CYBERSICHERHEIT

Lebenszyklus-Management für Geräte

Es gibt in jeder Phase des Lebenszyklus eines vernetzten Geräts Cyber-Risiken, von der Produktion bis zur Außerbetriebnahme. Wenn diese Risiken nicht berücksichtigt werden, können sie zu Betriebsunterbrechungen und zum Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Daten führen. Deshalb müssen alle Stakeholder, vom Lieferanten bis zum Endkunden, die Verantwortung für das Risikomanagement übernehmen.

Bei der Beschaffung ist es daher wichtig, den Lebenszyklus der Gerätesicherheit zu berücksichtigen. Ein Hersteller sollte Maßnahmen ergreifen, um Cyber-Risiken zu reduzieren, bevor der Kunde das Produkt erhält, während das Produkt in Betrieb ist und wenn das Produkt außer Betrieb genommen wird.

Auf den folgenden Seiten finden Sie einen Überblick über die von Axis unterstützten Technologien, Tools und Anleitungen sowie über die Ansätze und Prozesse zur Risikominimierung während des gesamten Lebenszyklus eines Axis Geräts.

Sicherheitsgrundlage: Axis Edge Vault, AXIS OS, Axis Security Development Model

Sicherheitsgrundlage – Hardware, Software und Ansatz

Schutz der Integrität des Produkts und Reduzierung des Risikos von Schwachstellen von Anfang an

Axis Edge Vault Cybersicherheitsplattform
Diese hardwarebasierte Plattform unterstützt Funktionen, die die Identität und Integrität des Geräts vor unbefugtem Zugriff schützen. Auf diese Weise können Sie das Gerät sicher starten, es integrieren und sicherstellen, dass sensible Daten wie kryptografische Schlüssel geschützt sind.

Betriebssystem AXIS OS
AXIS OS steuert eine Reihe von Axis Geräten. AXIS OS berücksichtigt die Best Practices der Branche für das Schwachstellen-Management und bietet eine Plattform für die schnelle und effiziente Veröffentlichung von Sicherheitsfunktionen und Patches für die Software zahlreicher Produkte.

Axis Security Development Model(ASDM)
Es ist eine Methode von Axis, um das Risiko der Veröffentlichung von Produkten mit Schwachstellen in der Software zu reduzieren. ASDM stellt sicher, dass Sicherheitsaspekte ein integraler Bestandteil der Softwareentwicklung sind. Dazu gehören unter anderem Risikobewertungen, Bedrohungsmodelle, Code-Analysen, Penetrationstests, Bug-Bounty-Programme sowie das Scannen und Verwalten von Schwachstellen.

Transparenz
Transparenz ist ein wichtiger Teil der Arbeitsweise von Axis, um Vertrauen aufzubauen. Axis ist eine Common Vulnerability and Exposures (CVE) Numbering Authority. Wir veröffentlichen Schwachstellen und benachrichtigen die Stakeholder darüber, damit die Kunden geeignete Maßnahmen ergreifen können. Wir veröffentlichen auch eine Software Bill of Materials (SBOM) für AXIS OS.

