WHITE PAPER

NIS 2

Giugno 2024

Sommario

1 Introduction 3

1.1 What is NIS 2? 3

1.2 Who does NIS 2 affect? 3

2 NIS 2 requirements 4

2.1 For essential and important entities 4

3 Impact on suppliers 4

4 The Axis response 5

4.1 Security by design 5

4.2 Regular updates and patches 5

4.3 Authentication and authorization 6

4.4 Data encryption 6

4.5 Incident reporting 7

4.6 Privacy considerations 7

4.7 Supply chain security 8

4.8 Training and guidance 9

1 Introduction

1.1 What is NIS 2?

NIS 2 is an EU directive that should be transposed into the national legislation of each EU member state by October 17, 2024. NIS 2 aims to achieve a high common level of cybersecurity across the EU, in order to contribute to the region's security and effective functioning of its economy and society. It requires entities providing essential and important services in key sectors of society to build cybersecurity capabilities, to mitigate threats to network and information systems, to ensure the continuity of services when facing incidents, and to report security incidents to the relevant authorities. It requires member states to adopt national cybersecurity strategies and to establish authorities, including cyber-crisis management authorities and computer security incident response teams. It outlines cybersecurity risk management measures, as well as enforcement measures. The consequences of non-compliance by essential and important entities can include heavy fines and legal ramifications for management teams.

For more information, visit:
eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 Who does NIS 2 affect?

NIS 2 affects all entities that provide **essential** or **important** services to the European economy and society, including companies and suppliers.

1.2.1 Directly affected

Essential Entities – Energy, Transport, Banking/Finance, Health, Drinking Water, Waste Water, Digital Infrastructure, Public Administration, Space

Important Entities – Postal Services, Waste Management, Chemicals, Food, Manufacturing (e.g. medical devices, electrical, transport equipment), Digital Providers (e.g. online marketplaces, search engines, social networks), Research Organizations

National Competent Authorities – National competent authorities are designated by EU member states to oversee the implementation and enforcement of NIS 2 within their respective countries.

1.2.2 Indirectly affected

Vendors and suppliers – NIS 2 indirectly affects vendors, suppliers, and third-party service providers that supply essential services or digital services to essential and important entities. These companies need to ensure the security of their products and services, and may be subject to contractual cybersecurity requirements from their customers.

Users of essential services and digital services – While not directly regulated by NIS 2, users of essential services and digital services benefit from the improved cybersecurity practices and incident response capabilities required by the directive. This indirectly enhances the security and reliability of the services they rely on.

2 NIS 2 requirements

2.1 For essential and important entities

Security measures – Implement appropriate security measures to manage risks and ensure the security of their network and information systems. These measures should be based on risk assessments and best practices.

Incident reporting – Report significant incidents that could have a substantial impact on the security of their network and information systems to competent authorities. Timely reporting is essential for coordinating responses and mitigating potential harm.

Risk management – Conduct risk assessments to identify potential threats and vulnerabilities, and take measures to mitigate those risks.

Cooperation with Competent Authorities – Cooperate with competent authorities designated by EU member states. This includes providing the necessary information and access to systems for regulatory oversight and incident response purposes.

Incident response planning – Develop and maintain incident response plans to effectively respond to cybersecurity incidents. These plans should outline procedures for detecting, reporting, and mitigating incidents.

Security of supply chains – Secure supply chains, including third-party vendors and suppliers, to ensure the overall resilience of network and information systems.

Continuous monitoring – Implement continuous monitoring and auditing of network and information systems to detect and respond to threats and vulnerabilities in real time.

3 Impact on suppliers

Suppliers can support NIS 2 entities by addressing the following requirements:

Security by design – IoT device manufacturers should incorporate security features into their devices from the design phase, ensuring that security is an integral part of the product.

Regular updates and patching – Manufacturers should provide regular security updates and patches to address vulnerabilities in their IoT devices.

Authentication and authorization – IoT devices should employ strong authentication mechanisms and proper authorization controls to prevent unauthorized access.

Data encryption – The transmission and storage of data by IoT devices should be encrypted to protect sensitive information from being intercepted or accessed by unauthorized parties.

