LIVRE BLANC

NIS 2

Juin 2024

Table des matières

1 Introduction

1.1 Qu'est-ce que NIS 2 ?

NIS 2 est une directive européenne qui devrait être transposée dans la législation nationale de chaque État membre de l'UE d'ici le 17 octobre 2024. Elle vise à atteindre un niveau commun élevé de cybersécurité dans l'ensemble de l'UE, afin de contribuer à la sécurité de la région et au fonctionnement efficace de son économie et de sa société. Elle impose aux entités fournissant des services essentiels et importants dans des secteurs clés de la société de se doter de capacités de cybersécurité, d'atténuer les menaces pesant sur les systèmes de réseaux et d'information, d'assurer la continuité des services lorsqu'elles sont confrontées à des incidents, et de signaler les incidents de sécurité aux autorités compétentes. Elle impose aux États membres d'adopter des stratégies nationales de cybersécurité et de mettre en place des autorités, notamment des autorités de gestion des cyber-crises et des équipes d'intervention en cas d'incident de sécurité informatique. Elle décrit les mesures de gestion des risques liés à la cybersécurité, ainsi que les mesures d'application. Les conséquences de la non-conformité d'entités essentielles et importantes peuvent inclure de lourdes amendes et des ramifications juridiques pour les équipes de gestion.

Pour plus d'informations, consultez :
eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 Qui est concerné par NIS 2 ?

NIS 2 concerne toutes les entités qui fournissent des services **essentiels** ou **importants** pour l'économie européenne et sa société, notamment les entreprises et fournisseurs.

1.2.1 Directement concernés

Entités essentielles – Énergie, transports, banques / finances, santé, eau potable, eaux usées, infrastructures numériques, administration publique, espace

Entités importantes – Services postaux, gestion des déchets, produits chimiques, alimentation, fabrication (par exemple, dispositifs médicaux, matériel électrique, matériel de transport), fournisseurs numériques (par exemple, places de marché en ligne, moteurs de recherche, réseaux sociaux), sociétés de recherche.

Autorités nationales compétentes – Les autorités nationales compétentes sont désignées par les États membres de l'UE pour superviser la mise en œuvre et l'application de NIS 2 dans leurs pays respectifs.

1.2.2 Indirectement concernés

Vendeurs et fournisseurs – NIS 2 concerne indirectement les vendeurs, les fournisseurs et les prestataires de services tiers qui fournissent des services essentiels ou des services numériques à des entités essentielles et importantes. Ces entreprises doivent assurer la sécurité de leurs produits et services, et peuvent être soumises à des exigences contractuelles de cybersécurité de la part de leurs clients.

Utilisateurs de services essentiels et de services numériques – Bien qu'ils ne soient pas directement réglementés par NIS 2, les utilisateurs de services essentiels et de services numériques bénéficient de l'amélioration des pratiques de cybersécurité et des capacités de réponse aux incidents, exigée par la directive. Cela a pour effet de renforcer indirectement la sécurité et la fiabilité des services dont ils dépendent.

2 Exigences NIS 2

2.1 Pour les entités essentielles et importantes

Mesures de sécurité – Mettre en œuvre des mesures de sécurité appropriées pour gérer les risques et garantir la sécurité de leur réseau et de leurs systèmes d'information. Ces mesures doivent être fondées sur des évaluations des risques et sur les meilleures pratiques.

Signalements d'incident – Signaler aux autorités compétentes les incidents importants susceptibles d'avoir un impact substantiel sur la sécurité de leur réseau et de leurs systèmes d'information. La notification en temps utile est essentielle pour coordonner les réponses et atténuer les dommages potentiels.

Gestion du risque – Évaluer les risques afin d'identifier les menaces et les vulnérabilités potentielles, et prendre des mesures pour atténuer ces risques.

Coopération avec les autorités compétentes – Coopérer avec les autorités compétentes désignées par les États membres de l'UE. Il s'agit notamment de fournir les informations et l'accès nécessaires aux systèmes à des fins de surveillance réglementaire et de réponse aux incidents.

