Cybersecurity reference guide

Benutzerhandbuch

Cybersecurity reference guide

Inhalt

Cybersecurity reference guide

Einführung

Einführung

Dieser Leitfaden soll als Grundlage für ein gemeinsames Basismaterial dienen und als Referenz für von Axis hergestellte Materialien zur Cybersicherheit dienen. Dies sind vereinfachte Beschreibungen, Modelle und Strukturmodelle auf Grundlage von NIST-, SANS-, ISO- und RSA-Skripten sowie Materialien von verschiedenen Organisationen der Cybersicherheitsbranche.

Links zu anderen Materialien von Axis:

- *axis.com/about-axis/cybersecurity*
- *help.axis.com/cybersecurity-qna*
- *axis.com/support/cybersecurity/resources*
- *help.axis.com/axis-security-development-model*
- *axis.com/support/cybersecurity/vulnerability-management*

Definition von Cybersicherheit

Zum Teil basierend auf der Definition von NIST:

Cybersicherheit ist der Schutz von Computersystemen und -diensten vor Cyberattacken. 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.

Organisationsarten

Verschiedene Organisationen verfügen über unterschiedliche Vermögenswerte, Ressourcen, Exposition und Cybermündigkeit. *Die CIS Controls (vormals Critical Security Controls)* definieren drei Profile, die für die Organisationsprofile empfohlen werden.

- **SANS Implementation Group 1 (IG1)**

  In den meisten Fällen sind IG1-Unternehmen kleine bis mittelgroße Unternehmen mit begrenztem IT- und Cybersicherheitswissen zum Schutz von IT-Anlagen und Mitarbeitern.

- **SANS Implementation Group 2 (IG2)**

  IG2-Unternehmen beschäftigen Mitarbeiter, die für die Verwaltung und den Schutz der IT-Infrastruktur verantwortlich sind. Diese Unternehmen haben in der Regel mehrere Abteilungen mit unterschiedlichen Risikoprofilen, die von Arbeit und Mission abhängen. Kleine Unternehmen haben möglicherweise Vorschriften zur Einhaltung gesetzlicher Bestimmungen.

- **SANS Implementation Group 3 (IG3)**

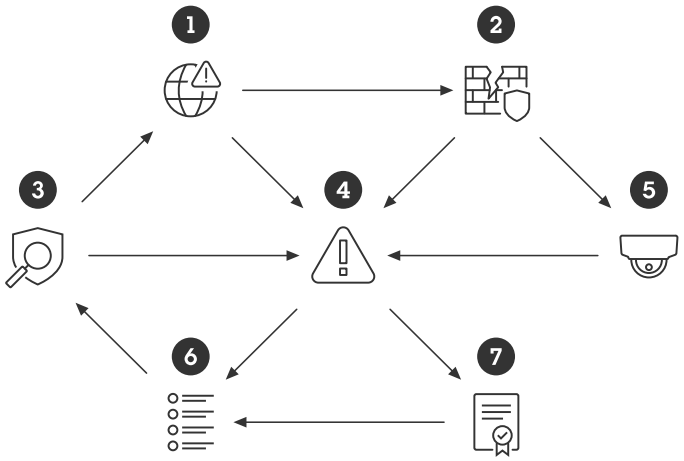
  IG3-Unternehmen beschäftigen in der Regel Sicherheitsexperten, die sich auf die unterschiedlichen Facetten der Cybersicherheit spezialisiert haben (z. B. Risikomanagement, Tests mit Penetrationsversuchen, Sicherheit von Anwendungen). IG3-Anlagen und -Daten enthalten vertrauliche Informationen oder Funktionen, die behördlichen Bestimmungen und Compliance-Bestimmungen unterliegen.

Terminologie

Terminologie

Terminologie

Die Terminologieübersicht zeigt das Verhältnis bestimmter, in diesem Dokument behandelter Schlüsselbegriffe zur Cybersicherheit.



