Q&A zur Cybersicherheit

Benutzerhandbuch

Weitere Fragen und Antworten finden Sie in der *FAQ-Datenbank* von Axis.

Allgemeine Fragen

Was ist Cybersicherheit?

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

Bei Cybersicherheit geht es darum, Risiken über einen längeren Zeitraum zu verwalten. Risiken können niemals eliminiert, nur verringert werden.

Was ist im Allgemeinen mit dem Management der Cybersicherheit verbunden?

Bei Cybersicherheit geht es um Produkte, Menschen, Technologie und Prozesse.

Es geht daher darum, verschiedene Aspekte Ihrer Organisation zu **identifizieren** und zu bewerten. Dazu gehören das Erstellen eines Geräte-, System-, Software- und Firmware-Inventars, das Festlegen unternehmenskritischer Ziele, das Dokumentieren von Verfahren und Sicherheitsrichtlinien, das Anwenden einer Risiko-Management-Strategie und das kontinuierliche Durchführen von Risikobewertungen für Ihre Anlagen.

Es geht dabei um die Implementierung von Sicherheitskontrollen und Maßnahmen zum **Schutz** der Daten, Geräte, Systeme und Einrichtungen, die Sie als Priorität gegen Cyberangriffe identifiziert haben.

Außerdem werden Aktivitäten entwickelt und durchgeführt, die Ihnen bei der **Erkennung** von Cyberangriffen helfen, sodass Sie zeitnah Maßnahmen ergreifen können. Dies kann beispielsweise ein SIEM-System (Security Information and Event Management) oder ein SOAR-System (Security Orchestration, Automation and Response) umfassen, das die Daten von Netzwerkgeräten und Verwaltungssoftware verwaltet, Daten auf anormales Verhalten oder potenzielle Cyberangriffe hin untersucht und diese Daten analysiert, um Echtzeitalarme zu liefern. Axis Geräte unterstützen SYS-Protokolle und Remote-SYS-Protokolle, die die Hauptdatenquelle für Ihr SIEM- bzw. SOAR-System sind.

Das Cybersicherheitsmanagement umfasst auch die Entwicklung und Implementierung von Verfahren zur **Reaktion** auf Cybersicherheitsvorfälle, sobald diese erkannt wurden. Beachten Sie dabei die örtlichen Vorschriften und internen Richtlinien sowie die Anforderungen bezüglich der Kommunikation von Cybersicherheitsvorfällen. Axis bietet einen *AXIS OS Forensic Guide* an, mit dem Sie erkennen, ob ein Axis Gerät während eines Cybersicherheitsangriffs gefährdet wurde.

Die Entwicklung und Umsetzung von Maßnahmen zur Aufrechterhaltung von Plänen für die Widerstandsfähigkeit und zur **Wiederherstellung** von Fähigkeiten oder Diensten, die durch einen Vorfall im Bereich der Cybersicherheit beeinträchtigt wurden, sind ebenfalls wichtig. Die Anwendung *Axis Device Manager* kann Axis Geräte beispielsweise einfach wiederherstellen, indem Wiederherstellungspunkte verwendet werden, die zu einem bestimmten Zeitpunkt als Schnappschüsse der Systemkonfiguration gespeichert wurden. Wenn kein relevanter Wiederherstellungspunkt vorhanden ist, kann das Tool dabei helfen, alle Geräte in ihren Standardzustand zurückzusetzen und gespeicherte Konfigurationsvorlagen über das Netzwerk zu übertragen.

Welche Risiken bestehen für die Cybersicherheit?

Cybersicherheitsrisiken (wie durch das RFC 4949 Internet Security Glossar definiert) bestehen in der Wahrscheinlichkeit, dass eine bestimmte Bedrohung eine bestimmte Schwachstelle ausnutzen wird, die ein besonders schädliches Ergebnis zur Folge hat.

Es ist wichtig, klare Systemrichtlinien und -prozesse festzulegen, um langfristig eine angemessene Risikoreduzierung zu erreichen. Es wird empfohlen, ein gut definiertes IT-Schutzgerüst zu verwenden, z. B. ISO 27001, NIST oder Ähnliches. Diese Aufgabe kann für kleinere Organisationen zwar eine Überforderung sein, doch ist eine selbst minimale Richtlinien- und Prozessdokumentation weitaus besser als gar keine.

Informationen zur Einschätzung und Priorisierung von Risiken finden Sie im *Referenzhandbuch zur Cybersicherheit*.

Welche Bedrohungen gibt es?

