DOCUMENTO TÉCNICO

NIS 2

Junho 2024

Índice

1 Introdução

1.1 O que é a NIS 2?

A NIS 2 é uma diretiva da UE que deve ser transposta para a legislação nacional de cada Estado-Membro da UE até 17 de outubro de 2024. A NIS 2 tem como objetivo alcançar um elevado nível comum de cibersegurança em toda a UE, a fim de promover a segurança da região e o funcionamento eficaz da sua economia e sociedade. Esta diretiva obriga a que as entidades que prestam serviços essenciais e importantes em setores-chave da sociedade desenvolvam capacidades de cibersegurança, atenuem as ameaças às redes e aos sistemas de informação, assegurem a continuidade dos serviços em caso de incidentes e comuniquem os incidentes de segurança às autoridades competentes. Desta forma, requer que os Estados-Membros adotem estratégias nacionais de cibersegurança e criem entidades, incluindo entidades de gestão de crises cibernéticas e equipas de resposta a incidentes de segurança informática. Define as medidas de gestão dos riscos de cibersegurança, bem como as medidas de execução. As consequências da não conformidade por parte das entidades essenciais e importantes incluem multas pesadas e ramificações legais para as equipas de gestão.

Para mais informações, visite:
eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 Quem é afetado pela NIS 2?

A NIS 2 afeta todas as entidades que prestam serviços **essenciais** ou **importantes** para a economia e a sociedade europeias, incluindo empresas e fornecedores.

1.2.1 Diretamente afetados

Entidades essenciais – Energia, transportes, banca/finanças, saúde, água potável, águas residuais, infra-estruturas digitais, administração pública, espaço

Entidades importantes – Serviços postais, gestão de resíduos, produtos químicos, produtos alimentares, fabrico (por exemplo, dispositivos médicos, equipamento elétrico e de transporte), fornecedores digitais (por exemplo, comércio online, motores de busca, redes sociais), organismos de investigação

Autoridades nacionais competentes – As Autoridades nacionais competentes são designadas pelos Estados-Membros da UE para supervisionar a aplicação e o cumprimento da diretiva NIS 2 nos respetivos países.

1.2.2 Indiretamente afetados

Fornecedores e distribuidores – A diretiva NIS 2 afeta indiretamente os fornecedores, os distribuidores e os prestadores de serviços externos que fornecem serviços essenciais ou serviços digitais a entidades essenciais e importantes. Estas empresas precisam de garantir a segurança dos seus produtos e serviços e podem estar sujeitas a requisitos contratuais de cibersegurança por parte dos seus clientes.

Utilizadores de serviços essenciais e de serviços digitais – Embora não sejam diretamente regulamentados pela diretiva NIS 2, os utilizadores de serviços essenciais e de serviços digitais beneficiam das melhores práticas de cibersegurança e das capacidades de resposta a incidentes por ela exigidas. Isto aumenta indiretamente a segurança e a fiabilidade dos serviços em que confiam.

2 Requisitos da diretiva NIS 2

2.1 Para entidades essenciais e importantes

Medidas de segurança – Aplicar medidas de segurança adequadas para gerir os riscos e garantir a segurança das respetivas redes e sistemas de informação. Estas medidas devem basear-se em avaliações de risco e nas melhores práticas.

Relatório de incidentes – Comunicar às autoridades competentes os incidentes significativos que possam afetar de forma significativa a segurança das suas redes e sistemas de informação. A comunicação atempada é essencial para coordenar as respostas e atenuar possíveis danos.

Gestão de riscos – Efetuar avaliações de risco para identificar possíveis ameaças e vulnerabilidades e tomar medidas para mitigar esses riscos.

Cooperação com as autoridades competentes – Cooperar com as autoridades competentes designadas pelos Estados-Membros da UE. Isto inclui fornecer as informações necessárias e dar acesso aos sistemas para efeitos de controlo regulamentar e de resposta a incidentes.

