Comprendre la directive NIS 2

AXIS COMMUNICATIONS

CONTENU DU MANUEL

1

Qu'est-ce que la directive NIS 2 ?

La directive NIS, également connue sous le nom de Directive (UE) 2016/1148, est une directive de l'Union européenne qui établit des exigences en matière de cybersécurité pour les opérateurs de services essentiels et les prestataires de services numériques dans l'Union européenne. La directive NIS vise à garantir un niveau élevé de sécurité des réseaux et des systèmes d'information dans l'ensemble de l'Union européenne, ainsi qu'à s'assurer que les opérateurs de services essentiels et les prestataires de services numériques prennent les mesures appropriées pour gérer les risques pesant sur leurs réseaux et systèmes d'information.

Le 10 novembre 2022, le Parlement européen a adopté la directive NIS 2. Elle remplace et abroge la directive NIS. La directive NIS 2 améliorera la gestion des risques de cybersécurité et introduira des obligations de déclaration dans des secteurs tels que l'énergie, les transports, la santé et l'infrastructure numérique. Les États membres disposeront de 21 mois à partir de l'entrée en vigueur de la directive pour incorporer les dispositions dans leur législation nationale.

La directive NIS 2 a trois objectifs généraux :

Cyberrésilience

Renforcer la cyberrésilience d'un large éventail d'entreprises basées dans l'Union européenne, opérant dans tous les secteurs pertinents et exerçant des activités essentielles.

Une approche unifiée

Réduire les incohérences en matière de résilience du marché intérieur dans les industries actuellement couvertes par la directive NIS. Directive visant à unifier les capacités de cybersécurité.

Définir des procédures

Renforcer la sensibilisation commune à la situation et la capacité collective de planifier et de réagir en renforçant le partage d'informations et en établissant des normes et des procédures en cas d'incident ou de crise à grande échelle.

La directive met l'accent sur :

> L'adoption de mesures techniques et organisationnelles visant à renforcer la sécurité de leurs réseaux et systèmes informatiques.

> L'adoption de mesures appropriées visant à prévenir les incidents de sécurité et/ou à minimiser leur impact afin d'assurer la continuité du service.

> La communication à l'autorité compétente, sans délai injustifié, de tout incident de service ayant un impact significatif sur la continuité du service.

2

Quelles sont les nouveautés ?

La nouvelle proposition élimine la distinction entre OSE (opérateurs de services essentiels) et FSN (fournisseurs de services numériques), et précise que les entités sont soit essentielles, soit importantes. Il convient également de noter qu'en vertu de l'ancienne directive NIS, il incombait aux États membres de déterminer quelles entités remplissaient les critères pour être qualifiées d'opérateurs de services essentiels. La nouvelle directive NIS 2 introduit une règle de limite de taille en tant que règle générale pour l'identification des entités réglementées. Cela signifie que toutes les moyennes et grandes entités opérant dans les secteurs ou fournissant des services couverts par la directive entreront dans son champ d'application.

Modifications Supplémentaires

1. Le champ d'application de la directive NIS 2 est élargi afin de couvrir de nouveaux secteurs (par exemple, la gestion des eaux usées, l'alimentation, l'espace, etc.) en fonction de leur caractère critique pour l'économie et la société, y compris, à cette fin, toutes les moyennes et grandes entreprises de ces secteurs. Parallèlement, les États membres bénéficient d'une flexibilité garantie pour identifier les entités de taille plus réduite présentant un profil à haut risque.

2. La création, par l'Agence de l'Union européenne pour la cybersécurité (ENISA), d'un réseau européen de liaison en cas de crise cybernétique (EU-CyCLONe) dans le but de soutenir la gestion coordonnée de la cybersécurité lors d'incidents et de crises à grande échelle au niveau de l'Union européenne.

3. Une meilleure coordination est mise en place pour la divulgation des nouvelles vulnérabilités découvertes dans l'ensemble de l'Union.

4. Une liste de sanctions administratives (similaire à celles du RGPD) est établie, comprenant des amendes en cas de violation des obligations de déclaration et de gestion des risques de cybersécurité.

