AXIS COMMUNICATIONS

Cybersicherheit

GEMEINSAM FÜR BESSEREN CYBERSCHUTZ

AXIS COMMUNICATIONS

INHALT

Das Risiko von Cybervorfällen mindern

Der Schutz von Netzwerkprodukten und Softwarediensten vor Cyber-Bedrohungen ist der Schlüssel zum Schutz der Daten und Systeme in Ihrem Netzwerk. Ein kompromittiertes System kann den Verlust der Vertraulichkeit und Integrität Ihrer Daten bedeuten, oder die Daten oder der Zugang können nicht verfügbar sein, wenn Sie sie benötigen.

Als verantwortungsbewusster Partner im Bereich der Cybersicherheit haben wir einige Überlegungen und Richtlinien zusammengestellt, die Ihnen bei der Beschaffung und Sicherung von IP-basierten physischen Sicherheitsprodukten helfen sollen. Wir möchten es Ihnen erleichtern, Schutzmaßnahmen zu ergreifen, damit Sie die Angebote von Axis so sicher wie möglich nutzen können.

Zusätzlich zu den folgenden Seiten erfahren Sie unter **www.axis.com/cybersecurity** mehr über Cybersicherheit und darüber, wie wir gemeinsam für einen besseren Cyberschutz sorgen können.

Eine gemeinsame Verantwortung

Cybersicherheit betrifft Produkte, Menschen, Technologien und laufende Prozesse. Und es ist klar, dass wir alle unsere Kräfte bündeln müssen, um sicherzustellen, dass jedes Glied der Cybersicherheitskette so stark wie möglich ist. Cybersicherheit ist eine gemeinsame Verantwortung, die die Zusammenarbeit der folgenden Akteure erfordert, einschließlich der Endnutzer.

Gerätehersteller

Hier beginnt die Cybersicherheit. Die Hersteller sollten bei Design, Entwicklung, Produktion und Softwarewartung bewährte Verfahren der Cybersicherheit anwenden, um das Risiko von Fehlern während des gesamten Produktlebenszyklus zu minimieren. Eine sorgfältige Kontrolle der eigenen Lieferkette ist wichtig. Produkte sollten über integrierte Funktionen verfügen, die die Implementierung verschiedener Sicherheitskontrollen ermöglichen. Es sollten Werkzeuge für eine effiziente Gerätekonfiguration und -verwaltung zur Verfügung stehen, die die Sicherheitsprozesse oder -richtlinien des Kunden unterstützen. Und es sollte Kanäle geben, um Partner und Kunden über neu entdeckte Schwachstellen zu informieren.

Distributoren

Für Händler, die nicht direkt mit den von ihnen vertriebenen Produkten in Berührung kommen, ist Cybersicherheit relativ einfach. Sie müssen jedoch dieselben Aspekte berücksichtigen wie Integratoren und Installateure, insbesondere wenn sie Geräte von einem Hersteller kaufen und unter einer anderen (oder ihrer eigenen) Marke weiterverkaufen. Transparenz ist der Schlüssel. Die Herkunft der Geräte muss klar sein.

Berater, Integratoren und Installateure

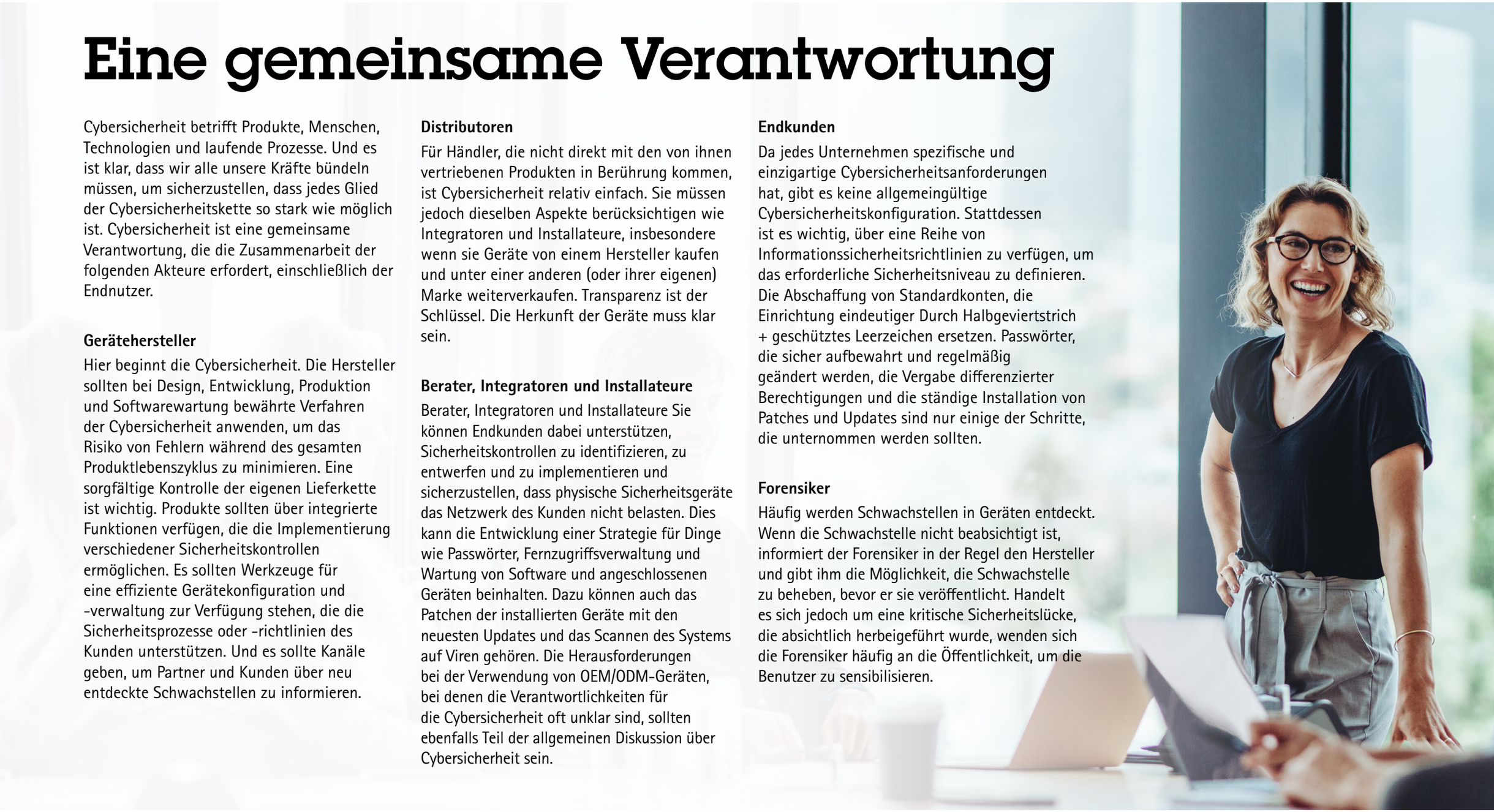
Berater, Integratoren und Installateure Sie können Endkunden dabei unterstützen, Sicherheitskontrollen zu identifizieren, zu entwerfen und zu implementieren und sicherzustellen, dass physische Sicherheitsgeräte das Netzwerk des Kunden nicht belasten. Dies kann die Entwicklung einer Strategie für Dinge wie Passwörter, Fernzugriffsverwaltung und Wartung von Software und angeschlossenen Geräten beinhalten. Dazu können auch das Patchen der installierten Geräte mit den neuesten Updates und das Scannen des Systems auf Viren gehören. Die Herausforderungen bei der Verwendung von OEM/ODM-Geräten, bei denen die Verantwortlichkeiten für die Cybersicherheit oft unklar sind, sollten ebenfalls Teil der allgemeinen Diskussion über Cybersicherheit sein.

Endkunden

Da jedes Unternehmen spezifische und einzigartige Cybersicherheitsanforderungen hat, gibt es keine allgemeingültige Cybersicherheitskonfiguration. Stattdessen ist es wichtig, über eine Reihe von Informationssicherheitsrichtlinien zu verfügen, um das erforderliche Sicherheitsniveau zu definieren. Die Abschaffung von Standardkonten, die Einrichtung eindeutiger Durch Halbgeviertstrich + geschütztes Leerzeichen ersetzen. Passwörter, die sicher aufbewahrt und regelmäßig geändert werden, die Vergabe differenzierter Berechtigungen und die ständige Installation von Patches und Updates sind nur einige der Schritte, die unternommen werden sollten.

Forensiker

Häufig werden Schwachstellen in Geräten entdeckt. Wenn die Schwachstelle nicht beabsichtigt ist, informiert der Forensiker in der Regel den Hersteller und gibt ihm die Möglichkeit, die Schwachstelle zu beheben, bevor er sie veröffentlicht. Handelt es sich jedoch um eine kritische Sicherheitslücke, die absichtlich herbeigeführt wurde, wenden sich die Forensiker häufig an die Öffentlichkeit, um die Benutzer zu sensibilisieren.



Was Cybersicherheit von physischer Sicherheit lernen kann

Physische Sicherheitsrisiken sind für die meisten Menschen leicht verständlich. Eine unverschlossene Tür erhöht das Risiko, dass Unbefugte eindringen. Offen liegende Wertgegenstände können leicht entwendet werden. Bei Fehlern und Unfällen können Menschen, Eigentum und Sachen zu Schaden kommen.

Physische Sicherheit und Cybersicherheit werden auf die gleiche allgemeine Weise angegangen:

> Identifizieren und klassifizieren Sie Ihre Vermögenswerte und Ressourcen (was muss geschützt werden?).

> Identifizieren Sie plausible Bedrohungen (was und vor wem muss geschützt werden).

> Identifizieren Sie plausible Schwachstellen, die von Bedrohungen ausgenutzt werden können (Wahrscheinlichkeit).

> Identifizieren Sie die zu erwartenden Kosten, wenn etwas Schlimmes passiert (die Folgen). Risiko wird oft als die Wahrscheinlichkeit einer Bedrohung multipliziert mit dem daraus resultierenden Schaden definiert. Wenn Sie dies festgestellt haben, müssen Sie sich fragen, was Sie bereit sind zu tun, um negative Auswirkungen zu vermeiden.

Was ist Cybersicherheit?

Cybersicherheit ist der Schutz von Computersystemen und -diensten vor Cyberbedrohungen. Zu den Cybersicherheitsmaßnahmen zählen Verfahren zur Schadensverhütung und zur Wiederherstellung von Computern, elektronischen Kommunikationssystemen und -diensten, Draht- und elektronischer Kommunikation sowie gespeicherten Informationen, um deren Vertraulichkeit, Integrität, Verfügbarkeit und Sicherheit, Authentizität und Nachweisbarkeit zu gewährleisten.

