

AXIS Camera Station Pro

Introduction

Une fonctionnalité tout-en-un et à toute épreuve susceptible de rendre tout système de sécurité et site 100 % cybersécurisé. Aussi séduisants que ces mots puissent paraître, aucun dispositif de ce type n'existe, ou n'est susceptible d'exister de sitôt. Il s'agit plutôt d'analyser le risque que présentent les menaces et les vulnérabilités propres à leur organisation et, lorsque ce risque est considéré comme inacceptable, de mettre en œuvre des contrôles afin d'atténuer ce risque. Des politiques et procédures bien définies garantissent une communication et une application cohérentes de ces contrôles dans l'ensemble d'une organisation et sur la base d'un programme de cybersécurité éprouvé.

L'une des méthodes recommandées consiste à utiliser des cadres normalisés de gestion des risques de sécurité informatique tels que ISO 27001, NIST CSF ou autres. Même si cette tâche peut sembler décourageante pour les petites organisations, il vaut mieux définir un ensemble de politiques de sécurité de l'information et de processus de support que de ne rien avoir du tout. Si votre société s'engage sur la voie de la cybersécurité et dispose de ressources limitées, nous vous recommandons de consulter le *Center for Internet Safety (CIS) Critical Security Controls Version 8*. Le CIS propose une liste de 18 activités de contrôle de la sécurité réparties en trois groupes de mise en œuvre afin d'aider les sociétés à développer et à faire évoluer leur programme de cybersécurité.

Les failles de sécurité surviennent au sein de nombreuses organisations car elles n'ont pas établi de politiques, de règles et de procédures claires régissant l'utilisation des droits d'accès pour leurs propres employés. Votre organisation travaille-t-elle sur les politiques et les processus d'exploitation de la gestion vidéo ? Sinon, il est temps de commencer à les définir.

Objectif

Ce document présente un certain nombre de politiques et de procédures de cybersécurité permettant de sécuriser le déploiement et la maintenance des systèmes AXIS Camera Station Pro. Même s'ils ne sont pas directement liés à un cadre de cybersécurité, nous nous inspirons principalement des contrôles de sécurité critiques (CSC) version 8, en mettant l'accent sur les activités de contrôle suivantes :

- *Contrôle 1 : Inventaire et contrôle des ressources d'entreprise*
- *Contrôle 2 : Inventaire et contrôle des ressources logicielles*
- *Contrôle 3 : Protection des données*
- *Contrôle 4 : Configuration sécurisée des ressources et logiciels d'entreprise*
- *Contrôle 5 : Gestion des comptes*
- *Contrôle 6 : Gestion du contrôle d'accès*
- *Contrôle 7 : Gestion continue des vulnérabilités*
- *Contrôle 10 : Défenses contre les logiciels malveillants*

Nos recommandations sont axées sur l'assistance des installateurs, intégrateurs et utilisateurs finaux pour réduire les risques courants dans le cadre du déploiement et de la gestion des systèmes AXIS Camera Station Pro.

Conditions préalables

On suppose que les recommandations et procédures définies et décrites dans le *guide de renforcement d'AXIS OS* sont comprises et suivies. En outre, ce document fait référence à plusieurs rôles utilisateur courants qui interagissent avec un système vidéo. Veuillez mapper les rôles utilisateur afin qu'ils correspondent à vos propres classifications d'utilisateurs et de rôles. Un utilisateur spécifique peut disposer de plusieurs rôles, selon l'organisation.

Rôles définis :

- **Installateur système** : installe, met en place, répare, met à niveau et passe des systèmes à une version antérieure

- **Administrateur réseau** : maintient l'infrastructure réseau, la connectivité du nœud final, les serveurs et les ressources réseau, ainsi que la protection du réseau
- **Administrateur du système vidéo** : définit et gère le système vidéo pour sécuriser ses utilisations, ses performances et ses privilèges utilisateur
- **Responsable du système vidéo** : surveille, ajuste et dépanne les composants afin de garantir les performances système pour le compte de l'administrateur du système vidéo
- **Utilisateurs** : personnes qui utilisent un client AXIS Camera Station Pro pour accéder à la vidéo en direct et enregistrée ; elles sont généralement responsables de la protection physique d'une entreprise.