- **(1) Bedrohungen** nutzen **(2) Schwachstellen** aus, exponieren **(5) Assets** und erhöhen **(4) Risiken**
- **(4) Risiken** beeinflussen **(7) Politik** und zeigen **(6) Anforderungen**
- **(6) Anforderungen** werden in **(3) Sicherheitskontrollen** angesprochen, die ständig konfrontiert sind mit **(1) Drohungen** und dabei gleichzeitig **(4) Risiken** mildern

Risiko

Bei Cybersicherheit geht es um das Verwalten von Risiken über einen Zeitraum. Risiken können niemals eliminiert, nur verringert werden. Manchmal verwechseln Menschen die Begriffe: Risiken, Vermögenswerte, Bedrohungen, Verletzlichkeit oder negative Auswirkungen

Das RFC 4949 Internet Security Glossar definiert Risiko als Wahrscheinlichkeit, dass eine bestimmte Bedrohung eine bestimmte Schwachstelle ausnutzen wird, die ein besonders schädliches Ergebnis zur Folge hat.

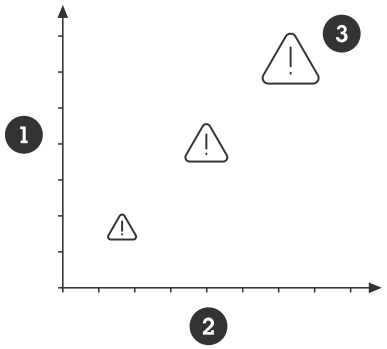
Eine Kurzversion wird häufig verwendet: **Risiko = Wahrscheinlichkeit x Auswirkung**

Diese Formel wird verwendet, um Risiken zu priorisieren. Die RFC-Definition enthält den Begriff „besonders" für Bedrohung, Verletzlichkeit und schädliche Folgen. Jede Bedrohung sollte einzeln überprüft werden, beginnend bei der plausibelsten Bedrohung mit den größten nachteiligen Auswirkungen.

Eine Herausforderung bei der Risikoanalyse ist der Wahrscheinlichkeitsfaktor. Es kann passieren oder nicht. Die Wahrscheinlichkeit, mit der ein Kontrahent eine Schwachstelle ausnutzen kann, wird häufig durch die Ausnutzung der Schwachstelle (Offenlegung) und den möglichen Vorteilen für den Widersacher bestimmt.

Es ist möglich, Risiken als zweidimensionales Diagramm darzustellen: Verwenden Sie die Wahrscheinlichkeit, dass ein Risiko auftritt als eine Achse, und die Auswirkungen des Risikos als die andere Achse. Damit erhalten Sie ein klares Bild der möglichen Auswirkungen und der Priorität, die Sie jedem Risiko zuordnen müssen.

Terminologie



1 ***Wahrscheinlichkeit*** *von niedrig nach hoch*
2 ***Negative Auswirkung*** *von niedrig nach hoch*
3 ***Risikostufen*** *von niedrig nach hoch*

Angriffswert = Angriffsvorteile – Angriffskosten

Das Hinzufügen von Schutz erhöht die Angriffskosten und senkt damit die Wahrscheinlichkeit. Die Angriffskosten beziehen sich darauf, wie viel Zeit, Ressourcen, Fähigkeiten und Raffinesse für einen erfolgreichen Angriff erforderlich sind. Zu den Angriffskosten gehören auch die Gefahr, entdeckt zu werden oder andere negative Folgen zu tragen.

Die Risikobewertung ist ein Verfahren zur Analyse von Risiken im Cyberraum, genau wie beim physischen Schutz. Folgende Fragen sollten beantwortet werden:

1. Was möchten Sie schützen?
2. Vor wem möchten Sie es schützen?
3. Mit welcher Wahrscheinlichkeit gibt es negative Auswirkungen?
4. Welche Folgen hat ein Scheitern?
5. Welche Maßnahmen sollten umgesetzt werden, um die Risiken zu verringern?

Die Implementierung jeglicher Art von Schutz- oder Sicherheitskontrollmaßnahmen führt zu Kosten in irgendeiner Form. Alle Organisationen verfügen über begrenzte finanzielle Ressourcen. Wenn Sie nicht wissen, welche Risiken bestehen, ist es schwierig, das Budget für Ihren Schutz einzuschätzen. Risiken müssen immer akzeptiert werden. Diese Entscheidung muss jedoch eine vorsätzliche risikobasierte Entscheidung sein.

