白皮书

NIS 2

六月 2024

目录

1 引言

1.1 什么是NIS 2?

NIS 2是欧盟的一项指令，应在2024年10月17日前转化为欧盟各成员国的国家立法。NIS 2旨在实现整个欧盟网络安全的高度共同化，以促进区域安全及其经济和社会的有效运作。它要求在社会关键部门提供基本和重要服务的实体建立网络安全能力，减轻对网络和信息系统的威胁，确保在面临事件时服务的连续性，并向有关当局报告安全事件。它要求成员国实施国家网络安全战略，并建立权威机构，包括网络危机管理机构和计算机安全事件应对小组。它概述了网络安全风险管理措施以及执行措施。基本和重要实体不合规的后果可能包括对管理团队的重罚和法律后果。

更多信息，请访问：*eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613*

1.2 NIS 2对谁有影响?

NIS 2影响为欧洲经济和社会提供**基本**或**重要**服务的实体，包括公司和供应商。

1.2.1 直接影响

基本实体 – 能源、交通、银行/金融、卫生、饮用水、废水处理、数字基础设施、公共管理、空间

重要实体 – 邮政服务、废物管理、化工、食品、制造业（如医疗设备、电气、运输设备）、数字供应商（如在线市场、搜索引擎、社交网络）、研究机构

国家主管机构 – 国家主管机构由欧盟成员国指定，负责监督NIS 2在各自国家的实施和执行情况。

1.2.2 间接影响

销售商和供应商 – NIS 2间接影响为基本和重要实体提供基本服务或数字服务的销售商、供应商和第三方服务提供商。这些公司需要确保其产品和服务的安全，并可能受到其客户的合同网络安全要求的制约。

基本服务和数字服务用户 – 虽然不受NIS 2的直接监管，但基本服务和数字服务用户可从该指令要求改进的网络安全实践和事件响应能力中受益。这间接提高了他们所依赖服务的安全性和可靠性。

2 NIS 2要求

2.1 对于必不可少的重要实体

安全措施 – 实施适当的安全措施，管理风险并确保其网络和信息系统的安全。这些措施应以风险评估和良好做法为基础。

事件报告 – 向主管当局报告可能对其网络和信息系统安全产生重大影响的重大事件。及时报告对于协调应对措施和减轻潜在危害至关重要。

风险管理 – 进行风险评估，以确定潜在威胁和薄弱环节，并采取措施降低这些风险。

与主管当局合作 – 与欧盟成员国指定的主管当局合作。这包括针对监管监督和事件响应目的提供必要的信息和系统访问。

事件响应计划 – 制定并维护事件响应计划，以有效应对网络安全事件。这些计划应概述侦测、报告和缓解事件的程序。

供应链安全 – 保护供应链（包括第三方销售商和供应商）的安全，以确保网络和信息系统的整体恢复能力。

持续监视 – 对网络和信息系统实施持续监视和审计，实时侦测并应对威胁和漏洞。

3 对供应商的影响

供应商可通过满足以下要求来支持NIS 2实体：

通过设计实现安全 – 物联网设备制造商应从设计阶段就在设备中加入安全功能，确保安全是产品不可分割的一部分。

定期更新与补丁 – 制造商应定期提供安全更新和补丁，以解决物联网设备中的漏洞。

认证和授权 – 物联网设备应采用强大的身份验证机制和适当的授权控制，以防止未经授权的访问。

数据加密 – 物联网设备对数据的传输和存储应进行加密，以保护敏感信息不被未经授权方拦截或访问。

事件报告 – 制造商应向有关当局报告与物联网设备相关的重大安全事件或违规行为，并可能向消费者或客户报告。

隐私方面的考虑 – 处理个人数据的物联网设备除应遵守NIS 2外，还应遵守GDPR（通用数据保护条例）等数据保护法规。

供应链安全 – 应要求确保从组件供应商到客户的整个供应链的安全，以防止在生产过程中的节点出现安全漏洞。

4 安讯士的回应

以下是作为供应商的安讯士如何满足NIS 2实体要求：

4.1 通过设计实现安全

通过设计实现安全是一种方法，旨在确保安全考虑和活动在产品设计和开发过程中完成，以降低漏洞风险，并确保在产品中默认设置稳健的安全配置。在安讯士，通过设计实现安全的原则适用于软件和硬件，主要包括以下内容：

- *安讯士安全开发模型 (ASDM)*：ASDM是一个由定义的流程和工具组成的框架，可确保安全考虑成为软件开发不可分割的一部分。活动包括开展风险评估、威胁建模、渗透测试、漏洞扫描、事件管理以及漏洞悬赏计划。安讯士软件开发人员使用ASDM确保将安全内置于软件开发中，以降低发布包含漏洞的软件的风险。