PRODUKTION UND DISTRIBUTION

Reduzierung des Risikos von kompromittierten Komponenten

- **Lieferkette:** Kritische Komponenten werden direkt von strategischen Lieferanten beschafft. Axis arbeitet eng mit Produktionspartnern 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.
- **Axis Edge Vault:** Wird während der Produktion auf einem Axis Gerät installiert und umfasst die folgenden Funktionen:
  - **Sicherer Schlüsselspeicher,** der kryptografische Rechenmodule (wie Secure Element, Trusted Platform Module, Trusted Execution Environment) zur manipulationssicheren Speicherung von kryptografischen Schlüsseln umfasst.
  - **Signierte Firmware,** die garantiert, dass das installierte AXIS OS wirklich von Axis ist. Sie stellt sicher, dass jede neue Firmware, die heruntergeladen und auf dem Gerät installiert wird, auch von Axis signiert ist.
  - **Sicherer Systemstart,** mit dem das Gerät prüfen kann, ob die Firmware eine Signatur von Axis hat. Wenn die Firmware nicht autorisiert ist oder verändert wurde, wird der Systemstart abgebrochen und das Gerät schaltet sich ab. Die Kombination aus signierter Firmware, sicherem Systemstart und dem Zurücksetzen auf Werkseinstellungen eines Geräts bietet Schutz vor schädlichen Änderungen während des Versands eines Geräts.
  - **Axis Geräte-ID,** ein eindeutiges Zertifikat mit entsprechenden Schlüsseln, das die Authentizität eines Axis Geräts nachweisen kann. Axis Geräte-ID basiert auf IEEE 802.1AR und ermöglicht die sichere Identifizierung von Geräten und die Integration in ein Netzwerk.
  - **Ein verschlüsseltes Dateisystem**, das die kundenspezifische Konfiguration und die im Dateisystem gespeicherten Informationen davor schützt, extrahiert oder manipuliert zu werden, wenn das Gerät nicht benutzt wird. Dies ist zum Beispiel der Fall, wenn es von einem Systemintegrator zum Endkunden geliefert wird.

IMPLEMENTIERUNG

Umgang mit den Risiken, die entstehen, wenn kompromittierte oder unzureichend gesicherte Produkte in das Netzwerk integriert werden. Dies kann zu unbefugtem Zugriff, zum Abgreifen sensibler Daten und zur Übertragung veränderter Daten zwischen Netzwerkendpunkten führen.

- **Werkseinstellung:** Setzen Sie das Gerät auf die Werkseinstellungen zurück, bevor Sie es konfigurieren. Dies garantiert, dass das Gerät völlig frei von unerwünschter Software oder Konfigurationen ist, da die einzige verbleibende Software AXIS OS und seine Standardeinstellungen sind.
- **Nach der neuesten Firmware für das Gerät suchen:** Zwischen der Produktion und der Implementierung kann einige Zeit vergangen sein. Daher ist es ratsam, auf der Axis Website nach der neuesten Firmware zu suchen, die möglicherweise die neuesten Fehlerbehebungen für das jeweilige Gerät enthält.
- **Axis Geräte-ID:** Um sicherzustellen, dass nur echte Axis Geräte im Netzwerk implementiert werden, kann die Axis Geräte-ID mithilfe der IEEE 802.1X-Authentifizierung oder beim Aufbau einer sicheren Netzwerkverbindung über das HTTPS-Protokoll überprüft werden. In einem IEEE 802.1X-Netzwerk kann die Axis Geräte-ID eingesetzt werden, um die Sicherheit zu erhöhen und die Bereitstellungszeit zu verkürzen.
- **Sicherer Schlüsselspeicher:** Der sichere Schlüsselspeicher umfasst kryptografische Rechenmodule und speichert sensible Daten wie die Axis Geräte-ID und vom Kunden hinterlegte Schlüssel. Er verhindert den unbefugten Zugriff und das böswillige Abgreifen sensibler Daten, selbst wenn das Gerät kompromittiert wird.
- **Verschlüsseltes Dateisystem:** Dies stellt sicher, dass keine im Dateisystem gespeicherten Daten abgegriffen oder verfälscht werden können, wenn das Gerät nicht benutzt wird.
- **Härtungsleitfaden:** Der AXIS OS Härtungsleitfaden, der auf dem AXIS OS Portal auf der Website von Axis verfügbar ist, bietet eine Basiskonfiguration für gängige Bedrohungen und enthält Best Practices sowie technische Empfehlungen. Es gibt auch einen Härtungsleitfaden für die Video Management Software (AXIS Camera Station VMS) sowie für Axis Netzwerk-Switches.
- **AXIS OS Security Scanner Guide:** Axis empfiehlt die Ausführung von Sicherheitsscans für Axis Geräte, um festzustellen, ob sie Schwachstellen aufweisen oder fehlerhaft konfiguriert sind. Der AXIS OS Security Scanner Guide enthält Empfehlungen, wie bestimmte Meldungen der Scanner gelöst werden können, und gibt einen Überblick über die häufigsten „False Positives".
- **AXIS Device Manager:** Dieses Tool unterstützt die effiziente lokale Konfiguration und Verwaltung von Axis Geräten. Der AXIS Device Manager ermöglicht die Batch-Verarbeitung von Installations- und Sicherheitsaufgaben, wie z. B. die Verwaltung der Geräte-Zugangsdaten, die Bereitstellung von Zertifikaten, die Deaktivierung nicht genutzter Dienste oder die Aktualisierung von AXIS OS.

