AXIS COMMUNICATIONS

Cybersécurité

ENSEMBLE POUR UNE MEILLEURE CYBERPROTECTION

AXIS COMMUNICATIONS

TABLE DES MATIÈRES

PARTAGE DES RESPONSABILITÉS 3

CYBERMENACES COURANTES 4

Cybersécurité : leçons à tirer de la sécurité physique 4

Panorama des menaces potentielles 5

Naïveté et erreur humaine 6

Détournement délibéré du système 7

Altération physique ou sabotage 8

Exploitation des vulnérabilités logicielles 9

CONSIDÉRATIONS DE CYBERSÉCURITÉ 10

Clients finaux : quel rôle ont-ils à jouer pour atténuer les risques ? 10

Que faut-il savoir sur son fournisseur en surveillance et ses sous-traitants ? 11

Partenaires de la chaîne logistique 12

Quel degré de sécurité dans la production de votre fournisseur ? 13

Réseaux Zero-Trust 14

Visite du moteur de politiques... 15

Le rôle critique d'une gestion efficace du cycle de vie 16

APPROCHE AXIS DE LA CYBERSÉCURITÉ 17

Socle de sécurité 18

Approche structurée et systématique de la sécurité interne 18

Protection de l'intégrité des produits et réduction du risque de vulnérabilités dans les logiciels 19

Gestion des nouvelles vulnérabilités 21

Production et distribution 22

Réduction du risque de compromission de composants matériels et logiciels 22

Fonctions de cybersécurité intégrées 23

Mise en œuvre 25

Cybersécurité en phase de mise en œuvre 25

En service 26

Cybersécurité des dispositifs en service 26

Retrait d'exploitation 28

Planification des retraits d'exploitation 28

CONFORMITÉ 29

POURQUOI AXIS ? 30

INTRODUCTION

Atténuation du risque de cyberincident

La protection des produits et services logiciels en réseau contre les cybermenaces est essentielle pour sécuriser les données et les systèmes de votre réseau. La compromission d'un système peut exposer la confidentialité et l'intégrité des données ou vous priver d'accès ou de données lorsque vous en avez besoin.

En tant que partenaire de cybersécurité rigoureux, nous avons compilé quelques principes et considérations pour vous aider à choisir et sécuriser des produits de sécurité physique basés sur IP. Nous cherchons à vous simplifier la mise en place de vos garde-fous afin que vous puissiez utiliser nos offres Axis de la manière la plus sûre possible.

En plus des pages suivantes, vous pouvez approfondir la question de la cybersécurité et des moyens de renforcer ensemble la cyberprotection à l'adresse www.axis.com/cybersecurity

Partage des responsabilités

La cybersécurité porte sur les produits, les personnes, les technologies et les processus continus. La participation de tous est clairement une nécessité pour que tous les maillons de la chaîne de cybersécurité soient aussi solides que possible. La cybersécurité est une responsabilité partagée qui impose à tous les acteurs, y compris les clients finaux, d'œuvrer dans ce sens.

Fabricants de dispositifs

C'est là où commence la cybersécurité. Pour minimiser le risque de faille sur tout le cycle de vie de leurs produits, les fabricants doivent appliquer des bonnes pratiques de cybersécurité dans la conception, le développement, la production et la maintenance des logiciels. Ils doivent donc appliquer un contrôle rigoureux de leur propre chaîne logistique. Les produits doivent intégrer des fonctions permettant l'application de divers contrôles de sécurité. Des outils doivent être à la disposition des clients pour configurer et gérer efficacement leurs dispositifs en appui de leurs procédures ou politiques de sécurité. Enfin, des canaux de communication doivent être en place pour informer les partenaires et les clients des nouvelles vulnérabilités détectées.

Distributeurs

Pour les distributeurs qui ne manipulent pas directement les produits, la cybersécurité est relativement simple. En revanche, les distributeurs à valeur ajoutée doivent tenir compte des mêmes considérations que les intégrateurs et les installateurs, notamment lorsqu'ils achètent des équipements d'un fabricant pour les commercialiser sous une autre marque (ou la leur). La transparence est fondamentale, et l'origine des équipements doit être claire.

Consultants, intégrateurs et installateurs

Ils peuvent aider les clients finaux à identifier, développer et mettre en pratique les contrôles de sécurité, mais aussi s'assurer que les dispositifs de sécurité physique ne présentent pas de vulnérabilité sur le réseau des clients. Cette assistance peut passer par l'élaboration d'une stratégie pour des éléments comme les mots de passe, la gestion des accès distants et la maintenance des logiciels et des dispositifs connectés. Elle peut également veiller à s'assurer que les matériels installés disposent des derniers correctifs et que le système fait l'objet d'analyses antivirus. La problématique des équipements OEM/ODM, où les responsabilités de cybersécurité sont souvent floues, doit faire partie de la discussion générale autour de la cybersécurité.

Clients finaux

Comme chaque entreprise a des besoins spécifiques et uniques en cybersécurité, il n'existe pas de configuration universelle en la matière. Néanmoins, un ensemble de politiques de sécurité informatique doit être en place pour définir l'étendue de la sécurité nécessaire. L'élimination des comptes par défaut, l'utilisation de mots de passe uniques et complexes, stockés de manière sûre et changés régulièrement, l'attribution d'autorisations différenciées et l'installation systématique des correctifs et des mises à jour ne sont que quelques-unes des procédures à appliquer.

Chercheurs

Ils découvrent souvent les vulnérabilités des dispositifs. Si la vulnérabilité n'est pas intentionnelle, le chercheur informe généralement le fabricant pour lui donner la possibilité de la corriger avant la publication. En revanche, si une vulnérabilité critique est intentionnelle, ils alertent plutôt le public pour sensibiliser les utilisateurs.

Cybersécurité : leçons à tirer de la sécurité physique

La plupart d'entre nous se représentent facilement les risques de sécurité physique. Une porte non verrouillée accroît le risque d'accès d'intrus. La visibilité de biens précieux augmente le risque de vol. Les erreurs et les accidents peuvent porter préjudice aux personnes, aux biens et aux objets. La sécurité physique et la cybersécurité sont généralement abordées de la même manière.

Que vous soyez responsable de la sécurité physique ou de la cybersécurité de votre entreprise, vous devez appliquer les mêmes principes :

> Identifier et classifier vos actifs et vos ressources (quoi protéger)

> Identifier les menaces plausibles (protéger de qui/quoi)

> Identifier les vulnérabilités plausibles que peuvent exploiter les menaces (probabilité)

> Identifier les coûts attendus en cas d'événement préjudiciable (conséquences) Le risque est souvent défini comme la probabilité d'une menace multipliée par le résultat négatif qu'elle engendre. Une fois le risque déterminé, vous devez savoir quelles mesures vous êtes prêt à prendre pour éviter les effets négatifs.

Notions sur la cybersécurité

La cybersécurité vise à protéger les systèmes et services informatiques des cyberattaques. Les pratiques de cybersécurité comprennent des processus de prévention des dommages et de restauration des ordinateurs, des systèmes et services de communications électroniques, des communications filaires et électroniques, ainsi que des informations stockées afin de garantir leur confidentialité, leur intégrité, leur disponibilité, leur sécurité, leur authenticité et leur non-répudiation.

Panorama des menaces potentielles

Les éléments essentiels à protéger dans un système informatique ou opérationnel sont la confidentialité, l'intégrité, la disponibilité et la sécurité. Un événement préjudiciable à l'un de ces éléments est un incident de sécurité.

Dans les pages suivantes, nous faisons le point sur les cybermenaces les plus courantes et les vulnérabilités qu'elles exploitent. Quatre cybermenaces courantes pèsent sur les systèmes de sécurité physique :

1. **Naïveté et erreur humaine**
2. **Détournement délibéré du système**
3. **Altération physique et sabotage**
4. **Exploitation des vulnérabilités logicielles**

1 Naïveté et erreur humaine

Quelle que soit l'efficacité des technologies utilisées pour protéger votre réseau, le facteur humain reste déterminant dans les compromissions de sécurité.

Plusieurs types d'erreur humaine peuvent ouvrir la voie à une cyberattaque :

> **Ingénierie sociale**

Utilisateur amené, par manipulation psychologique, à commettre des erreurs de sécurité ou à transmettre des informations sensibles. Le phishing et le « scareware » sont des exemples d'ingénierie sociale.

> **Usage impropre des mots de passe**

Non-utilisation de mots de passe renforcés ou négligence dans la protection et/ou le changement régulier des mots de passe.

> **Gestion négligente de composants critiques**

Perte ou oubli d'un objet permettant d'accéder au système : carte d'accès, téléphone, ordinateur portable, documents...

