WHITE PAPER

NIS 2

Junho 2024

Sumário

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 alto nível comum de segurança cibernética em toda a UE, a fim de contribuir para a segurança da região e o funcionamento eficaz de sua economia e sociedade. Ela exige que as entidades que prestam serviços essenciais e importantes em setores chave da sociedade desenvolvam recursos de segurança cibernética, mitiguem as ameaças aos sistemas em rede e de informação, garantam a continuidade dos serviços diante de incidentes e comuniquem incidentes de segurança às autoridades competentes. Ela exige que os estados membros adotem estratégias nacionais de segurança cibernética e estabeleçam autoridades, incluindo autoridades de gerenciamento de crises cibernéticas e equipes de resposta a incidentes de segurança de computadores. Ela descreve medidas de gerenciamento de riscos de segurança cibernética, bem como medidas de aplicação. As consequências da não conformidade de entidades essenciais e importantes podem incluir multas pesadas e implicações legais para as equipes de gerenciamento.

Para obter mais informações, acesse:
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 fornecem serviços **essenciais** ou **importantes** à economia e à sociedade europeia, incluindo empresas e fornecedores.

1.2.1 Diretamente afetados

Entidades essenciais – Energia, transportes, atividades bancárias e financeiras, saúde, água potável, águas residuais, infraestrutura digital, administração pública, espaço

Entidades importantes – Serviços postais, gerenciamento de resíduos, produtos químicos, alimentos, manufatura (por exemplo, dispositivos médicos, equipamentos elétricos e de transporte), provedores digitais (por exemplo, mercados on-line, mecanismos de busca, sistemas em redes sociais), organizações de pesquisa

Autoridades nacionais competentes – As autoridades nacionais competentes são designadas pelos estados membros da UE para supervisionar a implementação e a aplicação da NIS 2 em seus respectivos países.

1.2.2 Indiretamente afetados

Distribuidores e fornecedores – A NIS 2 afeta indiretamente distribuidores, fornecedores e prestadores de serviços terceirizados que fornecem serviços essenciais ou serviços digitais a entidades essenciais e importantes. Essas empresas precisam garantir a segurança de seus produtos e serviços e podem estar sujeitas aos requisitos contratuais de segurança cibernética de seus clientes.

Usuários de serviços essenciais e serviços digitais – Embora não sejam diretamente regulamentados pela NIS 2, os usuários de serviços essenciais e serviços digitais se beneficiam das práticas aprimoradas de segurança cibernética e dos recursos de resposta a incidentes exigidos pela diretiva. Isso aumenta indiretamente a segurança e a confiabilidade dos serviços dos quais eles dependem.

2 Requisitos da NIS 2

2.1 Para entidades essenciais e importantes

Medidas de segurança – Implementar medidas de segurança adequadas para gerenciar riscos e garantir a segurança em sua rede e em seus sistemas de informação. Essas medidas devem se basear em avaliações de risco e melhores práticas.

Relatórios de incidentes – Comunicar às autoridades competentes incidentes significativos que possam ter um impacto substancial na segurança de suas redes e nos sistemas de informação. A comunicação em tempo hábil é essencial para coordenar as respostas e reduzir possíveis danos.

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

Cooperação com autoridades competentes – Cooperar com autoridades competentes designadas pelos estados membros da UE. Isso inclui fornecer as informações necessárias e o acesso aos sistemas para fins de supervisão regulatória e resposta a incidentes.

Planejamento de resposta a incidentes – Desenvolver e manter planos de resposta a incidentes para responder a incidentes de segurança cibernética de forma eficaz. Esses planos devem descrever procedimentos para detecção, comunicação e mitigação de incidentes.

Segurança de cadeias de suprimentos – Proteger cadeias de suprimentos, incluindo distribuidores e fornecedores terceirizados, para garantir a resiliência geral dos sistemas em rede e de informações.

Monitoramento contínuo – Implementar o monitoramento e a auditoria contínuos dos sistemas em rede e de informações para detectar e responder a ameaças e vulnerabilidades em tempo real.

3 Impacto em fornecedores

Os fornecedores podem oferecer suporte a entidades NIS 2 atendendo aos seguintes requisitos:

Segurança desde a concepção – Fabricantes de dispositivos IoT devem incorporar recursos de segurança em seus dispositivos desde a fase de projeto, garantindo que a segurança seja parte integrante do produto.

Atualizações e patches regulares – Os fabricantes devem fornecer atualizações e patches de segurança regulares para resolver as vulnerabilidades em seus dispositivos IoT.