IM BETRIEB

Umgang mit Risiken, die entstehen, wenn Firmware mit bekannten Schwachstellen ausgeführt wird, wenn Geräte mit nicht authentifizierter Firmware aktualisiert werden oder wenn sichere Konfigurationen verfallen

> **Aktualisierung der Firmware:** Es ist wichtig, die Cybersicherheit eines Axis Geräts aufrechtzuerhalten, indem die Firmware entweder über den AXIS OS Active Track oder den Long Term Support (LTS) Track aktualisiert wird. Die kostenlosen Firmware-Updates, die über beide Tracks bereitgestellt werden, enthalten Sicherheits-Patches. Die signierte Firmware stellt sicher, dass nur echte Firmware von Axis installiert werden kann.

> **AXIS Device Manager Extend:** Dieses Tool, das den AXIS Device Manager ergänzt, ermöglicht die Fernverwaltung von Axis Geräten und vereinfacht die Skalierung von Wartungsaufgaben, wie z. B. die Aktualisierung der Firmware eines Geräts.

> **Schwachstellen-Management:** Axis bietet einen Benachrichtigungsdienst für Informationen über Schwachstellen und andere sicherheitsrelevante Angelegenheiten für Axis Produkte. Abonnieren Sie den Dienst, um künftig Benachrichtigungen zu erhalten.

> **AXIS OS Forensic Guide:** Der 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.

> **Signiertes Video:** Wenn diese Funktion in einer unterstützten Kamera aktiviert ist, werden dem Videostream kryptografische Signaturen hinzugefügt, bevor das Video das Gerät verlässt. So lässt sich nachprüfen, ob das Video manipuliert wurde oder nicht. Dies ist besonders wichtig bei einer Täter-Ermittlung oder Strafverfolgung.

AUSSERBETRIEBNAHME

Umgang mit dem Risiko von Geräten, die nicht mehr unterstützt werden und bekannte Schwachstellen aufweisen, die nicht gepatcht wurden, sowie mit dem Risiko sensibler Daten, die nach der Entsorgung auf den Geräten zurückbleiben

> **Einstellungsdatum des Firmware-Supports:** Auf der Support-Webseite für viele Produkte auf Axis.com wird das Einstellungsdatum des Firmware-Supports des jeweiligen Produkts angegeben. Kunden können dadurch die Außerbetriebnahme und den Austausch des Produkts rechtzeitig planen.

> **AXIS Device Manager Extend:** Ermöglicht die einfache Überprüfung des Garantiestatus für alle Geräte im System, einschließlich Informationen zur Produktabkündigung und zum Support-Ende. Mit diesen Informationen können Sie ein Gerät für die Außerbetriebnahme vorbereiten und das Risiko eines nicht unterstützten Geräts beseitigen.

> **Anleitung:** Auf dem AXIS OS Portal auf der Axis Website finden Sie Anleitungen zur Außerbetriebnahme eines Axis Geräts. Wenn Sie ein Gerät auf Werkseinstellungen zurücksetzen, werden alle Konfigurationen und Daten gelöscht.

Weitere Informationen finden Sie unter: **www.axis.com/de-de/cybersecurity**