> **Gestion négligente du système**

Non-installation des mises à jour et des correctifs de sécurité du système.

> **Améliorations contre-productives**

La résolution d'un problème par un utilisateur se traduit par une baisse des performances du système.

Vulnérabilités et erreur humaine

Certaines des vulnérabilités les plus communes dues à une erreur humaine découlent d'un manque de sensibilisation à la cybersécurité et de l'absence de politiques et de procédures de long terme de gestion du risque. Pour atténuer le risque d'erreur humaine, l'ensemble du personnel d'une organisation doit être formé aux bonnes pratiques de cybersécurité. Vous devez également restreindre l'accès aux dispositifs en réseau à seulement quelques personnes de confiance sur votre système de gestion vidéo (VMS) ou gestionnaire de dispositifs.

2 Détournement délibéré du système

Une autre cybermenace trop répandue est le détournement délibéré d'un système par des utilisateurs disposant d'un accès légitime.

Parmi les types de détournement intentionnel :

Manipulation des services et des ressources du système

Vol de données

Dommages délibérés au système

Vulnérabilités et détournements intentionnels

La mise en place de stratégies et de processus au long cours est indispensable pour faciliter la gestion des vulnérabilités et réduire le risque de détournement intentionnel du système. Une approbation formalisée des utilisateurs disposant d'autorisations d'accès à des données sensibles doit être en place, tout comme la limitation de leur nombre.

Les logiciels de gestion des dispositifs de sécurité physique en réseau, tels que les caméras, doivent être associés à un compte administrateur avec ses propres identifiants. Ce compte doit être unique et non partagé. Les opérateurs du site doivent ensuite avoir des comptes individuels dans le logiciel de gestion. Aucune personne ne doit avoir un accès direct aux dispositifs de sécurité physique. S'il existe des raisons valables d'autoriser un accès direct, cet accès doit être limité dans le temps.

3 Altération physique ou sabotage

La protection physique est capitale du point de vue de la cybersécurité :

> Les équipements physiquement accessibles peuvent être trafiqués.

> Les équipements physiquement accessibles peuvent être volés.

> Les câbles exposés peuvent être débranchés, réacheminés ou coupés.

Vulnérabilités et menaces physiques

Parmi les vulnérabilités courantes figurent les équipements réseau, par exemple les serveurs et les switches situés dans des locaux non verrouillés, les caméras facilement accessibles sans boîtier de protection ou les câbles non protégés par des murs ou des conduits. Les équipements en réseau peuvent également exposer d'autres ressources sur le même réseau.

Les conséquences sont ailleurs

Les systèmes vidéo, audio et de contrôle d'accès ne traitent pas de transactions financières et n'hébergent aucune donnée de clients. Une attaque sur ce type de système peut donc être difficile à monétiser et manquer d'intérêt pour les organisations cybercriminelles. Cependant, un système compromis peut devenir une menace pour les autres systèmes. L'estimation des coûts est donc délicate. Malheureusement, les entreprises les découvrent souvent à leurs dépens. La protection est comme la qualité : il faut en payer le prix. En achetant bon marché, vous risquez de voir les coûts s'envoler sur le long terme si les fournisseurs n'ont pas intégré la cybersécurité tout au long du cycle de vie de leurs produits.

4 Exploitation des vulnérabilités logicielles

Le développement logiciel comporte le risque de négliger des vulnérabilités de sécurité susceptibles de servir de porte d'entrée à une cyberattaque. Les bugs ou les erreurs dans le code en sont les sources les plus fréquentes. Plus un produit contient de vulnérabilités logicielles, plus le risque qu'il soit victime d'une attaque est élevé. Avant la commercialisation d'un produit, le fabricant doit en principe appliquer un modèle de développement logiciel incluant des processus et des outils qui minimisent le risque de vulnérabilité à toutes les phases de développement.

Or, les logiciels sont rarement parfaits lorsqu'ils sortent. C'est pourquoi le fabricant du produit se doit d'identifier, de corriger et de communiquer aux clients les erreurs, les bugs et les déploiements incorrects qui créent des failles de sécurité. Par conséquent, le fabricant doit faire preuve de transparence dans sa communication des nouvelles vulnérabilités détectées et proposer sans délai une solution aux clients. Il est également essentiel que le client applique systématiquement les mises à jour logicielles contenant des correctifs de sécurité dès que le fabricant les a publiées.

Clients finaux : quel rôleont-ils à jouer pour atténuer les risques ?

Tout d'abord, plusieurs éléments sont à considérer au plan de la cybersécurité lors de l'acquisition de produits de sécurité physique.

En premier lieu, examinez la stratégie de cybersécurité de vos fournisseurs de produits de sécurité physique : appliquent-ils une politique d'entreprise qui régit la cybersécurité, dans laquelle ils identifient et évaluent leurs ressources en continu et pratiquent des analyses de risque relevant de ces ressources ? Par ailleurs, vous devez comprendre comment vos fournisseurs interagissent avec leur chaîne logistique. Posez-vous également les bonnes questions : leurs produits sont-ils conçus et fabriqués en y intégrant des fonctions et une prise en charge de la cybersécurité ?

Quelles mesures en appui de la cybersécurité proposent-ils tout au long du cycle de vie d'un produit réseau ? Si votre système est victime d'une attaque, que se passe-t-il ? Vos fournisseurs publient-ils des consignes pour vous aider à réagir à un incident de cybersécurité impliquant leurs produits ?

Ce ne sont là que quelques-uns des sujets à évaluer. Nous allons les détailler dans les pages suivantes.

Que faut-il savoir sur son fournisseur en surveillance et ses sous-traitants ?

Les risques de sécurité sont toujours présents. De nouvelles menaces émergent et leur nature peut évoluer à tout moment. Souvent, les entreprises s'intéressent seulement à la manière dont leurs fournisseurs évaluent et neutralisent ces risques. Mais qu'en est-il des sous-traitants du fournisseur ? Comment les fournisseurs gèrent-ils toute leur chaîne logistique et veillent-ils à la sécurité de tous leurs produits, du composant au produit fini ?

Votre fournisseur s'attache-t-il à minimiser les risques de sécurité ?

> Contrôle-t-il toute sa chaîne d'approvisionnement, du composant au produit fini ?

> Applique-t-il un modèle de développement logiciel intégrant les considérations de sécurité ?

> Intègre-t-il la protection dans la conception et la fabrication de ses produits ?

> Partage-t-il des connaissances et des outils pour mettre en place des moyens de protection ?

> Propose-t-il une réaction rapide et des mises à jour gratuites en cas de détection d'une nouvelle vulnérabilité logicielle ?

Partenaires de la chaîne logistique

La sécurité de la chaîne logistique débute par un choix éclairé de partenaires selon un processus d'évaluation rigoureux. Ce processus doit comporter pour chaque candidat une analyse de ses processus de gestion qualité et de ses pratiques durables. A minima, elle doit être certifiée ISO 9001 ou IATF 16949 par un organisme indépendant.

Évaluation des sous-traitants

Votre fournisseur doit évaluer les processus de gestion du risque de ses sous-traitants, ainsi que leurs installations et procédés de production. Des visites de site et des audits de suivi sur place doivent avoir lieu pour évaluer si les installations respectent les conditions et critères définis pour la qualification de fournisseur approuvé. Dans le processus d'évaluation de nouveaux partenaires potentiels de la chaîne logistique, une analyse approfondie de la situation financière et du tour de table des sous-traitants doit être menée.

Sous-traitants stratégiques

Avec les sous-traitants de composants critiques et les partenaires fabricants, les relations sont généralement étroites et durables. Ce sont des acteurs stratégiques avec lesquels votre fournisseur codirige les projets et le développement, définit des objectifs et prend des engagements mutuels à long terme. Tous les composants critiques faisant partie des produits de votre fournisseur doivent être approvisionnés directement à partir de sous-traitants stratégiques et entreposés en interne. Les composants non critiques peuvent être achetés par les partenaires fabricants eux-mêmes, mais uniquement auprès de fournisseurs appartenant à une liste de fournisseurs approuvés.

Quel degré de sécurité dans la production de votre fournisseur ?

> Est-ce qu'il définit et contrôle les procédés de fabrication ?
> Est-ce qu'il développe et produit des équipements de production critiques ?
> Votre fournisseur propose-t-il un système de test des composants, modules et produits pendant la production, accompagné de logiciels, d'ordinateurs de test et d'autres structures informatiques physiques ?
> Votre fournisseur collecte-t-il les données de production 24 h/7 j pour l'analyse en temps réel des données, l'évaluation des risques de sécurité et l'application de plans de correction ?

