf die Bewertung von Schwachstellen und die Analyse von Bedrohungen spezialisiert haben, und zeigt den Einsatz von Axis für Transparenz in der Cybersicherheit.
- *Standard-Sicherheitseinstellungen von AXIS OS*: Geräte mit den neuesten Versionen von AXIS OS sind in der werksseitigen Standardeinstellung wie folgt vorkonfiguriert: kein Standardkennwort, HTTP und HTTPS aktiviert, sicheres Onboarding und sichere Kommunikation mit standardmäßiger Aktivierung von IEEE 802.1X/802.1AR/802.1AE und weniger sichere Protokolle deaktiviert. Weitere Informationen über die Standard-Schutzmaßnahmen finden Sie *hier*.
- *Axis Edge Vault*: Axis Edge Vault ist eine in Axis Geräte integrierte hardwarebasierte Sicherheitsplattform mit Funktionen, die die Integrität der Netzwerkprodukte von Axis schützen und die Ausführung von sicheren, auf kryptografischen Schlüsseln basierenden Operationen ermöglichen. Es bietet Schutz für die gesamte Lieferkette durch sicheres Booten und ein signiertes Betriebssystem, eine vertrauenswürdige Gerätekennung mit der integrierten eindeutigen Axis Geräte-ID zum Nachweis der Herkunft des Geräts,

einen sicheren Schlüsselspeicher zur manipulationsgeschützten Speicherung von kryptografischen Informationen und Video-Manipulationserkennung mit signiertem Video.

4.2 Regelmäßige Updates und Patches

Axis stellt Software-Updates zur Verfügung, um unter anderem neu festgestellte Schwachstellen in seinen Hardware- und Softwareprodukten zu beheben. Außerdem bietet Axis Tools zur Geräteverwaltung, die es Kunden erleichtern, die Software auf Geräten von Axis auf dem neuesten Stand zu halten. In AXIS Companion, AXIS Camera Station und Partnerlösungen für Video Management Software wie Milestone XProtect® und Genetec™ Security Center sowie in Axis Tools zur Geräteverwaltung wird auf neue Versionen von AXIS OS für vernetzte Geräte hingewiesen. Darüber hinaus bietet Axis einen Benachrichtigungsdienst zum Thema Sicherheit an, den jeder abonnieren kann. Ausführlichere Informationen erhalten Sie weiter unten.

- *AXIS OS*: Axis bietet zwei Hauptalternativen, um die Gerätesoftware auf dem neuesten Stand zu halten: den aktiven Track (Active Track) und den Track für langfristigen Support (Long Term Support, LTS). Der aktive Track bietet Zugriff auf die neuesten Features und Funktionen sowie Bugfixes und Sicherheitspatches. Die Software-Tracks für den langfristigen Support (LTS) maximieren die Stabilität, indem sie sich auf die Aufrechterhaltung eines gut integrierten Drittanbietersystems durch die Bereitstellung von Bugfixes und Sicherheitspatches konzentrieren.
- Tools zur Geräteverwaltung: *AXIS Device Manager* und *AXIS Device Manager Extend* sind Tools, die Kunden dabei unterstützen, die Software Ihrer Axis Geräte mit den neuesten Sicherheitspatches und Bugfixes auf dem aktuellsten Stand zu halten.

  Für die effiziente lokale Konfiguration und Verwaltung von Axis Geräten ermöglicht AXIS Device Manager die Stapelverarbeitung von Sicherheitsaufgaben wie die Verwaltung von Gerätezugangsdaten, die Herausgabe von Zertifikaten, die Deaktivierung nicht genutzter Dienste und die Aktualisierung von AXIS OS.

  AXIS Device Manager Extend bietet ein aggregiertes Dashboard, das Informationen über alle Ihre Geräte und Standorte in einer einheitlichen, benutzerfreundlichen Anwendung zusammenfasst. Sie werden informiert, wenn Upgrades für die Gerätesoftware verfügbar sind, und Sie können Upgrades und andere Aufgaben in Massenbearbeitung ausführen. Außerdem erhalten Sie Empfehlungen zu Ersatzprodukten. Aktivitäten sind vollständig nachverfolgbar und alle Systemgeräteinformationen können zu Berichts- oder Auditzwecken exportiert werden.
- *Benachrichtigungsdienst zum Thema Sicherheit von Axis*: Dieser Dienst, dessen Nutzung Axis empfiehlt, informiert Abonnenten zeitnah über Sicherheitsvorfälle und Schwachstellen.