Auf welche Bedrohungen sollten Sie achten?

Die wichtigsten Elemente, die in einem IT-System (Informationstechnologie) oder OT-System (Betriebstechnologie) geschützt werden müssen, sind Vertraulichkeit, Integrität, Verfügbarkeit und Sicherheit. Alles, was einen dieser Faktoren beeinträchtigt, ist ein Cybersicherheitsvorfall.

Werfen wir nun einen Blick auf die häufigsten Cybersicherheitsbedrohungen und die Schwachstellen, die sie ausnutzen. Die vier häufigsten Cyberbedrohungen für IP-basierte physische Sicherheitssysteme sind:

1. **Menschliche Naivität und Versagen ohne Vorsatz**
2. **Vorsätzlicher Missbrauch des Systems**
3. **Physische Manipulation und Sabotage**
4. **Ausnutzung von Schwachstellen in der Software**

1 Menschliche Naivität und Versagen ohne Vorsatz

Ganz gleich, wie gut die Technologie zum Schutz Ihres Netzwerks auch sein mag, der Faktor Mensch spielt bei Sicherheitsverletzungen nach wie vor eine große Rolle.

Folgende Arten von menschlichem Versagen öffnen Cyber-Angriffen Tür und Tor:

> **Social Engineering**
Wenn ein Benutzer durch psychologische Manipulation dazu verleitet wird, Sicherheitsfehler zu begehen oder sensible Informationen zu verraten. Phishing und Scareware sind Beispiele für Social Engineering.

> **Missbrauch von Kennwörtern**
Dazu gehört, keine sicheren Kennwörter zu verwenden oder die Kennwörter nicht angemessen zu schützen und/oder regelmäßig zu ändern.

> **Missmanagement von kritischen Komponenten**
Verlust oder Verlegung von etwas, das den Zugang zum System ermöglicht. Beispiele hierfür sind Zugangskarten, Telefone, Laptops und Dokumente

> **Schlechte Systemverwaltung**
Das Versäumnis, Systemupdates und und Sicherheitspatches zu installieren.

> **Gescheiterte Verbesserungen**
Der Versuch, etwas zu beheben, was zu einer reduzierten Systemleistung führt.

Schwachstellen und menschliches Versagen

Zu den häufigsten Schwachstellen, die auf menschliches Versagen zurückzuführen sind, gehören ein mangelndes Bewusstsein für Cybersicherheit und das Fehlen langfristiger Strategien und Prozesse für das Risikomanagement. Um Bedrohungen durch menschliches Versagen zu minimieren, müssen alle Mitarbeiter einer Organisation über bewährte Verfahren im Bereich der Cybersicherheit informiert sein. Darüber hinaus sollte der Zugriff auf vernetzte Geräte über das Video Management System (VMS) oder den Gerätemanager auf wenige vertrauenswürdige Personen beschränkt werden.

2 Vorsätzlicher Missbrauch des Systems

Eine weitere allzu häufige Gefahr in Hinblick auf die Cybersicherheit ist der vorsätzliche Missbrauch eines Videosystems durch Personen, die rechtmäßig Zugang darauf haben.

Zu vorsätzlichem Missbrauch gehört Folgendes:

Manipulation von Systemdiensten und Ressourcen

Datendiebstahl

Vorsätzliche Schädigung des Systems

Schwachstellen und vorsätzlicher Missbrauch

Langfristige Richtlinien und Prozesse sind wichtig, um Schwachstellen zu verwalten und das Risiko eines vorsätzlichen Missbrauchs des Systems zu verringern. Die ordnungsgemäße Sicherheitsüberprüfung von Personen mit Zugriffsrechten auf sensible Daten ist ebenso wichtig wie die Begrenzung der Anzahl der Personen mit solchen Zugriffsrechten.

Für Software zur Verwaltung vernetzter physischer Sicherheitsgeräte, wie z. B. Kameras, sollte ein Administratorkonto mit eigenen Anmeldedaten verwendet werden. Dieses Konto sollte eindeutig sein und nicht gemeinsam genutzt werden. Standortbetreiber sollten über individuelle Konten in der Verwaltungssoftware verfügen. Keine Person sollte direkten Zugriff auf die physischen Sicherheitsgeräte haben. Sollte aus bestimmten Gründen ein direkter Zugang erforderlich sein, so sollte dieser nur vorübergehend gewährt werden.

3 Physische Manipulation oder Sabotage

Physischer Schutz ist im Hinblick auf die Cybersicherheit sehr wichtig:

> Physisch exponierte Geräte können manipuliert werden.

> Physisch exponierte Geräte können gestohlen werden.

> Physisch exponierte Kabel können getrennt, umgeleitet oder durchtrennt werden.

Schwachstellen und physische Bedrohungen

Schwachstellen und physikalische Bedrohungen Weitere Schwachstellen sind Netzwerkkomponenten wie Server und Switches, die sich nicht in gesicherten Bereichen befinden, leicht zugängliche Kameras, die nicht durch Schutzgehäuse abgeschirmt sind, und Kabel, die nicht durch Wände oder Kanäle geschützt sind. Vernetzte Geräte können auch andere Anlagen im selben Netzwerk gefährden.

Denken Sie an die negativen Auswirkungen

In Video-, Audio- und Zutrittssystemen werden keine Finanztransaktionen verarbeitet oder Kundendaten gespeichert. Das bedeutet, dass sich ein Angriff auf solche Systeme kaum monetarisieren lässt und von daher für organisierte Cyberkriminelle von begrenztem Wert ist. Aber ein kompromittiertes System kann zur Bedrohung für andere Systeme werden. Deshalb lassen sich die Kosten schwer abschätzen. Leider müssen Organisationen in vielen Fällen Lehrgeld zahlen. Schutz ist wie Qualität: Sie erhalten, was Sie bezahlen. Und wenn Sie billige Lösungen kaufen, kann es Sie auf lange Sicht viel mehr kosten, wenn die Lieferanten die Cybersicherheit nicht über den gesamten Produktlebenszyklus hinweg berücksichtigt haben.

4 Ausnutzung von Schwachstellen in der Software

Softwareentwicklung ist mit verschiedenen Risiken verbunden (meist Bugs oder Programmierfehler), die Schwachstellen entstehen lassen. Diese wiederum können für einen Angriff ausgenutzt werden.
Je mehr Schwachstellen in der Software eines Produkts vorhanden sind, desto höher ist das Angriffsrisiko. Vor der Markteinführung eines Produkts sollte der Hersteller idealerweise über ein Softwareentwicklungsmodell mit Prozessen und Tools verfügen, die das Risiko von Schwachstellen in allen Phasen der Softwareentwicklung minimieren.

Zwar kommt es in der Branche nur sehr selten vor, dass Software-Releases vollständig fehlerfrei sind, doch Fehler und andere mangelhafte Implementierungen, die die Sicherheit gefährden, müssen vom Produkthersteller unbedingt erkannt, behoben und den Kunden gemeldet werden. Daher muss der Hersteller neu entdeckte Schwachstellen in der Software transparent kommunizieren und den Kunden rechtzeitig eine Lösung anbieten. Es ist auch wichtig, dass der Kunde kontinuierlich Softwareaktualisierungen mit Sicherheitspatches und Bugfixes installiert, sobald diese vom Produkthersteller zur Verfügung gestellt werden.

Welche Maßnahmen sollten die Endkunden ergreifen, um die Risiken zu minimieren?

Bei der Beschaffung von physischen Sicherheitsprodukten sind verschiedene Aspekte zu berücksichtigen, um sicherzustellen, dass auch die Cyber-Sicherheit berücksichtigt wird.

Prüfen Sie zunächst den Cybersicherheitsansatz Ihrer Lieferanten für physische Sicherheit. Verfügen sie über eine Unternehmensrichtlinie zur Cybersicherheit, in deren Rahmen sie ihre Vermögenswerte fortlaufend identifizieren und bewerten und Risikobewertungen in Bezug auf diese Vermögenswerte durchführen? Es ist auch wichtig, dass Sie verstehen, wie Ihre Lieferanten mit ihrer Lieferkette arbeiten. Stellen Sie sich die Frage, ob ihre Produkte mit integrierten Cybersicherheitsfunktionen entwickelt und hergestellt werden.

Welche Maßnahmen bieten sie an, um die Cybersicherheit während des gesamten Lebenszyklus eines Netzwerkprodukts zu unterstützen? Und was geschieht, wenn Ihr System angegriffen wird? Haben Ihre Lieferanten Richtlinien, die Ihnen im Falle eines Cyber-Vorfalls mit ihren Produkten helfen?

Dies sind nur einige der Fragen, die Sie sich stellen sollten. Auf den folgenden Seiten gehen wir näher auf diese Fragen ein.

Was müssen Sie über Ihre Lieferanten wissen – und über die Lieferanten Ihrer Lieferanten?

Sicherheitsbedrohungen gibt es immer. Es treten immer wieder neue Bedrohungen auf. Unternehmen konzentrieren sich oft darauf, wie ihre Lieferanten diese Risiken bewerten und ihnen begegnen. Aber was ist mit den Lieferanten der Lieferanten? Wie kontrolliert und pflegt der Lieferant seine gesamte Lieferkette und gewährleistet die Sicherheit aller Produkte von der Komponentenebene bis zum Endprodukt?

Konzentriert sich Ihr Lieferant auf die Minimierung von Sicherheitsrisiken?

- Kontrolliert er die gesamte Lieferkette von der Komponentenebene bis zum Endprodukt?
- Verfügt er über ein Softwareentwicklungsmodell, das Sicherheitsüberlegungen zu einem integralen Bestandteil macht?
- Entwirft und fertigt er Produkte mit eingebautem Schutz?
- Stellt er Wissen und Werkzeuge für den Einsatz von Schutzmechanismen zur Verfügung?
- Reagiert er schnell und bietet kostenlose Verbesserungen an, wenn neue Schwachstellen in der Software entdeckt werden?

Lieferkettenpartner

Lieferkettensicherheit beginnt mit der Auswahl der richtigen Lieferkettenpartner durch einen konsistenten Bewertungsprozess. Der Bewertungsprozess sollte eine Analyse des Qualitäts- und Nachhaltigkeitsmanagementprozesses jedes Unternehmens beinhalten. Als Mindestanforderung sollte eine Zertifizierung durch Dritte nach ISO 9001 oder IATF 16949 vorliegen.