Die Einschätzung möglicher negativer Auswirkungen auf die einzelnen Anlagetypen ist schwierig und komplex. In vielen Fällen sind die Einschätzungen subjektiv, und die Ereignisanalyse wird häufig unterschätzt. Die Verwendung des Ereignismodells und der Bezeichnungstypen gemäß ISO 27000 – eingeschränkt, schwerwiegend, stark oder katastrophal – hilft Ihnen dabei, schnell einen Überblick zu erhalten, um die Priorisierung zu erleichtern. Dies ist eine einfache Möglichkeit, einen genaueren Wert zu erhalten, indem die Schätzwerte für die Zeit bestimmt werden, die für die Wiederherstellung nach einem negativen Ereignis notwendig ist, also:

- **Begrenzt** = zwischen Stunden und Tagen
- **Ernsthaft** = von Tagen bis Wochen
- **Schwer** = von Wochen bis Monaten
- **Katastrophal** = von Monaten bis Jahren, wenn überhaupt

Vermögenswerte

Der physische Schutz konzentriert sich auf den Schutz von Personen und physischen Objekten. Der Cybersicherheitsschutz liegt jedoch auf dem Schutz von Datenressourcen und Computerressourcen. Es gibt drei Hauptbereiche:

Terminologie

- **Vertraulichkeit**: Offenlegung von Informationen oder Ressourcen
- **Integrität**: Zerstörung oder Änderung von Informationen oder Ressourcen
- **Verfügbarkeit**: Zugriff auf Informationen und Ressourcen

Diese Bereiche werden auch als CIA-Triade bezeichnet. Bei der Operation Technology (OT) wird häufig die Verwendbarkeit priorisiert, während IT-Anwender häufig die Sicherheit priorisieren. Oft ist es schwierig, das richtige Verhältnis zwischen Vertraulichkeit, Integrität und Verfügbarkeit zu finden.

Ressourcen müssen klassifiziert werden, um angemessene Schutzstufen zu ermitteln. Nicht alle Datenressourcen und Computerressourcen sind hinsichtlich der nachteiligen Auswirkungen gleich. Sie werden häufig wie folgt klassifiziert:

- **Öffentlich**: Die Ressource zielt auf einen öffentlichen Verbraucher. Die Auswirkungen auf die Öffentlichkeit sind jedoch begrenzt.
- **Privat**: Die Ressource ist für eine bestimmte bzw. ausgewählte Gruppe. In der Regel sind die Auswirkungen auf bestimmte Organisationen wie Unternehmen oder Familie begrenzt.
- **Eingeschränkt**: Die Ressource ist für ausgewählte Personen in einer Organisation.

Live-Video in einem Videosystem kann als öffentlich eingestuft werden. Dies bezieht sich sowohl auf die breite Öffentlichkeit als auch auf die Öffentlichkeit in einer Organisation. In den meisten Fällen wird Live-Video jedoch als privat eingestuft, d. h. es ist nur für eine bestimmte Einheit zugänglich. Mittlerweile werden aufgezeichnete Videos in den meisten Fällen als eingeschränkt eingestuft, da Szenen sehr empfindlich sein können. Anmeldeinformationen und Konfigurationen sind auch Daten, die als eingeschränkt eingeordnet werden sollten.

Bedrohungen

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 kommen nicht von ungefähr. Es gibt immer Motivation für die Kompromittierung von einem System und seinen Anlagen. Angriffe können entweder als opportunistisch oder als gezielt bezeichnet werden. In der Cybersicherheit werden Cyberattacken auch als böswilliger Angriff bezeichnet.

Die meisten Angriffe sind heute opportunistisch: Angriffe, die nur deshalb stattfinden, weil es eine günstige Gelegenheit gibt. In vielen Fällen weiß ein externer opportunistischer Angreifer nicht einmal, um wen es sich handelt. Diese Angriffe werden mit kostengünstigen Angriffsmethoden wie Phishing oder Austesten durchgeführt. In diesem Fall haben sie nicht den Durchsetzungswillen, bei einem fehlgeschlagenen Angriff Zeit und Ressourcen zu verwenden. Sie bewegen sich schnell zum nächsten Versuch. Das Anwenden eines Standardschutzes verringert die mit opportunistischen Angriffen verbundenen Risiken. Es ist schwieriger, sich gegen gezielte Angriffe zu schützen, bei denen die Angreifer 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.

