AXIS Camera Station Pro

Anleitung zum Härten des Systems

Einführung

Einführung

Einführung

Eine universell verwendbare, idiotensichere Funktion, die jedes Sicherheitssystem und jeden Standort zu 100% cybersicher machen kann. So verlockend diese Wörter auch sind, eine solche Funktion existiert nicht – oder wird wahrscheinlich nicht in Kürze existieren. Stattdessen müssen die Risiken geprüft werden, die durch bedrohungsgefährdete und Sicherheitslücken in ihrer Organisation vorhanden sind. Wenn das Risiko als nicht angemessen eingestuft wird, müssen diese Maßnahmen zur Minderung dieses Risikos umgesetzt werden. Gut definierte Richtlinien und Verfahren gewährleisten eine konsistente Kommunikation und Anwendung dieser Kontrollen innerhalb einer Organisation und auf Grundlage eines ausgereiften Cybersicherheitsprogramms.

Es wird empfohlen, standardisierte IT-Sicherheitsrahmen zum Risikomanagement zu verwenden, z. B. ISO 27001, NIST CSF oder anderen. Diese Aufgabe ist für kleinere Unternehmen zwar entmutigend, die Definition grundlegender Informationssicherheitsrichtlinien und Unterstützungsprozesse ist jedoch viel besser als gar nichts. Wenn Ihre Organisation den Weg zur Cybermündigkeit beginnt und über begrenzte Ressourcen verfügt, wird empfohlen, *das Center for Internet Safety (CIS) Critical Security Controls Version 8 zu betrachten.* CIS bietet eine Liste mit 18 Sicherheitskontrollaktivitäten, die in drei Implementierungsgruppen organisiert sind, um Organisationen bei der Entwicklung und Entwicklung ihres Cybersicherheitsprogramms zu unterstützen.

Sicherheitsverletzungen treten in vielen Organisationen auf, da das Unternehmen keine klaren Richtlinien, Regeln und Verfahren festgelegt hat, die die Nutzung und die Zugangsrechte für ihre eigenen Mitarbeiter regeln. Arbeitet Ihre Organisation mit Richtlinien und Verfahren für den Videoverwaltungsbetrieb? Falls nicht, ist es an der Zeit, diese zu definieren.

Zweck

Dieses Dokument zeigt eine Reihe von Maßnahmen und Verfahren zur Cybersicherheit, die den sicheren Einsatz und die Wartung von Systemen unterstützen. Obwohl wir nicht direkt einem Cybersicherheitsrahmen zugeordnet sind, konzentrieren wir uns in erster Linie auf CIS Security Controls v8 mit einem besonderen Fokus auf den folgenden Steuerungsaktivitäten:

- *Kontrolle 1: Inventar und Steuerung von Unternehmensressourcen*
- *Kontrolle 2: Inventar und Steuerung von Softwareressourcen*
- *Kontrolle 3: Datenschutz*
- *Kontrolle 4: Sichere Konfiguration von Unternehmensressourcen und Software*
- *Kontrolle 5: Kontenverwaltung*
- *Kontrolle 6: Verwaltung der Zutrittskontrolle*
- *Kontrolle 7: Kontinuierliches Management von Sicherheitslücken*
- *Kontrolle 10: Verteidigungslinie*

Im Mittelpunkt unserer Empfehlungen steht die Unterstützung von Installateuren, Integratoren und Endbenutzern, um gängige Risiken beim Einsatz und der Verwaltung von Systemen zu minimieren.

Voraussetzungen

Es wird davon angenommen, dass die im *AXIS OS Härtungsleitfaden* festgelegten und beschriebenen Empfehlungen und Verfahren verstanden und befolgt werden. Außerdem bezieht sich dieses Dokument auf mehrere gängige Benutzerrollen, die mit einem Videosystem interagieren. Ordnen Sie diese Benutzerrollen Ihren eigenen Benutzer- und Rollenklassifizierungen zu. Ein einzelner Benutzer kann je nach Organisation mehrere Rollen haben.