Lieferanten bewerten

Ihr Lieferant sollte auch die Risikomanagementprozesse seiner Zulieferer sowie deren Produktionsanlagen und -prozesse bewerten. Vor-Ort-Besuche und Follow-up-Audits sollten durchgeführt werden, um zu beurteilen, ob die Einrichtungen die Anforderungen und Standards erfüllen, die für die Qualifizierung zugelassener Lieferanten festgelegt wurden. Als Teil der Bewertung eines potenziellen neuen Partners in der Lieferkette sollte eine gründliche Analyse der finanziellen Situation und der Eigentümerstruktur des Lieferanten durchgeführt werden.

Strategische Lieferanten

Die Beziehungen zu Lieferanten kritischer Komponenten und Fertigungspartnern sind in der Regel besonders eng und langfristig. Es handelt sich um strategische Lieferanten, mit denen Ihr Lieferant gemeinsame Projekte und Entwicklungen vorantreibt, Ziele festlegt und langfristige gegenseitige Verpflichtungen und Pläne eingeht. Alle kritischen Komponenten in den Produkten Ihres Lieferanten sollten direkt von strategischen Lieferanten bezogen und intern gelagert werden. Unkritische Komponenten können von Produktionspartnern bezogen werden, jedoch nur von Lieferanten, die auf einer Liste zugelassener Lieferanten aufgeführt sind.

Wie sicher ist die Produktion Ihres Lieferanten?

- Definiert und überwacht er die Fertigungsprozesse?
- Entwickelt und produziert er kritische Produktionsanlagen?
- Bietet Ihr Lieferant ein System zum Testen von Komponenten, Modulen und Produkten während der Produktion zusammen mit Software, Prüfrechnern und sonstiger IT-Hardware-Infrastruktur?
- Erhebt Ihr Lieferant rund um die Uhr Produktionsdaten, damit Echtzeitanalysen, die Bewertung aller potenziellen Sicherheitsrisiken und die Implementierung von Minderungsplänen erfolgen können?

Der beste Weg für Ihren Lieferanten, die Einhaltung der Anforderungen sicherzustellen, ist die Durchführung regelmäßiger Audits vor Ort, entweder jährlich oder halbjährlich. Diese Audits sollten verschiedene wichtige Punkte abdecken, wie z. B. (mit geschütztem Leerzeichen!) die Einhaltung von Prozessen, Qualitätskontrolle und Rückverfolgbarkeit. Sie sollten auch Überprüfungen der physischen Handhabung in der Anlage, der Bestandsverwaltung und der Produktionsanlagen umfassen.

Vierteljährliche Geschäftsberichte (Quarterly Business Reviews, QBR) sind ebenfalls eine gute Möglichkeit, die Leistung im Vergleich zu den Erwartungen zu überwachen. Für strategische Lieferanten wird empfohlen, diese Überprüfungen auf höchster Managementebene durchzuführen.

Physische Sicherheit

Jedes Unternehmen in der Lieferkette, vom Komponentenlieferanten bis zum Distributionszentrum, muss hohe Anforderungen an die Gebäudesicherheit erfüllen. Sie müssen z. B. (mit geschütztem Leerzeichen!) sicherstellen, dass die Ein- und Ausgänge ständig überwacht werden und dass Zugangskontrollen und Besucherregistrierungen protokolliert und gespeichert werden. Außerdem sollten sie Scanner einsetzen, um unerwünschte Gegenstände oder Materialien zu erkennen. Darüber hinaus sollten Transporte nur durch anerkannte und renommierte Spediteure mit strengen Sicherheitsvorschriften und -kontrollen durchgeführt werden. Es wird auch empfohlen, den Warenein- und -ausgang regelmäßig mit Kameras zu überwachen und dies zu dokumentieren.

Zero-Trust-Netzwerke

Netzwerke werden immer anfälliger. Die exponentielle Zunahme von vernetzten Geräten schafft Netzwerk-Endpunkte, die für Angriffe anfällig sind. Cyberangriffe sind nicht nur zahlreicher, sondern auch raffinierter geworden. Infolgedessen hat sich das Konzept des „Zero-Trust" etabliert.

Nichts und niemandem im Netzwerk vertrauen

Wie der Name schon sagt, ist die Standardhaltung in einem Zero-Trust-Netzwerk, dass keiner Einheit, die mit dem Netzwerk verbunden ist und sich darin befindet, vertraut werden kann – egal, ob es sich um einen Menschen oder eine Maschine handelt. Dies gilt unabhängig davon, wo sich diese Einheiten befinden und wie sie miteinander verbunden sind. Vielmehr lautet die oberste Maxime von Zero-Trust-Netzwerken: „Niemals vertrauen, immer prüfen".

Beim erforderlichen Mindestzugriff bleiben

Das setzt voraus, dass die Identität jeder Einheit, die auf das Netzwerk zugreift oder sich darin befindet, mehrfach auf unterschiedliche Weise überprüft wird, je nach Verhalten und Sensibilität der spezifischen Daten, auf die zugegriffen wird. Im Wesentlichen erhalten Einheiten Zugriff in dem Mindestumfang, der zur Wahrnehmung ihrer Aufgabe erforderlich ist.

Zero-Trust-Netzwerke und -Architekturen

Da sich die Kunden zunehmend der Wichtigkeit einer verstärkten Cybersicherheit bewusst sind, implementieren sie Zero Trust-Netzwerke und -Architekturen, einschließlich HTTPS und des komplexeren IEEE 802.1X-Standards, der automatisch authentifizierte Geräte im Netzwerk zulässt oder nicht authentifizierte Geräte sperrt. Für die Hersteller von Netzwerkgeräten ist es daher essenziell, diese Anforderungen zu erfüllen. Sie müssen Technologien oder Schnittstellen anbieten, die solche Netzwerke unterstützen.

Der Grundsatz in einem Zero-Trust-Netzwerk lautet, dass keiner Entität, die sich mit dem Netzwerk verbindet und sich darin befindet, vertraut werden kann.

In der Richtlinien-Engine...

Im Zentrum jedes Zero-Trust-Netzwerks steht eine Policy Engine: Software, die es einer Organisation ermöglicht, Regeln für den Zugriff auf Daten und Netzwerkressourcen festzulegen, zu überwachen und durchzusetzen. Policy Engines verwenden eine Kombination aus Netzwerkanalyse und programmierten Regeln, um rollenbasierte Berechtigungen auf der Grundlage einer Reihe von Faktoren zu vergeben.

Ja oder Nein zu jeder Anfrage

Einfach ausgedrückt vergleicht die Policy Engine jede Anfrage nach Netzwerkzugriff mit der Richtlinie und teilt dem Verantwortlichen mit, ob die Anfrage genehmigt wird oder nicht. In einem Zero-Trust-Netzwerk definiert die Policy Engine die Datensicherheits- und Zugriffsrichtlinien und wendet sie auf Hosting-Modelle, Standorte, Benutzer und Geräte an.

Regeln definieren und anwenden

Damit eine Policy Engine funktioniert, müssen Organisationen die Regeln und Richtlinien innerhalb der wichtigsten Sicherheitskontrollen wie Next Generation Firewalls (NGFWs), E-Mail- und Cloud-Sicherheits-Gateways sowie Data Loss Prevention (DLP)-Software sorgfältig definieren. In Kombination erzwingen diese Kontrollen eine Mikrosegmentierung des Netzwerks über Hosting-Modelle und Standorte hinweg.

Wie wird der Zugriff auf Daten und Netzwerkressourcen am besten geregelt?

Mit Policy Engines können Sie:

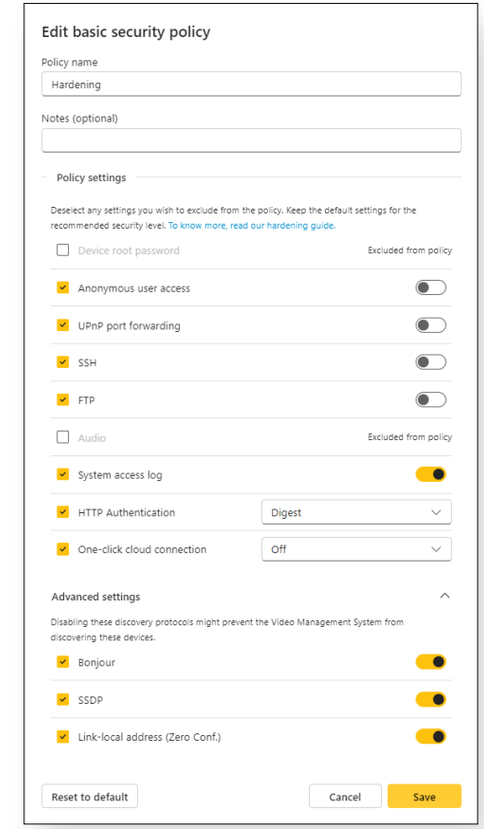
> Regeln erstellen

> Regeln überwachen

> Regeln durchsetzen

Policy Engines heute und morgen

Derzeit kann es erforderlich sein, Richtlinien in der Managementkonsole jeder Lösung festzuschreiben, aber integrierte Konsolen können zunehmend automatisch und produktübergreifend Richtlinien definieren und aktualisieren. Identity and Access Management (IAM), mehrstufige Authentifizierung, Push-Benachrichtigungen, Dateiberechtigungen, Verschlüsselung und Sicherheitsorchestrierung spielen beim Architekturdesign von Zero-Trust-Netzwerken alle eine Rolle.



Einstellen einer Richtlinien-Engine

Warum es entscheidend ist, effektives Lebenszyklus-Management zu implementieren

Mit Bedrohungen Schritt halten

Ein effektives Lebenszyklusmanagement kann Organisationen helfen, ihre Sicherheit zu gewährleisten und sich besser auf die Zukunft vorzubereiten. Voraussetzung dafür ist die Kenntnis der Risiken und die kontinuierliche Information über Bereiche, die zum Ziel von Angriffen werden können. Dies ist besonders wichtig für Sicherheitssysteme, da der Ausfall einer Sicherheitskamera in einem Netzwerk sehr schwerwiegende Folgen haben kann.

Vernetzte Geräte müssen aktualisiert werden

Alle vernetzten Geräte Durch Halbgeviertstrich + geschütztes Leerzeichen ersetzen von Netzwerk-Kameras bis hin zu VMS Durch Halbgeviertstrich + geschütztes Leerzeichen ersetzen müssen aktualisiert und gepatcht werden, um zu verhindern, dass Angreifer bekannte Schwachstellen ausnutzen und bestehende Schutzvorkehrungen umgehen.

Hersteller veröffentlichen regelmäßig Updates und Sicherheitspatches für die Gerätesoftware, um Schwachstellen zu beheben, Fehler zu korrigieren und andere Leistungsprobleme zu lösen und so ein stabiles und sicheres System zu gewährleisten.