Häufige Gegner (Angreifer)

- **Nahstehende Personen**: Personen, die in Ihr persönliches Leben hineindringen möchten
- **Mitarbeiter**: oder Personen, die aus Zufall oder vorsätzlich auf das System zugegriffen haben
- **Prankster**: Menschen, die das Eindringen in Computersysteme als Herausforderung empfinden
- **Hacktivisten**: Personen, die Organisationen aus politischen oder ideologischen Gründen angreifen möchten
- **Cyberkriminelle**: Personen, die durch Betrug oder den Verkauf wertvoller Informationen Geld verdienen möchten
- **Industrielle Konkurrenten**: Personen, die sich einen wirtschaftlichen Vorteil für ihre Unternehmen oder Organisationen verschaffen möchten

- **Cyberterroristen**: Personen oder Einrichtungen, die einen Anschlag durchführen, der Alarm oder Panik auslösen soll, oftmals aus ideologischen oder politischen Gründen.
- **Staaten**: Agenten ausländischer Geheimdienste, die entweder wirtschaftliche und politische Vorteile suchen oder kritischen Informationssystemen Schaden zufügen
- **Einzelpersonen**: Eine bestimmte Einzelperson oder Gruppe, deren Motivation sich von den oben aufgeführten unterscheiden kann. Dabei kann es sich um einen investigativen Journalisten, einen ethischen Hacker oder ähnliches handeln. Ethische Hacker können eine Bedrohung darstellen, wenn Sie das Verbergen der Schwachstellen priorisieren, anstatt sie zu beheben.

Sicherheitslücken

Alle Systeme haben Sicherheitslücken. Sicherheitslücken bieten Kontrahenten die Möglichkeit, Angriffe auszuführen oder Zugang zu einem System zu erhalten. Sie können auf Mängeln, Offenlegung, 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 oder schlecht gewartete Systeme zurück zu führen – oftmals aufgrund fehlender ausreichender Richtlinien, nicht festgelegter Verantwortlichkeiten und geringer Bekanntheit.

Sicherheitslücken von Software

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 kompensierende Sicherheitsmaßnahmen verringert werden. Andererseits steigt das Risiko für einen erfolgreichen Zero-Day-Exploit, wenn ein Angreifer einen neuen unbekannten Fehler entdeckt, da das Opfer keine Zeit hatte, das System zu schützen.

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 eine CVSS-Zahl in veröffentlichten Berichten zur Common Vulnerabilities and Exposures (CVE).

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

Richtlinie

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.

Sicherheitskontrollen

Sicherheitsmaßnahmen sind Maßnahmen oder Gegenmaßnahmen, die Sicherheitsrisiken für physisches Eigentum, Informationen, Computersysteme und andere Vermögenswerte erfassen, vermeiden und ihnen entgegenwirken. Die Verfahren zum Bereitstellen von Sicherheitskontrollen werden oft als Hardening (Härten) bezeichnet.

Die Kompensierung von Sicherheitskontrollen sind alternative Sicherheitsmaßnahmen. Diese können eingesetzt werden, wenn die bevorzugte Sicherheitskontrolle nicht eingesetzt werden kann oder wenn die bevorzugte Steuerung nicht verfügbar oder zu teuer ist.

Die Sicherheitsmaßnahmen müssen fortlaufend überwacht und aktualisiert werden, da sich Bedrohungen, Wert, Sicherheitslücken und die Exposition im Laufe der Zeit ändern. Dies erfordert das Definieren und Verfolgen von Richtlinien und Verfahren.

Das SANS Institute hat eine *Liste mit CIS Controls* veröffentlicht. Dabei handelt es sich um einen Satz priorisierter Best Practices zur Cybersicherheit. Hier finden Sie die vollständige Liste der Sicherheitskontrollen.

- CIS Control #1: Inventar und Steuerung von Unternehmensressourcen
- CIS Control #2: Inventar und Steuerung von Softwareressourcen
- CIS Control #3: Datenschutz

Terminologie

- CIS Control #4: Sichere Konfiguration von Unternehmensressourcen und Software
- CIS Control #5: Kontenverwaltung
- CIS Control #6: Verwaltung der Zutrittskontrolle
- CIS Control #7: Kontinuierliches Management von Sicherheitslücken
- CIS Control #8: Verwaltung der Prüfprotokolle
- CIS Control #9: Schutz der E-Mail- und Webbrowser
- CIS Control #10: Verteidigungslinie
- CIS Control #11: Datenwiederherstellung
- CIS Control #12: Verwaltung der Netzwerk-Infrastruktur
- CIS Control #13: Netzwerküberwachung und -schutz
- CIS Control #14: Schulungen zu Sicherheitserkenntnissen und -fertigkeiten
- CIS Control #15: Dienstanbieter verwalten
- CIS Control #16: Sicherheit von Anwendungs-Software
- CIS Control #17: Management von Vorfällen
- CIS Control #18: Penetrationstests

Der *AXIS OS Hardening Guide* basiert auf CIS.