Autenticação e autorização – Dispositivos IoT devem empregar mecanismos de autenticação fortes e controles de autorização adequados para impedir o acesso não autorizado.

Criptografia de dados – A transmissão e o armazenamento de dados por dispositivos IoT devem ser criptografados para proteger as informações confidenciais contra interceptação ou acesso por partes não autorizadas.

Relatórios de incidentes – Fabricantes devem relatar quaisquer incidentes ou violações de segurança significativos relacionados a seus dispositivos IoT às autoridades pertinentes e, potencialmente, a consumidores ou clientes.

Considerações sobre privacidade – Os dispositivos de IoT que processam dados pessoais devem estar em conformidade com os regulamentos de proteção de dados, como o GDPR (Regulamento Geral de Proteção de Dados), além da NIS 2.

Segurança da cadeia de suprimentos – Deve-se exigir a garantia da segurança de toda a cadeia de suprimentos, desde fornecedores de componentes até clientes, para evitar que vulnerabilidades de segurança sejam introduzidas em qualquer ponto do processo de produção.

4 A resposta da Axis

Veja a seguir como a Axis, como fornecedora, atende aos requisitos das entidades NIS 2:

4.1 Segurança desde a concepção

Segurança desde a concepção é a abordagem adotada para garantir que as considerações e as atividades de segurança sejam realizadas como parte integrante do projeto e do desenvolvimento do produto, com o fim de reduzir o risco de vulnerabilidades e garantir que configurações robustas de segurança sejam definidas nos produtos por padrão. Na Axis, o princípio de segurança desde a concepção se aplica a software e hardware e abrangem os principais elementos a seguir:

- *Axis Security Development Model (ASDM)*: o ASDM é uma estrutura de processos e ferramentas definidos que garantem que considerações de segurança sejam parte integrante do desenvolvimento de software. As atividades incluem a realização de avaliações de risco, modelagem de ameaças, testes de penetração, varredura de vulnerabilidades, gerenciamento de incidentes, bem como um programa de recompensas para a identificação de bugs. Os desenvolvedores de software da Axis usam o ASDM para garantir que a segurança seja incorporada ao desenvolvimento de software para reduzir o risco de versões de software com vulnerabilidades.
- *Programa de recompensas para a identificação de bugs*: A Axis apoia um programa privado de recompensas para a identificação de bugs que reforça os esforços da empresa para identificar, corrigir e divulgar proativamente as vulnerabilidades do SO AXIS, o sistema operacional baseado em Linux que aciona a maioria dos produtos Axis. Isso fortalece o compromisso da Axis de construir relacionamentos profissionais com pesquisadores de segurança externos e hackers éticos.
- *Lista de materiais de software (SBOM)*: a Axis fornece uma SBOM para o SO AXIS, o sistema operacional baseado em Linux usado na maioria dos dispositivos Axis. Ela oferece a pesquisadores de segurança, autoridades e clientes insights sobre os componentes de software que compõem o SO AXIS. É particularmente útil para quem que se especializa em avaliação de vulnerabilidades e análise de ameaças e é uma demonstração do compromisso da Axis com a transparência na segurança cibernética.
- *Configurações de segurança padrão do SO AXIS*: Os dispositivos que executam as versões mais recentes do SO AXIS são pré-configurados nos padrões de fábrica com o seguinte: nenhuma senha padrão; HTTP e HTTPS ativados; integração e comunicação seguras com IEEE 802.1X/802.1AR/802.1AE ativadas por padrão; protocolos menos seguros desativados. Mais informações sobre controles de proteção padrão estão disponíveis *aqui*.
- *Axis Edge Vault*: Integrado nos dispositivos Axis, o Axis Edge Vault é uma plataforma de segurança baseada em hardware que inclui recursos que protegem a integridade dos produtos de rede da Axis e que possibilitam a execução de operações seguras com base em chaves criptográficas. Ele fornece proteção da cadeia de suprimentos com inicialização segura e sistema operacional assinado, identidade de dispositivo confiável com a ID de dispositivo Axis exclusiva integrada para comprovar a origem do dispositivo, armazenamento seguro de chaves para armazenamento protegido contra violação de informações criptográficas e detecção de violações de vídeo com vídeo assinado.