Definierte Rollen:

- **Systeminstallateur**: Installation, Einrichtung, Reparatur, Aktualisierung und Rückstufung von Systemen
- **Netzwerkadministrator**: Erhält die Netzwerk-Infrastruktur, die Konnektivität von Endknoten, Netzwerk-Server und Ressourcen sowie den Netzwerkschutz

Einführung

- **Video Systemadministrator**: Definiert und verwaltet das Videosystem, um die Nutzung, Leistung und Benutzerrechte des Videosystems zu gewährleisten.
- **Video-Systemwartung**: überwacht, justiert und repariert Komponenten, um die Systemleistung im Namen des Videosystemadministrators zu gewährleisten.
- **Benutzer**: Personen, die den Client für den Zugriff auf Live-Video und aufgezeichnete Videos verwenden und in der Regel für den physischen Schutz einer Organisation verantwortlich sind.

Systemsicherheitsrichtlinien

Physische Sicherheit

Physische Schutzrichtlinie

Server, Geräte, Netzwerkausrüstung und Kabel sind physische Objekte, die beeinträchtigt, sabotiert oder gestohlen werden können. Wichtige Netzwerk basierte Geräte wie Router und Switches sowie der Host, auf dem die -Serversoftware ausgeführt wird, sollten in einer Umgebung mit eingeschränktem Zutritt installiert werden. Kameras und andere angeschlossene Geräte sollten an schwer zu erreichenden Orten angebracht werden und mit vandalismusgesicherten Modellen oder Gehäusen ausgestattet sein. Es sollte darauf achten, die Kabel in Wänden oder Kabelkanälen zu schützen, da diese das Risiko von Manipulation und Sabotage erhöhen.

Empfohlene Richtlinien und Verfahren
Definieren Sie eine Einzeleinheit oder eine Organisationsgruppe, die für den physischen Schutz von VMS-Servern, Netzwerkhardware, angeschlossenen Geräten und Verkabelung in definierten Intervallen verantwortlich ist. Es ist wichtig, ein genaues Inventar aller Server und Geräte einschließlich ihres Standorts zu erstellen.

Softwareverwaltung

Richtlinien für Drittanbieter-Anwendungssoftware

Da in einer Windows-Standardumgebung installiert ist, kann es verlockend sein, diese Umgebung für Softwareanwendungen zu nutzen, die nicht mit der Videoverwaltung in Verbindung stehen. Durch die Installation anderer Drittanbieter-Anwendungen kann Malware in die Umgebung eingeführt werden. Dies kann zu Systemausfällen führen oder einem Angreifer den Zutritt in das Netzwerk der Organisation ermöglichen.

Empfohlene Richtlinien und Prozeduren
Zudem sollten Sie nur die -Server-Software und vertrauenswürdige Integrationen von Drittanbietern auf der Host-Hardware ausführen. Wenn die physische Hardware für andere Zwecke verwendet werden soll, wird empfohlen, mehrere virtuelle Serverinstanzen zu verwenden und die Serversoftware in einer virtuellen Maschine und die Software von Drittanbietern, die nicht zu VMS gehört, auf einer anderen virtuellen Maschine auszuführen. Informationen zum Ausführen von in einer virtuellen Umgebung finden Sie *hier*.

Außerdem sollte auf allen mit dem -Server verbundenen Servern und Computern eine Antiviren-Software installiert sein. Bei der Bereitstellung mobiler Geräte muss zudem sichergestellt werden, dass auf den Geräten die neuesten Betriebssysteme und Patches installiert sind (jedoch nicht direkt gegen Viren). Prüfen Sie beim Scannen von Viren keine Verzeichnisse und Unterverzeichnisse mit Aufzeichnungsdatenbanken. Das Scannen von Viren in diesen Verzeichnissen kann sich auf die Systemleistung auswirken.

Kontenverwaltung

Allgemeine Kontorichtlinien

Administratorenrechte werden gelegentlich normalen Benutzern gewährt. Dies ist ein Vorteil. In vielen Organisationen ist es unklar, wer die Kontoberechtigungen überprüft und den Zugang von Mitarbeitern zu Systemen überwacht.

Empfohlene Richtlinien und Verfahren
Wir empfehlen, dass Unternehmen beim Definieren von Systemkonten das Prinzip der geringsten Rechte befolgen. Dies bedeutet, dass die Zugriffsrechte des Benutzers auf die Ressourcen beschränkt sind, die für die Durchführung ihrer spezifischen Aufgaben erforderlich sind. Außerdem ist es empfehlenswert, regelmäßig die Kontoberechtigungen der Systembenutzer zu prüfen, um diese vor Privilegien zu schützen.