Häufig versäumen es Organisationen jedoch, die Firmware oder das Betriebssystem, auf dem die Hardware läuft, zu aktualisieren.

Dies liegt in der Regel daran, dass sie keinen Überblick über alle Geräte in ihrem Netzwerk haben. Und selbst wenn man den Überblick hat, kann es mühsam und zeitaufwändig sein, alle Geräte zu aktualisieren.

Wird die Gerätesoftware nicht aktualisiert, können die Geräte anfällig für Cyberangriffe werden. Die Folgen reichen von Betriebsunterbrechungen bis hin zu hohen Geldbußen, die von Aufsichtsbehörden wegen Nichteinhaltung von Vorschriften verhängt werden.

Ein Netzwerk ist nur so sicher wie die Geräte, die daran angeschlossen sind. Daher ist es wichtig, den Lebenszyklus der vernetzten physischen Ressourcen effektiv zu verwalten.

Ein Gerät – zwei Lebenszeiten

Bei Hardware und Software gibt es zwei Arten von Lebenszyklen:

1) Die funktionelle Lebensdauer des Gerätes Durch Halbgeviertstrich + geschütztes Leerzeichen ersetzen oder wie lange ein Gerät realistischerweise arbeiten und funktionieren kann. Zum Beispiel hat eine Netzwerk-Kamera typischerweise eine funktionelle Lebensdauer von 10–15 Jahren.

2) Die wirtschaftliche Lebensdauer des Geräts Durch Halbgeviertstrich + geschütztes Leerzeichen ersetzen oder wie lange dauert es, bis die Wartung des Geräts mehr kostet als die Einführung einer neuen Technologie? Obwohl eine IP-Kamera 15 Jahre lang funktionsfähig sein kann, ist ihre tatsächliche Lebensdauer aufgrund der schnellen Veränderungen in der Cybersicherheitslandschaft kürzer.

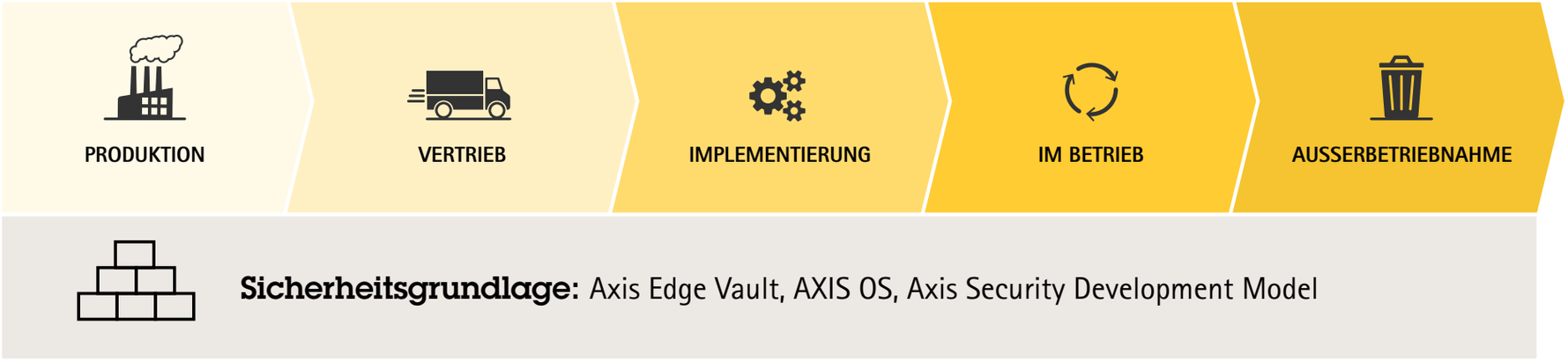
Anlagen proaktiv verwalten

Lebenszyklusmanagement ist die effektive Verwaltung sowohl des funktionalen als auch des wirtschaftlichen Lebenszyklus von Sachanlagen. Organisationen und Unternehmen benötigen einen klaren Überblick über alle Geräte in ihrem Netzwerk, um sicherzustellen, dass sie vor Bedrohungen geschützt sind.

Der Cybersicherheitsansatz von Axis

Axis setzt sich für ein hohes Maß an Cybersicherheit ein. Wir optimieren kontinuierlich unsere Cybersicherheitsangebote und -prozesse. Wir glauben, dass es wichtig ist, Transparenz darüber zu schaffen, wie wir unsere Aktivitäten und unsere Lieferkette sichern, wie wir bei der Softwareentwicklung vorgehen, um das Risiko von Schwachstellen zu reduzieren, wie wir mit neu entdeckten Schwachstellen umgehen und wie wir Sicherheit in unsere Produkte integrieren und Cybersicherheit während des gesamten Lebenszyklus unterstützen.

Auf den folgenden Seiten erfahren Sie, welche Sicherheitsmaßnahmen wir ergreifen und was wir in den verschiedenen Phasen des Produktlebenszyklus Durch Halbgeviertstrich + geschütztes Leerzeichen ersetzen von der Produktion über die Implementierung und den Betrieb bis hin zur Außerbetriebnahme Durch Halbgeviertstrich + geschütztes Leerzeichen ersetzen tun und anbieten, um Risiken zu minimieren und Sie beim Schutz Ihrer Axis Produkte zu unterstützen.



Sicherheitsbasis

Ein strukturierter und systematischer Ansatz für die interne Sicherheit

Bei Axis fördern wir einen kollaborativen Sicherheitsansatz, bei dem alle Mitarbeitenden zur kontinuierlichen Verbesserung unserer internen Sicherheit beitragen. Unser ISO 27001-zertifiziertes Information Security Management System (ISMS) bildet die Grundlage unseres Rahmenwerks für die Cybersicherheit. Als Teil des ISMS haben wir Cybersicherheitskontrollen eingeführt, um sicherzustellen, dass wir bei der Verwaltung unserer IT-Infrastruktur und der Entwicklungsplattform für Software sowie für verbundene Dienstleistungen Best Practices anwenden.

Dank eines strukturierten und systematischen Ansatzes schützen wir die Vertraulichkeit, Integrität und Verfügbarkeit unserer Assets. Axis erfüllt zudem verschiedenste regulatorische Anforderungen sowie strategisch ausgewählte Rahmenwerke und Standards, einschließlich des Standards für Cybersicherheit ETSI EN 303 645 für das Geräteportfolio mit AXIS OS. Aber wir setzen nicht nur auf Vorschriften und Zertifizierungen, denn zahlreiche Zertifizierungen zu haben, ist nicht unbedingt gleichbedeutend mit besserer Cybersicherheit.

Mehr über die Compliance von Axis erfahren

RI. SE

CERTIFIKAT

ISO/IEC 27001

Härmed intygas att/This is to certify that

Axis Communications AB

Gränden 1, 223 69 LUND, SWEDEN

har ett ledningssystem för informationssäkerhet som uppfyller kraven enligt ISO/IEC 27001:2022 vad gäller
has an information security management system that fulfils the requirements of ISO/IEC 27001:2022 with respect to

Product management, utveckling och drift inom IT-infrastrukturtjänster och Axis Connected Services
Allt i enlighet med uttalande om tillämplighet fastställt 2023-11-14

Product management, development and operations within IT infrastructure services and Axis Connected Services
All in accordance with Statement of Applicability established 2023-11-14

Ursprungligen utfärdat/Originally issued	2019-02-27
Giltigt till och med/Expiry date	2025-02-26
Beslutsdatum/Decision date	2023-12-07

Jonas Madsen

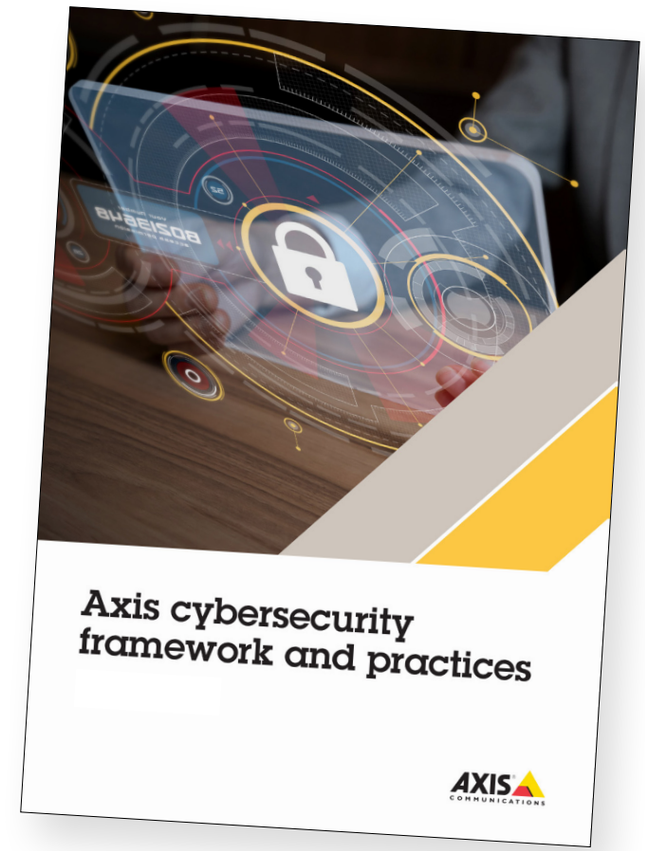
RISE Research Institutes of Sweden AB | Certification
Box 857, SE-501 15 Borås, Sweden
+46 10-516 50 00
certifiering@ri.se | www.ri.se

SP

Certifikat/Certificate 6134 I | version/issue 5 | 2023-12-07

This document is the property of RISE and may not be reproduced other than in full, except with the prior written approval by RISE.

Sida/Page 1(3)



Schutz der Produktintegrität und Reduzierung des Risikos von Schwachstellen in der Software

Die folgenden Maßnahmen – von der internen Sicherheit bis zur Produktsicherheit – bilden die Grundlage für die Sicherheit der Hardware und Software von Axis und stehen für unser Leitprinzip der Transparenz.

Axis Edge Vault Cybersicherheitsplattform

Diese in Axis Geräte integrierte, hardwarebasierte Plattform umfasst Funktionen, die die Integrität von Axis Geräten schützen. Auf diese Weise lassen sie sich sicher booten und integrieren, und es wird sichergestellt, dass sensible Daten wie kryptografische Schlüssel vor unbefugtem Zugriff geschützt sind.