4.2 Atualizações e patches regulares

A Axis fornece atualizações de software para solucionar, entre outras coisas, vulnerabilidades de segurança recém-descobertas em seus produtos de hardware e software. A Axis também fornece ferramentas de gerenciamento de dispositivos para facilitar para o cliente manter atualizado o software de dispositivos Axis. As novas versões do SO AXIS para dispositivos conectados são destacadas no AXIS Companion, AXIS Camera Station e em softwares de gerenciamento de vídeo de parceiros, como o Milestone XProtect® e o Genetec™ Security Center, bem como nas ferramentas de gerenciamento de dispositivos Axis. Além disso, a Axis fornece um serviço de notificação de segurança que pode ser assinado por qualquer pessoa. Informações mais detalhadas são fornecidas abaixo.

- *SO AXIS*: a Axis oferece duas alternativas principais para manter o software do dispositivo atualizado: a trilha ativa e a trilha de suporte de longo prazo (LTS). A trilha ativa fornece acesso aos mais recentes recursos e funcionalidades de última geração, bem como correções de bugs e patches de segurança. O software nas trilhas de suporte de longo prazo (LTS) maximiza a estabilidade fornecendo apenas correções de bugs e patches de segurança, pois o foco é manter um sistema de terceiros bem integrado.
- Ferramentas de gerenciamento de dispositivos: o *AXIS Device Manager* e o *AXIS Device Manager Extend* são ferramentas que facilitam para o cliente manter atualizado o software de dispositivos Axis com os patches de segurança e as correções de bugs mais recentes.

  Para a configuração e o gerenciamento locais eficientes dos dispositivos Axis, o AXIS Device Manager possibilita o processamento em lote de tarefas de segurança, como o gerenciamento de credenciais de dispositivos, a implantação de certificados, a desativação de serviços não utilizados e a atualização do sistema operacional AXIS (SO AXIS).

  O AXIS Device Manager Extend fornece um painel agregado que reúne informações sobre todos os seus dispositivos e locais em um único aplicativo fácil de usar. Você será informado quando houver atualizações de software do dispositivo disponíveis e poderá realizar atualizações em massa e outras tarefas em escala. Você também receberá recomendações de produtos de reposição. As atividades são totalmente rastreáveis e é possível exportar todas as informações do dispositivo do sistema para fins de relatório ou auditoria.
- *Axis security notification service*: Esse serviço, cuja inscrição a Axis incentiva as pessoas a fazer, fornece aos assinantes notificações oportunas sobre incidentes e vulnerabilidades de segurança.

4.3 Autenticação e autorização

Para impedir o acesso não autorizado e aumentar a segurança geral do dispositivo Axis, a Axis oferece suporte a:

- Direitos de acesso de gerenciamento de dispositivos de acesso baseados em função (Administrador/Operador/Visualizador) e a possibilidade de centralizar a autenticação/autorização conectando dispositivos Axis a integrações 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) a usuários em sistemas operacionais Windows Server. O ADFS permite que usuários além dos limites organizacionais acessem aplicativos em sistemas operacionais Windows Server usando um único conjunto de credenciais de login).
- Tecnologias que facilitam o *sistema em rede de confiança zero* . Nas versões mais recentes do SO AXIS, essas tecnologias incluem IEEE 802.1X, juntamente com IDs de dispositivos Axis compatíveis com IEEE 802.1AR, para integração automatizada e segura de dispositivos em uma rede IEEE 802.1X, e IEEE 802.1AE (MACsec) para criptografia automática de comunicação de dados.

4.4 Criptografia de dados

Para proteger informações confidenciais de interceptação ou acesso por pessoas não autorizadas, os produtos Axis oferecem suporte:

- HTTPS, em que toda a comunicação de dados é compatível com TLS 1.2 ou padrões mais recentes. A conexão de streaming de vídeo entre o servidor do software de gerenciamento de vídeo AXIS Camera Station e o cliente é criptografada com AES-256.
- *IEEE 802.1AE (MACsec)* para criptografia automática de comunicação de dados.
- O streaming de vídeo seguro por RTP, também chamado de SRTP/RTSPS (a partir do SO AXIS 7.40), usa um método de transporte criptografado seguro de ponta a ponta para garantir que somente clientes autorizados recebam o streaming de vídeo do dispositivo Axis.
- *Criptografia de armazenamento de borda* (cartão SD)
- *Exportação de gravação de borda criptografada por senha* (cartão SD, compartilhamento de rede), a partir do SO AXIS 10.10. Isso significa que é possível exportar uma gravação criptografada por senha, adicionando a possibilidade de compartilhar com segurança dados de vídeo confidenciais sem a necessidade de criptografar manualmente as gravações exportadas.