Schutzmaßnahmen gegen häufige Bedrohungen

Wenn Sie die gängigen Bedrohungen verstehen und ihnen entgegentreten, können Sie die meisten Risiken verringern.

Vorsätzlicher oder versehentlicher Missbrauch des Systems

Die Balance zwischen Verwendbarkeit und Sicherheit eines Systems ist schwierig. Viele Systeme sind aus der Perspektive des Komforts und nicht der Sicherheit gehärtet. Dadurch werden Möglichkeiten für vorsätzlichen oder zufälligen Missbrauch eröffnet. Personen mit einem legitimen Zugang zu einem System sind die häufigste Bedrohung für jedes System.

Beispiele häufiger Bedrohungen:

- Einzelpersonen können Zugang zu Diensten (z. B. Live- oder aufgezeichneten Videos) erhalten, zu denen sie nicht berechtigt sind.
- Einzelpersonen machen Fehler
- Einzelpersonen können versuchen, Probleme zu beheben, die zu einer verringerten Systemleistung führen.
- Unzufriedene Einzelpersonen können stehlen das System vorsätzlich schädigen
- Einzelpersonen sind anfällig für Social Engineering
- Einzelpersonen stehlen
- Einzelpersonen können wichtige Komponenten (Zugangskarten, Telefone, Laptops, Dokumentationen usw.) verlieren oder verlegen
- Die Computer von Einzelpersonen können kompromittiert werden und ein System unbeabsichtigt mit Malware infizieren

Zu den häufigsten empfohlenen Schutzmaßnahmen gehören:

- Definierte Benutzerkontenrichtlinien und -verfahren
- Ausreichendes Authentifizierungsschema für den Zugriff
- Tools zum Verwalten von Benutzerkonten und Rechten im Lauf der Zeit
- Exposition verringern
- Schulungen zur Sensibilisierung für Cyberfragen

So hilft Axis, dieser Bedrohung entgegen zu treten:

- *AXIS OS Hardening Guide* beschreibt gängige Sicherheitskontrollen für häufige Bedrohungen bei Geräten.
- *AXIS Camera Station Hardening Guide* beschreibt gängige Sicherheitskontrollen für Videosysteme
- *AXIS Device Manager* und *AXIS Device Manager Extend* erleichtern die Verwaltung gängiger Sicherheitskontrollen

Physische Manipulation und Sabotage

Der physische Schutz von IT-Systemen ist aus Sicht der Cybersicherheit sehr wichtig.

Beispiele häufiger Bedrohungen:

- Physisch exponierte Geräte können manipuliert werden
- Physisch exponierte Geräte können gestohlen werden
- Physisch exponierte Kabel können getrennt, umgeleitet oder abgeschnitten werden.

Schutzmaßnahmen gegen häufige Bedrohungen

Zu den häufigsten empfohlenen Schutzmaßnahmen gehören:

- Platzieren von Netzwerkgeräten (z. B. Servern und Switches) in verschlossenen Bereichen
- Kameras so montieren, dass sie schwer zu erreichen sind
- Bei physischer Exposition das Schutzgehäuse verwenden
- Schutz der Kabel in Wänden oder Leitungen

So hilft Axis, dieser Bedrohung entgegen zu treten:

- Verschlüsselte SD-Karte zur Verhinderung der Wiedergabe von Video, wenn ein nicht autorisierter Benutzer die SD-Karte auswerfen kann
- Erkennung von Manipulation in der Kameraansicht
- Erfassung von geöffnetem Gehäuse

Ausnutzung bekannter Sicherheitslücken in der Software

Alle softwarebasierten Produkte haben Sicherheitslücken, die ausgenutzt werden können. Diese können als bekannt oder unbekannt bezeichnet werden. Alle unbekannten Sicherheitslücken werden irgendwann bekannt. es ist nur eine Frage der Zeit. Die meisten Sicherheitslücken haben ein geringes Risiko, d. h. sie sind entweder nur schwer zu nutzen oder die nachteiligen Auswirkungen begrenzt. Gelegentlich werden Schwachstellen entdeckt und ausgenutzt, die erhebliche negative Auswirkungen haben können. MITRE hostet eine große Datenbank mit CVE (Common Vulnerabilities and Exposures), um anderen zu helfen, Risiken zu minimieren.