Planification de la réponse aux incidents – Élaborer et tenir à jour des plans de réponse aux incidents afin d'intervenir efficacement en cas d'incident de sécurité. Ces plans doivent décrire les procédures de détection, de signalement et d'atténuation des incidents.

Sécurité des chaînes d'approvisionnement – Sécuriser les chaînes d'approvisionnement, y compris les vendeurs et les fournisseurs tiers, afin de garantir la résilience globale des systèmes de réseaux et d'information.

Surveillance continue – Mettre en place une surveillance et un audit continus des systèmes de réseaux et d'information afin de détecter les menaces et les vulnérabilités et d'y répondre en temps réel.

3 Impact sur les fournisseurs

Les fournisseurs peuvent soutenir les entités NIS 2 en répondant aux exigences suivantes :

La sécurité dès la conception – Les fabricants de périphériques IoT devraient intégrer des fonctions de sécurité à leurs périphériques dès la phase de conception, en veillant à ce que la sécurité fasse partie intégrante du produit.

Mises à jour et correctifs réguliers – Les fabricants devraient fournir régulièrement des mises à jour de sécurité et des correctifs pour remédier aux vulnérabilités de leurs périphériques IoT.

Authentification et autorisation – Les périphériques IoT doivent utiliser des mécanismes d'authentification puissants et des contrôles d'autorisation appropriés pour empêcher tout accès non autorisé.

Chiffrement des données – La transmission et le stockage des données par les périphériques IoT doivent être chiffrés pour protéger les informations sensibles contre l'interception ou l'accès par des parties non autorisées.

Signalements d'incident – Les fabricants devraient signaler tout incident de sécurité important ou toute violation liée à leurs périphériques IoT aux autorités compétentes et potentiellement aux consommateurs ou aux clients.

Considérations relatives à la confidentialité – Les périphériques IoT qui traitent des données à caractère personnel doivent être conformes aux réglementations sur la protection des données telles que le RGPD (Règlement général sur la protection des données), en plus de la conformité à NIS 2.

Sécurité de la chaîne logistique – Il devrait être requis de garantir la sécurité de l'ensemble de la chaîne d'approvisionnement, des fournisseurs de composants aux clients, pour empêcher l'introduction de vulnérabilités en matière de sécurité à tout moment du processus de production.

4 La réponse d'Axis

Voici comment Axis, en tant que fournisseur, répond aux exigences des entités NIS 2 :

4.1 La sécurité dès la conception

La sécurité dès la conception est l'approche adoptée pour s'assurer que les considérations et les activités de sécurité font partie intégrante de la conception et du développement des produits, afin de réduire le risque de vulnérabilités et de garantir que des configurations de sécurité robustes sont paramétrées par défaut dans les produits. Chez Axis, le principe de sécurité dès la conception s'applique aux logiciels et au matériel, et est couvert par les principaux éléments suivants :

- *Modèle de développement de la sécurité d'Axis (ASDM)* : l'ASDM est un cadre de processus et d'outils définis qui garantissent que les considérations de sécurité font partie intégrante du développement des logiciels. Les activités comprennent l'évaluation des risques, la modélisation des menaces, les tests de pénétration, l'analyse des vulnérabilités, la gestion des incidents ainsi qu'un programme de chasse aux bogues. Les développeurs de logiciels Axis utilisent ASDM pour s'assurer que la sécurité est intégrée dans le développement des logiciels afin de réduire le risque de publier des logiciels contenant des vulnérabilités.

- *Programme de chasse aux bogues* : Axis soutient un programme privé de chasse aux bogues qui renforce les efforts de l'entreprise pour identifier, corriger et divulguer de manière proactive les vulnérabilités d'AXIS OS, le système d'exploitation basé sur Linux qui équipe la plupart des produits Axis. Il renforce l'engagement d'Axis à établir des relations professionnelles avec des chercheurs en sécurité externes et des hackers éthiques.

- *Facture des matériels logiciels (SBOM)* : Axis fournit une SBOM pour AXIS OS, le système d'exploitation basé sur Linux utilisé dans la plupart des périphériques Axis. Il donne aux chercheurs en sécurité, aux autorités et aux clients un aperçu des composants logiciels qui constituent AXIS OS. Il est particulièrement utile à ceux qui se spécialisent dans l'évaluation des vulnérabilités et l'analyse des menaces, et témoigne de l'engagement d'Axis en faveur de la transparence dans le domaine de la cybersécurité.