Le meilleur moyen pour votre fournisseur de garantir la conformité de ses sous-traitants au cahier des charges spécifié consiste à mener des audits réguliers sur site, annuellement ou tous les deux ans. Ces audits doivent porter sur une série de sujets importants, comme la conformité des processus, le contrôle de qualité et la traçabilité. Ils doivent également englober un examen de la manutention dans les installations, de la gestion d'inventaire et des équipements de production.

Un examen trimestriel de l'activité est un bon moyen de suivre la performance par rapport aux attentes. Pour les sous-traitants stratégiques, il est recommandé de mener ces évaluations au niveau de la direction.

Sécurité physique

Tous les sites de la chaîne d'approvisionnement, du fournisseur de composants au centre de distribution, doivent satisfaire les exigences rigoureuses concernant la sécurité des installations. Par exemple, les accès et les sorties doivent être gardés en permanence, et le contrôle et l'enregistrement des visiteurs doivent être consignés et conservés. Par ailleurs, ils doivent utiliser des équipements d'analyse pour détecter les objets ou matériaux indésirables. Le transport doit être assuré uniquement par des transporteurs de bonne réputation, qui appliquent des réglementations et des contrôles de sécurité rigoureux. Il est également recommandé de surveiller et de documenter les marchandises entrantes et sortantes à l'aide de caméras.

Réseaux « Zero-Trust »

Les réseaux sont de plus en plus vulnérables. La croissance exponentielle des dispositifs connectés se traduit par toujours plus de terminaux réseau exposés aux attaques. Les cyberattaques sont non seulement plus nombreuses, mais aussi plus sophistiquées. Pour s'en prémunir, le concept de « Zero-Trust » a émergé.

Ne faites confiance à rien ni personne sur le réseau

Comme son nom l'indique, la posture par défaut d'un réseau Zero-Trust consiste à ne se fier à aucune entité qui s'y connecte, qu'elle soit humaine ou matérielle. Et ce quel que soit le lieu où elle se trouve et son mode de connexion. La philosophie prépondérante des réseaux Zero-Trust est donc la suivante : ne jamais faire confiance, toujours vérifier.

Accordez l'accès minimal nécessaire

L'identité d'une quelconque entité qui accède au réseau ou qui s'y trouve est vérifiée plusieurs fois de différentes manières, en fonction de son comportement et de la sensibilité des données auxquelles elle accède sur le réseau. À la base, il est octroyé aux entités le niveau d'accès minimal nécessaire pour exécuter leurs tâches.

Réseaux et architectures Zero-Trust

En prenant conscience du besoin de renforcer la cybersécurité, les clients mettent en place des réseaux et des architectures Zero-Trust, notamment HTTPS et la norme plus sophistiquée IEEE 802.1X, qui peuvent autoriser automatiquement les dispositifs authentifiés sur le réseau et bloquer les autres. Pour les fabricants de dispositifs réseau, il devient indispensable de répondre à ces nouveaux environnements en incluant des technologies ou des interfaces qui prennent en charge ces réseaux.

La posture par défaut d'un réseau Zero-Trust consiste à ne se fier à aucune entité qui s'y connecte.

Visite du moteur de politiques…

Au cœur de tous les réseaux Zero-Trust réside un moteur de politiques : ce logiciel permet aux entreprises de créer, contrôler et appliquer des règles sur les modalités d'accès aux données et ressources réseau. Les moteurs de politiques exploitent un ensemble de fonctions d'analyse réseau et de règles programmées pour accorder les autorisations par rôle en fonction de plusieurs facteurs.

Oui ou non à chaque demande

En termes simples, le moteur de politiques compare chaque demande d'accès réseau à la politique, puis informe l'applicateur sur la légitimité ou non de la demande. Dans un réseau Zero-Trust, le moteur de politiques définit et applique des politiques d'accès et de sécurité des données à tous les modèles d'hébergement, sites, utilisateurs et dispositifs.

Définition et application de règles

Pour qu'un moteur de politiques fonctionne, les entreprises doivent définir soigneusement les règles et politiques dans les équipements de contrôle de sécurité essentiels, comme les pare-feux nouvelle génération (NGFW), les passerelles de sécurité e-mail et cloud et les logiciels de prévention de la perte des données (DLP). Ensemble, ces contrôles se conjuguent pour appliquer les micro-segmentations réseau au-delà des modèles d'hébergement et des sites.

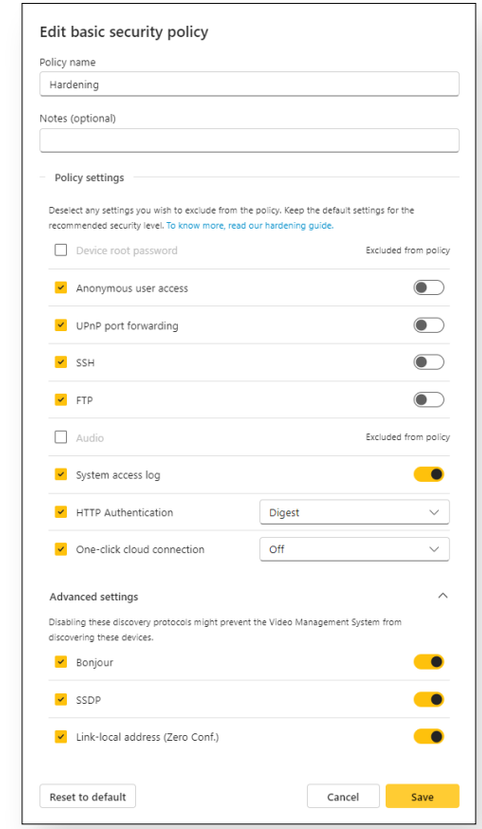
Modalités d'accès aux données et ressources réseau

Avec les moteurs de politiques, vous pouvez :

> Créer des règles
> Contrôler des règles
> Appliquer des règles

Moteurs de politiques actuels et futurs

Actuellement, la définition des politiques peut être nécessaire dans la console de gestion de chaque solution. Cependant, l'intégration toujours plus poussée des consoles peut favoriser la définition et l'actualisation automatiques des politiques sur tous les produits. La gestion des identités et des accès (IAM), l'authentification multifacteurs, les notifications push, les autorisations de fichiers, le chiffrement et l'orchestration de la sécurité jouent tous un rôle dans la conception d'architectures réseau Zero-Trust.



Configuration d'un moteur de politiques

Le rôle critique d'une gestion efficace du cycle de vie

Préparez-vous face aux menaces

Une gestion efficace du cycle de vie peut aider les entreprises à protéger leur activité et à mieux se préparer pour l'avenir. Cela suppose de situer les risques et de rester informé des domaines susceptibles d'être exploités à des fins malveillantes. Cette considération s'adresse particulièrement aux systèmes de sécurité, car si une caméra de surveillance réseau tombe en panne, les conséquences peuvent être désastreuses.

Mettez à jour les dispositifs en réseau

Tous les dispositifs en réseau, des caméras au système VMS, doivent être mis à jour et corrigés régulièrement pour éviter l'exploitation des vulnérabilités connues et le contournement des moyens de protection existants.

Les fabricants publient régulièrement des mises à jour et des correctifs de sécurité pour les logiciels des dispositifs, qui résolvent les vulnérabilités, les bugs et d'autres problèmes de performance afin de préserver la stabilité et la sécurité du système. Toutefois, les entreprises négligent souvent de mettre à jour le firmware ou le système d'exploitation qui pilote le matériel.

Généralement, c'est parce qu'elles n'ont pas une vue complète de tous les dispositifs de leur réseau. Et même avec un panorama complet, la mise à jour de tous les dispositifs peut être fastidieuse et chronophage.

Sans mise à jour régulière de leurs logiciels, les dispositifs sont plus vulnérables aux cyberattaques, dont le préjudice peut aller d'une perte d'exploitation à de fortes amendes pour non-conformité réglementaire.

Or, un réseau est seulement aussi sûr que les dispositifs qui le composent. Il est donc capital de gérer soigneusement le cycle de vie des ressources physiques en réseau.

Un dispositif, deux durées de vie

Le cycle de vie associé aux dispositifs pilotés par logiciel se divise en deux types:

1) Durée de vie fonctionnelle du dispositif, ou durée réaliste pendant laquelle un dispositif peut fonctionner. Par exemple, une caméra réseau possède une durée de vie fonctionnelle de 10 à 15 ans.

2) Cycle de vie économique du dispositif : combien de temps avant qu'il commence à coûter plus cher en maintenance que l'adoption de nouvelles technologies ? Alors qu'une caméra IP peut rester opérationnelle pendant 15 ans, sa durée de vie réelle sera plus courte en raison de l'évolution rapide de l'environnement de cybersécurité.