Zu den häufigsten empfohlenen Schutzmaßnahmen gehören:

- Durch kontinuierliches Patching wird die Anzahl der in einem System bekannten Sicherheitslücken minimiert.
- Minimieren Sie die Netzwerkbelastung, um die Prüfung und Ausnutzung bekannter Sicherheitslücken zu erschweren.
- Arbeiten Sie mit vertrauenswürdigen Subanbietern zusammen, die Richtlinien und Verfahren verfolgen, die Schwachstellen minimieren, Prozesse zur Bereitstellung von Patches anbieten und Nachforschungen anstellen, wenn kritische Sicherheitslücken entdeckt werden.

So hilft Axis:

- *Axis Security Development Model* ist ein Rahmenwerk, das Prozesse und Tools definiert, mit denen Axis das Risiko der Freigabe von Produkten mit Softwareschwachstellen reduziert.
- *Die Richtlinie von Axis zum Management von Sicherheitsschwachstellen* umfasst das Identifizieren, Beheben und Nachverfolgen von Sicherheitslücken, auf die die Kunden achten müssen, um geeignete Maßnahmen zu ergreifen. Seit April 2021 ist Axis eine Common Vulnerability and Exposures (CVE) Numbering Authority (CNA) für Axis Produkte, mit der wir unsere Prozesse an die Branchenstandards der MITRE Corporation anpassen können. Dies hilft uns, unsere Kunden besser zu unterstützen.
- *Axis Hardening Guides*, wie z. B. der *AXIS OS Hardening Guide*, geben Empfehlungen zur Reduzierung der Exposition sowie Ausgleichskontrollen, um das Risiko von Softwarefehlern zu verringern.
- Mit den LTS (Long Term Support) Firmware-Versionen können Kunden das Betriebssystem von Axis Geräten patchen, während das Risiko fehlender Kompatibilität durch Videoverwaltungssysteme von Drittanbietern minimiert wird.

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. Sie wird hauptsächlich verwendet, wenn andere Angriffsvektoren (wie Social Engineering, Phishing-Attacken und Sondieren der Schnittstelle zur Benutzeroberfläche) aufgrund eines hohen Niveaus an Systemschutz scheitern. Der Angriff erfolgt durch die Kompromittierung von Software/Firmware/Produkten und die Verlockung eines Administrators, diese in ihrem System zu installieren. Ein Produkt kann während des Transports zum Eigentümer des Systems beschädigt werden. Für einen erfolgreichen Abschluss eines Supply Chain-Angriffs sind Fähigkeiten, Zeit und Ressourcen erforderlich.

Schutzmaßnahmen gegen häufige Bedrohungen

Zu den häufigsten empfohlenen Schutzmaßnahmen gehören:

- Richtlinien, um Software nur von vertrauenswürdigen und verifizierten Quellen zu installieren.
- Überprüfung der die Software-Integrität, indem Sie vor der Installation die Prüfsumme (Digest) der Software mit der Prüfsumme des Herstellers vergleichen.
- Überprüfung bei der Lieferung des Pakets oder Produkts auf Manipulation.

So hilft Axis, dieser Bedrohung entgegen zu treten:

- Axis veröffentlicht Software mit einer Prüfsumme, damit Administratoren vor der Installation die Integrität der Software prüfen können.
- Signierte Firmware in einem Axis Gerät garantiert, dass das installierte Betriebssystem (AXIS OS) von Axis ist und dass jedes neue, auf das Gerät herunterladbare und zu installierende Betriebssystem auch von Axis signiert ist.
- Mit dem sicheren Hochfahren eines Axis Geräts kann das Gerät prüfen, ob die Firmware mit einer Axis Signatur ausgestattet ist. Wenn die Firmware nicht autorisiert ist oder verändert wurde, wird der Boot-Vorgang abgebrochen.
- Die IEEE 802.1AR-konforme Axis Geräte ID ist ein gerätespezifisches Axis Zertifikat, mit dem das System überprüfen kann, ob die Hardware im Gehäuse von Axis stammt.
- SD-Karten-Verschlüsselung und Dateisystem-Verschlüsselung verhindern das Auslesen gespeicherter Daten, wenn die Karte oder das Gerät gestohlen wird.

Benutzerhandbuch
Cybersecurity reference guide

Vers. M3.2
Datum: November 2023
Teil-Nr. T10201166