Planeamento de resposta a incidentes – Desenvolver e manter planos de resposta a incidentes para responder eficazmente a incidentes de cibersegurança. Estes planos devem definir procedimentos para a deteção, comunicação e atenuação de incidentes.

Segurança das cadeias de abastecimento – Proteger as cadeias de abastecimento, incluindo vendedores e fornecedores externos, para garantir a resiliência global da rede e dos sistemas de informação.

Monitorização contínua – Implementar a monitorização e a auditoria contínuas da rede e dos sistemas de informação para detetar e responder a ameaças e vulnerabilidades em tempo real.

3 Impacto nos fornecedores

Os fornecedores podem apoiar as entidades NIS 2 cumprindo os seguintes requisitos:

Segurança desde a conceção – Os fabricantes de dispositivos IoT devem incorporar funcionalidades de segurança nos seus dispositivos desde a fase de conceção, garantindo que a segurança é parte integrante do produto.

Atualizações e correções regulares – Os fabricantes devem fornecer regularmente atualizações e correções de segurança para resolver as vulnerabilidades dos seus dispositivos IoT.

Autenticação e autorização – Os dispositivos IoT devem utilizar mecanismos de autenticação fortes e controlos de autorização adequados para impedir o acesso não autorizado.

Encriptação de dados – A transmissão e o armazenamento de dados pelos dispositivos IoT devem ser encriptados para proteger as informações sensíveis de possível interceção ou acesso por partes não autorizadas.

Relatório de incidentes – Os fabricantes devem comunicar quaisquer incidentes ou violações de segurança significativos relacionados com os seus dispositivos IoT às autoridades competentes e, potencialmente, aos consumidores ou clientes.

Considerações relativas a privacidade – Os dispositivos IoT que efetuam o tratamento de dados pessoais devem cumprir os regulamentos de proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (RGPD), para além do NIS 2.

Segurança da cadeia de abastecimento – É necessário garantir a segurança de toda a cadeia de abastecimento, desde os fornecedores de componentes até aos clientes, para evitar a introdução de vulnerabilidades de segurança em qualquer ponto do processo de produção.

4 A resposta Axis

De seguida, apresentamos-lhe a forma como a Axis, enquanto fornecedor, cumpre os requisitos das entidades NIS 2:

4.1 Segurança desde a conceção

A segurança desde a conceção é a abordagem que adotamos para garantir que as considerações e atividades de segurança são realizadas como parte integrante da conceção e do desenvolvimento dos produtos, para reduzir o risco de vulnerabilidades e garantir que são predefinidas configurações de segurança robustas nos produtos. Na Axis, o princípio da segurança desde a conceção aplica-se tanto a software como a hardware e inclui os seguintes elementos principais:

- *Axis Security Development Model (ASDM)*: O ASDM é uma estrutura de ferramentas e processos definidos que garante que as considerações de segurança são parte integrante do desenvolvimento do software. As atividades incluem a realização de avaliações de risco, modelação de ameaças, testes de invasão, análise de vulnerabilidades, gestão de incidentes, bem como um programa de recompensa por deteção de erros. Os programadores de software da Axis usam o ASDM para garantir que a segurança é incorporada no desenvolvimento do software para reduzir o risco de lançamento de software com vulnerabilidades.
- *Programa de recompensa por deteção de erros*: A Axis apoia um programa privado de recompensa por deteção de erros que reforça os esforços da empresa para identificar, corrigir e divulgar proativamente as vulnerabilidades do AXIS OS, o sistema operativo baseado em Linux presente em grande parte dos produtos Axis. Reforça o compromisso da Axis de estabelecer relações profissionais com investigadores de segurança externos e hackers éticos.
- *Lista de materiais de software (SBOM)*: A Axis disponibiliza uma SBOM para o AXIS OS, o sistema operativo baseado em Linux utilizado em grande parte dos dispositivos Axis. Esta lista fornece aos investigadores de segurança, autoridades e clientes informações sobre os componentes de software que compõem o AXIS OS. É particularmente útil para os especialistas em avaliação de vulnerabilidades e análise de ameaças, e é uma demonstração do compromisso da Axis para com a transparência na cibersegurança.
- *Predefinições de segurança do AXIS OS*: Os dispositivos com as versões mais recentes do AXIS OS estão pré-configurados no estado de fábrica com o seguinte: nenhuma palavra-passe predefinida; HTTP e HTTPS ativados; segurança de integração e comunicações com IEEE 802.1X/802.1AR/802.1AE ativadas por predefinição; protocolos menos seguros desativados. Mais informações sobre os controlos de proteção predefinidos *aqui*.
- *Axis Edge Vault*: Integrado nos dispositivos Axis, o Axis Edge Vault é uma plataforma de segurança baseada em hardware que inclui funcionalidades que salvaguardam a integridade dos produtos de rede Axis e que permitem executar operações seguras com base em chaves criptográficas. Proporciona proteção da cadeia de abastecimento com arranque seguro e OS assinado, identidade de dispositivo fiável com a ID exclusiva de dispositivo Axis incorporada para provar a origem do dispositivo, armazenamento seguro de chaves para armazenamento protegido contra adulteração de informações criptográficas, e deteção de adulteração de vídeo com vídeo assinado.

4.2 Atualizações e correções regulares

A Axis fornece atualizações de software para resolver, entre outras coisas, as vulnerabilidades de segurança recém-descobertas nos seus produtos de hardware e software. A Axis disponibiliza também ferramentas de gestão de dispositivos para facilitar aos clientes a atualização do software dos dispositivos Axis. As novas versões do AXIS OS para dispositivos conectados são destacadas no AXIS Companion, AXIS Camera Station e software de gestão de vídeo de parceiros, como o Milestone XProtect® e o Genetec™ Security Center, bem como as ferramentas de gestão de dispositivos Axis. Para além disso, a Axis fornece um serviço de notificações de segurança que pode ser subscrito por qualquer pessoa. Seguem-se informações mais detalhadas.

- *AXIS OS*: A Axis oferece duas alternativas principais para manter o software do dispositivo atualizado: a via ativa e a via de suporte a longo prazo (LTS). A via ativa permite aceder às mais recentes características e funcionalidades de ponta, bem como a correções de erros e resolução de problemas de segurança. As vias de suporte a longo prazo (LTS) do software maximizam a estabilidade fornecendo apenas correções de erros e resolução de problemas de segurança, uma vez que o foco está em manter um sistema de terceiros bem integrado.
- Ferramentas de gestão de dispositivos: O *AXIS Device Manager* e o *AXIS Device Manager Extend* são ferramentas que permitem aos clientes manter o software dos dispositivos Axis atualizado com as mais recentes correções de erros e de segurança.

  Para maior eficiência na configuração e gestão dos dispositivos Axis a nível local, o AXIS Device Manager permite processar tarefas de segurança em lotes, como a gestão de credenciais de dispositivos, a implementação de certificados, a desativação de serviços não utilizados e a atualização do AXIS OS.

  O AXIS Device Manager Extend disponibiliza um painel de controlo agregado que reúne informações sobre todos os seus dispositivos e locais numa única aplicação de fácil utilização. Será informado quando existirem atualizações de software do dispositivo disponíveis, podendo efetuar atualizações em massa e outras tarefas em escala. Receberá também recomendações para produtos de substituição. As atividades são totalmente rastreáveis, sendo possível exportar todas as informações dos dispositivos do sistema para fins de relatório ou auditoria.
- *Serviço de notificações de segurança Axis*: Este serviço, que a Axis incentiva a subscrever, fornece aos subscritores notificações atempadas sobre vulnerabilidades e incidentes de segurança.