Eine Bedrohung kann als alles definiert werden, was Ihre Vermögenswerte oder Ressourcen gefährden oder schädigen kann. Im Allgemeinen neigen Menschen dazu, Cyber-Bedrohungen böswilligen Hackern und Malware zuzuordnen. In der Realität treten häufig negative Auswirkungen durch Unfälle, unbeabsichtigten Missbrauch oder Hardwarefehler auf. Angriffe können als opportunistisch oder gezielt bezeichnet werden. Die meisten Angriffe sind heute opportunistisch: Angriffe, die nur stattfinden, weil sich eine günstige Gelegenheit bietet. Solche Angriffe werden mit kostengünstigen Angriffsmethoden wie Phishing oder Austesten verwendet. Das Anwenden eines Standardschutzes verringert die mit opportunistischen Angriffen verbundenen Risiken.

Es ist schwieriger, sich gegen Angreifer zu schützen, die ein bestimmtes System mit einem bestimmten Ziel ins Visier nehmen. Gezielte Angriffe verwenden die gleichen kostengünstigen Angriffsmethoden wie opportunistische Angreifer. Wenn die anfänglichen Angriffe jedoch scheitern, sind sie entschlossener und sparen Zeit und Ressourcen, um ausgefeiltere Methoden zu verwenden, um ihre Ziele zu erreichen. Für sie geht es vor allem darum, wie viel Wert auf dem Spiel steht.

Welche Bedrohungen sind am häufigsten und wie können diese behandelt werden?

Vorsätzlicher oder versehentlicher Missbrauch eines Systems

Personen mit einem legitimen Zugang zu einem System sind eine der häufigsten Bedrohungen für jedes System. Sie können auf Dienste zugreifen, zu denen sie nicht berechtigt sind. Sie können stehlen oder das System vorsätzlich schädigen. Menschen können auch Fehler machen. Sie können beim Versuch, Probleme zu lösen, unbeabsichtigt die Systemleistung beeinträchtigen. Einzelpersonen sind auch für Social Engineering anfällig. Das sind Tricks, mit denen legitimierte Benutzer vertrauliche Informationen verraten. Einzelpersonen können wichtige Komponenten (Zugangskarten, Telefone, Laptops, Dokumentationen usw.) verlieren oder verlegen. Die Computer von Personen können kompromittiert werden und ein System unbeabsichtigt mit Malware infizieren.

Zu den empfohlenen Schutzmaßnahmen gehören definierte Benutzerkontenrichtlinien und -verfahren, ein ausreichendes Authentifizierungsschema für den Zugriff, Tools zum Verwalten von Benutzerkonten und Zugriffsrechten im Laufe der Zeit, Verringerung der Gefährdung und Schulungen zur Sensibilisierung für Cyberfragen.

Axis begegnet dieser Bedrohung mit den *Härtungsleitfäden* und der Software für das Gerätemanagement und *Video Management Software.*

Physische Manipulation und Sabotage

Physisch freiliegende Geräte können manipuliert, gestohlen, abgeklemmt, umgelenkt oder durchtrennt werden.

Zu den empfohlenen Schutzmaßnahmen gehören das Platzieren von Netzwerkbestandteilen (z. B. Servern und Switches) in verriegelten Bereichen, die Montage von Kameras an schwer zu erreichenden Stellen, die Verwendung eines geschützten Gehäuses bei physischer Exposition sowie der Schutz von Kabeln in Wänden oder Schächten.

Axis hilft, dieser Bedrohung durch *Schutzgehäuse* für Geräte, manipulationssichere Schrauben, Kameras mit der Möglichkeit zur Verschlüsselung von SD-Karten, Erkennung bei Manipulation der Kameraansicht und Erkennung eines offenen Gehäuses entgegen zu wirken.

Ausnutzung von Schwachstellen in der Software

Alle softwarebasierten Produkte haben Sicherheitslücken (bekannt oder unbekannt), die ausgenutzt werden können. Die meisten Sicherheitslücken haben ein geringes Risiko, d. h. sie sind nur schwer zu nutzen oder die nachteiligen Auswirkungen begrenzt. Gelegentlich können entdeckte und ausnutzbare Schwachstellen erhebliche negative Auswirkungen haben. MITRE beherbergt eine große Datenbank mit CVE (Common Vulnerabilities & Exposures), um andere bei der Risikominderung zu unterstützen.