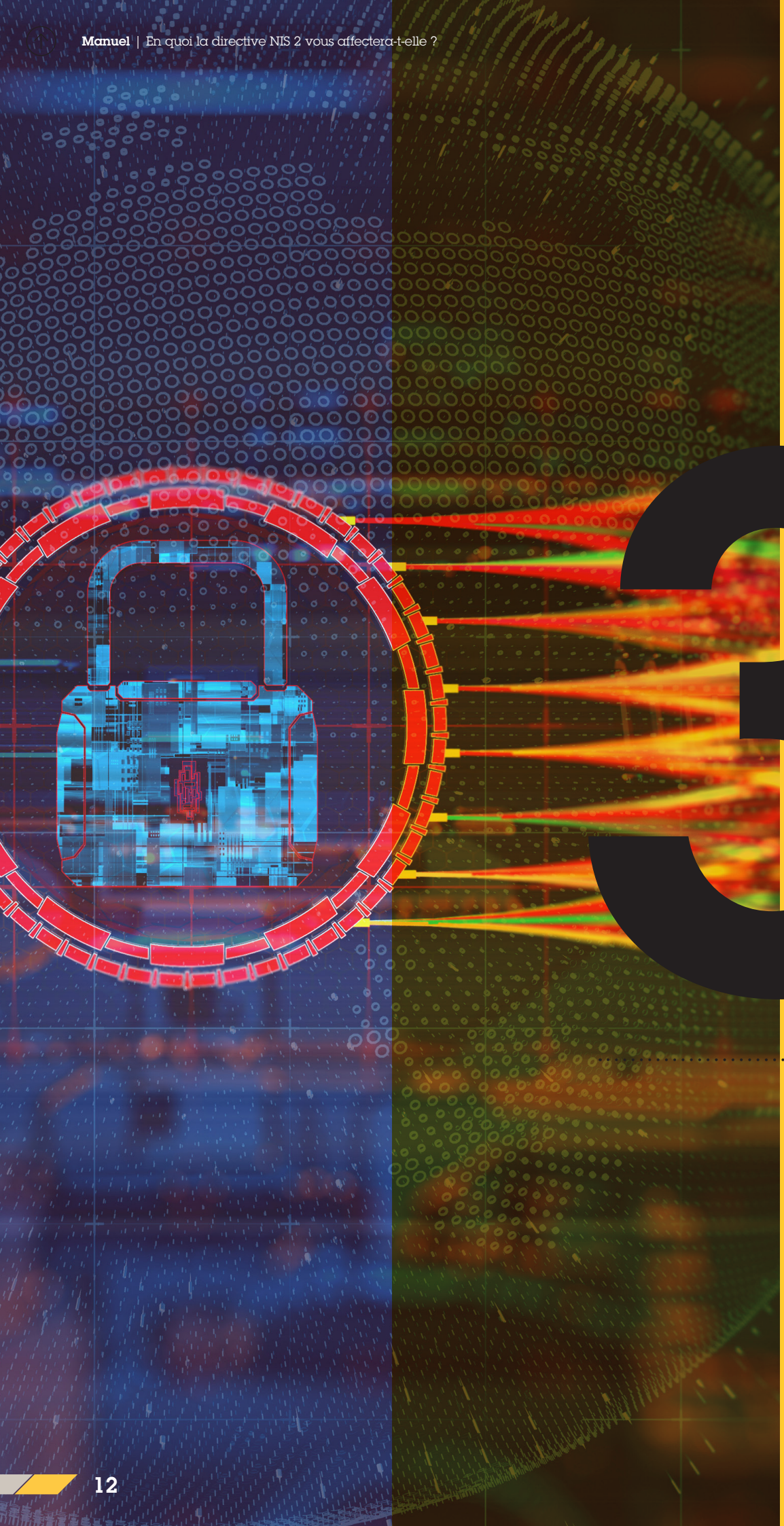
5. La directive comprend sept éléments que toutes les entreprises doivent prendre en compte ou mettre en œuvre pour renforcer leurs exigences en matière de sécurité :

- Analyse des risques et politiques de sécurité des systèmes d'information
- Gestion des incidents (prévention, détection et réponse aux incidents)
- Continuité des activités commerciales et gestion des crises
- Sécurité de la chaîne d'approvisionnement
- Sécurité des réseaux et des systèmes d'information
- Politiques et procédures relatives aux mesures de gestion des risques liés à la cybersécurité
- Utilisation de la cryptographie et du cryptage

6. La directive introduit des mesures de surveillance plus strictes pour les autorités nationales, des exigences de mise en œuvre plus strictes et vise à harmoniser les régimes de sanctions entre les États membres.