4.3 Autenticação e autorização

Para evitar o acesso não autorizado e aumentar a segurança geral dos dispositivos Axis, a Axis suporta:

- Direitos de acesso à gestão de dispositivos com base nas funções (Administrador/Operador/Visualizador) e a possibilidade de centralizar a autenticação/autorização, ligando os dispositivos Axis a integrações dispositivos padronizadas de TI *Active Directory Federation Service* (ADFS) . (O ADFS é um componente de software desenvolvido pela Microsoft para fornecer o serviço de autorização Single Sign-On (SSO) aos utilizadores dos sistemas operativos Windows Server. O ADFS permite que os utilizadores, para além das fronteiras organizacionais, acedam a aplicações nos sistemas operativos Windows Server utilizando um único conjunto de credenciais de início de sessão.)
- Tecnologias que facilitam as *redes zero-trust* . Nas versões mais recentes do AXIS OS, essas tecnologias incluem o IEEE 802.1X, juntamente com ID de dispositivos Axis compatíveis com IEEE 802.1AR, para integração automatizada e segura de dispositivos numa rede IEEE 802.1X, e IEEE 802.1AE (MACsec) para a encriptação automática de comunicações de dados.

4.4 Encriptação de dados

Para proteger informações confidenciais relativamente a interceção ou acesso não autorizado, os produtos Axis suportam:

- HTTPS, onde todas as comunicações de dados suportam a norma TLS 1.2 ou mais recentes. A ligação de transmissão de vídeo em sequência entre o servidor do software de gestão de vídeo AXIS Camera Station e o cliente é encriptada com AES-256.
- *IEEE 802.1AE (MACsec)* para encriptação automática da comunicação de dados.
- Transmissão de vídeo em sequência por RTP, também chamado de SRTP/RTSPS (a partir do AXIS OS 7.40). O SRTP/RTSPS usa um método seguro de transmissão criptografado de ponta a ponta para garantir que apenas clientes autorizados recebam a sequência de vídeo do dispositivo Axis.
- *Encriptação do armazenamento descentralizado* (cartão SD)
- *Exportação encriptada por palavra-passe do registo descentralizado* (cartão SD, partilha de rede), a partir do AXIS OS 10.10. Isto significa que é possível exportar uma gravação encriptada por palavra-passe, acrescentando a possibilidade de partilhar com segurança dados de vídeo sensíveis sem necessidade de encriptar manualmente as gravações exportadas.

4.5 Relatório de incidentes

A Axis fornece relatórios de incidentes de segurança ou vulnerabilidades descobertas nos respetivos produtos e serviços.

- A Axis é uma Autoridade de Numeração de Vulnerabilidades e Exposições Comuns (CVE). Isto significa que a Axis segue, com total transparência, as melhores práticas do setor em termos de gestão e resposta às vulnerabilidades descobertas nos respetivos produtos e serviços para minimizar o risco de exposição dos clientes. A Axis também pode atribuir números CVE a vulnerabilidades recém-descobertas e comunicá-las ao site *www.cve.org*. A *política de gestão de vulnerabilidades* da Axis está publicada em axis.com.
- Qualquer pessoa pode subscrever *aqui* para receber uma notificação de segurança da Axis.
- Nas novas versões do AXIS OS são incluídas correções de segurança e de erros. A disponibilidade de software atualizado de dispositivos também é destacada no AXIS Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend e VMS de terceiros, como o Milestone XProtect e o Genetec Security Center.
- A Axis tem como compromisso a transparência relativamente a ciberataques relacionados com a empresa e comunicará esses incidentes de acordo com as diretrizes fornecidas pelas autoridades suecas competentes.

4.6 Considerações relativas a privacidade

A Axis publica a sua *política de privacidade* e declaração online, onde descreve quais os dados pessoais que são recolhidos (por exemplo, a partir de uma conta online no My Axis) e a forma como são utilizados.