- *Paramètres de sécurité par défaut d'AXIS OS* : Les périphériques exécutant les dernières versions d'AXIS OS sont préconfigurés en paramètres d'usine avec les éléments suivants : pas de mot de passe par défaut ; HTTP et HTTPS activés ; intégration et communications sécurisées avec IEEE 802.1X/802.1AR/802.1AE activés par défaut ; protocoles moins sécurisés désactivés. De plus amples informations sur les contrôles des paramètres de protection par défaut sont disponibles *ici*.

- *Axis Edge Vault* : Intégrée aux périphériques Axis, Axis Edge Vault est une plate-forme de sécurité matérielle qui comprend des fonctions protégeant l'intégrité des produits réseaux Axis et activant l'exécution de fonctionnements sécurisés basés sur des clés cryptographiques. Il assure la protection de la chaîne d'approvisionnement grâce à un démarrage sécurisé et à une signature de système d'exploitation ; à une identification fiable du périphérique au moyen de l'identifiant unique d'Axis intégré

pour prouver l'origine du périphérique ; au stockage sécurisé des clés pour protéger les informations cryptographiques contre le sabotage ; et à la détection du sabotage vidéo par signature vidéo.

4.2 Mises à jour et correctifs réguliers

Axis fournit des mises à jour logicielles pour remédier, entre autres, aux failles de sécurité récemment découvertes dans ses produits matériels et logiciels. Axis propose également des outils de gestion des périphériques afin de faciliter la mise à jour des logiciels des périphériques Axis. Les nouvelles versions d'AXIS OS pour les périphériques connectés sont mises en avant sur AXIS Companion, AXIS Camera Station et les logiciels de gestion vidéo partenaires tels que Milestone XProtect@ et Genetec™ Security Center, ainsi que les outils de gestion des périphériques AXIS. En outre, Axis propose un service de notification de sécurité auquel tout le monde peut s'abonner. Des informations plus détaillées sont fournies ci-dessous.

- AXIS *OS* : Axis propose deux solutions principales pour la mise à jour des logiciels des périphériques : la voie active et la voie de support à long terme (LTS). La voie active permet d'accéder aux toutes dernières caractéristiques et fonctionnalités de pointe, ainsi qu'aux corrections de bogues et les correctifs de sécurité. Les logiciels bénéficiant d'un support à long terme (LTS) maximisent la stabilité en ne fournissant que des corrections de bogues et des correctifs de sécurité, l'objectif étant le maintien d'un système tiers bien intégré.
- Outils de gestion des périphériques : *AXIS Device Manager* et *AXIS Device Manager Extend* sont des outils qui permettent aux clients de faciliter la mise à jour des logiciels des périphériques Axis, avec les derniers correctifs de sécurité et les dernières corrections de bogues.

  Pour une configuration et une gestion efficaces des périphériques Axis au niveau local, AXIS Device Manager active le traitement par lots des tâches de sécurité telles que la gestion des informations d'identification des périphériques, le déploiement des certificats, la désactivation des services inutilisés et la mise à niveau d'AXIS OS.

  AXIS Device Manager Extend fournit un tableau de bord agrégé qui rassemble des informations sur tous vos périphériques et sites dans une application unique facile à utiliser. Vous serez informé de la disponibilité des mises à jour des logiciels des périphériques et vous pourrez effectuer des mises à jour en masse et d'autres tâches à grande échelle. Vous recevrez également des recommandations sur les produits de remplacement. Les activités sont entièrement traçables et il est possible d'exporter toutes les informations relatives aux dispositifs du système à des fins de rapport ou d'audit.
- *Service de notifications de sécurité Axis* : Ce service, auquel Axis encourage les gens à s'inscrire, fournit aux abonnés des notifications opportunes sur les incidents de sécurité et les vulnérabilités.