4.3 Authentifizierung und Autorisierung

Um unbefugten Zugriff zu verhindern und die allgemeine Sicherheit von Axis Geräten zu erhöhen, unterstützt Axis Folgendes:

- Rollenbasierte Zugriffsrechte für die Geräteverwaltung (Administrator/Bediener/Betrachter) und die Möglichkeit, die Authentifizierung/Autorisierung durch Integration von Axis Geräten in den IT-standardisierten *Active Directory Federation Service* (ADFS) zu zentralisieren. (ADFS ist eine Softwarekomponente, die von Microsoft entwickelt wurde, um Anwendern auf Windows-Server-Betriebssystemen einen Single-Sign-On-Autorisierungsdienst (SSO) zur Verfügung zu stellen. ADFS ermöglicht es Anwendern über Unternehmensgrenzen hinweg, mit einem einzigen Satz von Zugangsdaten auf Anwendungen auf Windows-Server-Betriebssystemen zuzugreifen).

- Technologien zur Vereinfachung von *Zero-Trust-Netzwerken*. In den neuesten Versionen von AXIS OS umfassen diese Technologien u. a. IEEE 802.1X sowie IEEE 802.1AR-kompatiblen Axis Geräte-IDs für das automatische und sichere Onboarding von Geräten bei einem IEEE 802.1X-Netzwerk sowie IEEE 802.1AE (MACsec) für die automatische Verschlüsselung der Datenkommunikation.

4.4 Datenverschlüsselung

Um sensible Informationen vor dem Abfangen oder dem Zugriff durch Unbefugte zu schützen, unterstützen Axis Produkte Folgendes:

- HTTPS, wobei die gesamte Datenkommunikation TLS 1.2 oder neuere Standards unterstützt. Die Video-Stream-Verbindung zwischen dem Server der AXIS Camera Station Video Management Software und dem Client ist AES-256-verschlüsselt.
- *IEEE 802.1AE (MACsec)* zur automatischen Verschlüsselung der Datenkommunikation.
- Sicheres Video-Streaming über RTP, auch SRTP/RTSPS genannt (ab AXIS OS 7.40). SRTP/RTSPS nutzt ein sicheres, durchgehend verschlüsseltes Datenübertragungsverfahren, um sicherzustellen, dass nur autorisierte Clients den Videostream vom Axis Gerät empfangen.
- *Verschlüsselung lokaler Speicher* (Edge-Storage-SD-Speicherkarte)
- *Kennwortverschlüsselter Export lokal aufgezeichneter Daten* (SD-Speicherkarte, Netzwerkfreigabe) ab AXIS OS 10.10. Das heißt, dass mit einem Kennwort verschlüsselte Aufzeichnungen exportiert werden können, was darüber hinaus das sichere Teilen sensibler Videodaten ermöglicht, ohne dass exportierte Aufzeichnungen manuell verschlüsselt werden müssen.

4.5 Meldung von Vorfällen

Axis meldet Sicherheitsvorfälle oder Schwachstellen, die in unseren Produkten und Diensten entdeckt wurden.

- Axis ist eine Common Vulnerabilities and Exposures (CVE) Numbering Authority. Das bedeutet, dass Axis beim Umgang mit und der Reaktion auf entdeckte Schwachstellen in unseren Produkten und Diensten transparent die bewährten Methoden der Branche anwendet, um das Schadensrisiko für Kunden zu minimieren. Darüber hinaus kann Axis neu entdeckten Schwachstellen CVE-Nummern zuweisen und meldet diese auf der Website *www.cve.org*. Die Axis *Vulnerability Management Policy* steht auf axis.com zur Verfügung.
- Jeder kann sich *hier* anmelden, um eine Sicherheitsbenachrichtigung von Axis zu erhalten.
- Sicherheitspatches und Bugfixes werden mit den neuen Versionen von AXIS OS bereitgestellt. Außerdem wird in AXIS Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend und VMS von Drittanbietern wie Milestone XProtect und Genetec Security Center auf verfügbare Gerätesoftware-Updates hingewiesen.
- Axis verpflichtet sich zur Transparenz in Bezug auf alle unternehmensbezogenen Cyberangriffe und meldet diese Vorfälle gemäß den Vorgaben der zuständigen schwedischen Behörden.

4.6 Überlegungen zum Datenschutz

Axis veröffentlicht seine *Datenschutzrichtlinie* und -hinweise online und legt in diesen dar, welche personenbezogenen Daten erhoben (z. B. von einem Online-Konto bei My Axis) und wie diese verwendet werden.