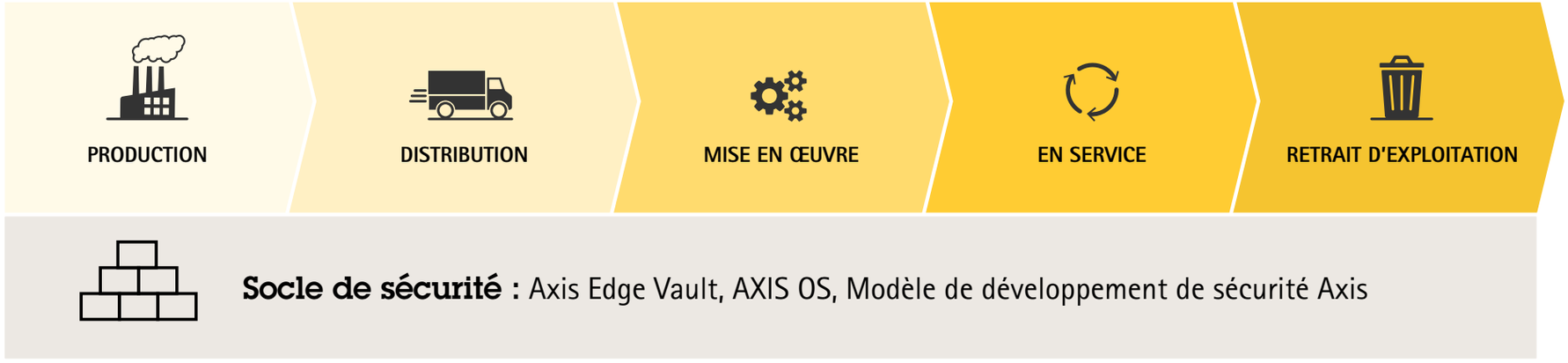
Gérez vos ressources de manière proactive

La gestion du cycle de vie se rapporte à la gestion efficace du cycle de vie fonctionnel et économique des ressources physiques. Les entreprises doivent compter sur un panorama clair de tous les dispositifs déployés sur le réseau pour s'assurer qu'ils sont protégés des cybermenaces.

Approche Axis de la cybersécurité

Axis tient à favoriser un niveau élevé de cybersécurité. Nous œuvrons constamment à l'amélioration de nos offres et de nos processus de cybersécurité. Pour nous, la transparence est cruciale dans toutes nos actions : sécurisation de nos opérations et de notre chaîne logistique, pratiques de développement logiciel pour réduire les risques de vulnérabilité, traitement des nouvelles vulnérabilités détectées, intégration de la sécurité dans nos produits, appui à la cybersécurité sur tout leur cycle de vie…

Les pages suivantes détaillent nos mesures en place comme socle de sécurité et notre accompagnement à toutes les phases du cycle de vie d'un produit, de la production au retrait d'exploitation, en passant par la mise en œuvre et l'exploitation, pour atténuer les risques et vous aider à sécuriser les produits Axis.



Socle de sécurité

Approche structurée et systématique de la sécurité interne

Axis encourage une approche collaborative de la cybersécurité, où l'ensemble du personnel contribue à l'amélioration continue de notre sécurité en interne. Notre système de gestion de la sécurité des informations (ISMS) certifié ISO 27001 forme le socle de notre programme de cybersécurité. Dans le cadre de ce système, nous avons mis en place des contrôles de cybersécurité pour vérifier que nous respectons les bonnes pratiques dans la gestion de notre infrastructure informatique, de notre plateforme de développement logiciel et de nos services connectés.

En adoptant une approche structurée et systématique, nous protégeons la confidentialité, l'intégrité et la disponibilité de nos ressources. Axis respecte également plusieurs exigences réglementaires ainsi que des cadres et des critères judicieusement sélectionnés, notamment la norme de cybersécurité ETSI EN 303 645 pour la gamme de dispositifs AXIS OS. Cependant, nous ne comptons pas seulement sur les réglementations et les certifications. En effet, beaucoup de certifications ne se traduisent pas nécessairement par un renforcement de la cybersécurité.

RI. SE

CERTIFIKAT

ISO/IEC 27001

Härmed intygas att/This is to certify that

Axis Communications AB

Gränden 1, 223 69 LUND, SWEDEN

har ett ledningssystem för informationssäkerhet som uppfyller kraven enligt ISO/IEC 27001:2022 vad gäller
has an information security management system that fulfils the requirements of ISO/IEC 27001:2022 with respect to

Product management, utveckling och drift inom
IT-infrastrukturtjänster och Axis Connected Services
Allt i enlighet med uttalande om tillämplighet fastställt 2023-11-14

Product management, development and operations within
IT infrastructure services and Axis Connected Services
All in accordance with Statement of Applicability established 2023-11-14

Ursprungligen utfärdat/Originally issued	2019-02-27
Giltigt till och med/Expiry date	2025-02-26
Beslutsdatum/Decision date	2023-12-07

Jonas Madsen

RISE Research Institutes of Sweden AB | Certification
Box 857, SE-501 15 Borås, Sweden
+46 10-516 50 00
certifiering@ri.se | www.ri.se

SP

Certifikat/Certificate 6134 | | version/issue 5 | 2023-12-07

This document is the property of RISE and may not be reproduced other than in full, except with the prior written approval by RISE.

Sida/Page: 1(1)

Plus de détails sur la Conformité Axis

Protection de l'intégrité des produits et réduction du risque de vulnérabilités dans les logiciels

Pour passer de la sécurité interne à la sécurité des produits, les mesures suivantes forment le socle de sécurité des matériels et logiciels Axis et traduisent le principe de transparence qui nous guide.

Plateforme de cybersécurité Axis Edge Vault

Intégrée aux dispositifs Axis, cette plateforme matérielle contient des fonctionnalités qui préservent leur intégrité. Vous pouvez dès lors démarrer les dispositifs Axis en toute sécurité, les intégrer et protéger leurs données sensibles, notamment les clés cryptographiques, des accès illégitimes.

Pour en savoir plus sur Axis Edge Vault

Modèle de développement de sécurité Axis (ASDM)

Le modèle ASDM est la méthodologie de développement qu'applique Axis pour réduire le risque de commercialiser des produits contenant des vulnérabilités logicielles. Ce modèle veille à inscrire les considérations de sécurité au cœur du développement logiciel. Entre autres, il couvre des domaines comme les analyses de risques, la modélisation des menaces, l'analyse du code, les tests de pénétration, un programme de chasse aux bugs, la recherche de vulnérabilités et leur gestion. Par une détection et une résolution rapides des faiblesses à toutes les phases du développement, le modèle ASDM contribue à atténuer les risques liés à la sécurité pour nos clients.

En savoir plus sur ASDM

AXIS OS

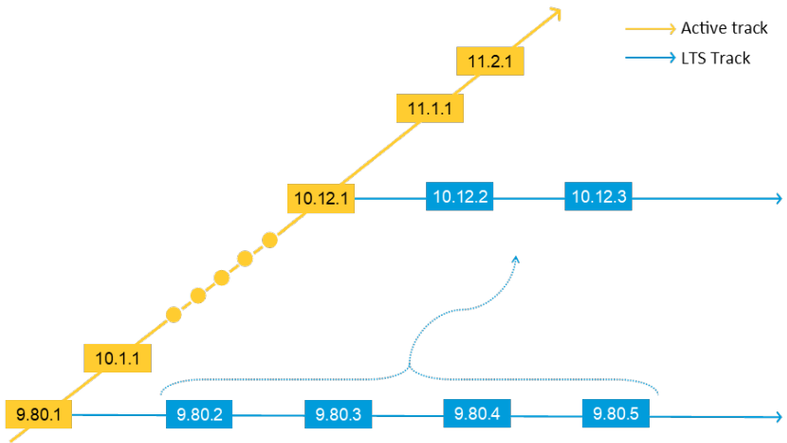
AXIS OS est le système d'exploitation basé sur Linux qui pilote nos dispositifs en périphérie de réseau. Articulé autour de l'open source, de la transparence de la cybersécurité, ce puissant système d'exploitation propose plusieurs voies pour les dispositifs Axis, permettant à Axis de publier rapidement des fonctions de sécurité et des correctifs logiciels sur un grand nombre de produits. Il est conçu pour vous aider à atténuer les risques et à maintenir vos produits et services Axis à jour et protégés. Le site web Axis précise la date de fin du support technique de nombreux produits pour vous permettre d'anticiper le retrait d'exploitation et le remplacement de vos produits en temps utile.

