WHITE PAPER

NIS 2

Giugno 2024

Sommario

1 Introduzione

1.1 Che cos'è la NIS 2?

La NIS 2 è una direttiva dell'UE che deve essere recepita nella legislazione nazionale di ogni Stato membro dell'UE entro il 17 ottobre 2024. La NIS 2 mira a raggiungere un elevato livello comune di sicurezza informatica in tutto il territorio dell'UE, al fine di contribuire alla sicurezza della regione e all'efficace funzionamento della sua economia e società. La direttiva prevede che le entità che forniscono servizi essenziali e importanti in settori fondamentali della società adottino sistemi di cybersecurity, attenuino le minacce ai sistemi di rete e informatici, garantiscano la continuità dei servizi in caso di incidenti e segnalino gli incidenti in materia di sicurezza alle autorità competenti. La norma richiede agli Stati membri di adottare strategie nazionali di sicurezza informatica e di istituire autorità, tra cui autorità per la gestione delle crisi informatiche e squadre di risposta agli incidenti di cybersecurity. Il documento delinea le misure di gestione dei rischi per la cybersecurity e le misure di applicazione. Le conseguenze della mancata conformità da parte di entità essenziali e importanti possono includere multe salate e ramificazioni legali per i team addetti alla gestione.

Per ulteriori informazioni, visita:
eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 A chi si rivolge la NIS 2?

La NIS 2 interessa tutte le entità che forniscono servizi **essenziali** o **importanti** all'economia e alla società europea, comprese le aziende e i fornitori.

1.2.1 Direttamente interessati

Entità essenziali – Energia, trasporti, banche e istituti finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione, spazio

Entità importanti – Servizi postali, gestione dei rifiuti, prodotti chimici, alimentari, industria manifatturiera (ad es. dispositivi medici, elettricità, attrezzature di trasporto), fornitori di servizi digitali (ad es. marketplace online, motori di ricerca, social network), organizzazioni di ricerca

Autorità nazionali competenti – Le autorità nazionali competenti sono designate dagli Stati membri dell'UE per supervisionare l'attuazione e l'applicazione della norma NIS 2 nei rispettivi Paesi.

1.2.2 Indirettamente interessati

Venditori e fornitori – La NIS 2 interessa indirettamente i venditori, i fornitori e i service provider terzi che forniscono servizi essenziali o servizi digitali a entità essenziali e importanti. Queste aziende devono garantire la sicurezza dei loro prodotti e servizi e possono essere soggette a requisiti contrattuali in termini di sicurezza informatica da parte dei loro clienti.

Utenti di servizi essenziali e servizi digitali – Anche se non sono direttamente regolamentati dalla NIS 2, gli utenti dei servizi essenziali e dei servizi digitali beneficiano del miglioramento delle pratiche di cybersecurity e delle capacità di risposta agli incidenti imposte dalla direttiva. Ciò incrementa indirettamente la sicurezza e l'affidabilità dei servizi su cui fanno affidamento.

2 Requisiti della NIS 2

2.1 Per le entità essenziali e importanti

Misure di sicurezza – Implementare misure di sicurezza adeguate per gestire i rischi e garantire la protezione della rete e dei sistemi informatici. Queste misure devono essere basate sulle valutazioni del rischio e sulle best practice.

Report eventi – Segnalare alle autorità competenti gli incidenti degni di nota che potrebbero avere un impatto ingente sulla protezione della rete e dei sistemi informatici. La tempestività delle segnalazioni è essenziale per coordinare le risposte e ridurre i potenziali danni.

Gestione dei rischi – Condurre valutazioni dei rischi per identificare le potenziali minacce e vulnerabilità e adottare misure per ridurre tali rischi.

Cooperazione con le autorità competenti – Collaborare con le autorità competenti designate dagli Stati membri dell'UE. Ciò include la fornitura delle informazioni necessarie e l'accesso ai sistemi a scopo di supervisione normativa e di risposta agli incidenti.