Außerdem hat Axis seine *Rahmenbedingungen und Praktiken für die Cybersicherheit* veröffentlicht, worin es auf sein ISO/IEC 27001-zertifiziertes Information Security Management System eingeht. Der Geltungsbereich des ISO/IEC 27001-Zertifikats von Axis umfasst die Entwicklung und den Betrieb interner IT-Infrastrukturen und IT-Dienste. ISO 27001 ist eine international anerkannte Norm mit Leitlinien für den Schutz und die Verwaltung von Unternehmensinformationen durch ein effektives Risikomanagement.

Die Konformität mit der *ISO/IEC 27001* verdeutlicht, dass Axis beim Management seiner internen Informationsinfrastruktur und der Systeme zur Unterstützung und Erbringung seiner Services für Kunden und Partner international anerkannte Prozesse und bewährte Praktiken anwendet.

Zudem unterstützt Axis Kunden dabei, bei der Überwachung Datenschutzbedenken im Hinblick auf Video- und Audioaufnahmen auszuräumen. Lösungen hierfür umfassen:

- Statische Maskierung sensibler Bereiche bei Axis Kameras und dynamische Maskierung mit der Software-Anwendung *AXIS Live Privacy Shield*
- Edge-basierte Analysen wie die Anwendung *AXIS People Counter* oder *AXIS P8815-2 3D People Counter*, die nur statistische numerische Daten erfassen und speichern, ohne Verarbeitung von Daten, die einen Rückschluss auf Personen zulassen
- *Wärmebildkameras*
- *Radar-Produkte*
- Tool zur Anonymisierung von Videos in *AXIS Camera Station* zur Maskierung von Objekten oder Bereichen, die nicht von Interesse sind
- *Standardmäßig deaktivierte Audio-Funktionen* in Axis Videosicherheitsprodukten

Weitere Informationen zu Datenschutzlösungen finden Sie auf: *axis.com/solutions/privacy-in-surveillance*

4.7 Sicherheit der Lieferkette

Der Schutz der gesamten Lieferkette von den Zulieferern bis zu den Kunden ist wichtig, um das Entstehen von Schwachstellen zu verhindern.

Axis verfolgt beim Thema Cybersicherheit für Produkte einen *Lebenszyklusansatz*. Wir verpflichten uns zur Risikominderung, und zwar nicht nur in der gesamten Lieferkette von der Komponente bis zum fertigen Produkt, sondern auch während der Vertriebs- und Implementierungsphase über die Nutzungsphase bis hin zur Stilllegung.

Im Folgenden finden Sie einige Beispiele dafür, wie Axis die Sicherheit der Lieferkette gewährleistet:

- Axis bezieht wichtige Komponenten direkt von strategischen Lieferanten. Wir arbeiten eng mit unseren Partnern in der Produktion zusammen. Die Produktionsprozesse werden überwacht und die Daten werden rund um die Uhr an Axis übermittelt, was Analysen in Echtzeit ermöglicht und für Transparenz sorgt. Erfahren Sie mehr über die *Sicherheit der Lieferkette von Axis*.
- Integrierte Gerätesicherheit durch Axis Edge Vault, das die Integrität von Axis Geräten durch die folgenden Features schützt:

- **Signiertes Betriebssystem**: Garantiert, dass das installierte AXIS OS wirklich von Axis stammt. So lässt sich auch sicherstellen, dass jedes neue AXIS OS, das auf dem Gerät installiert werden soll, ebenfalls von Axis signiert wurde.

- **Sicheres Booten**: Versetzt das Gerät in Lage zu prüfen, ob das Betriebssystem über eine Axis Signatur verfügt. Wenn das Betriebssystem nicht autorisiert ist oder verändert wurde, wird der Systemstart abgebrochen und das Gerät schaltet sich ab. Die Kombination von signiertem Betriebssystem, sicherem Booten und Zurücksetzen des Geräts auf Werkseinstellungen bietet Schutz vor Manipulationsversuchen während des Geräteversands.

- Die **Axis Geräte-ID** ist IEEE 802.1AR-konform und ermöglicht die sichere Identifizierung von Geräten und das Onboarding in einem Netzwerk. Die Axis Geräte-ID wird im sicheren Schlüsselspeicher des Geräts (sicheres Element, TPM, TEE) gespeichert.

- **Verschlüsseltes Dateisystem:** Schützt die kundenspezifische Konfiguration und die im Dateisystem gespeicherten Informationen davor, extrahiert oder manipuliert zu werden, wenn das Gerät nicht benutzt wird. Dies ist zum Beispiel beim Versand von einem Systemintegrator zu einem Kunden der Fall.