Pour en savoir plus sur AXIS OS

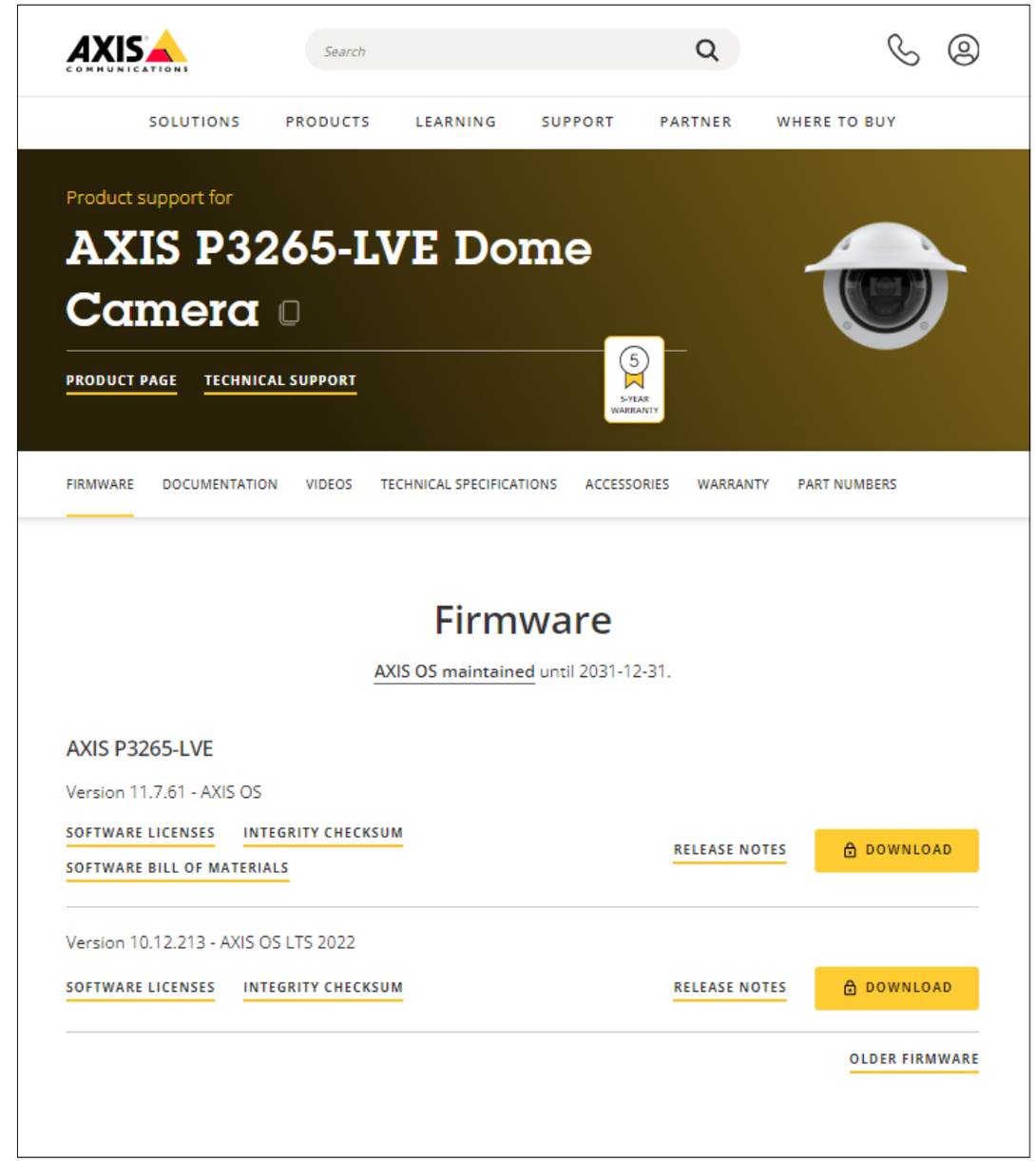
Nomenclature logicielle (SBOM)

De plus, nous publions une nomenclature logicielle (SBOM, Software Bill of Materials) pour AXIS OS précisément axée sur la cybersécurité et favorisant la transparence pour les clients, les chercheurs en sécurité et les autorités. La SBOM fournit une liste détaillée de tous les composants utilisés pour construire le système d'exploitation des dispositifs Axis. Elle donne des renseignements sur les bonnes pratiques de cybersécurité qu'appliquent les fournisseurs et contient de précieuses informations pour les autres acteurs spécialisés dans l'évaluation des vulnérabilités, l'analyse des menaces et les plans de remédiation.

En savoir plus sur la nomenclature logicielle



Voies AXIS OS.



Gestion des nouvelles vulnérabilités

En tant que membre de l'autorité de numérotation des vulnérabilités et expositions communes (CVE, Common Vulnerabilities and Exposures), Axis publie des informations sur les vulnérabilités et en avise toutes les parties prenantes pour que nos clients puissent prendre sans délai les mesures appropriées. Collaborant avec des chercheurs externes, Axis révèle les vulnérabilités et les expositions selon un processus transparent, responsable et coordonné. Axis fournit des correctifs aux dispositifs, logiciels ou services concernés et publie toutes les informations nécessaires sur **le site web Axis** et dans la base de données des vulnérabilités du programme CVE accessible au public. Par ailleurs, nous proposons un service de notifications de sécurité auquel vous pouvez vous inscrire pour recevoir des informations sur les vulnérabilités et d'autres sujets liés à la sécurité. Axis insiste sur l'importance de maintenir le système d'exploitation des produits installés à jour pour s'assurer que les correctifs de sécurité les plus récents sont appliqués.

En savoir plus à propos de la Politique de gestion des vulnérabilités d'Axis

Programme de chasse aux bugs

Dans le cadre de notre stratégie transparente de gestion des vulnérabilités, nous animons un programme de chasse aux bugs. Ce programme est mené en collaboration avec Bugcrowd, leader de la cybersécurité crowdsourcée. Nous sommes résolus à établir des relations professionnelles avec les chercheurs en sécurité externes et les hackers bien intentionnés (« white hats » en anglais). Ce programme prévoit que les chercheurs qui découvrent des vulnérabilités avec les produits basés sur AXIS OS peuvent prétendre à une récompense financière. Axis publiera ensuite ces vulnérabilités détectées avec les autres en toute transparence et fournira des correctifs pour les produits concernés.

PRODUCTION

DISTRIBUTION

Réduction du risque de compromission de composants matériels et logiciels

Sécurité de la chaîne logistique

Comme tous les produits, les dispositifs de sécurité physique doivent fonctionner comme prévu et leur intégrité doit être maintenue. Pour ce faire, les composants matériels et le système d'exploitation du produit doivent être efficacement protégés de toute modification ou manipulation non autorisée pendant son cheminement sur la chaîne logistique.

Contrôles qualité

Avec ses sous-traitants et partenaires fabricants, Axis applique une multitude de contrôles qualité pour protéger l'intégrité de ses produits. Les composants proviennent toujours d'un fournisseur de la liste des fournisseurs agréés, selon le cahier des charges Axis. Le fournisseur ne peut pas modifier les spécifications, les consignes de travail ou les documents d'inspection qualité sans l'accord d'Axis. Tous les changements approuvés doivent être documentés et consignés.

Traçabilité

Un processus de gestion des marchandises veille toujours à leur état et révèle tout écart susceptible de mettre en jeu la qualité. Les sous-traitants et partenaires fabricants doivent appliquer un système de traçage pour garantir la traçabilité des lots produits, depuis les intrants jusqu'aux composants finis. Pendant la production, le composant physique subit une multitude de tests pour vérifier la conformité et détecter tout défaut.

Détection des composants contrefaits

Une inspection optique automatisée permet de vérifier l'absence de composant contrefait. Axis met au point et produit ses moyens de production critiques, ainsi que le système pour tester les composants, modules et produits à différents stades de fabrication. Ce processus réduit le risque de sabotage. Mesure de sécurité supplémentaire : toutes les données de test sont communiquées à Axis 24 h/7 j, de sorte que les modifications non autorisées sont immédiatement identifiées.

En savoir plus sur
Sécurité de la chaîne logistique

Neutralisation des menaces pendant la distribution

Les fonctions de cybersécurité intégrées et les paramètres d'usine par défaut des dispositifs Axis les protègent des altérations logicielles non autorisées pendant le transport. Les fonctionnalités prises en charge par Axis Edge Vault (détaillées page suivante) protègent les informations sensibles dans les dispositifs et vérifient qu'ils exécutent uniquement un système d'exploitation Axis authentique.

La sécurité de la chaîne logistique doit être bien comprise lorsque vous réalisez l'analyse de risque d'un fournisseur pour déterminer s'il a mis en place des mesures d'atténuation des risques pesant sur votre organisation.