Richtlinien für Administratorenkonten

Ein häufiger Fehler beim Bereitstellen von in einer Windows-Umgebung besteht in der Definition eines einzelnen Administratorkontos für den Windows-Host. Im Laufe der Zeit kann das Kennwort innerhalb der Organisation geteilt werden. Dabei besteht die Gefahr, dass unbefugte Personen Administratorrechte für die Windows-Umgebung erhalten. Dies kann leicht dazu führen, dass auf diesem Server zahlreiche unerwünschte Benutzer-Anwendungen oder Malware installiert werden.

Empfohlene Richtlinien und Verfahren
Der Windows-Computerhosting-Server sollte über mindestens ein Administratorkonto und ein Benutzerkonto verfügen. Beide Konten sollten nicht mit dem standardmäßigen Administratorkonto für Windows identisch sein. Das Standardkonto für den Administrator muss deaktiviert werden, nachdem der Administrator und die Benutzerkonten erstellt wurden. Nach der Bereitstellung sollte das Kennwort für das Administratorkonto nur den **Netzwerkadministratoren** bekannt sein und von ihnen verwendet werden. Das Benutzerkonto sollte vom **Videosystemadministrator** verwendet werden, wenn/sobald dieser sich am Server anmelden muss. Es ist darauf hinzuweisen, dass für Zwecke der Überprüfung weiterhin empfohlen wird, wenn die beiden oben genannten Rollen von derselben Person ausgeführt werden. Es wird empfohlen, separate Konten für Netzwerk- und Videosystemadministratoren einzurichten. Um andere, wie zuvor definierte, Rollen zu unterstützen, sollten für jeden einzelnen **Benutzer**, der sich am System anmelden wird, weitere, nicht privilegierte Benutzerkonten erstellt werden.

Wenn der Host, der ausführt, in einer Windows Active Directory-Domainumgebung platziert wird, können Administratoren- und Benutzerkonten im Kontext der Domain erstellt werden, oder das vorhandene Domainnkonto eines Mitarbeiters kann zum Authentifizieren beim Host verwendet werden. Dies vereinfacht die Kontoverwaltung, da keine zusätzlichen Konten erstellt und verwaltet werden müssen. Dies ermöglicht auch die Verwendung von Gruppenrichtlinienverwaltung, um die Kennwortkomplexität, die Zertifikatbereitstellung und andere Sicherheitsfunktionen in Domainnumgebungen zu erzwingen.

Benutzerkontenrichtlinien

Benutzerkonten werden in bestimmte Rollen zugewiesen, die wiederum die spezifischen Rechte für jeden Benutzer im System bestimmen, z. B. Ansichten und Videos, auf die er keinen Zugriff hat. Wenn mehrere Personen ein einzelnes Benutzerkonto teilen, besteht ein erhöhtes Risiko, dass ein Kennwort mit anderen Personen in der Organisation geteilt wird. Das Teilen von Konten macht die Überprüfung des Zugriffs auf die Kamera/das Video zu welcher Zeit praktisch unmöglich.

Empfohlene Richtlinien und Verfahren

Wir empfehlen Ihnen, mithilfe von **Kerberos** Client-Benutzer zu authentifizieren. Siehe dazu *Authentifizierung mit Hilfe von Kerberos auf Seite 5*.

Verwenden Sie nach Möglichkeit Microsoft Active Directory für eine einfache Benutzer- und Gruppenverwaltung. Es wird außerdem empfohlen, vor dem Einrichten des Systems zu überprüfen, ob die relevanten Sicherheitsgruppen für alle Benutzerrollen definiert wurden.

Active Directory bietet außerdem:

- Eine Kennwortrichtlinie, die Benutzer dazu verpflichtet, regelmäßig ihr Kennwort zu ändern.
- Brute-Force-Schutz, sodass das Windows AD-Konto nach mehreren fehlgeschlagenen Authentifizierungsversuchen im Einklang mit der Kennwortrichtlinien der Organisation gesperrt ist
- Rollenbasierte Berechtigungen, sodass die Zutrittskontrollen in der gesamten Domain angewendet werden können

Wenn lokale Windows-Konten verwendet werden müssen, wird empfohlen, für jeden Benutzer des Systems ein eindeutiges Konto zu erstellen und nur auf die Einheiten im System zuzugreifen, die zur Wahrnehmung seiner Verantwortlichkeiten erforderlich sind. Durch die Verwendung von Gruppen für Benutzer kann die Zuweisung von Berechtigungen vereinfacht werden, wenn mehrere Benutzer identische Berechtigungen besitzen.