Pianificazione della risposta agli incidenti – Sviluppare e mantenere piani di risposta per rispondere in maniera efficace agli incidenti di cybersecurity. Questi piani devono delineare le procedure per il rilevamento, la segnalazione e la riduzione degli incidenti.

Sicurezza delle catene di fornitura – Proteggere le catene di fornitura, compresi i venditori e i fornitori terzi, per garantire la resilienza globale della rete e dei sistemi informatici.

Monitoraggio continuo – Implementare il monitoraggio e l'auditing continuo della rete e dei sistemi informatici per rilevare e rispondere alle minacce e alle vulnerabilità in tempo reale.

3 Impatto sui fornitori

I fornitori possono supportare le entità NIS 2 soddisfacendo i seguenti requisiti:

Sicurezza sin dalla progettazione – I produttori di dispositivi IoT devono integrare le funzioni di sicurezza nei loro dispositivi sin dalla fase di progettazione, garantendo così che la sicurezza sia parte integrante del prodotto.

Aggiornamenti e patch regolari – I produttori devono fornire regolarmente aggiornamenti e patch di sicurezza per risolvere le vulnerabilità dei loro dispositivi IoT.

Autenticazione e autorizzazione – I dispositivi IoT devono usare meccanismi di autenticazione forti e controlli degli accessi adeguati per prevenire gli accessi non autorizzati.

Crittografia dei dati – La trasmissione e l'archiviazione dei dati da parte dei dispositivi IoT devono essere crittografate per proteggere le informazioni sensibili dall'intercettazione o dall'accesso da parte di terzi non autorizzati.

Report eventi – I produttori devono segnalare qualsiasi incidente o violazione significativa della sicurezza relativa ai loro dispositivi IoT alle autorità competenti e potenzialmente ai consumatori o ai clienti.

Considerazioni sulla privacy – I dispositivi IoT che elaborano dati personali devono essere conformi alle normative sulla protezione dei dati, come il GDPR (Regolamento generale sulla protezione dei dati), oltre che alla NIS 2.

Sicurezza della catena di fornitura – Occorre garantire la sicurezza dell'intera catena di fornitura, dai fornitori di componenti ai clienti, in modo da evitare che le falle nella sicurezza possano essere introdotte in qualsiasi punto del processo di produzione.

4 La risposta di Axis

Di seguito viene illustrato in che modo Axis, in qualità di fornitore, soddisfa i requisiti delle entità NIS 2:

4.1 Sicurezza sin dalla progettazione

La sicurezza sin dalla progettazione è l'approccio adottato per garantire che le considerazioni e le attività relative alla sicurezza siano intraprese come parte integrante della progettazione e dello sviluppo dei prodotti al fine di ridurre il rischio di vulnerabilità e garantire che nei prodotti siano impostate in modo predefinito solide configurazioni di sicurezza. In Axis, il principio della sicurezza sin dalla progettazione viene applicato ai software e agli hardware e prevede i seguenti elementi principali:

- *Axis Security Development Model (ASDM)*: l'ASDM è un quadro di processi e strumenti definiti che garantiscono che le considerazioni sulla sicurezza siano parte integrante dello sviluppo del software. Le attività comprendono la valutazione del rischio, la modellizzazione delle minacce, i penetration test, la scansione delle vulnerabilità, la gestione degli incidenti e un programma bug bounty. Gli sviluppatori software Axis utilizzano l'ASDM per garantire la sicurezza nello sviluppo del software e ridurre il rischio di pubblicare software affetti da vulnerabilità.
- *Programma bug bounty*: Axis supporta un programma bug bounty privato che rafforza l'impegno dell'azienda a identificare, correggere e divulgare in modo proattivo le vulnerabilità di AXIS OS, il sistema operativo basato su Linux e integrato su gran parte dei prodotti Axis. Ribadisce l'impegno di Axis a instaurare relazioni professionali con ricercatori di sicurezza esterni e hacker etici.
- *Distinta base del software (SBOM)*: Axis fornisce una SBOM per AXIS OS, il sistema operativo basato su Linux usato sulla maggior parte dei dispositivi Axis. Lo strumento fornisce ai ricercatori di sicurezza, alle autorità e ai clienti dati sui componenti software di AXIS OS. È particolarmente utile per chi è specializzato nella valutazione delle vulnerabilità e nell'analisi delle minacce ed è una dimostrazione dell'impegno di Axis a promuovere la trasparenza nella cybersecurity.
- *Impostazioni predefinite di sicurezza di AXIS OS*: i dispositivi con le ultime versioni di AXIS OS installate sono preconfigurati con i seguenti valori predefiniti di fabbrica: nessuna password predefinita; HTTP e HTTPS abilitati; onboarding e comunicazioni sicure con IEEE 802.1X/802.1AR/802.1AE abilitati per impostazione predefinita; protocolli meno sicuri disabilitati. Ulteriori informazioni sui controlli di protezione predefiniti sono disponibili *qui*.
- *Axis Edge Vault*: Axis Edge Vault, integrata sui dispositivi Axis, è una piattaforma di sicurezza basata su hardware con funzioni che tutelano l'integrità dei prodotti di rete Axis e che consentono l'esecuzione di operazioni sicure basate su chiavi crittografiche. Protegge la catena di fornitura grazie a Secure Boot e al sistema operativo con firma digitale, all'identità affidabile del dispositivo grazie all'ID univoco integrato del dispositivo Axis per dimostrarne l'origine, all'archivio chiavi sicuro per l'archiviazione protetta da manomissioni delle informazioni crittografiche e al rilevamento di manomissioni video tramite la firma digitale.

4.2 Aggiornamenti e patch regolari

Axis fornisce aggiornamenti software per risolvere, tra le altre cose, le falle nella sicurezza recentemente riscontrate nei suoi prodotti hardware e software. Axis fornisce anche strumenti di gestione dei dispositivi per facilitare ai clienti l'aggiornamento del software dei dispositivi Axis. Le nuove versioni di AXIS OS per i dispositivi connessi sono evidenziate su AXIS Companion, AXIS Camera Station e sui software per la gestione video dei partner, come Milestone XProtect® e Genetec™ Security Center, nonché sugli strumenti di gestione dei dispositivi Axis. Inoltre, Axis fornisce un servizio di notifica di sicurezza a cui chiunque può iscriversi. Di seguito sono fornite informazioni più dettagliate.

- *AXIS OS*: Axis offre due alternative principali per mantenere aggiornato il software dei dispositivi: il percorso Active e il percorso LTS (Long-Term Support). Il percorso Active consente di accedere alle ultime caratteristiche e funzionalità, nonché a correzioni di bug e patch di sicurezza. I software che seguono il percorso LTS massimizzano la stabilità fornendo solo correzioni di bug e patch di sicurezza, poiché l'attenzione principale è rivolta sul mantenimento di un sistema di terze parti ben integrato.
- Strumenti di gestione dei dispositivi: *AXIS Device Manager* e *AXIS Device Manager Extend* sono strumenti che facilitano ai clienti l'aggiornamento del software dei dispositivi Axis con le ultime patch di sicurezza e correzioni di bug.

  Per una configurazione e una gestione efficienti dei dispositivi Axis a livello locale, AXIS Device Manager consente l'elaborazione in batch delle attività di sicurezza, come la gestione delle credenziali dei dispositivi, la distribuzione di certificati, la disattivazione dei servizi non utilizzati e l'aggiornamento di AXIS OS.