Fonctions de cybersécurité intégrées

Les dispositifs Axis sont fournis avec des fonctions de sécurité intégrée vous permettant de les démarrer en toute sécurité et de les intégrer au réseau en sachant que les informations sensibles sont protégées.

Plateforme de cybersécurité Axis Edge Vault

Notre plateforme de cybersécurité matérielle constitue une base solide pour sécuriser et fiabiliser votre dispositif Axis sur votre réseau. Axis Edge Vault comporte plusieurs fonctionnalités* :

> **Magasin de clés sécurisé**, qui fait appel à des modules de calcul cryptographique pour le stockage sécurisé des clés cryptographiques, qui protègent l'identité du dispositif et d'autres informations sensibles contre les accès illégitimes, même en cas de compromission du dispositif. Les modules de calcul cryptographique peuvent être un environnement d'exécution de confiance (TEE) intégré au processeur SoC (System on Chip) Axis. Ils peuvent également prendre la forme d'un élément sécurisé ou d'un module TPM (Trusted Platform Module), qui sont des composants électroniques indépendants sur la carte mère. Les dispositifs Axis accueillent un ou plusieurs de ces trois modules.

> **Firmware signé** et **amorçage sécurisé**, qui s'assurent que le dispositif télécharge et exécute uniquement un système d'exploitation Axis authentique (AXIS OS).

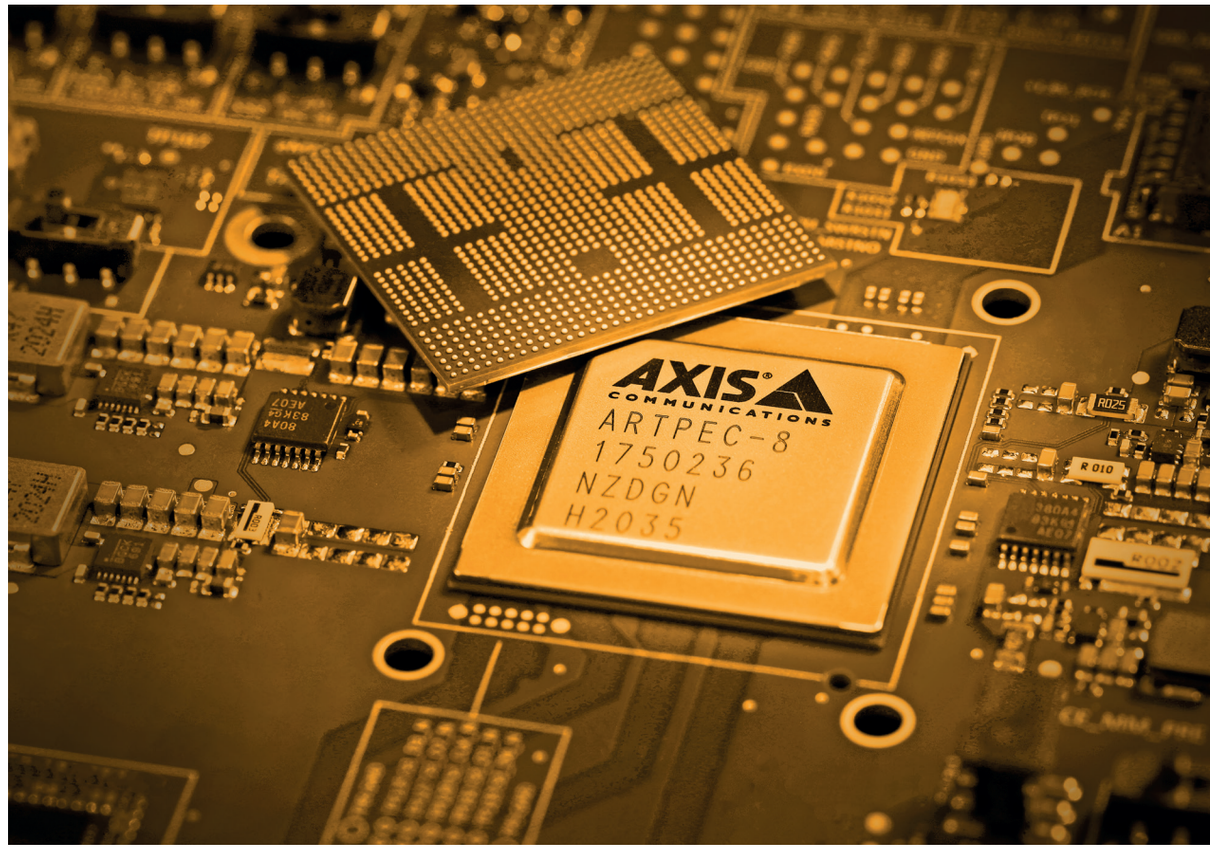
> **ID de dispositif Axis**, conforme à la norme IEEE 802.1AR , pour l'identificationet l'intégration sécurisées du dispositif à un réseau.

> **Système de fichiers chiffré**, qui empêche l'extraction ou l'altération des données dans le système de fichiers lorsque le dispositif est inutilisé, par exemple pendant son transport depuis un intégrateur de système chez le client final.

> **Vidéo signée**, qui permet aux utilisateurs de confirmer l'authenticité de la vidéo capturée et de vérifier qu'elle n'a pas été modifiée.

**Remarque : Certains dispositifs ne prennent pas en charge toutes les fonctionnalités d'Axis Edge Vault. Consultez la fiche technique ou le Sélecteur de produits Axis pour connaître les fonctions prises en charge par le produit.*

Pour en savoir plus Axis Edge Vault



Paramètres par défaut

Au-delà de leurs fonctions de sécurité, les dispositifs Axis sont livrés avec des paramètres de protection par défaut prédéfinis.

Identifiants et protocoles réseau

Le dispositif Axis n'est pas opérationnel avant la définition d'un compte avec nom d'utilisateur et mot de passe. Une fois le compte créé, l'accès aux fonctions d'administration et/ou au flux vidéo est accordé uniquement en utilisant ces identifiants.

Par ailleurs, seul le minimum de protocoles et de services réseau sont activés par défaut dans les dispositifs Axis, notamment HTTP et HTTPS pour accéder à l'interface des dispositifs, RTSP et RTP pour transmettre les flux audio et vidéo, ainsi que certains protocoles comme UPnP et Bonjour pour que les applications tierces puissent détecter les dispositifs Axis.

Adaptation aux réseaux Zero-Trust des clients

Axis a répondu aux exigences du Zero-Trust en proposant des produits affectés d'ID de dispositif Axis uniques et compatibles avec le protocole HTTPS et la norme IEEE 802.1X, ainsi que IEEE 802.1AR pour l'authentification des dispositifs et IEEE 802.1AE MACsec pour le chiffrement automatique des données.

Le protocole HTTPS est activé par défaut pour protéger la sécurité des mots de passe des dispositifs. Il permet également aux logiciels de gestion vidéo utilisant HTTPS de vérifier le certificat SSL signé par une AC de confiance, qui est pris en charge par l'ID de dispositif Axis dans les produits récents.

La prise en charge des normes IEEE 802.1X, IEEE 802.1AR et IEEE 802.1AE, activée par défaut dans les produits Axis, permet l'enregistrement automatique des dispositifs sur le réseau, leur authentification et le chiffrement de bout en bout. Les informaticiens disposent ainsi de mécanismes standard pour intégrer les dispositifs Axis de manière efficace et sûre dans un réseau d'entreprise compatible IEEE 802.1X. Les clients qui utilisent des dispositifs Axis sur un réseau Aruba peuvent télécharger le guide d'intégration, qui explique les bonnes pratiques de configuration pour l'intégration et la gestion sécurisées des dispositifs Axis.

Plus de détails sur les solutions Axis pour l'informatique d'entreprise

MISE EN ŒUVRE

Cybersécurité en phase de mise en œuvre

Un dispositif Axis est un terminal réseau comme tout autre appareil connecté (ordinateur portable, poste fixe ou téléphone). Mais contrairement à un ordinateur portable, les dispositifs Axis n'ont pas d'utilisateurs qui visitent des sites web dangereux, ouvrent des pièces jointes malveillantes ou installent des applications non approuvées. Cependant, un produit vidéo, audio ou de contrôle d'accès en réseau possède une interface susceptible de faire courir un risque au système auquel il est connecté.

Des guides de renforcement de la protection, disponibles pour les produits Axis, fournissent des recommandations pour limiter leur exposition au cyber-risque. Nous allons rappeler ici quelques recommandations de base. Par exemple, nous vous conseillons d'effectuer une remise en paramètres d'usine du dispositif avant de le configurer pour le débarrasser d'éventuels logiciels ou configurations indésirables.

De même, vérifiez qu'il exécute la dernière version d'AXIS OS, qui contient les correctifs de sécurité et améliorations les plus récents pour le dispositif concerné.