Politiques de sécurité du système

Sécurité physique

Politique de protection physique

Les serveurs, les périphériques, les équipements réseau et les câbles sont des objets physiques qui peuvent être manipulés, sabotés ou volés. L'hôte exécutant le logiciel serveur AXIS Camera Station Pro et des équipements réseau stratégiques (routeurs, commutateurs, etc.) doivent être placés dans un environnement dont les accès physiques et logiques sont restreints. Les caméras et autres appareils connectés doivent être installés dans des endroits difficiles d'accès et équipés de boîtiers résistants aux actes de vandalisme. Une attention particulière doit être portée à la protection des câbles dans les murs ou les conduits, car les risques de sabotage sont accrus avec cette configuration.

Politiques et procédures recommandées

Définissez une unité individuelle ou un groupe d'intervention responsable du contrôle visuel de la protection physique des serveurs VMS, du matériel réseau, des périphériques connectés et du câblage à des intervalles définis. Il est essentiel de maintenir un inventaire précis de tous les serveurs et périphériques, et d'indiquer notamment leur emplacement.

Gestion de logiciel

Politique logicielle des applications tierces

Comme AXIS Camera Station Pro est installé dans un environnement Windows standard, cela peut être tentant d'utiliser cet environnement pour des applications logicielles non liées à la gestion vidéo. L'installation d'autres applications tierces ouvre la possibilité d'introduire des logiciels malveillants dans l'environnement, ce qui peut entraîner un arrêt du système ou de fournir une porte d'entrée à un cybercriminel lui permettant de pénétrer dans le réseau de l'organisation.

Politiques et procédures recommandées

N'exécutez que le logiciel serveur de AXIS Camera Station Pro et les intégrations tierces sécurisées sur le matériel hôte. Si le matériel physique doit être utilisé à d'autres fins, il est recommandé d'utiliser plusieurs instances de serveur virtuels et d'exécuter le logiciel serveur de AXIS Camera Station Pro dans une machine virtuelle et le logiciel tiers non-VMS dans une autre machine virtuelle. Vous pouvez trouver des informations sur l'exécution d'AXIS Camera Station Pro dans un environnement virtuel [ici](#).

Il est recommandé de déployer des logiciels antivirus sur tous les serveurs et ordinateurs qui se connectent au serveur AXIS Camera Station Pro. Si des périphériques mobiles sont déployés, il faut notamment s'assurer que les périphériques sont installés avec les systèmes d'exploitation et les correctifs les plus récents (mais pas directement anti-antivirus). Lorsque vous scannez des virus, ne lancez pas l'opération sur les répertoires et les sous-répertoires contenant des bases de données d'enregistrement. En effet, la recherche de virus sur ces répertoires peut avoir un impact sur les performances du système.

Gestion de compte

Politique générale des comptes

Des droits de niveau administrateur sont parfois octroyés à des utilisateurs standard pour des raisons pratiques. Dans de nombreuses organisations, on ne sait pas précisément qui est responsable de l'examen des privilèges des comptes et du contrôle d'accès des employés aux systèmes.

Politiques et procédures recommandées

Nous recommandons aux organisations de respecter le principe de moindre privilège au moment de définir des comptes système. Cela signifie que les privilèges d'accès des utilisateurs sont limités aux seules ressources nécessaires à l'exécution de leurs tâches spécifiques. Il est également conseillé d'auditer régulièrement les privilèges de compte des utilisateurs du système afin d'éviter le détournement de privilèges.

AXIS Camera Station Pro Politique des comptes administrateur de

Lors du déploiement d' AXIS Camera Station Pro dans un environnement Windows, une erreur courante consiste à définir un compte administrateur unique pour l'hôte Windows. En effet, le mot de passe peut être partagé au fil du temps dans l'organisation, avec le risque que des utilisateurs non autorisés profitent des droits administrateur d'accès à l'environnement Windows. Cette situation entraîne facilement l'installation de nombreuses applications indésirables ou l'installation de programmes malveillants sur ce serveur.