- Darüber hinaus erlaubt die Unterstützung von **signiertem Video** durch Axis dem Betrachter zu überprüfen, ob das von einem Gerät exportierte Video manipuliert wurde. Dies ist besonders wichtig bei einer Täter-Ermittlung oder Strafverfolgung. Weitere Informationen erhalten Sie auf *axis.com/solutions/edge-vault*.

- Für Software-Downloads von axis.com ist eine Prüfsumme verfügbar. Mit dieser lässt sich die Integrität einer Datei überprüfen.

- ETSI-Zertifizierung: Mehr als 150 Axis Produkte mit AXIS OS 11 oder höher sind nach der *Cybersicherheitsnorm ETSI EN 303 645* zertifiziert. ETSI steht für „European Telecommunications Standards Institute". Diese Anforderungen beziehen sich auf die Geräte selbst, einschließlich Unterstützung für Hardware-basierte Sicherheitsfunktionen wie sichere Schlüsselspeicher, ebenso wie auf Standard-Sicherheitsfunktionen wie standardmäßig aktiviertes HTTPS und keine Verwendung von Standardkennwörtern. Ein weiterer Aspekt betrifft das Lebenszyklus-Management, wie etwa einen festgelegten Support-Zeitraum für Sicherheits-Updates für die Geräte. Weitere Anforderungen sind beispielsweise ein Verfahren zur Reduzierung der Gefahr von Schwachstellen, eine transparente Schwachstellenmanagement-Richtlinie sowie die Unterstützung bewährter Verfahren für die Verarbeitung personenbezogener Daten. Diese Anforderungen berücksichtigen bewährte Branchenverfahren, die sicherstellen, dass zertifizierte Produkte während ihrer gesamten Nutzungsdauer einen Mindest-Sicherheitsstandard erfüllen. Die Norm ist eng mit dem EU-Gesetz über Cyberresilienz, der EU-Funkanlagen-Richtlinie und anderen Normen und Rechtsvorschriften aus der ganzen Welt abgestimmt.

4.8 Schulung und Beratung

Axis bietet Mitarbeitern, Partnern und Kunden Informationen und Schulungen zu bewährten Verfahren im Bereich Cybersicherheit an. Diese umfassen die folgenden Themen:

- Sensibilisierung und Schulung zum Thema interne Sicherheit: Axis hat ein Programm zur Förderung des Sicherheitsbewusstseins entwickelt, um unsere Mitarbeiter fortlaufend darin zu schulen, Cyberbedrohungen für das Unternehmen zu vermeiden und zu mindern. Diese Sensibilisierungsschulung ist für alle Mitarbeiter von Axis obligatorisch. Abhängig von Rolle und Zuständigkeiten der einzelnen Personen im Unternehmen werden zusätzliche Sicherheitsschulungen für Entwickler und Systemverantwortliche angeboten.

- *Schulungen der Axis Communications Academy*: Zu den Schulungskursen für Kunden gehört ein Online-Kurs über Cybersicherheit und den *Ansatz von Axis in diesem Bereich*.
- Online verfügbare *Härtungsleitfäden* für:
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Axis Netzwerk-Switches*
- *AXIS OS Security Scanner Guide*: Axis empfiehlt, Axis Geräte mit Sicherheitsscans auf Schwachstellen oder Konfigurationsmängel zu überprüfen. Der AXIS OS Security Scanner Guide enthält Empfehlungen, wie bestimmte ermittelte Probleme gelöst werden können, und gibt einen Überblick über die häufigsten „False Positives".
- *AXIS OS Forensic Guide*: Dieser Leitfaden enthält technische Empfehlungen für alle, die forensische Analysen von Axis Geräten durchführen. Dies gilt für den Fall eines Angriffs auf die Cybersicherheit auf das umgebende Netzwerk und die IT-Infrastruktur, in der ein Axis Gerät installiert ist.

Weitere Informationen zu Axis und Cybersicherheit finden Sie im *Axis Cybersecurity Portal*.

T10210486/DE/M3.3/2406

Über Axis Communications

Axis ermöglicht eine intelligente und sichere Welt durch Lösungen zur Verbesserung der Sicherheit und Geschäftsperformance. Als Unternehmen für Netzwerktechnologie und Branchenführer bietet Axis Lösungen in den Bereichen Videosicherheit, Zutrittskontrolle sowie Intercoms und Audiosysteme. Sie werden verstärkt durch intelligente Analyseanwendungen und unterstützt durch gute Schulungen.

Axis beschäftigt rund 4.000 engagierte Mitarbeiter in über 50 Ländern und arbeitet weltweit mit Technologie- und Systemintegrationspartnern zusammen, um den Kunden Lösungen anbieten zu können. Axis wurde 1984 gegründet und der Hauptsitz befindet sich in Lund, Schweden