Incident reporting – Manufacturers should report any significant security incidents or breaches related to their IoT devices to relevant authorities and potentially to consumers or customers.

Privacy considerations – IoT devices that process personal data should comply with data protection regulations such as GDPR (General Data Protection Regulation) in addition to NIS 2.

Supply chain security – Ensuring the security of the entire supply chain, from component suppliers to customers, should be required to prevent security vulnerabilities from being introduced at any point in the production process.

4 The Axis response

The following is how Axis, as a supplier, meets NIS 2 entities' requirements:

4.1 Security by design

Security by design is the approach taken to ensure that security considerations and activities are undertaken as an integral part of product design and development, to reduce the risk of vulnerabilities and to ensure that robust security configurations are set in products by default. At Axis, the security by design principle applies to software and hardware, and are covered by the following main elements:

- *Axis Security Development Model (ASDM)*: ASDM is a framework of defined processes and tools that ensure security considerations are an integral part of software development. Activities include conducting risk assessments, threat modeling, penetration testing, vulnerability scanning, incident management as well as a bug bounty program. Axis software developers use ASDM to ensure security is built into software development to reduce the risk of releasing software containing vulnerabilities.
- *Bug bounty program*: Axis supports a private bug bounty program that reinforces the company's efforts to proactively identify, patch, and disclose vulnerabilities in AXIS OS, the Linux-based operating system that drives most Axis products. It strengthens the Axis commitment to building professional relationships with external security researchers and ethical hackers.
- *Software bill of materials (SBOM)*: Axis provides an SBOM for AXIS OS, the Linux-based operating system used in most Axis devices. It gives security researchers, authorities and customers insights into the software components that comprise AXIS OS. It is particularly helpful to those specializing in vulnerability assessment and threat analysis, and is a demonstration of Axis' commitment to transparency in cybersecurity.
- *AXIS OS default security settings*: Devices running the latest AXIS OS versions are pre-configured in factory default state with the following: no default password; HTTP and HTTPS enabled; secure onboarding and communications with IEEE 802.1X/802.1AR/802.1AE enabled by default; less secure protocols disabled. More information on default protection controls is available *here*.
- *Axis Edge Vault*: Built into Axis devices, Axis Edge Vault is a hardware-based security platform that includes features that safeguard the integrity of Axis network products and that enable the execution of secure operations based on cryptographic keys. It provides for supply chain protection with secure boot and signed OS; trusted device identity with the built-in unique Axis device ID for proving the device's origin; secure key storage for tamper-protected storage of cryptographic information; and video tampering detection with signed video.

4.2 Regular updates and patches

Axis provides software updates to address, among other things, newly discovered security vulnerabilities in its hardware and software products. Axis also provides device management tools to make it easier for customers to keep the Axis device software up to date. New AXIS OS releases for connected devices are highlighted on AXIS Companion, AXIS Camera Station, and partner video management software such as Milestone XProtect® and Genetec™ Security Center, as well as Axis device management tools. In addition, Axis provides a security notification service that anyone may subscribe to. More detailed information is provided below.

- *AXIS OS*: Axis offers two main alternatives for keeping device software up to date: the active track and the long-term support (LTS) track. The active track provides access to the latest state-of-the-art

features and functionalities, as well as bug fixes and security patches. Software on the long-term support (LTS) tracks maximize stability by providing only bug fixes and security patches, since the focus is on maintaining a well-integrated, third-party system.

- Device management tools: *AXIS Device Manager* and *AXIS Device Manager Extend* are tools that make it easier for customers to keep the Axis device software up to date with the latest security patches and bug fixes.

  For the efficient configuration and management of Axis devices locally, AXIS Device Manager enables batch processing of security tasks such as managing device credentials, deploying certificates, disabling unused services, and upgrading AXIS OS.

  AXIS Device Manager Extend provides an aggregated dashboard that gathers information about all your devices and sites in a single, easy-to-use application. You'll be informed when device software upgrades are available, and you can perform bulk upgrades and other tasks at scale. You'll also receive recommendations for replacement products. Activities are fully traceable, and it's possible to export all system device information for reporting or auditing purposes.

- *Axis security notification service*: This service, which Axis encourages people to sign up for, provides subscribers with timely notifications of security incidents and vulnerabilities.