Politiques et procédures recommandées

Le serveur AXIS Camera Station Pro qui héberge la machine Windows doit avoir au moins un compte administrateur et un compte utilisateur. Aucun de ces comptes ne doit être identique au compte administrateur de Windows par défaut. Le compte administrateur par défaut doit être désactivé après la création des comptes administrateur et utilisateur. Après le déploiement, le mot de passe du compte administrateur ne doit être connu et utilisé que par les **administrateurs du réseau**. Le compte utilisateur doit être utilisé par l'**administrateur du système vidéo** si/quand il doit se connecter au serveur AXIS Camera Station Pro. Notez que même si les deux rôles ci-dessus incombent à la même personne, il est toujours recommandé d'avoir des comptes d'administrateur réseau et vidéo séparés à des fins d'audit. Pour prendre en charge d'autres rôles, tels que ceux définis précédemment, d'autres comptes sans privilèges utilisateur doivent être créés pour chaque **utilisateur** qui se connectera au système.

Si l'hôte qui exécute AXIS Camera Station Pro se trouve dans un environnement du domaine Windows Active Directory, des comptes administrateur et utilisateur peuvent être créés dans le contexte du domaine ou le compte de domaine existant d'un employé permet de s'authentifier auprès de l'hôte AXIS Camera Station Pro. Cela simplifie la gestion des comptes, car il est inutile de créer ou d'entretenir d'autres comptes. En outre, il est possible d'utiliser la gestion des politiques de groupe pour mettre en œuvre des mots de passe complexes, déployer des certificats et d'autres fonctions de sécurité disponibles dans les environnements de domaine.

AXIS Camera Station Pro Politique des comptes utilisateur de

Les comptes utilisateurs sont attribués à des rôles spécifiques dans AXIS Camera Station Pro, qui déterminent à leur tour les droits spécifiques dont chaque utilisateur dispose dans le système, en lien notamment avec les vues et les vidéos qu'ils sont autorisés à accéder. Si plusieurs personnes partagent un compte utilisateur unique, le risque qu'un mot de passe soit partagé avec d'autres personnes de la société est accru. Le partage de comptes rend pratiquement impossible l'audit des personnes ayant accédé à telle ou telle caméra vidéo à un moment donné.

Politiques et procédures recommandées

Si possible, utilisez Microsoft Active Directory pour faciliter la gestion des utilisateurs et des groupes. Il est également recommandé de vérifier que les groupes de sécurité concernés ont été définis pour tous les rôles utilisateurs avant la configuration du système.

Active Directory fournit également :

- Une stratégie de mot de passe qui oblige les utilisateurs à modifier régulièrement leur mot de passe.
- Une protection contre les attaques par force brute, de sorte que le compte Windows AD est bloqué après l'échec de plusieurs tentatives d'authentification, dans la ligne de la politique de mot de passe de l'organisation
- Des autorisations basées sur des rôles, afin que les contrôles d'accès puissent être appliqués dans tout le domaine

Si des comptes Windows locaux doivent être utilisés, il est recommandé de créer un compte unique pour chaque utilisateur du système et de n'avoir accès qu'aux entités du système nécessaires à l'exercice de leurs responsabilités. L'utilisation de groupes pour les utilisateurs peut faciliter l'attribution des autorisations si plusieurs utilisateurs disposent des mêmes autorisations.

S'authentifier à l'aide de Kerberos

AXIS Camera Station Pro utilise l'authentification Windows intégrée pour authentifier les utilisateurs du client AXIS Camera Station Pro. AXIS Camera Station Pro utilise le protocole Microsoft Authentication (SPNEGO), ce

qui signifie que Kerberos est le protocole d'authentification préféré et par défaut. Le protocole de négociation tente d'utiliser Kerberos et utilise NTLM comme système de secours.

Remarque

À partir de la version 6.17, AXIS Camera Station Pro ne nécessite plus de SPN pour utiliser Kerberos. Ce qui suit ne s'applique qu'aux versions antérieures à la version 6.17.

Pour utiliser Kerberos, vous devez enregistrer les nom de principal de service (SPN) dans Active Directory à l'aide de la commande suivante :

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

HOST – Nom d'hôte du serveur d'exécution du serveur AXIS Camera Station Pro.

ACCOUNT_NAME – Nom de l'ordinateur (compte informatique) qui exécute le serveur AXIS Camera Station Pro.

Pour que Kerberos fonctionne correctement, nous vous recommandons d'enregistrer à la fois le nom d'hôte court et le nom de domaine complet (FQDN) du serveur AXIS Camera Station Pro cible.