4.5 Relatórios de incidentes

A Axis fornece relatórios de incidentes de segurança ou vulnerabilidades descobertas em nossos produtos e serviços.

- A Axis é uma Autoridade de numeração de vulnerabilidades e exposições comuns (CVE). Isso significa que a Axis segue as melhores práticas do setor no gerenciamento e na resposta - com transparência - às vulnerabilidades descobertas em nossos 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 no site *www.cve.org*. A *política de gerenciamento de vulnerabilidades* da Axis é publicada em axis.com.
- Qualquer pessoa pode se inscrever *aqui* para receber uma notificação de segurança da Axis.
- Patches de segurança e correções de bugs são implementados nas novas versões do SO AXIS. A disponibilidade de software de dispositivo atualizado 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 está comprometida com a transparência em relação a qualquer ataque cibernético relacionado à empresa e informará tais incidentes de acordo com as diretrizes fornecidas pelas autoridades suecas pertinentes.

4.6 Considerações sobre privacidade

A Axis publica sua *política de privacidade* e aviso on-line, onde descreve quais dados pessoais são coletados (por exemplo, de uma conta on-line no My Axis) e como eles são usados.

A Axis também publicou sua *estrutura e práticas de segurança cibernética* relacionadas a seu Sistema de Gerenciamento de Segurança da Informação, que é certificado pela ISO/IEC 27001. O escopo do certificado ISO/IEC 27001 da Axis abrange o desenvolvimento e as operações da infraestrutura e dos serviços internos

de TI. A ISO 27001 é uma norma reconhecida internacionalmente que fornece orientação sobre como proteger e gerenciar as informações de uma organização por meio de um gerenciamento de riscos eficaz.

A conformidade com a *ISO/IEC 27001* demonstra que a Axis usa processos reconhecidos internacionalmente e as melhores práticas para gerenciar sua infraestrutura e sistemas de informação internos que respaldam e fornecem seus serviços a clientes e parceiros.

A Axis também ajuda clientes a lidar com questões de privacidade no monitoramento com relação à captura de vídeo e áudio. As soluções incluem:

- Máscara de privacidade estática em câmeras Axis e máscara de privacidade dinâmica com o software aplicativo *AXIS Live Privacy Shield*
- Analíticos baseados em borda, como o aplicativo *AXIS People Counter* ou o *AXIS P8815-2 3D People Counter*, que apenas capturam e armazenam dados numéricos estatísticos - nenhuma informação pessoal identificável é processada
- *Câmeras térmicas*
- *Produtos de radar*
- Ferramenta de edição de vídeo no *AXIS Camera Station* para mascarar objetos ou áreas que não sejam de interesse
- *Recursos de áudio desativados por padrão* em produtos de videomonitoramento da Axis

Mais informações sobre soluções de privacidade estão disponíveis em *axis.com/solutions/privacy-in-surveillance*

4.7 Segurança da cadeia de suprimentos

A proteção da cadeia de suprimentos, de fornecedores de componentes a clientes, é importante para impedir a introdução de vulnerabilidades de segurança.

A Axis adota uma *abordagem de ciclo de vida* do produto ao abordar a segurança cibernética. Temos o compromisso de mitigar os riscos, não apenas em toda a cadeia de suprimentos, do nível do componente ao produto acabado, mas também durante a distribuição e a implementação, bem como nas fases de serviço e desativação.

A seguir mostramos algumas das maneiras pelas quais a Axis aborda a segurança da cadeia de suprimentos:

- A Axis adquire componentes críticos diretamente de fornecedores estratégicos. Trabalhamos em estreita colaboração com parceiros de fabricação. Os processos de fabricação são monitorados, e os dados pertinentes são compartilhados ininterruptamente com a Axis, permitindo análises em tempo real e garantindo transparência. Saiba mais sobre *segurança da cadeia de suprimentos da Axis*.
- Segurança de dispositivo integrada por meio do Axis Edge Vault, que protege a integridade de dispositivos Axis por meio dos seguintes recursos:
    - **Sistema operacional assinado**: garante que o SO AXIS instalado seja original da Axis. Ele também garante que qualquer novo SO AXIS destinado à instalação no dispositivo também seja assinado pela Axis.
    - **Inicialização segura**: ativa o dispositivo para verificar se o sistema operacional tem uma assinatura Axis. Se o sistema operacional não for autorizado ou tiver sido alterado, o processo de inicialização é interrompido e o dispositivo para de funcionar. A combinação de sistema operacional assinado,

inicialização segura e redefinição de fábrica do dispositivo oferece proteção contra tentativas de modificação durante o envio de um dispositivo.