Imposez des mots de passe renforcés, limitez l'accès direct à l'interface web du dispositif, configurez-le pour qu'il utilise uniquement HTTPS (qui chiffre le trafic de données entre client et dispositif) et désactivez les services et fonctions inutilisés pour limiter les risques inutiles. Il est également essentiel de régler correctement la date et l'heure du dispositif pour garantir la précision des journaux système et s'assurer que les certificats numériques, sur lesquels reposent des services comme HTTPS et IEEE 802.1X, peuvent être validés et utilisés.

Pour la configuration et la gestion locales des dispositifs Axis, AXIS Device Manager est un outil efficace. Il permet de traiter de manière globale les tâches d'installation et de sécurité, comme la gestion des identifiants des dispositifs, le déploiement des certificats numériques, la désactivation des services inutilisés et la mise à niveau d'AXIS OS. Pour en savoir plus sur les logiciels de gestion des dispositifs, voyez la page suivante.

Pour des recommandations complètes et exhaustives sur le renforcement de la protection des dispositifs exécutants AXIS OS, lisez le Guide de protection d'AXIS OS. Pour accéder aux guides de protection Axis pour les logiciels de gestion vidéo et les commutateurs, visitez la page des ressources en cybersécurité. Et pour en savoir plus sur l'intégration transparente des dispositifs Axis dans l'infrastructure informatique et les réseaux d'entreprise, consultez les solutions Axis pour l'informatique d'entreprise.

Axis propose des outils, de la documentation et des formations pour vous aider à atténuer les risques et à maintenir vos produits et services Axis à jour et protégés. **Accédez à nos ressources en cybersécurité.**

EN SERVICE

Cybersécurité des dispositifs en service

Tant qu'un dispositif est en exploitation, un des moyens essentiels de préserver sa cybersécurité consiste à maintenir à jour son firmware ou son système d'exploitation AXIS OS. Ainsi, le dispositif comporte toujours les correctifs de sécurité et améliorations logicielles les plus récents. Les fonctions de signature du firmware et d'amorçage sécurisé des dispositifs Axis contrôlent que seul un système d'exploitation AXIS OS authentique peut être installé et utilisé. Fournies gratuitement, les versions AXIS OS s'appliquent soit à la voie active, soit à la voie LTS (Long-Term Support). Les versions d'AXIS OS de la voie active comporte de nouvelles fonctionnalités, tandis que celles de la voie LTS en sont dépourvues pour minimiser le risque d'incompatibilités. Cependant, les deux options incluent les correctifs de sécurité et les améliorations logicielles. Pour rester informé des nouvelles vulnérabilités détectées, vous pouvez vous inscrire au service de notifications de sécurité Axis. Les vulnérabilités publiées contiennent des instructions sur la correction des produits concernés avec de nouvelles mises à jour.

Pour simplifier la mise à jour du système d'exploitation d'une grande quantité de dispositifs, Axis propose deux logiciels de gestion des dispositifs : AXIS Device Manager et AXIS Device Manager Extend.

Principe des logiciels de gestion des dispositifs

Un logiciel de gestion des dispositifs peut rapidement constituer un inventaire complet en temps réel de la totalité des caméras, encodeurs et dispositifs de contrôle d'accès, audio et autres connectés au réseau. Il analyse l'ensemble du réseau et, lorsqu'un dispositif nouveau ou mis à jour est détecté, il en capture toutes les informations clés, y compris numéro de modèle, adresses IP et MAC, version du logiciel du dispositif et statut des certificats.

Tour d'horizon complet

Un panorama très détaillé de tous les écosystèmes réseau permet d'appliquer plus facilement des pratiques et politiques de gestion du cycle de vie sur tous les dispositifs et de gérer en toute sécurité les tâches majeures d'installation, déploiement, configuration, sécurité et maintenance.

Les politiques et bonnes pratiques de cybersécurité dans la gestion des dispositifs doivent aborder plusieurs domaines : complexité des mots de passe et fréquence de leur changement, services inutilisés à désactiver pour réduire la surface d'attaque, fréquence d'analyse des vulnérabilités des dispositifs, procédures en place pour évaluer le niveau de risque lorsqu'un fabricant publie des exploits connus, etc.

Gains de temps et de ressources

Un logiciel de gestion des dispositifs aide les entreprises à gagner du temps en simplifiant la gestion des risques de cybersécurité.

Il peut avoir plusieurs utilités :

> Déployer des changements au système, des mises à jour logicielles et des nouveaux certificats numériques à tous les dispositifs concernés en même temps

> Créer ou reconfigurer facilement les paramètres de sécurité et les déployer sur l'ensemble de votre réseau pour que tous les dispositifs respectent les pratiques et politiques de sécurité les plus récentes

> Vérifier que tous les dispositifs exécutent la version logicielle la plus récente et la plus sûre

> Gérer les niveaux de privilèges utilisateur sur l'ensemble du réseau et configurer les changements.

Informations en temps réel

Les outils de gestion des dispositifs offrent aux entreprises des éclairages en temps réel sur l'état de leur écosystème. Par exemple, vous pouvez voir les dispositifs à actualiser avec les mises à jour logicielles et les certificats les plus récents, mais aussi connaître les dates de fin de production et de fin de prise en charge pour pouvoir anticiper le remplacement des dispositifs.

Outils Axis de gestion des dispositifs

Nos logiciels de gestion des dispositifs AXIS Device Manager et AXIS Device Manager Extend vous aident à gérer vos dispositifs Axis avec efficacité. AXIS Device Manager et AXIS Device Manager Extend se complètent mutuellement.

AXIS Device Manager

AXIS Device Manager facilite et accélère l'installation et la configuration de nouveaux dispositifs. Cet outil résidant sur site assiste toutes les grandes tâches d'installation, de sécurité et d'exploitation, notamment l'installation de mises à niveau logicielles et d'applications. Il vous permet de configurer les dispositifs Axis avec des paramètres de sauvegarde et de restauration, et vous pouvez consulter la situation de leur garantie. Il est également possible d'appliquer des contrôles de cybersécurité tels que les certificats HTTPS et IEEE 802.1X.

En savoir plus sur AXIS Device Manager

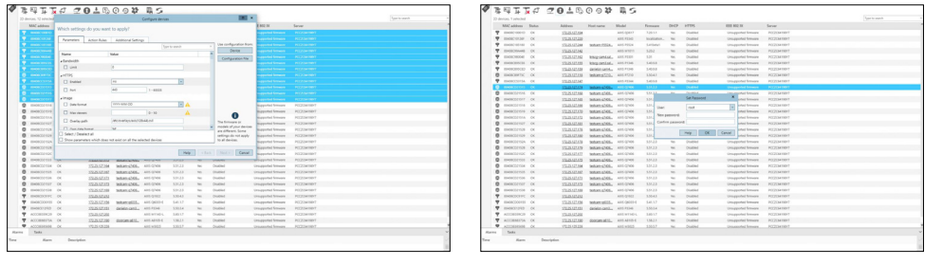
AXIS Device Manager Extend

Idéal pour les opérations multisite, AXIS Device Manager Extend vous aide à gérer vos ressources à distance sur l'ensemble de vos sites. Cette application simple d'utilisation facilite le déploiement de tâches de maintenance cruciales, comme la mise à niveau d'AXIS OS, la définition, l'application et le contrôle des politiques de sécurité ou la gestion des applications. Proposant un tableau de bord en temps réel, cet outil accélère la recherche de panne en donnant un état des lieux des problèmes potentiels du système, par exemple les dispositifs déconnectés ou dont la garantie a expiré. De plus, il présente des conseils de paramétrage des dispositifs afin de minimiser les menaces de sécurité et de neutraliser les vulnérabilités. Il permet également de définir et d'appliquer simultanément des politiques de sécurité à tous les dispositifs Axis.

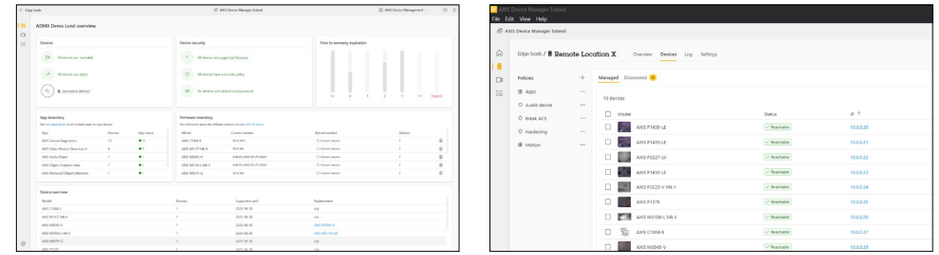
En savoir plus sur AXIS Device Manager Extend

En cas de compromission de sécurité

Si votre réseau est victime d'une intrusion, Axis a rédigé le Guide forensique AXIS OS pour vous aider à mener une analyse forensique de vos dispositifs Axis en réseau.