Exemple:

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

Pour plus d'informations, consultez *Setspn sur microsoft.com*.

Politique des comptes de périphérique

Les comptes des périphériques Axis sont principalement des comptes ordinateurs/clients. Les **utilisateurs** ne doivent jamais être autorisés à accéder directement au périphérique. Le seul client qui doit accéder aux périphériques dans le cadre d'un fonctionnement normal est le serveur AXIS Camera Station Pro. Une stratégie commune consiste à faire en sorte que tous les périphériques ont le même mot de passe. Cette politique introduit des risques supplémentaires, mais elle permet également de simplifier la gestion des mots de passe de sorte qu'il faut évaluer sa tolérance aux risques. AXIS Camera Station Pro prend en charge l'attribution de mots de passe uniques à chaque périphérique via son interface de gestion.

Une erreur courante consiste à ajouter des périphériques à AXIS Camera Station Pro via un seul compte partagé entre plusieurs rôles. À un moment donné, l'**intervenant de maintenance du système vidéo** doit utiliser un navigateur pour effectuer des ajustements, le mot de passe du compte principal (racine) du périphérique est divulgué. D'ici quelques mois, la plupart des employés de la société connaîtront le mot de passe de tous les périphériques et auront les droits administrateur d'accès au système.

Politiques et procédures recommandées

Le périphérique doit disposer d'au moins deux comptes d'administrateur : un compte unique créé pour les administrateurs de périphériques et le compte racine par défaut pour l'ajout de périphériques au serveur AXIS Camera Station Pro. L'accès temporaire, par exemple lorsqu'un **intervenant de maintenance du système vidéo** accède à un périphérique via un navigateur Web, doit être géré avec des comptes temporaires.

AXIS Device Manager doit être le principal outil de gestion des comptes et des mots de passe des périphériques. Une version d'AXIS Device Manager est intégrée directement à AXIS Camera Station Pro. Elle est accessible dans l'onglet Management (Gestion). Le mot de passe racine du périphérique ne doit être utilisé que par AXIS Device Manager AXIS Camera Station Pro et ne doit être connu que de ceux qui utilisent AXIS Device Manager ou AXIS Camera Station Pro comme outil de gestion des périphériques.

Utilisez AXIS Camera Station Pro pour fournir un compte temporaire lorsqu'un intervenant de maintenance doit utiliser un navigateur Web pour accéder aux périphériques à des fins de dépannage ou de maintenance. Sélectionnez les périphériques et créez un compte, de préférence avec les privilèges opérateur, que l'intervenant de maintenance peut utiliser. Une fois la tâche terminée, supprimez le compte temporaire.

Maintenance du système

AXIS Camera Station Pro Politique de gestion des correctifs de l'hôte Windows

AXIS Camera Station Pro Le serveur et les clients s'exécutent sur un environnement Windows. Il est important que ces systèmes soient à jour pour s'assurer que les systèmes hébergeant le logiciel de AXIS Camera Station Pro ne présentent pas de vulnérabilités ouvertes pouvant être exploitées pour accéder sans autorisation au système de gestion vidéo.

Politiques et procédures recommandées

Pour tous les systèmes AXIS Camera Station Pro, qu'ils soient en cours d'exécution sur des enregistreurs vidéo Axis ou du matériel personnalisé, il est recommandé de désactiver la mise à jour automatique. Par le passé, les mises à jour Windows ont provoqué une certaine instabilité au niveau du système d'exploitation Windows sous-jacent. Il est donc recommandé de tester les mises à jour disponibles sur certaines machines afin d'assurer la stabilité du système avant de les transférer vers tous les systèmes hôtes qui exécutent AXIS Camera Station Pro. Cependant, un équilibre entre sécurité et stabilité doit être atteint, car un système Windows qui reste sans correctif trop longtemps peut introduire des risques pour l'environnement dans son ensemble. En fonction du niveau d'exposition du système du client à des menaces externes, la politique de gestion des correctifs doit prévoir un calendrier pour s'assurer que les systèmes reçoivent les dernières mises à jour.