7. Au niveau européen, la directive renforce la cybersécurité des principales technologies de l'information et de la communication. Les États membres, en coopération avec la Commission et l'ENISA, devront réaliser des évaluations coordonnées des risques liés aux chaînes d'approvisionnement critiques, s'appuyant sur l'approche efficace adoptée dans le cadre de la Recommandation de la Commission sur la cybersécurité des réseaux 5 G.

8. La nouvelle directive a été alignée sur la législation sectorielle spécifique à chaque secteur, notamment le Règlement sur la résilience opérationnelle numérique (Digital Operational Resilience Act-DORA), applicable au secteur financier, et la Directive sur la résilience des entités critiques (Critical Entities Resilience Directive-CER), renforçant la résilience des entités critiques qui fournissent des services vitaux dont dépendent les moyens de subsistance des citoyens de l'UE, tels que l'énergie, les transports, la santé et l'eau potable. Cela garantira une clarté juridique et assurera la cohérence entre la directive NIS 2 et ces règlements.



3

En quoi la directive NIS 2 vous affectera-t-elle ?

La directive NIS exige que les entités essentielles ou importantes sécurisent leurs actifs critiques afin de minimiser les risques qu'un incident de sécurité présente pour la prestation de leurs services. En théorie, chaque organization sait ce qui est important pour fournir ses services et gérer ses activités. On pourrait faire valoir que les technologies, telles que les caméras de surveillance en réseau, ne sont pas considérées comme des actifs critiques. Cependant, il est important d'adopter une approche holistique lors de la définition du champ d'application. Certains systèmes peuvent présenter un risque même s'ils sont exclus du champ d'application. Par exemple, même si une caméra n'est pas essentielle au service, elle peut présenter des vulnérabilités qui permettraient à un pirate de lancer une attaque contre des actifs critiques. Il est donc necessaire que les entités essentielles ou importantes évaluent ces risques lors de l'évaluation de la directive NIS.

Soutenir la conformité

Avec une plus grande attention portée à la sécurité de la chaîne d'approvisionnement, il est prévu que les organisations soumises à la conformité de la directive NIS 2 devront effectuer un niveau accru de diligence raisonnable à l'égard de leurs partenaires technologiques. Dans le cadre de ce processus d'évaluation et d'une évaluation des risques liés aux fournisseurs, il est prévu que le rôle des politiques et des processus devienne plus important.

Démontrer une maturité en matière de cybersécurité

Sécuriser un réseau, ses appareils et les services qu'il prend en charge exige une participation active de l'ensemble de la chaîne d'approvisionnement des fournisseurs, ainsi que de l'organisation de l'utilisateur final. Axis fournit des outils, de la documentation et des formations pour aider à atténuer les risques et garantir que les produits et services d'Axis sont à jour et protégés. Axis dispose d'une liste exhaustive de politiques et de processus en place, ainsi que de certifications tierces.

Il s'agit des certifications suivantes :

- Certification ISO/IEC 27001 pour notre système de gestion de la sécurité de l'information (ISMS)
- Cyber Essentials Plus
- Modèle de maturité pour la sécurité intégrée dans le développement logiciel (BSIMM)
- Le modèle de développement de sécurité Axis (ASDM) est un cadre qui définit le processus et les outils utilisés par Axis pour construire des logiciels intégrant la sécurité à toutes les étapes, de la conception à la mise hors service
- Axis est une autorité de numérotation CVE (CNA) relevant du domaine MITRE
- Politique de gestion de la vulnérabilité
- Notifications d'avis de sécurité

Intégrité des produits de la chaîne d'approvisionnement

L'intégrité du produit peut être garantie lorsque le hardware et le firmware sont protégés avec succès contre toute modification ou manipulation non autorisée tout au long du parcours du produit le long de la chaîne d'approvisionnement. En collaboration avec ses fournisseurs et ses partenaires de fabrication, Axis applique une multitude de contrôles qualité pour maintenir et protéger l'intégrité de ses produits. Par exemple:

- Le système de gestion de la sécurité de l'information (ISMS) d'Axis est certifié ISO 27001, ce qui signifie qu'il suit des processus et des bonnes pratiques reconnus internationalement pour gérer l'infrastructure d'information interne et les systèmes qui soutiennent le parcours du produit le long de la chaîne d'approvisionnement.
- Axis applique le concept de « confiance zéro » qui repose sur le principe de ne jamais faire confiance et de toujours vérifier, que ce soit pour les humains ou les machines, lors de la connexion aux réseaux et architectures, ainsi qu'à l'intérieur de ceux-ci.
- Les composants sont toujours obtenus auprès d'un fournisseur figurant sur la liste des fournisseurs approuvés, conformément à la nomenclature des matériaux spécifiée par Axis.
- Le fournisseur n'est pas autorisé à modifier les spécifications de production critiques sans l'accord préalable d'Axis. Toute modification approuvée doit être documentée et enregistrée.
- Un processus de manipulation des matériaux garantit toujours le suivi des matériaux, révélant ainsi toute déviation qui pourrait compromettre la qualité.
- Les fournisseurs et partenaires de fabrication sont tenus de maintenir un système garantissant la traçabilité des lots produits, depuis les matériaux entrants jusqu'à la pièce finie. Pendant la production, la pièce subira plusieurs tests, tels que le contrôle de qualité à la réception (CQR) et l'inspection optique automatique (AOI), qui permettent de vérifier qu'aucun composant contrefait n'est installé.
- Les équipements de production critiques et le système de test sous-jacent sont développés, produits et fournis par Axis, tout comme le système de test des composants, des modules et des produits aux différents niveaux de la production. Cela limite les risques liés aux manipulations indésirables. Axis fournit une liste de fonctionnalités de sécurité renforcée intégrées.
- ARTPEC® est un système sur puce (SoC) développé en interne par Axis, qui est conforme à la loi d'autorisation de la défense nationale (NDAA). ARTPEC dispose de fonctionnalités de sécurité intégrées exclusivement conçues pour les appareils Axis. Ces fonctionnalités comprennent le firmware signé, garantissant que seul un firmware sécurisé et autorisé peut être installé, ainsi que le démarrage sécurisé, qui empêche le démarrage d'un firmware non autorisé.
- Pour renforcer davantage les contrôles de sécurité, toutes les données de test sont partagées avec Axis 24h/24 et 7j/7 par nos partenaires de production, de sorte que les modifications non autorisées puissent être identifiées immédiatement.

4

Quelles fonctionnalités de nos produits peuvent contribuer à atténuer les menaces et à protéger contre des attaques ?

Cette section décrit certaines des fonctionnalités de sécurité avancées disponibles dans les produits Axis.

Firmware signé

Le firmware signé est mis en œuvre par le fournisseur de logiciels et implique la signature de l'image du firmware avec une clé privée. Lorsque le firmware est doté de cette signature, un appareil vérifiera l'intégrité du firmware avant d'accepter son installation.
Si l'appareil détecte que l'intégrité du firmware est compromise, la mise à jour du firmware sera rejetée.

Démarrage sécurisé

Le démarrage sécurisé est un processus de démarrage qui consiste en une chaîne ininterrompue de logiciels validés de façon cryptographique, commençant dans une mémoire immuable (ROM de démarrage). Basé sur l'utilisation de firmware signé, le démarrage sécurisé garantit qu'un appareil ne peut démarrer qu'avec un firmware autorisé.

Axis Edge Vault

Axis Edge Vault est un module de calcul cryptographique sécurisé qui peut être utilisé pour des opérations cryptographiques sur des certificats stockés de manière sécurisée. Edge Vault offre un stockage protégé contre les manipulations, permettant à chaque appareil de protéger ses secrets. Il établit une base pour la mise en œuvre sûre de fonctionnalités de sécurité plus avancées.

Identifiant de périphérique Axis (ADM)

L'identifiant de périphérique Axis fonctionne comme un passeport numérique et est unique pour chaque unité de périphérique. Il est stocké de manière sécurisée et permanente dans Edge Vault sous forme de certificat, signé par le certificat racine Axis.
L'identifiant de périphérique Axis est conçu pour prouver l'origine du périphérique, permettant ainsi un nouveau niveau de confiance dans le périphérique tout au long du cycle de vie du produit.