Authentifizierung mit Hilfe von Kerberos

verwendet die integrierte Windows-Authentifizierung, um die Benutzer des Client zu authentifizieren. verwendet das Microsoft Negotiate protocol (SPNEGO), d. h., bei Kerberos handelt es sich um das bevorzugte und standardmäßige Authentifizierungsprotokoll. Das Negotiate-Protokoll versucht, Kerberos zu verwenden und NTLM als Notlösung.

Um Kerberos zu verwenden, müssen Sie Service Principal Names (SPN) mit folgendem Befehl in Active Directory registrieren:

```
setspn -s ACSService/{HOST} {ACCOUNT_NAME}
```

HOST – Der Host-Name des Servers, auf dem Server ausgeführt wird.

ACCOUNT_NAME – Der Name des Computers (Computerkonto), auf dem der Server ausgeführt wird.

Damit Kerberos ordnungsgemäß funktioniert, wird empfohlen, sowohl den kurzen Host-Namen als auch den FQDN für den Zielserver zu registrieren.

Beispiel:

```
setspn -s ACSService/CompanyServer CompanyServerAccount setspn -s
ACSService/CompanyServer.domain.local CompanyServerAccount
```

Weitere Informationen finden Sie unter *Setspn auf microsoft.com*.

Gerätekontorichtlinien

Die Konten von Axis Geräten sind in erster Linie Computer-/Clientkonten. **Benutzer** sollten niemals direkt auf das Gerät zugreifen dürfen. Der einzige Client, der während des normalen Betriebs auf Geräte zugreifen soll, ist der Server. Eine gängige Strategie ist, dass alle Geräte über dasselbe Kennwort verfügen. Dies führt zu zusätzlichen Risiken, kann jedoch auch das Kennwortmanagement vereinfachen, sodass die eigene Risikoverträglichkeit einzuschätzen ist. unterstützt das Zuweisen eindeutiger Kennwörter für jedes Gerät über die Verwaltungsschnittstelle.

Ein häufiger Fehler ist, dass Geräte zu einem einzelnen Konto hinzugefügt werden, das von mehreren Rollen geteilt wird. Wenn bei einer **Videosystem-Wartung** ein Browser verwenden werden muss, um etwas anzupassen, wird das Root-Kennwort des Geräts mitgeteilt. Innerhalb von Monaten kennen die meisten Menschen in der Organisation das Kennwort für alle Geräte und haben Administratorrechte für das System.

Empfohlene Richtlinien und Verfahren
Das Gerät sollte über mindestens zwei Administratorkonten verfügen: Ein eindeutiges, für Geräteadministratoren erstelltes Konto und das Standard-Root-Konto zum Hinzufügen von Geräten zum Server. Ein vorübergehender Zugriff, z. B. wenn bei einer **Videosystem-Wartung** über einen Web-Browser auf ein Gerät zugegriffen wird, sollte mithilfe von temporären Konten verwaltet werden.

Der AXIS Device Manager sollte als das primäre Tool zum Verwalten von Gerätekonten und Kennwörtern verwendet werden. Eine Version des AXIS Device Manager ist direkt in integriert und befindet sich in der Registerkarte Verwaltung. Das Root-Kennwort des Geräts sollte nur vom AXIS Device Manager und verwendet werden und sollte nur denjenigen bekannt sein, die den AXIS Device Manager oder als Tool zum Verwalten von Geräten verwenden.

Verwenden Sie , um ein befristetes Konto zu erstellen, wenn eine Wartungsfunktion einen Webbrowser verwenden muss, um auf Geräte zur Fehlerbehebung oder Wartung zu zugreifen. Wählen Sie die Geräte aus und erstellen Sie ein neues Konto, vorzugsweise mit Bedienerrechten, das der Servicetechniker verwenden darf. Entfernen Sie das temporäre Konto, sobald die Aufgabe abgeschlossen ist.

Systemwartung

Windows-Host-Patching-Richtlinie

Server und Clients werden in einer Windows-Umgebung ausgeführt. Es ist wichtig, dass diese Systeme auf dem neuesten Stand sind, um sicherzustellen, dass die Hosting-Software von des Systems keine offenen Sicherheitslücken aufweist, die ausgenutzt werden können, um unbefugten Zugriff auf das Video Management System zu erhalten.