  AXIS Device Manager Extend fornisce una dashboard aggregata che raccoglie informazioni su tutti i dispositivi e i siti in un'unica applicazione facile da usare. Ti informeremo ogni volta che gli aggiornamenti del software dei dispositivi sono disponibili e potrai eseguire aggiornamenti in blocco e altre attività su scala. Riceverai anche consigli sui prodotti sostitutivi. Le attività sono completamente tracciabili ed è possibile esportare tutte le informazioni sui dispositivi di sistema a scopi di reporting o verifica.
- *Servizio di notifiche di sicurezza Axis*: Axis incoraggia i clienti a iscriversi a questo servizio, che fornisce agli abbonati notifiche tempestive in merito a incidenti di sicurezza e vulnerabilità.

4.3 Autenticazione e autorizzazione

Per prevenire accessi non autorizzati e aumentare la sicurezza complessiva dei dispositivi Axis, Axis supporta:

- Diritti di accesso basati sui ruoli per la gestione dei dispositivi (amministratore/operatore/visualizzatore) e possibilità di centralizzare l'autenticazione/autorizzazione collegando i dispositivi Axis alle integrazioni standard IT dell' *Active Directory Federation Service* (ADFS). (ADFS è un componente software sviluppato da Microsoft per fornire un servizio di autorizzazione Single Sign-On (SSO) agli utenti sui sistemi operativi Windows Server. ADFS consente agli utenti al di là dei confini della società di accedere ad applicazioni sui sistemi operativi Windows Server utilizzando un unico set di credenziali di accesso).
- Tecnologie che facilitano le *connessioni di rete zero trust*. Nelle ultime versioni di AXIS OS, queste tecnologie includono IEEE 802.1X, insieme agli ID dei dispositivi Axis conformi a IEEE 802.1AR, per l'onboarding automatico e sicuro dei dispositivi in una rete IEEE 802.1X, e IEEE 802.1AE (MACsec) per la crittografia automatica della comunicazione dei dati.

4.4 Crittografia dei dati

Per proteggere le informazioni sensibili dall'intercettazione o dall'accesso di parti non autorizzate, i prodotti Axis supportano:

- HTTPS, in cui tutte le comunicazioni di dati supportano gli standard TLS 1.2 o più recenti. La connessione del flusso video tra il server del software per la gestione di video AXIS Camera Station e il client è crittografata AES-256.
- *IEEE 802.1AE (MACsec)* per la crittografia automatica della comunicazione dati.
- Streaming video sicuro su RTP, noto anche come SRTP/RTSPS (a partire da AXIS OS 7.40). SRTP/RTSPS utilizza un metodo di trasporto sicuro e crittografato end-to-end per garantire che solo i client autorizzati ricevano il flusso video dal dispositivo Axis.
- *Crittografia edge storage* (scheda di memoria)
- *Esportazione criptata con password della registrazione in modalità edge* (scheda di memoria, disco di rete), a partire da AXIS OS 10.10. Ciò significa che è possibile esportare una registrazione criptata con password, aggiungendo la possibilità di condividere in modo sicuro i dati video sensibili senza dover criptare manualmente le registrazioni esportate.

4.5 Report eventi

Axis segnala i problemi di sicurezza o vulnerabilità scoperti nei suoi prodotti e servizi.

- Axis è una Common Vulnerabilities and Exposures (CVE) Numbering Authority. Ciò significa che Axis segue le migliori pratiche del settore nella gestione e nella risposta, con trasparenza, alle vulnerabilità scoperte nei nostri prodotti e servizi per ridurre al minimo il rischio di esposizione dei clienti. Axis è anche in grado di assegnare numeri CVE alle nuove vulnerabilità rilevate e di segnalarle sul sito web *www.cve.org*. La *policy di gestione delle vulnerabilità* di Axis è pubblicata su axis.com.
- Chiunque può iscriversi *qui* per ricevere una notifica di sicurezza da Axis.
- Le patch di sicurezza e le correzioni di bug vengono distribuite nelle nuove versioni di AXIS OS. La disponibilità di software aggiornati per i dispositivi è evidenziata anche in AXIS Camera Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend e nei software di terze parti come Milestone XProtect e Genetec Security Center.
- Axis si impegna a garantire la trasparenza in merito a qualsiasi cyberattacco legato all'azienda e a segnalare tali incidenti secondo gli orientamenti forniti dalle autorità svedesi competenti.