Stockage sécurisé des clés avec un module de plateforme sécurisée (TPM)

Un module de plateforme sécurisée (TPM) est un composant qui offre un ensemble de fonctionnalités cryptographiques adaptées à la protection des informations contre l'accès non autorisé. La clé privée est stockée dans le TPM et ne quitte jamais le TPM. Toutes les opérations cryptographiques nécessitant l'utilisation de la clé privée sont envoyées au TPM pour être traitées. Cela garantit que la partie secrète du certificat ne quitte jamais l'environnement sécurisé du TPM et reste en sécurité même en cas de violation de sécurité.

Vidéo signée

La vidéo signée garantit que les preuves vidéo peuvent être vérifiées comme n'ayant pas été altérées sans avoir à prouver la chaîne de possession du fichier vidéo. Chaque caméra utilise son identifiant de périphérique Axis unique, stocké de manière sécurisée dans Axis Edge Vault, pour ajouter une signature dans le flux vidéo. Lorsque la vidéo est lue, le lecteur de fichiers indique si la vidéo est intacte. La vidéo signée permet de retracer la vidéo jusqu'à la caméra d'origine et de vérifier que la vidéo n'a pas été modifiée ou éditée, et qu'elle est toujours dans sa forme originale sans altération.

HTTPS activé

HTTPS est activé par défaut avec un certificat auto-signé depuis AXIS OS 7.20. Cela permet de définir le mot de passe de l'appareil de manière sécurisée.
Dans AXIS OS 10.10 et versions ultérieures, le certificat auto-signé a été remplacé par le certificat de l'identifiant sécurisé du dispositif conforme à la norme IEEE 802.1AR.

Les outils et guides Axis destinés à faciliter l'installation, la mise en service et la maintenance sont énumérés ci-dessous :

Guide de renforcement de la sécurité

Dans le but de structurer nos recommandations dans le contexte d'un cadre de cybersécurité, Axis a choisi de suivre les méthodes décrites dans la version 8 des contrôles du CSI, lancées par le Centre pour la sécurité internet (CSI). Auparavant connus sous le nom de 20 contrôles de sécurité essentiels de SANS (SANS Top 20 Critical Security Controls), les contrôles du CSI fournissent 18 catégories de contrôles de sécurité critiques (CSC) axés sur la gestion des catégories de risques de cybersécurité les plus courantes auxquelles une organisation est confrontée. Ces informations se trouvent dans le Guide de renforcement de la sécurité d'Axis.

AXIS Device Manager (Gestionnaire de périphériques AXIS)

AXIS Device Manager est l'outil de référence pour une installation et une configuration rapides et faciles des nouveaux appareils. Il offre aux installateurs de sécurité et aux administrateurs système un outil hautement efficace pour gérer toutes les principales tâches d'installation, de sécurité et de maintenance, soit individuellement, soit par lots. C'est la manière la plus efficace de suivre les périphériques Axis sur un réseau, de mettre en œuvre des politiques de sécurité sur les périphériques et d'effectuer toutes les mises à jour du firmware de manière rapide et efficace.

Conclusion

S'il est très peu probable que les systèmes de sécurité soient considérés comme des biens essentiels, il est important que les entités essentielles ou importantes envisagent une approche globale de la sécurité. Il est vital pour ces entités d'envisager une approche holistique lors de la définition du champ d'application. Cela signifie que les technologies de sécurité physique doivent faire l'objet d'une évaluation approfondie dans le cadre de l'évaluation de la directive NIS 2 afin de mettre en évidence les risques potentiels. afin de mettre en évidence tout risque potentiel.

Axis adopte une vision à 360° en ce qui concerne son offre de cybersécurité. Les produits sont conçus avec des fonctions intégrées pour répondre aux préoccupations en matière de cybersécurité, tandis qu'une liste exhaustive de politiques et de processus, d'outils, de documentation et de formation permet d'atténuer les risques et de préserver la sécurité. Formation permet de limiter les risques et de protéger les clients.

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.