4.3 Authentification et autorisation

Pour empêcher tout accès non autorisé et renforcer la sécurité générale des périphériques Axis, Axis prend en charge :

- les droits d'accès basés sur les rôles (Administrateur / Opérateur / Observateur) et la possibilité de centraliser l'authentification / l'autorisation en connectant les périphériques Axis aux intégrations organisationnelles normalisées *Active Directory Federation Service* (ADFS) . (ADFS est un composant logiciel développé par Microsoft pour fournir un service d'autorisation Single Sign-On (SSO) aux utilisateurs des systèmes d'exploitation Windows Server. ADFS permet aux utilisateurs à travers les frontières du logiciel d'utiliser un ensemble unique d'identifiants de connexion).
- Des technologies qui facilitent l'accès aux *réseaux Zero Trust* . Dans les dernières versions d'AXIS OS, ces technologies comprennent l'IEEE 802.1X, ainsi que les identifiants de périphériques Axis conformes à

IEEE 802.1AR, pour l'intégration automatique et sécurisée des périphériques à un réseau IEEE 802.1X, et à IEEE 802.1AE (MACsec) pour le chiffrement automatique des communications de données.

4.4 Chiffrement des données

Pour protéger les informations sensibles contre l'interception ou l'accès par des personnes non autorisées, les produits Axis prennent en charge :

- HTTPS, où toutes les communications de données sont compatibles avec les normes TLS 1.2 ou plus récentes. La connexion du flux vidéo entre le serveur du logiciel de gestion vidéo AXIS Camera Station et le client est chiffrée AES-256.
- *IEEE 802.1AE (MACsec)* pour le chiffrement automatique des communications de données.
- Flux vidéo sécurisé sur RTP, également appelé SRTP/RTSPS (à partir d'AXIS OS 7.40). SRTP/RTSPS utilise une méthode de transport sécurisée et chiffrée de bout en bout pour s'assurer que seuls les clients autorisés reçoivent le flux vidéo du périphérique Axis.
- *Chiffrement du stockage local* (carte SD)
- *Exportation chiffrée par mot de passe d'un enregistrement à la périphérie* (carte SD, partage réseau), à partir d'AXIS OS 10.10. Cela signifie qu'il est possible d'exporter un enregistrement qui est chiffré par mot de passe avec, en outre, la possibilité de partager en toute sécurité des données vidéo sensibles sans avoir besoin de chiffrer manuellement les enregistrements exportés.

4.5 Signalements d'incident

Axis assure le signalement des incidents de sécurité ou des vulnérabilités découvertes dans ses produits et services.

- Axis est une autorité de numérotation CVE (Common Vulnerability and Exposures), Cela signifie qu'Axis suit les meilleures pratiques de l'industrie pour gérer et répondre – avec transparence – aux vulnérabilités découvertes dans ses produits et services, afin de minimiser le risque d'exposition des clients. Axis peut également assigner des numéros CVE aux vulnérabilités nouvellement découvertes et les signaler sur le site *www.cve.org*. La *politique de gestion des vulnérabilités* d'Axis est publiée sur axis.com.
- Tout le monde peut s'inscrire *ici* pour recevoir une notification de sécurité de la part d'Axis.
- Les correctifs de sécurité et les corrections de bogues sont intégrés dans les nouvelles versions d'AXIS OS. La disponibilité des logiciels des périphériques mis à jour est également soulignée dans AXIS Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend et les VMS tiers tels que Milestone XProtect et Genetec Security Center.
- Axis s'engage à faire preuve de transparence concernant toute cyberattaque liée à l'entreprise et signalera ces incidents conformément aux directives fournies par les autorités suédoises compétentes.

4.6 Considérations relatives à la confidentialité

Axis publie en ligne sa *politique de confidentialité* et son avis de confidentialité, où elle indique quelles données à caractère personnel sont collectées (par exemple, à partir d'un compte en ligne sur My Axis) et comment elles sont utilisées.

Axis a également publié son *cadre de cybersécurité et ses pratiques* relatives à son système de gestion de la sécurité de l'information, qui est certifié ISO/IEC 27001. Le champ d'application du certificat ISO/IEC 27001 d'Axis couvre le développement et le fonctionnement de l'infrastructure et du service informatique interne. La norme ISO 27001 est une norme internationalement reconnue qui fournit des orientations sur la façon de protéger et de gérer les informations d'une société par une gestion du risque efficace.