Empfohlene Richtlinien und Verfahren
Für alle Systeme, die mit Axis NVR oder benutzerdefinierter Hardware ausgeführt werden, wird empfohlen, die automatische Aktualisierung zu deaktivieren. Windows-Aktualisierungen haben in der Vergangenheit zu Instabilität des zugrundeliegenden Windows-Betriebssystems geführt. Daher wird empfohlen, die verfügbaren Aktualisierungen auf ausgewählten Geräten zu testen, um die Stabilität des Systems zu gewährleisten, bevor alle ausgeführten Host-Systeme mit aktualisiert werden. Es muss jedoch ein Balance zwischen Sicherheit und Stabilität erreicht werden, da ein zu langes Verlassen des Windows-Systems eine Gefahr für die allgemeine Umwelt darstellen kann. Je nachdem, wie stark das System des Kunden externen Bedrohungen ausgesetzt ist, sollte in der Patching-Richtlinie ein Zeitrahmen festgelegt werden, in dem sichergestellt wird, dass die Systeme die neuesten Updates erhalten.

Richtlinien für Softwareaktualisierungen

In den meisten Fällen wird durch die Verwendung der neuesten Software-Versionen für sichergestellt, dass Sie Sicherheits-Patches für alle neu entdeckten Sicherheitslücken verwenden. Wenn das System über einen längeren Zeitraum ungepatcht bleibt, wird das Risiko erhöht, dass ein Angreifer die Sicherheitslücken ausnutzt und möglicherweise das System kompromittiert.

Empfohlene Richtlinien und Verfahren
Es ist wichtig, eine Patching-Richtlinie mit regelmäßigen Ausbesserungen bereitgestellter Softwareversionen zu definieren, um sicherzustellen, dass auf dem neuesten Stand ist. Mit der Patching-Richtlinie sollte auch identifiziert werden, wer für die Verwaltung der mit der Aktualisierung der Server- und Clientsoftware verbundenen Arbeit verantwortlich ist. Die aktuelle Version von ist auf *www.axis.com* zu finden. erfordert die neuesten .NET-Bibliotheken, daher muss darauf geachtet werden, die Windows-Patching-Richtlinie an der Richtlinie für auszurichten.

Richtlinie zur Aktualisierung der Gerätefirmware

Durch das Ausführen der aktuellen Firmware-Versionen auf den Geräten werden häufige Risiken verringert, da die aktuellen Firmware-Versionen Patches für bekannte Sicherheitslücken bieten, die Angreifer ausnutzen könnten. Axis bietet eine Langzeit-Support (LTS)-Version für Geräte-Firmware, die Sicherheits-Patches und Bugfixes enthält, aber deren Funktionen begrenzt sind, um die langfristige Stabilität der Plattform zu gewährleisten. Weitere Informationen zur Strategie von Axis zur Firmware-Entwicklung *finden Sie im Whitepaper zur Firmwareverwaltung von Axis*.

Empfohlene Richtlinien und Verfahren
Die Firmware für Hardwaregeräte muss auf dem neuesten Stand sein. Prozesse können mit der integrierten Firmware-Update-Funktion in oder AXIS Device Manager Extend verwenden, um zu ermitteln, ob neue Firmware-Versionen für Axis Geräte verfügbar sind. Um alle Firmware-Aktualisierungen für alle Kameras durchzuführen, sollte eine geplante Zeit festgelegt werden, in der Regel außerhalb der Geschäftszeiten. /AXIS Device Manager Extend kann auch überprüfen, ob die Firmware-Aktualisierungen angenommen wurden. Wenn das System über spezifische Integrationen verfügt, die von der Aktualisierung betroffen sein könnten, sollten Sie eine LTS-Firmware-Verfolgung standardisieren.

Netzwerk-Sicherheit

Richtlinien für Fernzugriff

Geräte und Dienste, die dem Internet ausgesetzt sind, erhöhen das Risiko, dass externe Gegenspieler bekannte Sicherheitslücken überprüfen oder ausnutzen. Kameras, die dem Internet ausgesetzt sind, z. B. von kleinen Organisationen, die einen Fernzugriff auf Video benötigen, werden leicht attackiert, wenn schwache Kennwörter verwendet oder eine neue kritische Schwachstelle entdeckt wird. Der Fernzugriff auf die Windows-Umgebung sollte nach Möglichkeit streng gesteuert oder verhindert werden. In der Windows-Umgebung ist möglicherweise eine Internetverbindung erforderlich, um Systeme zu aktualisieren. Die Remotedesktopdienste wie Windows Remote Desktop, TeamViewer und AnyDesk führen jedoch zu Pfaden, mit denen sie Zugriff auf Ihr System erhalten, wenn sie nicht ordnungsgemäß verwaltet werden.