Zu den empfohlenen Schutzmaßnahmen gehören ein kontinuierliches Patching-Verfahren, das die Anzahl der bekannten Sicherheitslücken in einem System minimiert, die Netzwerkbelastung minimiert, das Ausnutzen bekannter Sicherheitslücken erschwert und die Zusammenarbeit mit vertrauenswürdigen Subanbietern ermöglicht, die Richtlinien und Verfahren zur Minimierung von Schwachstellen verwenden, Patches bereitstellen und bezüglich entdeckter kritischer Sicherheitslücken transparent sind.

Axis begegnet der Bedrohung mit dem *Axis Security Development Model*, das darauf abzielt, ausnutzbare Schwachstellen in der Axis Software zu minimieren; und mit der *Axis Vulnerability Management Policy*, die Schwachstellen identifiziert, behebt und ankündigt, über die Kunden Bescheid wissen müssen, um geeignete Aktionen zu ergreifen. (Ab April 2021 ist *Axis eine Common Vulnerabilities and Exposures Numbering Authority* für Axis Produkte, wodurch wir unsere Prozesse an den Industriestandardprozess der MITRE Corporation anpassen können.) Axis bietet auch *Härtungsleitfäden* mit Empfehlungen, wie die Belichtung reduziert und Kontrollen hinzugefügt werden können, um das Risiko einer Ausnutzung zu verringern. Axis bietet Benutzern *verschiedene Tracks für die Gerätesoftware*, um das Betriebssystem eines Axis Geräts auf dem neuesten Stand zu halten: Zwei der Haupt-Tracks sind:

1. Der aktive Track bietet Aktualisierungen für die Gerätesoftware, die neue Funktionen sowie Bugfixes und Sicherheits-Patches unterstützen.
2. Der Long-Term Support (LTS)-Track bietet Aktualisierungen für die Gerätesoftware, die Bugfixes und Sicherheits-Patches unterstützen und gleichzeitig das Risiko von Inkompatibilitäten mit Systemen von Drittanbietern minimieren.

Supply Chain-Angriffe

Ein Supply Chain-Angriff ist eine Cyberattacke, die Unternehmen schaden soll, indem sie auf weniger sichere Elemente in der Supply Chain zielt. Der Angriff erfolgt durch die Kompromittierung von Software/Betriebssystem/Produkten und die Verlockung eines Administrators, diese im System zu installieren. Ein Produkt kann während des Transports zum Eigentümer des Systems beschädigt werden.

Zu den empfohlenen Schutzrichtlinien gehören die Installation von Software nur von vertrauenswürdigen und verifizierten Quellen, die Überprüfung der Software-Integrität durch Vergleichen der Software-Prüfsumme (Digest) mit der Prüfsumme des Herstellers vor der Installation sowie die Überprüfung der Produktlieferdaten auf Manipulation.

Axis kontert diese Bedrohung auf unterschiedliche Weise. Axis veröffentlicht Software mit einer Prüfsumme, damit Administratoren vor der Installation die Integrität prüfen können. Wenn ein neues Betriebssystem (OS) auf das Gerät geladen werden soll, akzeptieren vernetzte Axis Geräte nur von Axis signierte Gerätesoftware. *Sicheres Hochfahren* auf vernetzten Axis Geräten gewährleistet zudem, dass die Geräte nur mit signiertem OS ausgeführt werden. Und jedes Gerät verfügt über eine eindeutige Axis Geräte-ID, mit der das System überprüfen kann, ob es sich bei dem Gerät um ein echtes Axis Produkt handelt. Details zu solchen Cybersicherheitsfunktionen finden Sie im Whitepaper *Axis Edge Vault*.

Weitere Informationen zu Bedrohungen finden Sie in unserem *Referenzhandbuch zur Cybersicherheit*.

Was sind Sicherheitslücken?

Sicherheitslücken bieten Kontrahenten die Möglichkeit, Angriffe auszuführen oder Zugang zu einem System zu erhalten. Sie können auf Mängeln, Merkmalen oder menschlichen Fehlern beruhen. Böswillige Angriffe können bekannte Sicherheitslücken ausnutzen, und dabei häufig eine oder mehrere kombinieren. Die meisten erfolgreichen Angriffe sind auf menschliche Fehler, schlecht konfigurierte Systeme und schlecht gewartete Systeme zurück zu führen – oftmals aufgrund fehlender ausreichender Richtlinien, nicht festgelegter Verantwortlichkeiten und geringer Bekanntheit.

Welche Sicherheitslücken in der Software gibt es?