La conformité *ISO/IEC 27001* démontre qu'Axis adopte des processus et des meilleures pratiques internationalement reconnus pour gérer son infrastructure et ses systèmes d'information internes en appui des services fournis à ses clients et partenaires.

Axis aide également ses clients à répondre aux préoccupations de confidentialité dans le domaine de la surveillance, et plus particulièrement en ce qui concerne la capture de vidéos et d'audio. Les solutions comprennent :

- le masquage statique de la confidentialité dans les caméras Axis et le masquage dynamique de la confidentialité avec l'application logicielle *AXIS Live Privacy Shield*
- les analyses basées sur la périphérie, telles que l'application *AXIS People Counter* ou *AXIS P8815-2 3D People Counter*, qui ne capturent et ne stockent que des données statistiques numériques — aucune information personnelle identifiable n'est traitée.
- *Caméras thermiques*
- *Produits radar*
- l'outil de rédaction vidéo de *AXIS Camera Station* destiné à masquer les objets ou les domaines d'intérêt.
- *les fonctions audio désactivées par défaut* dans les produits de vidéosurveillance Axis

De plus amples informations sur les solutions en matière de confidentialité sont disponibles à l'adresse *axis.com/solutions/privacy-in-surveillance*.

4.7 Sécurité de la chaîne logistique

Il est important de sécuriser la chaîne d'approvisionnement, depuis les fournisseurs de composants jusqu'aux clients, afin d'éviter l'introduction de vulnérabilités en matière de sécurité.

En matière de cybersécurité, Axis adopte une *approche fondée sur le cycle de vie des produits*. Nous nous engageons à atténuer les risques, non seulement tout au long de la chaîne d'approvisionnement, du niveau des composants au produit fini, mais aussi pendant la distribution et la mise en œuvre, ainsi que pendant les phases de service et de déclassement.

Voici quelques-uns des moyens mis en œuvre par Axis pour assurer la sécurité de la chaîne d'approvisionnement :

- Axis s'approvisionne en composants critiques directement auprès de fournisseurs stratégiques. Nous travaillons en étroite collaboration avec des partenaires manufacturiers. Les procédés de production sont contrôlés et les données sont partagées avec Axis 24 heures sur 24 et 7 jours sur 7, ce qui permet des analyses en temps réel et une transparence totale. En savoir plus sur la *sécurité de la chaîne d'approvisionnement d'Axis*.
- Sécurité intégrée des périphériques grâce à Axis Edge Vault, qui protège l'intégrité des périphériques Axis à l'aide des fonctions suivantes :

- **Signature d'OS** : garantit l'authenticité du système d'exploitation AXIS OS installé. Il garantit également que tout nouveau système d'exploitation AXIS OS destiné à être installé sur le périphérique est également signé par Axis.
- **Démarrage sécurisé** : Active le périphérique pour vérifier que le système d'exploitation possède une signature Axis. Si l'OS n'est pas autorisé ou a été modifié, le processus d'amorçage est interrompu et le périphérique cesse de fonctionner. La combinaison d'une signature d'OS, d'un démarrage sécurisé et d'une réinitialisation d'usine du périphérique offre une protection contre les tentatives de modification lors de l'expédition d'un périphérique.
- L'**identifiant de périphérique Axis** est conforme à IEEE 802.1AR, ce qui active l'identification et l'intégration sécurisées des périphériques sur un réseau. L'identifiant de périphérique Axis est stocké dans la base de données sécurisée du périphérique (élément sécurisé, TPM, TEE).
- Le **système de fichiers chiffré** protège la configuration et les informations spécifiques au client stockées qu'il contient contre l'extraction ou le sabotage quand le périphérique est inutilisé, par exemple pendant son transport entre un intégrateur systèmes et un client.
- En outre, la prise en charge par Axis de la **signature vidéo** active la possibilité pour les observateurs de vérifier si la vidéo exportée à partir d'un périphérique a été sabotée ou non. Cette fonction est particulièrement importante dans le cadre d'une enquête ou de poursuites judiciaires. De plus amples informations sont disponibles sur le site *axis.com/solutions/edge-vault*.