Empfohlene Richtlinien und Verfahren
Legen Sie niemals die IP-Adresse/den Port einer Kamera so offen, dass direkt über das Internet darauf zugegriffen werden kann. Falls ein Fernzugriff auf Video erforderlich ist, verwenden Sie Axis Secure Remote Access. verwendet einen cloudbasierten Fernzugriffsserver, der den verschlüsselten Fernzugriff auf das System über den Client oder die AXIS Camera Station ermöglicht. Der Fernzugriffsserver ist nicht nur für die Verbindungsverwaltung für Remote-Benutzer und Mobilgeräte zuständig, sondern spielt auch beim Schutz der Integrität bei der Verwendung durch Remote-Benutzer eine wichtige Rolle. Weitere Informationen zu Axis Secure Remote Access finden Sie *hier*. Axis liefert offiziell unterstützte Mobil-Anwendungen sowohl für Android als auch für Apple iOS. Die AXIS Camera Station App darf nur von offiziellen Quellen, dem Google Play Store bzw. dem Apple App Store heruntergeladen werden.

Wenn es um den Fernzugriff auf Desktops in der Windows-Umgebung geht, wird davon abgeraten, diesen Zugang zu einem System zu ermöglichen, auf dem ausgeführt wird. Wenn dies erforderlich ist, muss jedoch mit äußerster Sorgfalt sichergestellt werden, dass die Desktop-Anwendung Ihrer Wahl sicher ist und nur den Personen zugänglich ist, die sie benötigen. Es wird empfohlen, zusätzliche Ebenen von Steuerelementen wie die Multi-Authentifizierung (MFA) zu implementieren. Es wird dringend empfohlen, die Personen und zu welchen Zeitpunkten der Fernzugriff auf die Windows-Umgebung erfolgt, nachzuverfolgen und zu kontrollieren.

Richtlinie zur lokalen Sichtbarkeit im Netzwerk

Eine Verringerung der lokalen Sichtbarkeit im Netzwerk kann dazu beitragen, viele gängige Bedrohungen durch Reduzierung der Angriffsfläche zu verringern. Es gibt viele Möglichkeiten, die Sichtbarkeit im Netzwerk zu reduzieren, einschließlich physischer Netzwerksegmentierung (separate Netzwerkhardware und Kabel), logische Netzwerksegmentierung über virtuelle LANs (VLANs) und IP-Filterung. Die Kameras von Axis unterstützen einen IP-Filter (IP-Tabellen), sodass das Gerät nur auf Verbindungsanfragen von zulässigen IP-Adressen reagiert.

Empfohlene Richtlinien und Verfahren
AXIS Camera Station S22 NVRs sind Hardwareserver mit dualen Netzwerkports. Einer der Ports erstellt ein segmentiertes Netzwerk

für Kameras, der andere verbindet sich mit dem primären Netzwerk (Domain), um Videoclients zu bedienen. Der Server fungiert als Brücke und Firewall zum Kamera-Netzwerk und verhindert, dass Clients direkt auf Kameras zugreifen können. Dies verringert die Bedrohung durch Kontrahenten im primären Netzwerk.

Wenn sich Server und Kameras alle im primären Netzwerk befinden, wird empfohlen, den IP-Filter der Kamera zu konfigurieren, um den Zugriff nur auf die Server, den AXIS Device Manager und weitere Wartungsclients zu begrenzen.

Richtlinie zur Netzwerkverschlüsselung

Netzwerk-Datenverkehr, der über unsichere Netzwerke übertragen wird, sollte stets verschlüsselt werden. Das Internet wird als unsicheres Netzwerk eingestuft. Ein lokales Netzwerk kann auch als ungesichert eingestuft werden. Daher sollte auch der Netzwerkverkehr verschlüsselt werden. Welche Richtlinien für den Videoverkehr im Netzwerk gelten, hängt von der Einstufung des Videos und dem Risiko eines Netzwerkzugriffs auf das Videosystem ab. Es wird empfohlen, davon auszugehen, dass das Netzwerk bereits gefährdet ist. Größere Organisationen verfügen normalerweise über eine Richtlinie, die definiert, wie das Netzwerk klassifiziert wird.