4.6 Considerazioni sulla privacy

Axis pubblica online la sua *informativa sulla privacy* e la nota informativa in cui vengono descritti i dati personali raccolti (ad esempio, da un account online My Axis) e le modalità di utilizzo.

Axis ha inoltre pubblicato un *quadro di riferimento per la sicurezza informatica e relative pratiche* in merito al suo sistema di gestione della sicurezza delle informazioni, certificato ISO/IEC 27001. L'ambito di applicazione del certificato ISO/IEC 27001 di Axis riguarda lo sviluppo e le operazioni dell'infrastruttura e del servizio IT interno. ISO 27001 è uno standard riconosciuto a livello internazionale che fornisce indicazioni su come proteggere e gestire le informazioni di una società con un'efficace gestione del rischio.

La conformità con la normativa *ISO/IEC 27001* dimostra che Axis utilizza processi e best practice riconosciuti a livello internazionale per gestire le infrastrutture informatiche interne e i sistemi che supportano e forniscono servizi a clienti e partner.

Axis aiuta inoltre i clienti a risolvere problemi di privacy nella videosorveglianza per quanto riguarda l'acquisizione di video e audio. Le soluzioni includono:

- Mascheramento statico della privacy nelle telecamere Axis e mascheramento dinamico della privacy con applicazione *AXIS Live Privacy Shield*
- Analitiche edge, come l'applicazione *AXIS People Counter* o *AXIS P8815-2 3D People Counter*, che si limitano ad acquisire e memorizzare dati numerici statistici. Non vengono elaborate informazioni di identificazione personale.
- *Telecamere termiche*
- *Prodotti radar*
- Strumento di rielaborazione video in *AXIS Camera Station* per mascherare gli oggetti o le aree che non sono di interesse
- *Funzionalità audio disabilitate per impostazione predefinita* nei prodotti di videosorveglianza Axis

Ulteriori informazioni sulle soluzioni per la privacy sono disponibili all'indirizzo *axis.com/solutions/privacy-in-surveillance*

4.7 Sicurezza della catena di fornitura

La sicurezza della catena di fornitura, dai fornitori di componenti ai clienti, è importante per prevenire l'introduzione di vulnerabilità di sicurezza.

Axis adotta un *approccio al ciclo di vita* del prodotto in questioni di cybersecurity. Ci impegniamo a ridurre i rischi, non solo nell'intera catena di fornitura (dai componenti fino al prodotto finito), ma anche durante la distribuzione e l'implementazione, nonché nelle fasi di servizio e smaltimento.

Di seguito sono elencati alcuni dei modi in cui Axis garantisce la sicurezza della catena di fornitura:

- Axis acquista i componenti critici direttamente da fornitori strategici. Lavoriamo a stretto contatto con i partner di produzione. I processi di produzione sono monitorati e i dati vengono condivisi 24 ore su 24 e 7 giorni su 7 con Axis, per un'analisi in tempo reale e la massima trasparenza. Maggiori informazioni sulla *sicurezza della catena di fornitura di Axis*.
- Sicurezza integrata dei dispositivi con Axis Edge Vault, che tutela l'integrità dei dispositivi Axis attraverso le seguenti funzioni:
  - **OS con firma digitale**: garantisce che la versione installata di AXIS OS provenga effettivamente da Axis. Inoltre, assicura che qualsiasi nuovo AXIS OS destinato all'installazione sul dispositivo sia firmato da Axis.
  - **Secure Boot**: consente al dispositivo di verificare che il sistema operativo sia provvisto di una firma digitale di Axis. Se il sistema operativo non è autorizzato o è stato alterato, il processo di avvio viene interrotto e il dispositivo smette di funzionare. La combinazione di OS firmato digitalmente, Secure Boot e reset di fabbrica protegge dai tentativi di modifica durante la spedizione del dispositivo.