Captures d'écran de l'interface d'AXIS Device Manager.



Captures d'écran de l'interface d'AXIS Device Manager Extend.

RETRAITS D'EXPLOITATION

Planification des retraits d'exploitation

Les mises à jour et les correctifs représentent le meilleur moyen de préserver la cybersécurité d'un produit, mais ils ne sont pas toujours disponibles lorsqu'un produit est trop ancien et cesse d'être pris en charge. En matière de cybersécurité, les produits obsolètes non corrigés posent un risque majeur. Un dispositif négligé peut facilement devenir une proie facile pour les attaquants.

Il est donc essentiel d'anticiper le retrait d'exploitation des produits pour éliminer le risque d'utiliser des dispositifs dont la prise en charge est abandonnée et qui sont exposés à de possibles vulnérabilités non corrigées. Axis indique la date de fin de prise en charge du système d'exploitation de ses produits pour vous aider à anticiper leur retrait d'exploitation et les remplacer en temps opportun. De plus, AXIS Device Manager Extend contient des informations sur la garantie, la fin de production et la fin de prise en charge de tous les dispositifs du système.

L'élimination des données résidant dans un produit retiré d'exploitation est également importante. En effectuant une remise en paramètres d'usine, vous pouvez rapidement effacer toutes les configurations et données du dispositif. Visitez le portail AXIS OS pour des détails sur le retrait d'exploitation des produits.

Conformité

Les États adoptent toujours plus de réglementations et de lois liées à la cybersécurité, que doivent respecter toutes les entreprises exerçant sur leur sol. De même, certains secteurs d'activité et organisations imposent de respecter certaines normes, notamment par la certification de produits et services. Il incombe à tous les acteurs de vérifier qu'ils respectent les lois et réglementations, et qu'ils mettent en œuvre les directives et spécifications relevant de leur activité.

Conformité en matière de cybersécurité

La conformité relevant de la cybersécurité revient à respecter les normes et contraintes réglementaires définies par les pouvoirs publics. Néanmoins, même si les normes et les certifications ont incontestablement un intérêt, elles ne forment qu'un aspect de la cybersécurité.

Le respect de ces exigences risque toujours de se transformer en exercice consistant à cocher des cases. C'est pourquoi les entreprises doivent considérer les normes et les certifications comme un cadre de référence, c'est-à-dire des exigences minimales plutôt que des objectifs. Le véritable enjeu pour les fournisseurs consiste à fournir à leurs clients des produits et services exploitables de la manière la plus sûre possible. Sans oublier des guides et une communication transparente en soutien aux pratiques continues de cybersécurité.

La conformité en matière de cybersécurité évolue en permanence, et ce qui était considéré comme un plus auparavant devient vite une nécessité.

Réglementations

Les règlements de cybersécurité visent à imposer aux entreprises de protéger leurs systèmes et leurs informations, mais aussi d'assurer un niveau minimal de sécurité aux produits et services qu'elles fournissent. Passons en revue quelques réglementations importantes et leurs modalités d'application.

En 2023, la Directive SRI2 est entrée en vigueur et les États membres de l'Union européenne ont jusqu'en octobre 2024 pour transposer ces mesures dans leur législation nationale. Cette directive impose à toutes les entreprises de l'UE opérant dans des secteurs essentiels d'appliquer un niveau élevé de cybersécurité commun. Les entreprises peuvent être pénalisées si leur cybersécurité est défaillante, même si elle est due à une négligence de l'un de leurs fournisseurs.

Par suite, l'évaluation des fournisseurs et la sécurité de la chaîne logistique prendront encore plus d'importance. Par ricochet, la directive va imposer des obligations sur les fabricants, les importateurs et les distributeurs, qui auront un devoir d'attention pendant tout le cycle de vie de leurs produits.

En décembre 2023, l'UE est parvenue à un accord provisoire sur un nouveau règlement sur la cyber-résilience, qui définit des normes de sécurité communes pour les produits matériels et logiciels comportant des éléments numériques. Ce règlement concerne les produits connectés directement ou indirectement à un autre dispositif ou réseau, comme les dispositifs IoT. La proposition de règlement a pour ambition de réduire le nombre d'incidents de cybersécurité, tout en renforçant la protection des données et la transparence. Le Royaume-Uni a voté une loi comparable dénommée UK Product Security and Telecommunications Infrastructure, qui entre en vigueur en avril 2024.

Les entreprises qui traitent avec le gouvernement des États-Unis devront également respecter des normes comme le programme CMMC (Cybersecurity Maturity Model Certification), qui impose un audit de certification de la gestion interne des procédures de cybersécurité.

Une cybersécurité efficace exige une vigilance et un entretien de tous les instants.

Normes et certifications

La plupart des normes et des certifications portent sur les fonctions, les contre-mesures et les processus qui prouvent que l'aspect sécurité est intégré aux produits. Elles peuvent être complétées par des essais menés par des organismes indépendants, par exemple des tests de pénétration et des programmes de chasse aux bugs, pour découvrir des vulnérabilités logicielles.

La certification des produits apporte une certaine sérénité aux clients et aux pouvoirs publics, mais ne doit pas occulter le fait qu'une certification reste pertinente pendant un an en général, après quoi elle doit être renouvelée. En raison du développement continu de nouvelles technologies et fonctionnalités, les certifications peuvent vite devenir obsolètes.

Notez que même si les normes peuvent contribuer à élever la posture de cybersécurité, elles ne garantissent pas l'absence d'incident. C'est pourquoi les entreprises doivent en permanence réévaluer les menaces et leurs politiques de sécurité.

Pourquoi Axis ?

À la pointe de la cybersécurité

La cybersécurité est un élément central pour Axis. Elle guide notre système interne de sécurité des informations, la gestion de notre chaîne logistique, le développement de nos produits et services et la gestion des vulnérabilités de nos logiciels. Nous considérons la sécurité comme une responsabilité partagée au long cours, où la transparence est déterminante. Nous tenons à ce que vous puissiez utiliser nos produits et services de la manière la plus sûre possible. C'est pourquoi nos produits sont conçus et fabriqués avec des fonctions de cybersécurité intégrées et des paramètres par défaut conservatoires. Nous fournissons aussi des guides de renforcement de la protection. Nous assurons une veille continue sur les menaces et recherchons constamment des moyens d'améliorer la sécurité. En tant qu'autorité de numérotation CVE, nous réagissons aux nouvelles vulnérabilités détectées en publiant des correctifs pour que vous puissiez prendre les mesures nécessaires à temps. Nous proposons des mises à niveau logicielles pour vous permettre de poursuivre le renforcement de la sécurité des dispositifs Axis après l'installation.

Enfin, des outils comme AXIS Device Manager et AXIS Device Manager Extend facilitent la gestion de vos dispositifs Axis pour réduire le cyber-risque tout au long de leur cycle de vie.

Autres raisons d'opter pour Axis

> **Une qualité omniprésente :**

Tous nos produits sont soumis à des essais approfondis, gage de sérénité pour nos clients.

> **Technologies innovantes :**

Nous associons les technologies et l'imagination humaine pour renforcer les performances et la simplicité d'utilisation. Basées sur des standards ouverts, nos technologies sont flexibles, évolutives et faciles à intégrer.

> **Développement durable à tous les niveaux :**

Axis est résolument engagé envers un développement écoresponsable avec l'utilisation de matériaux durables. Environ 90 % des caméras et encodeurs Axis sortis en 2022 ne contenaient pas de PVC.

> **Présence mondiale, expertise locale :**

Axis dispose de la plus grande base installée au monde de produits vidéo sur IP et emploie des collaborateurs dans plus de 50 pays. Nous partageons nos perspectives et nos expériences, en restant informés des dernières nouveautés.

> **Le pouvoir des partenariats :**

Notre modèle de partenariat fait d'Axis la marque de caméras la plus intégrée du marché.

À propos d'Axis Communications

En créant des solutions qui renforcent la sécurité et améliorent la performance des entreprises, Axis contribue à un monde plus intelligent et plus sûr. Leader de son secteur dans les technologies sur IP, Axis propose des solutions en vidéosurveillance, contrôle d'accès, visiophonie et systèmes audio. Ces solutions sont enrichies par des applications d'analyse intelligente et soutenues par des formations de haute qualité.

L'entreprise emploie environ 4000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et intégrateurs de systèmes du monde entier pour fournir des solutions sur mesure à ses clients. Axis a été fondée en 1984, son siège est situé à Lund en Suède.