- A **ID de dispositivo Axis** é compatível com IEEE 802.1AR, o que possibilita a identificação e a integração seguras de dispositivos em uma rede. A ID de dispositivo Axis é armazenada no repositório de chaves seguro do dispositivo (elemento seguro, TPM, TEE).
- O **Sistema de arquivos criptografados** protege as configurações e informações específicas do cliente armazenadas no sistema de arquivos contra extração ou violação quando elas estão armazenadas no sistema enquanto o dispositivo não está em uso, como ocorre quando o produto está em trânsito entre um integrador de sistemas e o cliente final, por exemplo.
- Além disso, o suporte da Axis para **vídeos assinados** permite ao visualizador verificar se o vídeo exportado de um dispositivo foi ou não violado. Isso é particularmente importante em investigações ou processos judiciais. Mais informações estão disponíveis em *axis.com/solutions/edge-vault*.

- Uma soma de verificação é fornecida para downloads de software do site axis.com. A soma de verificação ativa a verificação da integridade de um arquivo.
- Certificação ETSI: Mais de 150 produtos Axis que executam o SO AXIS 11 ou posterior são certificados pelo *padrão de segurança cibernética ETSI EN 303 645*. ETSI significa Instituto Europeu de Normas de Telecomunicações. Os requisitos abrangem os próprios dispositivos, incluindo suporte para recursos de segurança baseados em hardware, como armazenamento seguro de chaves, e recursos de segurança padrão, como HTTPS habilitado por padrão e sem senhas padrão. Outro aspecto envolve o gerenciamento do ciclo de vida, como ter um período de suporte definido para atualizações de segurança dos dispositivos. Outros fatores incluem ter uma metodologia para reduzir o risco de vulnerabilidades no desenvolvimento de software, ter uma política transparente de gestão de vulnerabilidades e apoiar as melhores práticas no tratamento de dados pessoais. Esses requisitos levam em consideração as melhores práticas do setor que ajudam a garantir que os produtos certificados tenham um nível mínimo de segurança de base durante todo o ciclo de vida. O padrão se alinha estreitamente com a Lei de Resiliência de Segurança Cibernética da UE, a Diretiva de Equipamentos de Rádio da UE e outras normas e legislações de todo o mundo.

4.8 Treinamento e orientação

A Axis fornece à equipe, aos parceiros e aos clientes informações e treinamento sobre melhores práticas de segurança cibernética. Entre elas:

- Conscientização e treinamento sobre segurança interna: a Axis desenvolveu um programa de conscientização de segurança que visa treinar continuamente nossos funcionários para evitar e mitigar ameaças à segurança na organização. Esse treinamento de conscientização é obrigatório para todos os funcionários da Axis. Dependendo da função e das responsabilidades organizacionais do indivíduo, é fornecido treinamento adicional de segurança para desenvolvedores e proprietários de sistemas.
- *Treinamento na Axis Academy*: disponíveis para os clientes, os cursos de treinamento incluem um curso on-line sobre segurança cibernética e a *abordagem da Axis sobre o assunto*.
- *Guias para aumento do nível de proteção* disponíveis on-line para:
  - *SO AXIS*
  - *AXIS Camera Station*
  - *Switches de rede Axis*

- *Guia do verificador de segurança do SO AXIS*: a Axis recomenda a execução de varreduras de segurança de dispositivos Axis para verificar configuração inadequada ou se foram afetados por vulnerabilidades. O Guia do Verificador de Segurança do SO AXIS oferece recomendações sobre como corrigir alguns resultados de verificações e descreve os "falsos positivos" mais comuns.
- *Guia forense do SO AXIS*: esse guia fornece orientações técnicas para a condução de análises forenses de dispositivos Axis em caso de ataque à segurança cibernética da rede e da infraestrutura de TI onde haja um dispositivo Axis instalado.

Para obter mais informações sobre a Axis e segurança cibernética, acesse o *Portal de segurança cibernética da Axis*.

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e seguro criando soluções para melhorar a segurança e o desempenho dos negócios. Como empresa de tecnologia de rede e líder do setor, a Axis oferece soluções em videomonitoramento, controle de acesso, intercomunicação e áudio. Nossas soluções são aprimoradas por aplicativos de análise inteligentes e apoiados por treinamento de alta qualidade.

A Axis tem cerca de 4.000 funcionários dedicados em mais de 50 países e colabora com parceiros de tecnologia e integração de sistemas em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e tem sede em Lund, Suécia