A Axis publicou igualmente as suas *diretrizes e práticas de cibersegurança* relativas ao seu sistema de gestão de segurança da informação, que possui a certificação ISO/IEC 27001. O âmbito da certificação ISO/IEC 27001 da Axis abrange o desenvolvimento e as operações de infra-estruturas e serviços internos de

TI. A ISO 27001 é uma norma reconhecida internacionalmente que fornece orientações sobre a forma de proteger e gerir as informações de uma organização através de uma gestão eficaz dos riscos.

A conformidade com a norma *ISO/IEC 27001* demonstra que a Axis utiliza processos reconhecidos internacionalmente e as melhores práticas para gerir a sua infraestrutura de informação interna e os sistemas que suportam e fornecem os seus serviços a clientes e parceiros.

A Axis também ajuda os seus clientes a lidar com questões de privacidade na vigilância, no que diz respeito à captura de vídeo e áudio. As soluções incluem:

- Máscara de privacidade estática nas câmaras Axis e máscara de privacidade dinâmica com a aplicação do software *AXIS Live Privacy Shield*
- Análises descentralizadas, tais como a aplicação *AXIS People Counter* ou *AXIS P8815-2 3D People Counter*, que apenas capturam e armazenam dados numéricos estatísticos — não são processados dados pessoais identificáveis
- *Câmaras térmicas*
- *Produtos de radar*
- Ferramenta de edição de vídeo no *AXIS Camera Station* para mascarar objetos ou áreas não significativas
- *Capacidades de áudio desativadas por defeito* nos produtos de videovigilância Axis

Para mais informações sobre soluções de privacidade, aceda a *axis.com/solutions/privacy-in-surveillance*

4.7 Segurança da cadeia de abastecimento

Proteger a cadeia de abastecimento, desde os fornecedores de componentes até aos clientes, é importante para evitar a introdução de vulnerabilidades de segurança.

No que diz respeito à segurança cibernética, a Axis adota uma abordagem de *ciclo de vida do produto*. Estamos empenhados em mitigar os riscos, não só ao longo de toda a cadeia de abastecimento, desde o componente inicial até ao produto acabado, mas também durante a distribuição e implementação, bem como nas fases de assistência e desativação.

Veja a seguir algumas das formas que a Axis aborda a segurança da cadeia de abastecimento:

- A Axis adquire componentes críticos diretamente de fornecedores estratégicos. Trabalhamos em estreita colaboração com os nossos parceiros de fabrico. Os processos de produção são monitorizados e os dados são partilhados com a Axis 24 horas por dia, 7 dias por semana, permitindo uma análise em tempo real e total transparência. Saiba mais sobre a *segurança da cadeia de abastecimento Axis*.
- Segurança integrada no dispositivo através do Axis Edge Vault, o qual protege a integridade dos dispositivos Axis através das seguintes funcionalidades:
  - **Signed OS**: Assegura que o AXIS OS instalado é genuinamente da Axis. Garante também que qualquer novo AXIS OS destinado a ser instalado no dispositivo também possui a assinatura Axis.
  - **Arranque seguro**: Permite que o dispositivo verifique se o sistema operativo tem uma assinatura Axis. Se o OS não for autorizado ou tiver sido alterado, o processo de arranque é interrompido e o dispositivo deixa de funcionar. A combinação de OS assinado, arranque seguro e a execução de uma reposição de fábrica do dispositivo oferece proteção contra tentativas de modificação durante o envio de um dispositivo.

- **A ID de dispositivo Axis** é compatível com a norma IEEE 802.1AR, que permite identificar e integrar de forma segura os dispositivos numa rede. A ID de dispositivo Axis é armazenada no repositório de chaves seguro do dispositivo (elemento seguro, TPM, TEE).
- **O sistema de ficheiros encriptados** protege a configuração específica do cliente e as informações armazenadas no sistema de ficheiros relativamente a extração ou adulteração quando o dispositivo não está a ser utilizado, como, por exemplo, quando em trânsito de um integrador de sistemas para um cliente.
- Além disso, o suporte da Axis para **vídeo assinado** permite que os visualizadores verifiquem se o vídeo exportado de um dispositivo foi adulterado ou não. Isto é particularmente importante no caso de uma investigação ou processo judicial. Para mais informações, consulte *axis.com/solutions/edge-vault*.