4.3 Authentication and authorization

To prevent unauthorized access and increase overall Axis device security, Axis supports:

- Role-based access device management access rights (Administrator/Operator/Viewer) and the possibility to centralize authentication/authorization by connecting Axis devices to IT-standardized *Active Directory Federation Service* (ADFS) integrations. (ADFS is a software component developed by Microsoft to provide Single Sign-On (SSO) authorization service to users on Windows Server Operating Systems. ADFS allows users across organizational boundaries to access applications on Windows Server Operating Systems using a single set of login credentials.)
- Technologies that make *zero-trust networking* easier. In the latest AXIS OS releases, these technologies include IEEE 802.1X, together with IEEE 802.1AR-compliant Axis device IDs, for automated and secure onboarding of devices to an IEEE 802.1X network, and IEEE 802.1AE (MACsec) for the automatic encryption of data communication.

4.4 Data encryption

To protect sensitive information from being intercepted or accessed by unauthorized parties, Axis products support:

- HTTPS, where all data communication supports TLS 1.2 or newer standards. The video stream connection between AXIS Camera Station video management software server and the client is AES-256 encrypted.
- *IEEE 802.1AE (MACsec)* for automatic data communication encryption.
- Secure video streaming over RTP, also referred to as SRTP/RTSPS (starting from AXIS OS 7.40). SRTP/RTSPS uses a secure end-to-end encrypted transportation method to make sure that only authorized clients receive the video stream from the Axis device.
- *Edge storage encryption* (SD card)

- *Password-encrypted export of edge recording* (SD card, network share), starting from AXIS OS 10.10. This means it is possible to export a recording that is password encrypted, adding the possibility to securely share sensitive video data without the need to manually encrypt exported recordings.

4.5 Incident reporting

Axis provides incident reporting of security incidents or vulnerabilities discovered in our products and services.

- Axis is a Common Vulnerabilities and Exposures (CVE) Numbering Authority. This means that Axis follows industry best practices in managing and responding – with transparency – to discovered vulnerabilities in our products and services to minimize customers' risk of exposure. Axis can also assign CVE numbers to newly discovered vulnerabilities and will report these to *www.cve.org* website. Axis *vulnerability management policy* is published on axis.com.
- Anyone can subscribe *here* to receive a security notification from Axis.
- Security patches and bug fixes are rolled out in new AXIS OS versions. The availability of updated device software is also highlighted in AXIS Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend, and third-party VMS such as Milestone XProtect and Genetec Security Center.
- Axis is committed to transparency regarding any company-related cyberattacks and will report such incidents according to the guidelines provided by the relevant Swedish authorities.

4.6 Privacy considerations

Axis publishes its *privacy policy* and notice online, where it outlines which personal data is collected (for example, from an online account at My Axis) and how it is used.

Axis has also published its *cybersecurity framework and practices* relating to its Information Security Management System, which is ISO/IEC 27001-certified. The scope of the Axis ISO/IEC 27001 certificate covers the development and operations of internal IT infrastructure and service. ISO 27001 is an internationally recognized standard that provides guidance on how to protect and manage an organization's information through effective risk management.

Compliance with *ISO/IEC 27001* demonstrates that Axis uses internationally recognized processes and best practices to manage its internal information infrastructure and systems that support and deliver its services to customers and partners.

Axis also helps customers address privacy concerns in surveillance with regard to capturing video and audio. Solutions include:

- Static privacy masking in Axis cameras, and dynamic privacy masking with *AXIS Live Privacy Shield* software application
- Edge-based analytics such as *AXIS People Counter* application or *AXIS P8815-2 3D People Counter*, which only capture and store statistical numerical data — no personally identifiable information is processed
- *Thermal cameras*
- *Radar products*
- Video redaction tool in *AXIS Camera Station* for masking objects or areas of no interest
- *Audio capabilities disabled by default* in Axis video surveillance products

More information about privacy solutions is available at *axis.com/solutions/privacy-in-surveillance*

4.7 Supply chain security

Securing the supply chain from component suppliers to customers is important to prevent security vulnerabilities being introduced.