Weitere Informationen zu Axis Edge Vault

Axis Security Development Model (ASDM)

ASDM ist die Entwicklungsmethodik von Axis, um das Risiko der Veröffentlichung von Produkten mit Schwachstellen in der Software zu reduzieren. Es stellt sicher, dass Sicherheitsaspekte ein integraler Bestandteil der Softwareentwicklung sind. Dazu gehören unter anderem Bereiche wie Risikobewertungen, Bedrohungsmodelle, Code-Analysen, Penetrationstests, Bug-Bounty-Programme sowie das Scannen und Verwalten von Schwachstellen. Indem ASDM Probleme in jeder Entwicklungsphase sofort erkennt und behebt, hilft es unseren Kunden, sicherheitsrelevante Risiken zu reduzieren.

Weitere Informationen zu ASDM

AXIS OS

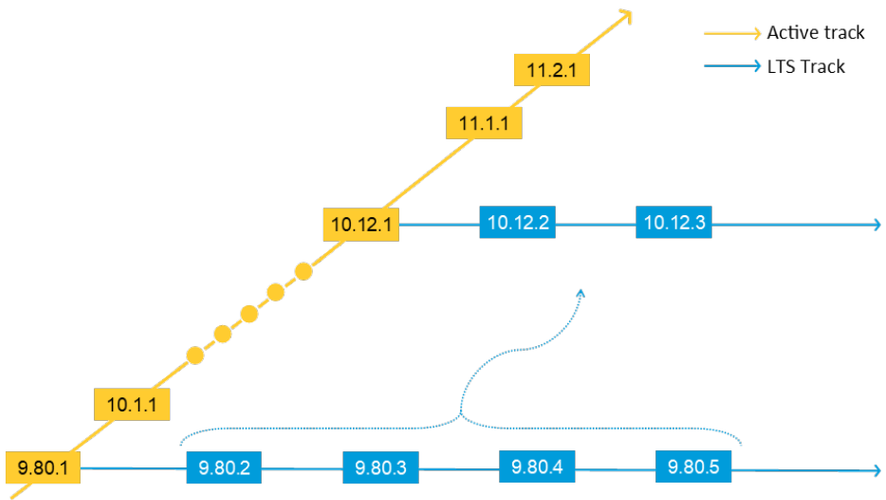
AXIS OS ist unser Linux-basiertes Betriebssystem für Edge-Geräte. Dieses leistungsstarke Betriebssystem, bei dem Offenheit, Transparenz und Cybersicherheit im Vordergrund stehen, umfasst verschiedene OS-Tracks für Axis Geräte. So kann Axis schnell Software-Sicherheitsfunktionen und -Patches für eine große Anzahl von Produkten veröffentlichen. Es wurde entwickelt, um Ihnen zu helfen, Risiken zu mindern und Ihre Produkte und Dienstleistungen von Axis auf dem neuesten Stand und geschützt halten zu können. Das Datum des Supportendes vieler Produkte wird auf der Axis Website angezeigt, sodass Sie die Außerbetriebnahme und den Ersatz der Produkte rechtzeitig planen können.

Weitere Informationen zu AXIS OS

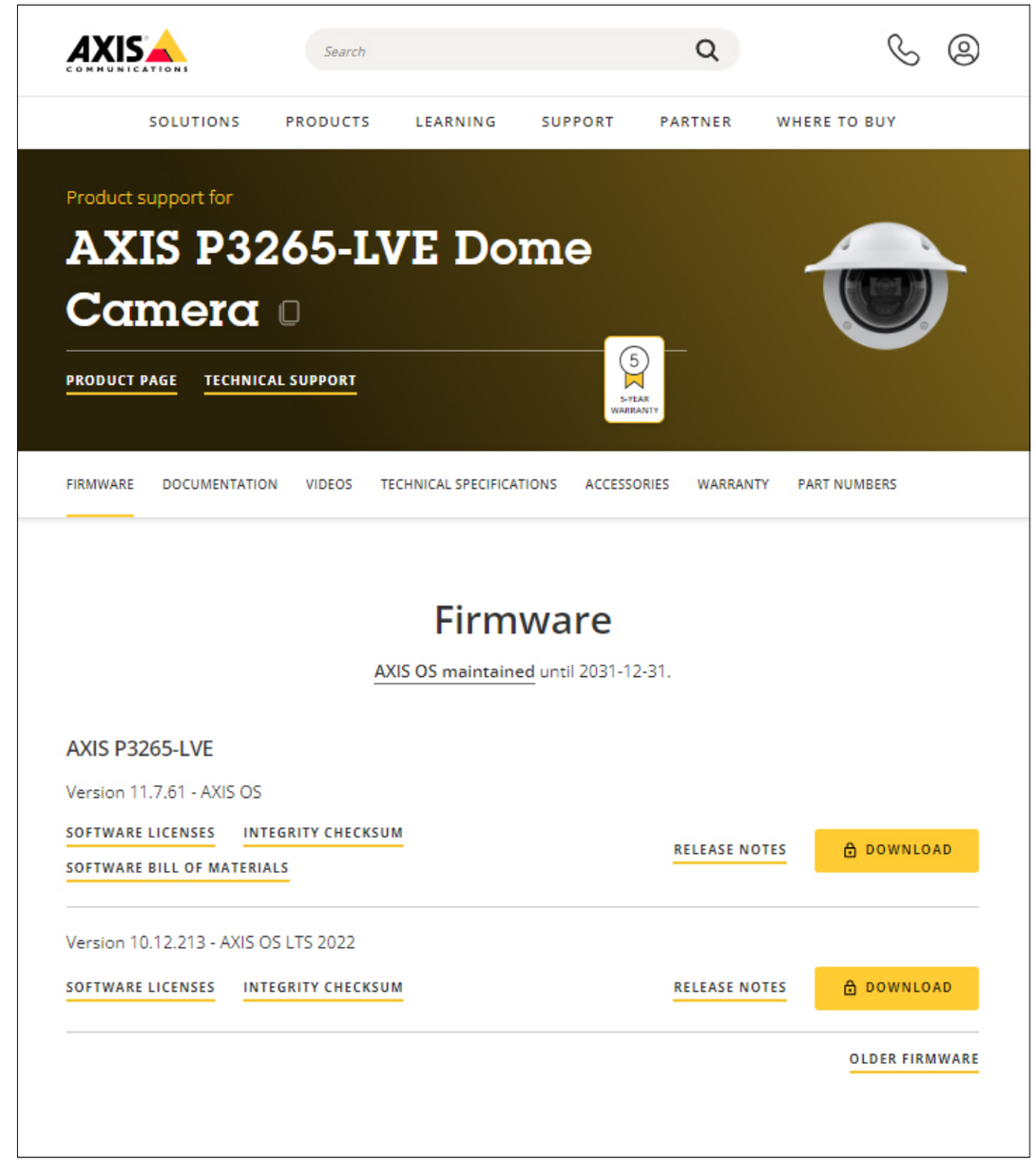
Software-Materialliste

Außerdem veröffentlichen wir eine Software-Materialliste für AXIS OS mit zusätzlichem Fokus auf Cybersicherheit und verbesserter Transparenz für Kunden, Sicherheitsforensiker und Behörden. Die Software-Materialliste ist eine ausführliche, detaillierte Übersicht über die Komponenten, die zur Entwicklung des Betriebssystems für Axis Geräte verwendet werden. Sie gewährt Einblicke in die Best Practices der Anbieter in Sachen Cybersicherheit und enthält wertvolle Informationen für Drittanbieter, die sich auf die Bewertung von Schwachstellen, die Bedrohungsanalyse und Abhilfepläne spezialisiert haben.

Weitere Informationen über die Software-Materialliste



AXIS OS-Tracks.



Umgang mit neu entdeckten Schwachstellen

Als Mitglied der Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA) veröffentlicht und benachrichtigt Axis die Betroffenen über Schwachstellen, damit unsere Kunden rechtzeitig geeignete Maßnahmen ergreifen können. In Zusammenarbeit mit externen Forensikern legt Axis Schwachstellen und Sicherheitsrisiken in einem transparenten, verantwortungsvollen und aufeinander abgestimmten Prozess offen. Axis veröffentlicht Patches für betroffene Geräte, Software oder Dienste und stellt alle notwendigen Informationen auf **der Axis Website** und in der öffentlich zugänglichen Datenbank für Schwachstellen des CVE-Programms zur Verfügung. Außerdem bieten wir einen Benachrichtigungsdienst zum Thema Sicherheit. Sie können sich registrieren und erhalten dann Informationen über Schwachstellen und andere sicherheitsrelevante Themen. Axis legt großen Wert darauf, das Betriebssystem der installierten Produkte auf dem neuesten Stand zu halten, um sicherzustellen, dass die neuesten Sicherheitspatches eingespielt sind.

Mehr über die Axis Vulnerability Management-Richtlinie erfahren

Bug-Bounty-Programm

Wir haben ein Bug-Bounty-Programm als Teil unserer transparenten Strategie zum Umgang mit Schwachstellen. Dieses Programm erfolgt in Zusammenarbeit mit Bugcrowd, dem Marktführer im Bereich Cybersicherheit durch Crowdsourcing. Wir engagieren uns für den Aufbau beruflicher Beziehungen zu externen Sicherheitsforensikern und ethischen Hackern. Als Teil des Programms haben Forensiker, die Schwachstellen in AXIS OS-basierten Produkten entdecken, Anspruch auf eine Geldprämie. Axis wird dann diese und andere gefundene Schwachstellen veröffentlichen und Patches für die betroffenen Produkte bereitstellen.

PRODUKTION

VERTRIEB

Reduzierung des Risikos von kompromittierten Hardware- und Softwarekomponenten

Sicherheit der Lieferkette

Wie alle Produkte müssen auch physische Sicherheitsprodukte so funktionieren, wie es ihre Konzeption und ihr Zweck ist, und dabei ihre Integrität bewahren. Dies lässt sich erreichen, wenn die Hardware und das Betriebssystem des Produkts erfolgreich vor nicht autorisierten Änderungen oder Manipulationen geschützt werden, während das Produkt die Lieferkette durchläuft.

Qualitätskontrollen

Zusammen mit unseren Lieferanten und Fertigungspartnern wendet Axis eine Vielzahl von Qualitätskontrollen an, um die Integrität unserer Produkte zu wahren und zu schützen. Komponenten werden immer bei einem Lieferanten aus der Liste zugelassener Anbieter gemäß der Bestellliste in der Axis Spezifikation beschafft. Der Lieferant darf ohne Genehmigung von Axis keine Änderungen an Spezifikationen, Arbeitsanweisungen oder Qualitätsprüfungsdokumenten vornehmen. Alle genehmigten Änderungen müssen dokumentiert und protokolliert werden.