AXIS Camera Station Pro Politique de mise à jour du logiciel

Dans la plupart des cas, l'utilisation de la dernière version du logiciel de AXIS Camera Station Pro garantit que vous utilisez des correctifs de sécurité pour toutes les vulnérabilités récemment découvertes. Laisser le système sans correctif pendant une durée plus longue augmente le risque de voir un cybercriminel exploiter les vulnérabilités et compromettre le système.

Politiques et procédures recommandées

Il est important de définir une politique de gestion des correctifs permettant d'évaluer régulièrement les versions logicielles déployées, afin de garantir que AXIS Camera Station Pro est à jour. La politique de gestion des correctifs doit également identifier les responsables des tâches liées à la mise à jour des logiciels serveur et client. Pour AXIS Camera Station Pro, la version la plus récente se trouve sur www.axis.com. AXIS Camera Station Pro requiert les dernières bibliothèques .NET. Il faut donc veiller à aligner la politique de gestion des correctifs Windows sur la politique relative à AXIS Camera Station Pro.

Politique de mise à jour du firmware des périphériques

L'utilisation de périphériques dotés d'une version de firmware à jour atténue la plupart des risques courants, car les dernières versions de firmware comportent des correctifs pour les vulnérabilités connues que les pirates peuvent tenter d'exploiter. Axis propose une solution de support à long terme (LTS) pour le firmware des périphériques qui comprend des correctifs de sécurité et des résolutions de bogues, mais les ajouts de fonctionnalités sont limités pour garantir la stabilité à long terme de la plate-forme. Pour plus d'informations sur la stratégie d'Axis en matière de développement de firmware, consultez le livre blanc sur la *gestion des firmwares d'Axis*.

Politiques et procédures recommandées

Pour les périphériques matériels, la politique doit préciser que l'ensemble des firmwares doivent être mis à jour. Les processus peuvent s'appuyer sur la fonction de mise à jour du firmware intégrée dans AXIS Camera Station Pro, ou sur AXIS Device Manager Extend, pour identifier si de nouvelles versions du firmware sont disponibles pour les périphériques Axis. Il convient de définir un calendrier, généralement en dehors des heures de bureau, pour déployer toutes les mises à jour de firmware pour toutes les caméras. AXIS Camera Station Pro / AXIS Device Manager Extend peut également vérifier si les mises à jour de firmware ont été acceptées. Si le système dispose d'intégrations spécifiques susceptibles d'être impactées par la mise à jour, pensez à la normalisation sur une piste de firmware LTS.

Sécurité réseau

Politique d'accès à distance

Les périphériques et les services exposés à Internet augmentent le risque de risque d'attaques externes visant à sonder ou exploiter les vulnérabilités connues. Les caméras exposées à Internet, par exemple par de petites organisations qui ont besoin d'un accès vidéo à distance, deviennent facilement vulnérables en cas d'utilisation de mots de passe faibles ou de détection d'une nouvelle vulnérabilité critique. L'accès distant à l'environnement Windows doit être étroitement contrôlé ou, si possible, évité. Dans la mesure où l'environnement Windows peut disposer d'une connectivité Internet pour la mise à jour des systèmes, l'utilisation de services de bureau distant comme Windows Remote Desktop, TeamViewer et AnyDesk introduit des chemins pour accéder à votre système s'il n'est pas géré correctement.

Politiques et procédures recommandées

N'exposez jamais l'adresse IP ou le port d'une caméra de façon à ce qu'elle/il soit accessible directement depuis Internet. Si un accès vidéo distant est nécessaire, utilisez l'accès distant sécurisé Axis. AXIS Camera Station Pro utilise un serveur d'accès distant basé sur le cloud pour faciliter l'accès distant crypté au système via le client AXIS Camera Station Pro ou l'application mobile AXIS Camera Station. En plus d'assumer la responsabilité de la gestion des connexions pour les utilisateurs distants et mobiles, le serveur d'accès distant joue un rôle important dans la protection de l'intégrité lorsqu'il est utilisé par les utilisateurs distants. Pour plus d'informations sur l'accès distant sécurisé Axis, cliquez [ici](#). Axis fournit des applications mobiles de marque officielle pour Android et Apple iOS. L'application mobile AXIS Camera Station ne doit être téléchargée qu'à partir de sources officielles, respectivement le Google Play Store et l'Apple App Store.