Axis takes a product *lifecycle approach* when addressing cybersecurity. We are committed to mitigating risks, not only through the entire supply chain from component level to finished product, but also during distribution and implementation, as well as in service and decommissioning phases.

The following are some of the ways Axis addresses supply chain security:

- Axis procures critical components directly from strategic suppliers. We work closely with manufacturing partners. Production processes are monitored and data is shared 24/7 with Axis, enabling real-time analysis and transparency. Learn about *Axis supply chain security*.
- Built-in device security through Axis Edge Vault, which safeguards the integrity of Axis devices through the following features:
  - **Signed OS**: Ensures that the installed AXIS OS is genuinely from Axis. It also makes sure that any new AXIS OS intended for installation on the device is also signed by Axis.
  - **Secure boot**: Enables the device to check that the operating system has an Axis signature. If the OS is unauthorized or has been altered, the boot process is aborted and the device stops running. The combination of signed OS, secure boot and doing a device factory reset offers protection against attempted modifications during the shipment of a device.
  - **Axis device ID** is IEEE 802.1AR-compliant, which enables secure device identification and onboarding on a network. The Axis device ID is stored in the device's secure keystore (secure element, TPM, TEE).
  - **Encrypted file system** protects the customer-specific configuration and information stored in the file system from being extracted or tampered with while the device is not in use, such as when in transit from a system integrator to a customer.
  - Furthermore, Axis support for **signed video** enables viewers to verify if the video exported from a device has been tampered with or not. This is particularly important in an investigation or prosecution. More information is available at *axis.com/solutions/edge-vault*.
- A checksum is provided for software downloads from axis.com. The checksum enables verification of a file's integrity.
- ETSI certification: More than 150 Axis products running AXIS OS 11 or higher are certified to the *ETSI EN 303 645 cybersecurity standard*. ETSI stands for European Telecommunications Standards Institute. The requirements cover the devices themselves, including support for hardware-based security features such as secure key storage, and default security features such as HTTPS being enabled by default and no default passwords. Another aspect involves lifecycle management, such as having a defined support period for device security updates. Others include having a methodology for reducing the risk of vulnerabilities in software development; having a transparent vulnerability management policy; and supporting best practices in the processing of personal data. These requirements take into consideration industry best practices that help ensure certified products have a minimum baseline security level throughout their lifecycle. The standard aligns closely with the EU Cybersecurity Resilience Act, EU Radio Equipment Directive, and other standards and legislation from around the world.

4.8 Training and guidance

Axis provides staff, partners and customers with information and training on cybersecurity best practices. These include the following:

- Internal security awareness and training: Axis has developed a security awareness program to continuously train our employees in avoiding and mitigating security threats to the organization. This awareness training is mandatory for all Axis personnel. Depending on the individual's organizational role and responsibilities, additional security training is provided for developers and system owners.
- *Axis Academy training*: Available for customers, training courses include an online course on cybersecurity and the *Axis approach to the topic*.
- *Hardening guides* available online for:
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Axis network switches*
- *AXIS OS Security Scanner Guide*: Axis recommends running security scans of Axis devices to check if they are affected by vulnerabilities or poor configuration. The AXIS OS Security Scanner Guide offers recommendations on how to remedy certain scan results and outlines the common "false positives".
- *AXIS OS Forensic Guide*: This guide provides technical advice for anyone conducting forensic analysis of Axis devices in the event of a cybersecurity attack on the surrounding network and IT infrastructure where an Axis device is installed.

For more information about Axis and cybersecurity, please visit the *Axis cybersecurity portal*.

T10210486/IT/M3.3/2406

Informazioni su Axis Communications

Axis consente un mondo più intelligente e più sicuro creando soluzioni per migliorare la sicurezza e le prestazioni aziendali. Come società di tecnologie di rete e leader nel settore, Axis offre soluzioni nella videosorveglianza, controllo degli accessi, interfono e sistemi audio. Queste sono ottimizzate da applicazioni di analisi intelligente e supportate da formazione di alta qualità.

Axis ha circa 4.000 impiegati dedicati in più di 50 paesi e collabora con partner di tecnologia e integrazione di sistema in tutto il mondo per offrire soluzioni di clienti. Fondata nel 1984, Axis e con sede a Lund, in Svezia