Rückverfolgbarkeit

Ein Materialmanagementprozess stellt zu jeder Zeit den Status des Materials sicher und deckt alle Abweichungen auf, die die Qualität beeinträchtigen könnten. Lieferanten und Fertigungspartner müssen ein Rückverfolgbarkeitssystem unterhalten, um die Rückverfolgbarkeit der produzierten Chargen vom eingehenden Material bis zum fertigen Bauteil zu gewährleisten. Während der Produktion wird das physische Bauteil mehreren Tests unterzogen, um die Konformität zu überprüfen und eventuelle Abweichungen zu erkennen.

Gefälschte Komponenten erkennen

Eine Automatische Optische Inspektion (AOI) trägt zur Verifizierung bei, damit keine gefälschten Komponenten montiert werden. Bei Axis entwickeln und produzieren wir unsere kritische Produktionsausrüstung sowie das System zum Testen von Komponenten, Modulen und Produkten auf den verschiedenen Produktionsebenen. Dieser Prozess schränkt das Manipulationsrisiko ein. Als zusätzliche Sicherheitskontrolle werden alle Testdaten rund um die Uhr mit Axis geteilt, sodass Änderungen durch Unbefugte sofort festgestellt werden.

Weitere Informationen zur Sicherheit der Axis Lieferkette

Abwehr von Bedrohungen während des Vertriebs

Die in den Axis Geräten integrierten Cybersicherheitsfunktionen schützen zusammen mit den Werkseinstellungen der Geräte vor unbefugten Softwareänderungen während des Versands. Die von Axis Edge Vault unterstützten Funktionen (siehe nächste Seite) schützen sensible Daten in den Geräten und stellen sicher, dass auf den Geräten nur die Originalversion des Axis Betriebssystems läuft.

Die Sicherheit der Lieferkette zu verstehen, ist für die Risikobewertung von Anbietern notwendig. Nur so können Sie feststellen, ob ein Anbieter Maßnahmen ergreift, um die Risiken für Ihr Unternehmen zu minimieren.

Integrierte Cybersicherheitsfunktionen

Axis Geräte sind mit integrierten Sicherheitsfunktionen ausgestattet. Dadurch können Sie sie sicher booten, onboarden und sicher sein, dass sensible Daten geschützt sind.

Axis Edge Vault Cybersicherheitsplattform
Unsere hardwarebasierte Cybersicherheitsplattform ist eine solide Grundlage, um sicherzustellen, dass Ihr Axis Gerät ein vertrauenswürdiger und zuverlässiger Teil Ihres Netzwerks ist. Axis Edge Vault bietet unter anderem folgende Funktionen*:

> **Sicherer Keystore**, der kryptografische Rechenmodule für die sichere Speicherung von kryptografischen Schlüsseln umfasst und die Identität des Geräts und andere sensible Informationen vor unbefugtem Zugriff schützt – auch wenn das Gerät kompromittiert werden sollte. Die kryptografischen Rechenmodule können eine Trusted Execution Environment sein, die in das Axis System-on-Chip (SoC) integriert ist. Er kann auch ein sicheres Element oder ein Trusted Platform Module sein, bei denen es sich um separate Chips auf der Hauptplatine handelt. Axis Geräte werden mit einem oder einer beliebigen Kombination dieser drei Module hergestellt.

> **Signierte Firmware** und **sicheres Booten**, die sicherstellen, dass das Gerät nur die Originalversion des Axis Betriebssystems (AXIS OS) herunterlädt und ausführt.

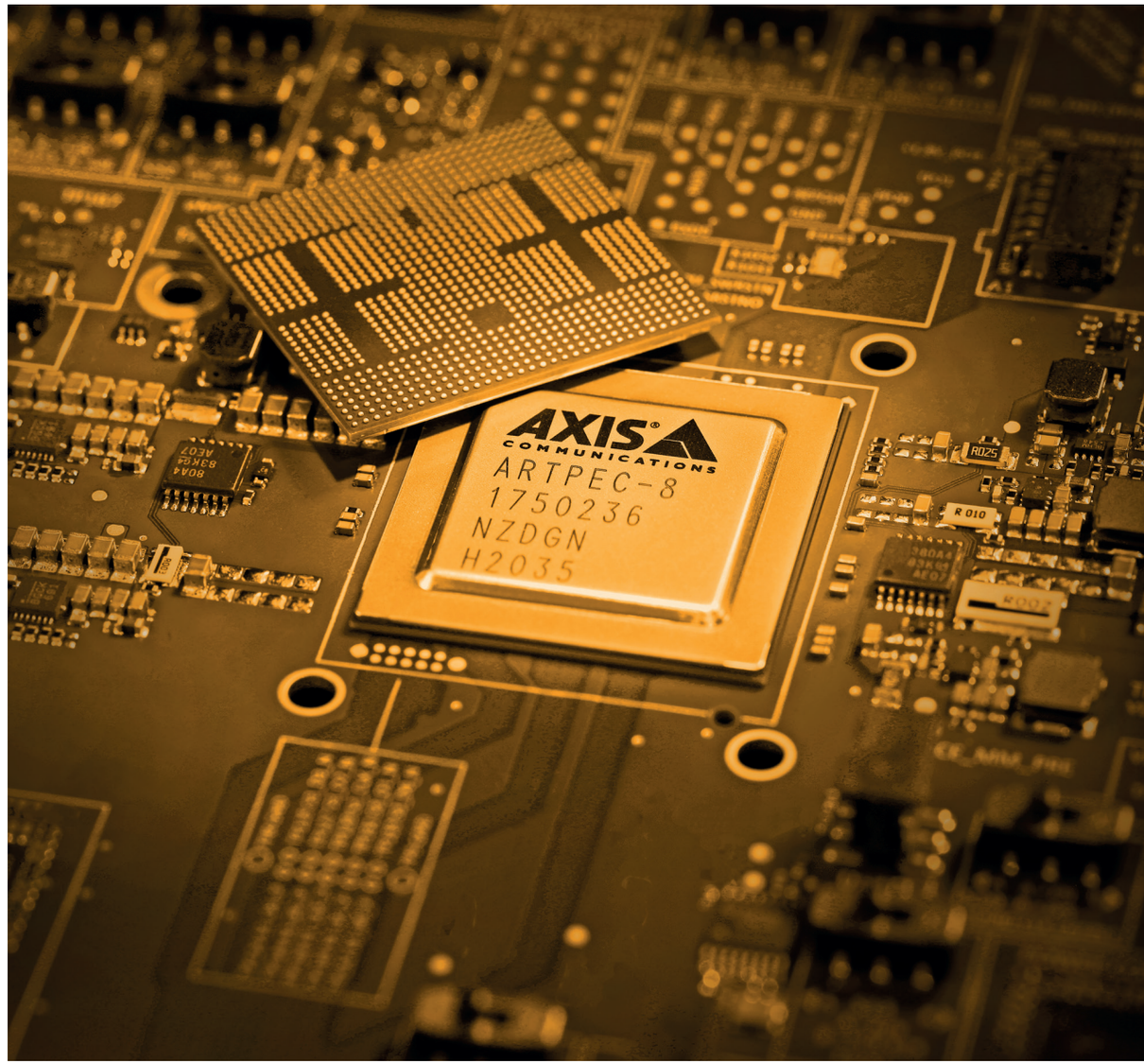
> **Axis Geräte-ID**, die IEEE 802.1AR-konform ist, für die sichere Identifizierung von Geräten und das Onboarding in ein Netzwerk.

> **Verschlüsseltes Dateisystem**, das die Daten im Dateisystem davor schützt, extrahiert oder manipuliert zu werden, wenn das Gerät nicht benutzt wird, z. B. während des Transports von einem Systemintegrator zum Endkunden.

> **Signierte Videos**, mit denen Benutzer die Echtheit der aufgenommenen Videos überprüfen und sicherstellen können, dass sie nicht manipuliert wurden.

**Hinweis: Nicht alle Gerätemodelle unterstützen alle Funktionen von Axis Edge Vault. Im Datenblatt oder im Axis Produktauswahl-Tool können Sie nachsehen, welche Funktionen das Produkt unterstützt.*

Mehr über Axis Edge Vault



Standardeinstellungen

Neben den Sicherheitsfunktionen der Produkte werden Axis Geräte mit vordefinierten Standard-Schutzeinstellungen ausgeliefert.

Zugangsdaten und Netzwerkprotokolle

Das Axis Gerät funktioniert erst nach der Einrichtung von Konten mit einem Benutzernamen und Kennwort. Nachdem diese eingerichtet wurden, ist der Zugriff auf Admin-Funktionen und/oder Videostreams nur möglich, wenn diese Zugangsdaten verwendet werden.

Darüber hinaus sind in Axis Geräten nur wenige Netzwerkprotokolle und -dienste standardmäßig aktiviert, z. B. HTTP und HTTPS für den Zugriff auf Geräteschnittstellen, RTSP und RTP für Video- und Audiostreaming und einige Protokolle wie UPnP und Bonjour für die Erkennung von Axis Geräten durch Anwendungen von Drittanbietern.

Kompatibilität mit den Zero-Trust-Netzwerken der Kunden

Axis hat auf die Zero-Trust-Anforderungen reagiert und Produkte mit eindeutigen Axis Geräte-IDs und Unterstützung für das HTTPS-Protokoll und den IEEE 802.1X-Standard sowie IEEE 802.1AR für die Authentifizierung von Geräten und IEEE 802.1AE MACsec für die automatische Datenverschlüsselung entwickelt.

HTTPS ist standardmäßig aktiviert, sodass die Kennwörter für Geräte sicher festgelegt werden können. Außerdem kann die Video Management Software mit HTTPS das vertrauenswürdige CA-signierte SSL-Zertifikat überprüfen, das von der Axis Geräte-ID in neueren Produkten unterstützt wird.

Die Unterstützung von IEEE 802.1X, IEEE 802.1AR und IEEE 802.1AE, die in den Axis Produkten standardmäßig aktiviert sind, ermöglicht das automatische Onboarding von Geräten, Authentifizierung und End-to-End-Verschlüsselung. Dies stellt IT-Experten Standardmechanismen zur effizienten und sicheren Integration von Axis Geräten in ein Unternehmensnetzwerk mit Unterstützung für IEEE 802.1X zur Verfügung. Kunden, die Axis Geräte in einem Aruba-Netzwerk verwenden, können den Integrationsleitfaden herunterladen. Darin werden die besten Konfigurationen für das sichere Onboarding und die Verwaltung von Axis Geräten beschrieben.