- **L'ID dispositivo Axis** è conforme allo standard IEEE 802.1AR, che abilita l'identificazione e l'onboarding sicuri dei dispositivi in rete. L'ID dispositivo Axis è memorizzato nell'archivio chiavi sicuro del dispositivo (Secure Element, TPM, TEE).
- **Il file system crittografato** protegge la configurazione specifica del cliente e le informazioni memorizzate nel file system dall'estrazione o dalla manomissione mentre il dispositivo non è in uso, ad esempio nel transito da un system integrator a un cliente finale.
- Inoltre, il supporto di Axis per i **video con firma digitale** consente agli utenti di verificare se il video esportato da un dispositivo è stato manomesso o meno. Questo è particolarmente importante in un'indagine o in un'azione penale. Ulteriori informazioni sono disponibili su *axis.com/solutions/edge-vault*.

- Per i software scaricati da axis.com viene fornito un checksum che consente di verificare l'integrità di un file.
- Certificazione ETSI: oltre 150 prodotti Axis con AXIS OS 11 o versioni successive sono certificati secondo lo *standard di sicurezza informatica ETSI EN 303 645*. ETSI sta per European Telecommunications Standards Institute (Istituto europeo per gli standard di telecomunicazione). I requisiti riguardano i dispositivi, incluso il supporto per funzionalità di sicurezza basate su hardware, come l'archiviazione sicura delle chiavi, e funzionalità di sicurezza predefinite, come l'attivazione predefinita di HTTPS e l'assenza di password predefinite. Un altro aspetto riguarda la gestione del ciclo di vita, come la disponibilità di un periodo di supporto ben definito per gli aggiornamenti di sicurezza del dispositivo. Altri comprendono una metodologia per ridurre il rischio di vulnerabilità nello sviluppo software, policy trasparenti di gestione delle vulnerabilità e l'adozione delle best practice nel trattamento dei dati personali. Questi requisiti tengono in considerazione le best practice del settore, contribuendo a garantire che i prodotti certificati abbiano un livello di sicurezza di base durante l'intero ciclo di vita. Lo standard si allinea strettamente con il Cybersecurity Resilience Act (Legge dell'UE sulla resilienza informatica) dell'UE, la direttiva sulle apparecchiature radio dell'UE e altri standard e legislazioni di tutto il mondo.

4.8 Formazione e orientamento

Axis fornisce al personale, ai partner e ai clienti informazioni e corsi sulle best practice di cybersecurity. Ad esempio:

- Sensibilizzazione e formazione sulla sicurezza interna: Axis ha sviluppato un programma di sensibilizzazione alla sicurezza per formare costantemente il personale, in modo che sappia evitare e ridurre le minacce alla sicurezza all'interno della società. Questo corso è obbligatorio per tutto il personale Axis. A seconda del ruolo e delle responsabilità organizzative del singolo individuo, agli sviluppatori e ai proprietari dei sistemi viene offerta una formazione aggiuntiva in materia di sicurezza.
- *Formazione presso la Axis Academy*: i corsi di formazione disponibili per i clienti comprendono un corso online sulla cybersecurity e sull'*approccio di Axis a questo tema*.
- *Hardening Guide* disponibili online per:
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Switch di rete Axis*

- *AXIS OS Security Scanner Guide*: Axis consiglia di eseguire scansioni di sicurezza dei dispositivi Axis per verificare se sono affetti da vulnerabilità o configurazioni deboli. La AXIS OS Security Scanner Guide spiega come rimediare a determinati risultati di scansione e descrive i "falsi positivi" più comuni.
- *AXIS OS Forensic Guide*: questa guida offre consigli tecnici a chi conduce analisi forensi sui dispositivi Axis in caso di attacco alla rete e all'infrastruttura IT in cui è installato un dispositivo Axis.

Per ulteriori informazioni su Axis e la cybersecurity, visita il *portale Axis sulla cybersecurity*.

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