- Une somme de contrôle est fournie pour les logiciels téléchargés à partir d'axis.com. La somme de contrôle active la vérification de l'intégrité d'un fichier.
- Certification ETSI : Plus de 150 produits Axis fonctionnant avec AXIS OS 11 ou une version plus récente sont certifiés conformes à la *norme de cybersécurité ETSI EN 303 645*. ETSI est l'acronyme de European Telecommunications Standards Institute. Ces exigences couvrent les périphériques proprement dits, notamment la prise en charge des fonctionnalités de sécurité matérielles telles que le stockage sécurisé des clés et les fonctionnalités de sécurité par défaut comme l'activation de HTTPS et l'absence de mots de passe. Un autre aspect implique la gestion du cycle de vie, comme le fait d'avoir une période d'assistance définie pour les mises à jour de sécurité des périphériques. D'autres comprennent une méthodologie de réduction du risque de vulnérabilités dans le développement des logiciels ; une politique de gestion des vulnérabilités transparente ; et le soutien des meilleures pratiques dans le traitement des données personnelles. Ces exigences prennent en compte les meilleures pratiques du secteur qui permettent d'assurer que les produits certifiés respectent un niveau de sécurité de référence minimal au cours de leur cycle de vie. La norme s'aligne étroitement sur la loi de l'UE sur la résilience en matière de cybersécurité, la directive de l'UE sur les équipements radioélectriques et d'autres normes et législations du monde entier.

4.8 Formation et orientation

Axis fournit à son personnel, à ses partenaires et à ses clients des informations et des formations sur les meilleures pratiques en matière de cybersécurité. Ces informations et formations portent notamment sur les éléments suivants :

- Sensibilisation et formation à la sécurité interne : Axis a mis au point un programme de sensibilisation à la sécurité afin de former en permanence ses employés à la prévention et à l'atténuation des menaces qui pèsent sur la sécurité de la société. Cette formation de sensibilisation est obligatoire pour tout le personnel d'Axis. En fonction du rôle et des responsabilités de l'individu au sein de l'organisation, une formation supplémentaire à la sécurité est dispensée aux développeurs et aux propriétaires de systèmes.

- *Formation Axis Academy* : Disponibles pour les clients, les formations comprennent un cours en ligne sur la cybersécurité et l'*approche d'Axis en la matière*.
- *Guides de durcissement* disponibles en ligne pour :
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Commutateurs réseaux Axis*
- *Guide d'analyse de sécurité AXIS OS* : Axis recommande d'effectuer des analyses de sécurité des périphériques Axis pour vérifier s'ils sont affectés par des vulnérabilités ou une mauvaise configuration. Le guide d'analyse de sécurité AXIS OS fournit des recommandations pour remédier à certains résultats d'analyses et recense les « faux positifs » courants.
- *Guide forensique AXIS OS* : Ce guide propose des conseils techniques à l'intention des personnes chargées de l'analyse forensique des périphériques Axis, en cas de cyberattaque sur le réseau environnant et l'infrastructure informatique où est installé un périphérique Axis.

Pour plus d'informations sur Axis et la cybersécurité, consultez le *portail de cybersécurité Axis*.

À propos d'Axis Communications

En concevant des solutions qui améliorent la sécurité et les performances de l'entreprise, Axis crée monde plus clairvoyant et plus sûr. En tant qu'entreprise de technologie de réseau et leader de l'industrie, Axis propose des solutions de vidéosurveillance, de contrôle d'accès, d'interphonie et de systèmes audio. Les performances de ces solutions sont améliorées grâce à des applications d'analyse intelligentes et une formation de haute qualité.

Axis emploie près de 4 000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et d'intégration de systèmes dans le monde entier pour fournir des solutions clients adaptées. Axis a été fondée en 1984 et le siège social se trouve à Lund, en Suède

©2024 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC et VAPIX sont des marques déposées d'Axis AB dans diverses juridictions. Toutes les autres marques appartiennent à leurs propriétaires respectifs. Nous nous réservons le droit d'effectuer des modifications sans préavis.