Empfohlene Richtlinien und Verfahren

Der Datenverkehr zwischen Videoclient und Server muss verschlüsselt werden. Der Datenverkehr zwischen Server und Kameras sollte je nach Infrastruktur verschlüsselt werden. Axis Kameras sind mit einem eigensigniertem Zertifikat und HTTPS in der Standardeinstellung aktiviert. Wenn die Gefahr einer Netzwerk-Vortäuschung besteht, z. B. wenn ein böswilliger Computer die Identität einer Kamera vortäuscht, sollte eine private Schlüsselinfrastruktur (PKI) mit CA-signierten Zertifikaten verwendet werden. verfügt über eine integrierte lokale Zertifizierungsstelle (CA), die das Signieren und Verteilen von Serverzertifikaten für Axis Geräte kostengünstig verwalten kann.

TLS-Version:

Es wird empfohlen, die TLS-Versionen 1.1 und 1.0 zu deaktivieren. Der AXIS Camera Station Installer bietet Unterstützung bei der Installation oder Aktualisierung an.

HTTPS-Verschlüsselungen

unterstützt und verwendet TLS-Verschlüsselungssuites, um HTTPS-Verbindungen sicher zu verschlüsseln. Die spezifische Verschlüsselungssuite hängt vom Client ab, der mit verbunden ist oder dem kontaktierten Dienst, und erfolgt via gemäß dem TLS-Protokoll. Es wird empfohlen, Windows so zu konfigurieren, dass keine TLS 1.2-Verschlüsselungssuites verwendet werden, *die in RFC 7540 aufgeführt sind.* Die Möglichkeit zur Deaktivierung einer Verschlüsselungssuite hängt von den zusammen mit verwendeten Geräten und Kameras ab. Wenn ein Gerät oder eine Kamera eine bestimmte Verschlüsselungssuite erfordert, ist es möglicherweise nicht möglich, die schwache Verschlüsselungssuite zu deaktivieren.

Datenverwaltung

Videoklassifizierung

Live-Video und aufgezeichnetes Video sollte klassifiziert werden. Video kann als öffentlich, privat, eingeschränkt oder als beliebige andere, durch eine Richtlinie der Organisation definierte Klasse klassifiziert werden. In vielen Fällen sind Videoaufnahmen gesetzlichen und regionalen Vorschriften sowie internen IT-Richtlinien unterliegen. Es obliegt daher der Verantwortung des Systembetreibers, sich der Gesetze und Bestimmungen für die Videodaten bewusst zu sein.

Empfohlene Richtlinien und Verfahren
Klassifizieren von Live-Video, aufgezeichnetem Video und Audio in Übereinstimmung mit Datenklassifizierungsrichtlinien. Konfigurieren Sie die Benutzerzugriffsrechte und das Härten des Systems entsprechend der Empfindlichkeit der Video- und Audiodaten. Falls nicht erforderlich, kann Audio auf Geräteebene deaktiviert werden.

Zusätzliche Sicherheitskontrollen

Je nach Ausgereiftheitsgrad und Risikobereitschaft Ihrer Organisation werden von CIS Controls v8 mehrere zusätzliche Sicherheitskontrollen genannt, die wir zur Verringerung von Cybersicherheitsrisiken im täglichen Betrieb empfehlen.

Zusätzliche CIS-Steuerelemente:

Kontrolle 8: Prüfprotokollverwaltung
Erfassen, Alarmieren, Überprüfen und Speichern der Prüfprotokolle von Ereignissen, die das Erkennen, Verstehen und die Erholung von Angriffen unterstützen.

Kontrolle 14: Ein Schulungsprogramm zum Sicherheitserkenntnis und zum
Verstehen der Fähigkeiten und des Verhaltens von Mitarbeitern implementieren. Die Mitarbeiter schulen, wie unterschiedliche Formen von Angriffen identifiziert werden können.

Kontrolle 17: Reaktion auf Vorfälle und Verwaltung
Verwendung von schriftlichen Plänen für die Reaktion auf Vorfälle mit klar definierten Phasen für die Behandlung/Verwaltung von Vorfällen und die Rolle des Personals sowie für die Meldung eines Sicherheitsvorfalls an die zuständigen Behörden und Dritte.

Anleitung zum Härten des Systems
AXIS Camera Station Pro

Vers. M1.7
Datum: April 2024
Teil-Nr. T10203603