Eine Geräte-API (Application Programming Interface) und Softwaredienste können Schwachstellen oder Funktionen aufweisen, die bei Angriffen ausgenutzt werden können. Kein Anbieter kann garantieren, dass Produkte keine Mängel aufweisen. Wenn die Schwachstellen bekannt sind, können die Risiken durch Sicherheitsmaßnahmen verringert werden. Andererseits steigt das Risiko, wenn ein Angreifer einen neuen unbekannten Fehler entdeckt, da das Opfer keine Zeit hatte, das System zu schützen.

Was ist das Common Vulnerability Scoring System (CVSS)?

Das *Common Vulnerability Scoring System* (CVSS) ist eine Möglichkeit, die Schwere einer Software-Schwachstelle einzuordnen. Es handelt sich um eine Formel, die berücksichtigt, wie leicht ein Angriff erfolgen kann und welche negativen Auswirkungen er haben könnte. Die Punktzahl liegt zwischen 0 und 10. Der Wert 10

entspricht der größten Schwere. Häufig finden Sie CVSS-Zahlen in veröffentlichten Berichten zur Common Vulnerability and Exposure (CVE).

Axis verwendet CVSS als eine der Maßnahmen, um zu ermitteln, wie kritisch eine identifizierte Schwachstelle in der Software/dem Produkt sein kann.

Spezifische Fragen zu Axis

Welche Schulungen und Anleitungen unterstützen mich dabei, mehr über Cybersicherheit zu erfahren und was ich tun kann, um Produkte und Dienstleistungen besser vor Cyber-Vorfällen zu schützen?

Auf der Webseite *Ressourcen* erhalten Sie Zugang zu Hardening-Anleitungen (z. B. *AXIS OS Hardening Guide*, *AXIS Camera Station Pro System Hardening Guide* und *Axis Network Switches Hardening Guide*), Richtliniendokumente und mehr. Axis bietet zudem *E-Learning-Kurse* zur Cybersicherheit an.

Wo finde ich das aktuelle Betriebssystem für mein Gerät?

Rufen Sie *Gerätesoftware* auf und suchen Sie nach Ihrem Produkt.

Wie kann ich das Betriebssystem auf meinem Gerät einfach aktualisieren?

Zur Aktualisierung der Software für Ihr Gerät können Sie die *Software für das Gerätemanagement von Axis verwenden.*

Wie kann ich bei Störungen der Axis Dienste informiert werden?

Besuchen Sie *status.axis.com*.

Wie kann ich über eine entdeckte Sicherheitslücke benachrichtigt werden?

Sie können den *Axis Security Notification Service* abonnieren.

Wie geht Axis mit Sicherheitslücken um?

Siehe *Schwachstellenmanagement bei Axis*.

Wie minimiert Axis die Sicherheitslücken in der Software?

Lesen Sie den Artikel *Cybersicherheit als integraler Bestandteil der Softwareentwicklung von Axis*.

Wie unterstützt Axis die Cybersicherheit über den gesamten Lebenszyklus eines Geräts hinweg?

Besuchen Sie *A lifecycle approach to cybersecurity*.

Welche Cybersicherheitsmerkmale sind in Axis Produkte integriert?

Mehr lesen:

- *Axis Edge Vault*
- *AXIS OS*
- *Cybersicherheit, auf die Verlass ist – ein Geräteleben lang*
- *Verpflichtung zur Sicherheit durch Design (Secure by Design)*

Ist Axis ISO-zertifiziert und mit welchen anderen Cybersicherheit-relevanten Vorschriften ist Axis konform?

Ja, AXIS ist nach *ISO/IEC 27001:2023* zertifiziert. Das Unternehmen verfügt über ein Verwaltungssystem für Informationssicherheit (ISMS), das die Anforderungen in Bezug auf die Entwicklung und den Betrieb von Software, Cloud-Diensten und IT-Infrastruktur erfüllt.

Die Axis Communications UK Ltd. besitzt eine *Cyber Essentials Plus*-Zertifizierung.

Axis Geräte mit *AXIS OS 11*oder höher sind nach dem Cybersicherheitsstandard *ETSI EN 303 645 zertifiziert*. AXIS OS Netzwerkprodukte sind außerdem mit dem IT-Sicherheitskennzeichen des deutschen Bundesamtes für Sicherheit in der Informationstechnik (*BSI - Bundesamt für Sicherheit in der Informationstechnik*) versehen.

Die neuesten Informationen über die Erfüllung der Cybersicherheitsanforderungen und Zertifizierungen von AXIS finden Sie unter *Axis Trust Center*.

Wie unterstützt Axis Unternehmen bei der Einhaltung von NIS 2?

Lesen Sie hierzu den Artikel zu *NIS 2*.

T10189380_de

2026-01 (M7.2)