- É fornecida uma soma de verificação para as transferências de software provenientes de axis.com. A soma de verificação permite verificar a integridade de um ficheiro.
- Certificação ETSI: Mais de 150 produtos Axis com o AXIS OS 11 ou superior possuem certificação de acordo com o padrão de segurança cibernética *ETSI EN 303 645*. ETSI significa European Telecommunications Standards Institute (Instituto Europeu de Normas de Telecomunicações). Os requisitos abrangem os próprios dispositivos, incluindo o suporte de funcionalidades de segurança físicas, como o armazenamento seguro de chaves, e funcionalidades de segurança predefinidas, como a ativação predefinida de HTTPS e a ausência de palavras-passe predefinidas. Outro aspeto envolve a gestão do ciclo de vida, como a definição de um período de assistência para as atualizações de segurança dos dispositivos. Outros incluem a existência de uma metodologia para reduzir o risco de vulnerabilidades no desenvolvimento de software, a existência de uma política transparente de gestão de vulnerabilidades e de utilização das melhores práticas no tratamento de dados pessoais. Estes requisitos têm em consideração as melhores práticas do setor que ajudam a garantir que os produtos certificados têm por base um nível mínimo de segurança ao longo de todo o ciclo de vida. A norma está estreitamente alinhada com o Regulamento de Ciber-resiliência da UE, com a Diretiva de Equipamentos de Rádio da UE e com outras normas e legislação de todo o mundo.

4.8 Formação e orientação

A Axis proporciona ao seu pessoal, parceiros e clientes informações e formação sobre as melhores práticas de cibersegurança. Estas incluem:

- Sensibilização e formação em matéria de segurança interna: A Axis desenvolveu um programa de sensibilização para a segurança para proporcionar formação contínua aos seus funcionários no sentido de evitar e atenuar as ameaças à segurança da organização. Esta formação de sensibilização é obrigatória para todo os colaboradores da Axis. Consoante a função e as responsabilidades organizacionais de cada indivíduo, é fornecida formação de segurança adicional aos programadores e proprietários de sistemas.
- *Formação na Axis Academy*: Disponíveis para os clientes, os cursos de formação incluem um curso online sobre cibersegurança e a *abordagem da Axis a este tema*.
- *Guias de proteção* disponíveis online para:
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Switches de rede Axis*

- *AXIS OS Security Scanner Guide*: A Axis recomenda a execução de análises de segurança aos dispositivos Axis para verificar se estão afetados por vulnerabilidades ou por má configuração. O AXIS OS Security Scanner Guide oferece recomendações sobre a forma de solucionar determinados resultados de análise e descreve os "falsos positivos" mais comuns.
- *AXIS OS Forensic Guide*: Este guia contém conselhos técnicos para a análise forense de dispositivos Axis no caso de um ataque de cibersegurança à rede circundante e à infraestrutura de TI onde existe um dispositivo Axis instalado.

Para obter mais informações sobre a Axis e a cibersegurança, visite o *portal de cibersegurança da Axis*.

T10210486/PT_PT/M3.3/2406

Acerca da Axis Communications

A Axis contribui para um mundo mais inteligente e mais seguro ao criar soluções para melhorar a segurança e o desempenho empresarial. Na sua qualidade de empresa de tecnologia de rede e líder do setor, a Axis disponibiliza soluções de videovigilância, controlo de acessos, sistemas de intercomunicação e áudio. Estas soluções são melhoradas através de aplicações de análise inteligentes e suportadas por uma formação de alta qualidade.

A Axis possui cerca de 4000 empregados dedicados em mais de 50 países e colabora com parceiros tecnológicos e de integração de sistemas a nível mundial com o objetivo de proporcionar soluções para os clientes. A Axis foi fundada em 1984 e tem sede em Lund, na Suécia