Lorsqu'il s'agit d'un accès au bureau distant dans l'environnement Windows, il est déconseillé de fournir ce type d'accès à un système qui exécute AXIS Camera Station Pro. Toutefois, si nécessaire, d'extrêmes précautions doivent être prises pour s'assurer que l'application de bureau à distance de votre choix est sécurisée, et que l'accès est uniquement fourni aux personnes qui en ont besoin. La mise en œuvre de niveaux supplémentaires de contrôles tels que l'authentification multifacteur (MFA) est vivement conseillée. Il est fortement recommandé de consigner et de vérifier ultérieurement les tentatives de connexion à distance pour suivre les utilisateurs et les heures d'accès à distance à l'environnement Windows.

Politique d'exposition du réseau local

La réduction de l'exposition du réseau local permet d'atténuer de nombreuses menaces courantes en limitant la surface d'attaque. Il existe de nombreux moyens de réduire l'exposition au réseau, y compris la segmentation physique (matériel et câbles réseau distincts), la segmentation logique via des réseaux locaux virtuels (VLAN) et le filtrage IP. Les caméras Axis prennent en charge un filtre IP (tableaux IP) de sorte que le périphérique ne répond qu'aux requêtes de connexion établies à partir d'adresses IP explicitement autorisées.

Politiques et procédures recommandées

Les enregistreurs vidéo AXIS Camera Station S22 sont des serveurs matériels dotés de deux ports réseau. L'un des ports crée un réseau segmenté pour les caméras et l'autre se connecte au réseau principal (domaine) pour servir les clients vidéo. Le serveur agit comme un pont et un pare-feu pour le réseau de caméras, ce qui empêche les clients d'accéder directement aux caméras. Cette configuration réduit le risque de menaces de cybercriminels sur le réseau principal.

Si le serveur AXIS Camera Station Pro et les caméras se trouvent tous sur le réseau principal, il est recommandé de configurer le filtre IP de la caméra, en limitant l'accès aux serveurs hébergeant AXIS Camera Station Pro, à AXIS Device Manager et aux clients de maintenance supplémentaires.

Applications et services supplémentaires

Si vous hébergez des applications supplémentaires sur le serveur AXIS Camera Station Pro qui sont destinées à rester confinées à localhost (le serveur lui-même), veuillez noter que les administrateurs peuvent être en mesure d'y accéder à distance via le client. Cela pourrait involontairement exposer ces applications.

Le même risque s'applique à tous les autres services fonctionnant sur le réseau. Afin de réduire les risques, nous vous recommandons de placer un pare-feu entre le réseau hébergeant AXIS Camera Station Pro et ses caméras, et tout autre réseau hébergeant des applications ou des services non liés. Cette segmentation contribue à limiter les risques potentiels et restreint les chemins d'accès non nécessaires.

Politique de cryptage du réseau

Le trafic réseau transféré sur des réseaux non sécurisés doit toujours être crypté. Internet est considéré comme un réseau non sécurisé. Un réseau local peut également être considéré comme non sécurisé et le trafic réseau doit donc également être crypté. La politique applicable au trafic vidéo sur le réseau dépend du classement des vidéos et du risque d'accès au système vidéo par des cybercriminels. Il est recommandé de partir du principe que le réseau est déjà compromis. Généralement, les grandes entreprises ont une politique de classification du réseau.

Politiques et procédures recommandées

Le trafic entre le client vidéo et le serveur AXIS Camera Station Pro doit être crypté. Le trafic entre le serveur AXIS Camera Station Pro et les caméras doit être crypté en fonction de l'infrastructure. Les caméras Axis sont disponibles avec un certificat auto-signé et le protocole HTTPS activé par défaut. En cas de risque d'usurpation de réseau, comme lorsqu'un ordinateur malveillant tente d'utiliser l'identité d'une caméra, il est nécessaire d'utiliser une infrastructure de clé privée avec des certificats signés par une autorité de certification. AXIS Camera Station Pro dispose d'une autorité de certification locale intégrée (CA) qui peut gérer de manière rentable la signature et la distribution des certificats de serveur pour les périphériques Axis.

Versions TLS :

Nous recommandons de désactiver les versions 1.1 et 1.0 de TLS. L'installateur AXIS Camera Station propose de vous assister lors de l'installation ou de la mise à niveau.