Mehr über Axis Lösungen für die Unternehmens-IT erfahren

IMPLEMENTIERUNG

Cybersicherheit während der Implementierung

Ein Axis Gerät ist ein Netzwerk-Endpunkt wie jedes andere Gerät, z. B. ein Laptop, ein Desktop-Computer oder ein mobiles Gerät. Im Gegensatz zu Laptops müssen Benutzer mit Axis Geräten jedoch keine potenziell schädlichen Websites besuchen, bösartige E-Mail-Anhänge öffnen oder nicht vertrauenswürdige Anwendungen installieren. Ein Netzwerk-Video-, Audio- oder Zutrittskontrollgerät ist jedoch ein Produkt mit einer Schnittstelle, die für das System, an das es angeschlossen ist, ein Risiko darstellen kann

Die für die Produkte von Axis erhältlichen Härtungsleitfäden enthalten Empfehlungen zur Reduzierung der Risiken durch Cyberangriffe. Im Folgenden finden Sie einige der grundlegenden Empfehlungen. Wir empfehlen zum Beispiel, dass Sie ein Gerät vor seiner Konfiguration auf die Werkseinstellungen zurücksetzen. So können Sie sicherstellen, dass das Gerät frei von unbefugten Softwareänderungen ist.

Überprüfen Sie außerdem, ob auf dem Gerät die aktuellste Version von AXIS OS läuft, da diese die neuesten Sicherheitspatches und Bugfixes für das jeweilige Gerät enthält.

Sie sollten sichere Kennwörter einrichten, den direkten Zugriff auf die Weboberfläche des Geräts einschränken, das Gerät so konfigurieren, dass es nur HTTPS verwendet (das den Datenverkehr zwischen Client und Gerät verschlüsselt), und nicht genutzte Dienste und Funktionen deaktivieren, um unnötige Risiken zu reduzieren. Des Weiteren ist es wichtig, Datum und Uhrzeit auf dem Gerät korrekt einzustellen, um das Erstellen genauer Systemprotokolle zu ermöglichen und sicherzustellen, dass digitale Zertifikate – auf die Dienste wie HTTPS und IEEE 802.1X angewiesen sind – validiert und verwendet werden können.

Ein Tool von Axis, das lokal die effiziente Konfiguration und Verwaltung von Axis Geräten ermöglicht, ist AXIS Device Manager.

Der AXIS Device Manager ermöglicht die Batch-Verarbeitung von Installations- und Sicherheitsaufgaben, wie z. B. die Verwaltung der Geräte-Zugangsdaten, die Bereitstellung von digitalen Zertifikaten, die Deaktivierung nicht genutzter Dienste oder die Aktualisierung von AXIS OS. Auf der nächsten Seite finden Sie weitere Informationen über Geräteverwaltungssoftware.

Umfassende und erweiterte Härtungsempfehlungen für AXIS OS-basierte Geräte finden Sie im AXIS OS Hardening Guide. Härtungsleitfäden für Axis Video Management Software und die Netzwerk-Switches finden Sie auf der Ressourcenseite für Cybersicherheit. Und Informationen zur nahtlosen Integration von Axis-Geräten in die IT-Infrastruktur und Netzwerke von Unternehmen finden Sie auf der Seite zu Axis Lösungen für die Unternehmens-IT.

Axis bietet Tools, Dokumentationen und Schulungen, mit denen Sie Risiken minimieren und Ihre Produkte und Dienste von Axis auf dem neuesten Stand und geschützt halten können. **Zugang zu unseren Ressourcen für Cybersicherheit.**

IM BETRIEB

Cybersicherheit von Geräten im Betrieb

Während ein Gerät in Betrieb ist, besteht eine der wichtigsten Maßnahmen zur Gewährleistung der Cybersicherheit darin, die Firmware oder das Betriebssystem, AXIS OS, auf dem neuesten Stand zu halten. Dadurch wird sichergestellt, dass das Gerät über die neuesten Sicherheitspatches und Bugfixes verfügt. Die signierte Firmware und das sichere Booten in Axis Geräten stellen sicher, dass nur die Originalversion von AXIS OS installiert und ausgeführt werden kann. Die kostenlosen AXIS OS Versionen befinden sich entweder auf dem Active Track oder auf dem Long Term Support (LTS) Track. Die AXIS OS Versionen auf dem Active Track unterstützen neue Funktionen, während die Versionen auf dem LTS Track dies nicht tun, um das Risiko von Kompatibilitätsproblemen zu minimieren. Beide Tracks enthalten jedoch Sicherheitspatches und Bugfixes. Sie können den Axis Security Alert Service abonnieren, um über neu entdeckte Schwachstellen auf dem Laufenden zu bleiben. Zu den veröffentlichten Schwachstellen gibt es Anleitungen, wie die betroffenen Produkte mit neuer Gerätesoftware aktualisiert werden sollten.

Um die Aktualisierung des Betriebssystems für eine große Anzahl von Geräten einfacher und effizienter zu gestalten, bietet Axis Geräteverwaltungssoftware wie AXIS Device Manager und AXIS Device Manager Extend an.

Wie funktioniert Gerätemanagement-Software?

Die Geräteverwaltungssoftware kann schnell ein vollständiges Echtzeit-Inventar aller Kameras, Encoder, Zutrittskontroll-, Audio- und anderen Geräte erstellen, die mit dem Netzwerk verbunden sind. Sie scannt das gesamte Netzwerk, und wenn ein neues oder aktualisiertes Gerät gefunden wird, erfasst sie alle wichtigen Informationen, einschließlich Modellnummer, IP- und MAC-Adressen, Gerätesoftwareversion und Zertifikatsstatus

Der vollständige Überblick

Mit einem sehr detaillierten Überblick über das gesamte Ökosystem des Netzwerks ist es einfacher, konsistente Richtlinien und Praktiken für das Lebenszyklus-Management aller Geräte umzusetzen und alle wichtigen Aufgaben in den Bereichen Installation, Bereitstellung, Konfiguration, Sicherheit und Wartung sicher zu verwalten.

Cybersicherheitsrichtlinien und Best Practices für die Geräteverwaltung müssen sich unter anderen mit den folgenden Fragen befassen: Wie stark müssen die Kennwörter sein und wie oft müssen Benutzer diese ändern? Welche ungenutzten Dienste sollten deaktiviert werden, um weniger Angriffsfläche zu bieten? Wie häufig sollten Geräte auf Schwachstellen gescannt werden?

Welche Verfahren für die Risikobewertung sind vorhanden, wenn ein Hersteller bekannte Sicherheitslücken veröffentlicht?

Zeit und Arbeit sparen

Mithilfe einer Geräteverwaltungssoftware können Unternehmen bei der Verwaltung von Cybersicherheitsrisiken Zeit und Aufwand sparen. Sie kann für folgende Zwecke eingesetzt werden:

> Gleichzeitige Veröffentlichung von Systemänderungen, Updates der Gerätesoftware und neuen digitalen Zertifikaten auf allen betroffenen Geräten.

> Sicherheitseinstellungen einfach erstellen oder neu konfigurieren und im gesamten Netzwerk anwenden, damit alle Geräte den neuesten Sicherheitsrichtlinien und -praktiken entsprechen.

> Überprüfung, ob alle Geräte mit der neuesten und sichersten Softwareversion ausgestattet sind.

> Benutzerberechtigungen im gesamten Netzwerk verwalten und Änderungen konfigurieren.

Echtzeit-Erkenntnisse gewinnen

Tools zur Geräteverwaltung bieten Organisationen Echtzeit-Einblicke in den Zustand ihres Ökosystems. So können Sie zum Beispiel sehen, welche Geräte mit den neusten Software-Updates und Zertifikaten aktualisiert werden müssen. Außerdem erhalten Sie Informationen über Produktabkündigungen und das Datum des Supportendes, sodass Sie den Ersatz der Geräte rechtzeitig planen können.

Axis Tools zur Geräteverwaltung

Unsere Geräteverwaltungssoftware, AXIS Device Manager und AXIS Device Manager Extend, helfen Ihnen bei der effizienten Verwaltung Ihrer Axis Geräte. AXIS Device Manager und AXIS Device Manager Extend ergänzen sich gegenseitig.

AXIS Device Manager

AXIS Device Manager ermöglicht die schnelle und einfache Installation und Konfiguration neuer Geräte. Dieses On-Premise-Tool unterstützt alle wichtigen Aufgaben in den Bereichen Installation, Sicherheit und Betrieb, einschließlich der Installation von Software-Upgrades und Anwendungen. Damit können Sie Axis Geräte mit Einstellungen für Sicherungen und Wiederherstellung konfigurieren, und Sie können den Gewährleistungsstatus anzeigen. Sie können auch Cybersicherheitskontrollen wie HTTPS und IEEE 802.1X-Zertifikate einsetzen.

Weitere Informationen zu
AXIS Device Manager

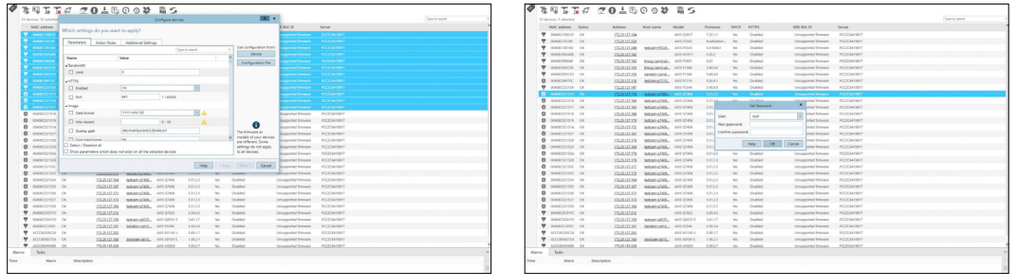
AXIS Device Manager Extend

AXIS Device Manager Extend ist ideal für den Einsatz an mehreren Standorten und hilft Ihnen, Ihre Geräte an allen Standorten ferngesteuert zu verwalten. Diese benutzerfreundliche Anwendung vereinfacht die Skalierung wichtiger Wartungsaufgaben, wie z. B. Updates von AXIS OS, die Definition, Anwendung und Durchsetzung von Sicherheitsrichtlinien sowie die Verwaltung von Anwendungen. Es verfügt über ein Live-Dashboard und beschleunigt die Fehlerbehebung, indem es ein Situationsbewusstsein für potenzielle Probleme im System schafft, z. B. für Geräte, die offline oder nicht mehr in der Gewährleistung sind. Außerdem bietet es Empfehlungen für Geräteeinstellungen, um Sicherheitsbedrohungen zu minimieren und Schwachstellen zu mindern. Sicherheitsrichtlinien können für alle Axis Geräte gleichzeitig definiert, angewendet und durchgesetzt werden.