Cryptogrammes HTTPS

AXIS Camera Station Pro prend en charge et utilise des suites de cryptage TLS pour crypter les connexions HTTPS en toute sécurité. La suite de cryptogrammes spécifique dépend du client qui se connecte à AXIS Camera Station Pro ou du service contacté et AXIS Camera Station Pro négocie en fonction du protocole TLS. Nous recommandons de configurer Windows pour qu'il n'utilise pas les suites de chiffrement TLS 1.2 répertoriées *dans la RFC 7540*. La possibilité de désactiver une suite de chiffrement dépend des périphériques et des caméras utilisés avec AXIS Camera Station Pro. Si un périphérique ou une caméra nécessite une suite de cryptogrammes spécifique, il sera peut-être impossible de désactiver la suite de cryptogrammes faible.

Gestion des données

Installation

AXIS Camera Station Pro permet l'installation dans un dossier situé en dehors du répertoire standard des fichiers de programme. Cela peut toutefois impliquer des contrôles d'accès moins stricts et présenter des risques potentiels pour la sécurité. Nous vous recommandons d'utiliser le chemin d'installation par défaut ou de vérifier les droits d'accès propres au dossier choisi.

Classification des vidéos

Les vidéos en direct et enregistrées doivent être classées. Les vidéos peuvent être classées en catégories publiques, privées, restreintes ou autres, telles que définies par les politiques d'entreprise. Dans de nombreux cas, la vidéo est réglementée par la législation et des réglementations régionales, ainsi que par des politiques informatiques internes. Les propriétaires des systèmes doivent donc connaître les lois et réglementations qui s'appliquent à leurs données vidéo.

Politiques et procédures recommandées

Classez les vidéos en direct, les vidéos enregistrées et l'audio conformément aux politiques de classification des données de l'entreprise. Configurez les privilèges d'accès des utilisateurs et renforcez le système selon la sensibilité des données vidéo et audio. S'il est inutile, l'audio peut être désactivé au niveau d'un périphérique.

Contrôles de sécurité supplémentaires

Selon le niveau de maturité et la tolérance aux risques de votre organisation, plusieurs autres contrôles de sécurité sont mis en place à partir des contrôles de sécurité critiques version 8 recommandés pour contribuer à réduire les risques de cybersécurité dans les opérations quotidiennes.

Contrôles de sécurité critiques supplémentaires :

Contrôle 8 : Gestion des journaux d'audit

Recueillez, alertez, analysez et conservez les journaux d'audit des événements qui peuvent aider à détecter, comprendre ou récupérer d'une attaque.

Contrôle 14 : Mise en œuvre d'un programme de sensibilisation et de formation à la sécurité

Comprendre les compétences et les comportements des membres de votre personnel. Formez le personnel à l'identification des différentes formes d'attaques.

Contrôle 17 : Réponse et gestion des incidents

Utilisez des plans d'intervention écrits en cas d'incident avec des phases de traitement/gestion des incidents et des rôles du personnel clairement définies, et qui décrivent le signalement des incidents de sécurité aux autorités concernées et aux tiers.

Sécurité des sauvegardes de bases de données

Si vous changez le lieu des sauvegardes de la base de données, utilisez un lieu sécurisé dont l'accès est limité. Un partage de réseau à large accès est moins sûr.

DbConsole

DbConsole est un outil de ligne de commande qui vous permet d'effectuer des sauvegardes et restaurations de bases de données lorsque AXIS Camera Station Pro n'est pas en cours d'exécution. Consultez *Manual backup (Sauvegarde manuelle)* et *Restore database (Restauration de la base de données)* pour plus d'informations.

- Ne fournissez pas le mot de passe en tant que paramètre à l'outil, car il pourrait être visible dans la liste des processus et l'historique du shell. Exécutez plutôt l'outil en tant qu'utilisateur disposant des droits administrateur, ou fournissez le mot de passe à l'invite.
- Lorsque vous exécutez la commande de sauvegarde, assurez-vous de spécifier un lieu sécurisé pour la sortie.
- Lorsque vous exécutez la commande de restauration, utilisez uniquement des fichiers de sauvegarde provenant de sources fiables. La restauration de fichiers de sauvegarde malveillants peut compromettre la sécurité de votre système.

T10203603_fr

2026-07 (M5.2)

© 2024 – 2026 Axis Communications AB