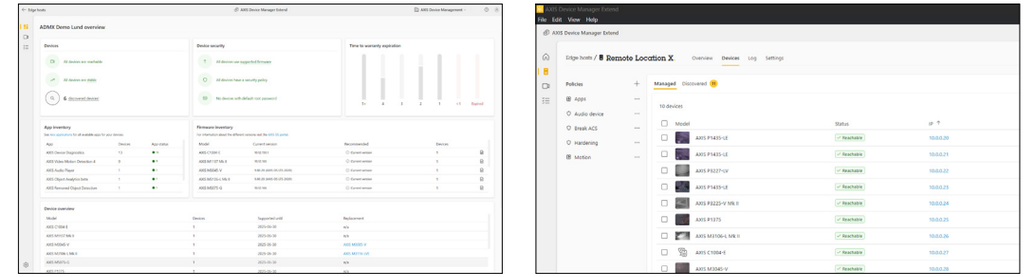
Weitere Informationen zu
AXIS Device Manager Extend

Sicherheitsverletzungen

Im Falle einer Sicherheitsverletzung in Ihrem Netzwerk stellen wir den AXIS OS Forensic Guide zur Verfügung, um Sie bei der Durchführung einer forensischen Analyse Ihrer Axis Netzwerk-Geräte zu unterstützen.



Screenshots der Oberfläche von AXIS Device Manager.



Screenshots der Oberfläche von AXIS Extend Manager.

AUSSERBETRIEBNAHME

Planung der Außerbetriebnahme

Updates und Patches sind der beste Weg, um die Cybersicherheit eines Produkts zu gewährleisten. Sie sind jedoch nicht immer verfügbar, wenn ein Produkt zu alt ist, um noch unterstützt zu werden. Aus Sicht der Cybersicherheit stellen ältere, nicht gepatchte Produkte ein großes Risiko dar. Ein vernachlässigtes Gerät kann leicht zum Einfallstor für Angreifer werden.

Es ist wichtig zu planen, wann Produkte abgekündigt werden sollten, um das Risiko zu vermeiden, Geräte zu verwenden, die nicht mehr unterstützt werden und möglicherweise ungepatchte Schwachstellen aufweisen. Axis zeigt an, wann die Unterstützung für das Betriebssystem eines Produkts endet. Auf diese Weise können Sie sich rechtzeitig darauf vorbereiten, ein Gerät außer Betrieb zu nehmen und zu ersetzen. Darüber hinaus können Sie mit AXIS Device Manager Extend Informationen zu Garantie, Produktabkündigungen und Supportende für alle Geräte im System abrufen.

Es ist auch wichtig, die Daten auf einem außer Betrieb genommenen Gerät zu löschen. Durch Zurücksetzen auf die Werkseinstellungen können Sie schnell alle Konfigurationen und Daten auf dem Gerät löschen. Weitere Informationen zur Außerbetriebnahme von Produkten finden Sie auf dem AXIS OS-Portal.

Compliance

Regierungen erlassen immer mehr Gesetze und Vorschriften zur Cybersicherheit. Jedes Unternehmen, das in diesen Ländern tätig ist, muss sie einhalten. Gleichzeitig verlangen Branchen und Organisationen zunehmend die Einhaltung bestimmter Standards, einschließlich der Zertifizierung von Produkten und Dienstleistungen. Alle Beteiligten sind dafür verantwortlich, Gesetze und Vorschriften einzuhalten und die für ihre Geschäftsprozesse relevanten Richtlinien und Vorgaben umzusetzen.

Cybersicherheits-Compliance als Ausgangspunkt

Cybersicherheits-Compliance bedeutet, dass die von den Behörden festgelegten Standards und regulatorischen Anforderungen eingehalten werden. Standards und Zertifizierungen sind zwar wichtig, aber nur eine Seite der Medaille.

Es besteht immer die Gefahr, dass die Einhaltung von Standards und Zertifizierungen zu einer reinen Formsache wird.

Die Cybersicherheit-Compliance entwickelt sich ständig weiter, und was früher „nice to have" war, wird schnell zur Pflicht.

Aus diesem Grund müssen Organisationen und Unternehmen Standards und Zertifizierungen als Ausgangspunkt betrachten Durch Halbgeviertstrich + geschütztes Leerzeichen ersetzen als Mindestanforderung und nicht als Ziel. Das eigentliche Ziel ist, dass Lieferanten Produkte und Dienstleistungen liefern, die auf die sicherste Art und Weise verwendet werden können. Ein weiteres Ziel ist die Transparenz gegenüber den Kunden und die Beratung, damit diese ihre Cybersicherheit gewährleisten und kontinuierlich verbessern können.

Vorschriften

Die Vorschriften im Bereich der Cybersicherheit verpflichten Organisationen, ihre Systeme und Informationen zu schützen und sicherzustellen, dass die von ihnen angebotenen Produkte und Dienstleistungen ein Mindestmaß an Sicherheit aufweisen. Im Folgenden werden einige wichtige Vorschriften und ihre Umsetzung erläutert.

Die NIS2-Richtlinie wird 2023 in Kraft treten und die Mitgliedstaaten der Europäischen Union haben bis Oktober 2024 Zeit, sie in nationales Recht umzusetzen. Diese Richtlinie wird alle EU-Unternehmen in wichtigen Sektoren dazu verpflichten, ein einheitlich hohes Cybersicherheitsniveau zu gewährleisten. Unternehmen können für mangelnde Cybersicherheit bestraft werden, auch wenn dies auf Fehler ihrer Zulieferer zurückzuführen ist.

Die Bewertung von Lieferanten und die Sicherheit der Lieferkette werden daher in Zukunft noch wichtiger werden. Die Richtlinie nimmt Hersteller, Importeure und Händler indirekt in die Pflicht. Sie müssen sicherstellen, dass sie die Sorgfaltspflicht während des gesamten Produktlebenszyklus einhalten.

Im Dezember 2023 erzielte die EU eine vorläufige Einigung über eine neue Verordnung mit der Bezeichnung Cyber Resilience Act. Darin werden gemeinsame Cybersicherheitsstandards für Hardware- und Softwareprodukte mit digitalen Elementen festgelegt. Dazu gehören Produkte, die direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden sind, wie beispielsweise IoT-Geräte. Die vorgeschlagene Verordnung zielt darauf ab, die Zahl der Cybervorfälle zu verringern und gleichzeitig die Transparenz zu erhöhen und den Datenschutz zu verbessern. Das Vereinigte Königreich hat ein ähnliches Gesetz mit dem Titel UK Product Security and Telecommunications Infrastructure verabschiedet, das im April 2024 in Kraft treten wird

Organisationen, die mit US-Behörden Geschäfte machen, müssen möglicherweise auch Standards wie die Cybersecurity Maturity Model Certification einhalten, die ein Audit-Zertifikat auf der Grundlage des internen Managements von Cybersicherheitsprozessen vorschreibt.

Um Cybersicherheit sicherzustellen, bedarf es ständiger Wachsamkeit und Wartung.

Standards und Zertifizierungen

Die meisten Standards und Zertifizierungen beziehen sich auf Funktionen, Gegenmaßnahmen und Prozesse, um sicherzustellen, dass Sicherheit ein integraler Bestandteil ist. Dies kann durch Tests Dritter wie Penetrationstests und Bug-Bounty-Programme ergänzt werden, um Schwachstellen in der Software zu finden.

Produktzertifizierungen können Kunden und Behörden ein gewisses Maß an Sicherheit geben, allerdings ist zu beachten, dass Zertifizierungen in der Regel nur ein Jahr gültig sind und das Produkt danach erneut zertifiziert werden muss. Da ständig neue Technologien und Funktionen entwickelt und eingeführt werden, können Zertifizierungen veraltet sein.

Beachten Sie auch, dass Standards zwar die Cybersicherheit verbessern können, aber keinen garantierten Schutz vor Cybervorfällen bieten. Organisationen müssen Bedrohungen und Sicherheitsrichtlinien ständig überprüfen.

Warum Axis?

Cybersicherheit fördern

Cybersicherheit ist ein zentraler Bestandteil von Axis. Sie ist die Grundlage für unser internes Informationssicherheitssystem, unser Lieferkettenmanagement, die Entwicklung unserer Produkte und Dienstleistungen und unseren Umgang mit Schwachstellen in der Software. Cybersicherheit ist für uns eine gemeinsame und fortwährende Verantwortung, bei der Transparenz der Schlüssel ist. Wir möchten, dass Sie unsere Angebote so sicher wie möglich nutzen können. Aus diesem Grund entwickeln und produzieren wir unsere Produkte mit integrierten Cybersicherheitsfunktionen sowie mit schützenden Standardeinstellungen und stellen Härtungsleitfäden zur Verfügung. Wir beobachten kontinuierlich die Bedrohungslage und prüfen, wie wir die Sicherheit verbessern können. Als CVE Numbering Authority reagieren wir auf neu entdeckte Schwachstellen, indem wir sie patchen und veröffentlichen. So können Sie rechtzeitig geeignete Maßnahmen ergreifen. Wir stellen Ihnen Software-Upgrades zur Verfügung, mit denen Sie die Sicherheit von Axis Geräten auch nach der Installation weiter verbessern können. Und mit Tools wie AXIS Device Manager und AXIS Device Manager Extend erleichtern wir Ihnen die Verwaltung Ihrer Axis Geräte, um Cybersicherheitsrisiken während ihres gesamten Lebenszyklus zu minimieren.

Weitere Gründe, die für Axis sprechen

> **Unsere Arbeit zeichnet sich durch Qualität aus:**
Alle unsere Produkte werden umfassend getestet, damit unsere Kunden sich keine Sorgen machen müssen.

> **Innovative Technologie:**
Wir kombinieren Technologie und menschliche Vorstellungskraft, um sowohl die Leistung als auch die Nutzbarkeit zu verbessern. Sie beruht auf offenen Branchenstandards, ist flexibel, skalierbar und problemlos integrierbar.

> **Nachhaltigkeit auf jeder Ebene:**
Axis zeigt fortlaufendes und anerkanntes Engagement für ökologisch verantwortliche Entwicklung unter Einsatz nachhaltiger Materialien. Etwa 90 % der 2022 eingeführten Axis Kameras und Encoder sind frei von PVC.

> **Globale Präsenz mit lokaler Expertise:**
Axis hat die weltweit größte installierte Basis von Netzwerk-Videoprodukten und Mitarbeitende in über 50 Ländern. Wir teilen Erkenntnisse und Erfahrungen und halten uns über die neuesten Entwicklungen auf dem Laufenden.

> **Die Stärke von Partnerschaften:**
Unser Engagement für unsere Partner hat Axis zur am häufigsten integrierten Marke für Sicherheitsprodukte auf dem Markt gemacht.

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.