- *漏洞悬赏计划*：安讯士支持一项私人漏洞悬赏计划，该计划加强了公司主动识别、修补和披露AXIS OS（驱动大多数安讯士产品的基于Linux的操作系统）漏洞的工作。它加强了安讯士与外部安全研究人员和道德黑客建立专业关系的承诺。
- *软件物料清单 (SBOM)*：安讯士为AXIS OS提供SBOM，AXIS OS是大多数安讯士设备使用的基于Linux的操作系统。安全研究人员、权威机构和客户可深入了解构成AXIS OS的软件组件，对专门从事漏洞评估和威胁分析的人员特别有帮助，体现了安讯士对网络安全透明度的承诺。
- *AXIS OS默认安全设置*：运行新版AXIS OS的设备在出厂默认状态下进行了以下预配置：无默认密码；启用HTTP和HTTPS；默认启用IEEE 802.1X/802.1AR/802.1AE安全加载和通信；禁用安全性较低的协议。有关默认保护控件的更多信息，请*点击此处*。
- *Axis Edge Vault*：Axis Edge Vault内置于安讯士设备中，是一个基于硬件的安全平台，其功能包括保护安讯士网络产品的完整性，并启用基于加密密钥的安全操作。它通过安全启动和签名操作系统提供供应链保护；通过内置唯一安讯士设备ID提供设备来源，从而提供可信设备身份；通过安全密钥存储提供加密信息的防破坏保护；通过签名视频提供视频篡改侦测。

4.2 定期更新与补丁

安讯士提供软件更新，以解决硬件和软件产品中新发现的安全漏洞等问题。安讯士还提供设备管理工具，方便客户及时更新安讯士设备软件。AXIS Camera Companion、AXIS Camera Station、合作伙伴视频管理软件Milestone XProtect®和Genetec™ Security Center等，以及安讯士设备管理工具都突出显示针对联网设备发布的新版AXIS OS。此外，安讯士还提供安全通知服务，可以自由订阅。更多详细信息见下文。

- *AXIS OS*：安讯士提供两种主要的备选方案来保持设备软件处于最新版本：主动跟踪和长期支持 (LTS) 跟踪。通过主动跟踪可访问最新的先进特性和功能，以及错误修复和安全补丁。对于长期支持 (LTS) 跟踪的软件，只提供错误修复和安全补丁，从而提高稳定性，因为其重点是维护一个集成良好的第三方系统。
- 设备管理工具：*AXIS Device Manager*和*AXIS Device Manager Extend*工具让客户能够更轻松地使用最新安全补丁和错误修复来更新安讯士设备软件。

  为了在本地高效配置和管理安讯士设备，AXIS Device Manager可批量处理安全任务，如管理设备凭证、部署证书、禁用未使用的服务以及升级AXIS OS。

  AXIS Device Manager Extend提供汇总仪表板，在一个简单易用的应用中收集有关您各种设备和场所的信息。设备软件升级可用时会通知您，您可以大规模执行批量升级和其他任务。您还将收到替换产品的建议。活动可完全追溯，还可以导出系统设备信息，用于报告或审计目的。
- *安讯士安全通知服务*：安讯士鼓励用户注册这项服务，它可为用户提供有关安全事件和漏洞的及时通知。

4.3 认证和授权

为防止未经授权的访问并提高安讯士设备的整体安全性，安讯士支持：

- 基于角色的访问设备管理访问权限（管理员/操作员/观察员），以及通过将安讯士设备连接到IT标准化的*活动目录联合服务* (ADFS) 集成来集中验证/授权的可能性。（ADFS是微软开发的一种软件组件，为Windows服务器操作系统上的用户提供单点登录 (SSO) 授权服务。ADFS允许跨企业边界的用户使用一套登录凭证访问Windows服务器操作系统上的应用）。

- 使*零信任网络*更加容易的技术。在新发布的AXIS OS中，这些技术包括IEEE 802.1X（以及符合IEEE 802.1AR标准的安讯士设备ID），用于将设备自动安全地加载到IEEE 802.1X网络，以及IEEE 802.1AE (MACsec)，用于自动加密数据通信。

4.4 数据加密

为了保护敏感信息不被未经授权方截获或访问，安讯士产品支持以下功能：

- HTTPS，其中的数据通信都支持TLS 1.2或更新的标准。AXIS Camera Station视频管理软件服务器与客户端之间的视频流连接经过AES–256加密。
- 用于自动数据通信加密的*IEEE 802.1AE (MACsec)*。
- 通过RTP进行安全视频流处理，也称为SRTP/RTSPS（从AXIS OS 7.40开始）。SRTP/RTSPS使用安全的端到端加密传输方法，保障只有经过授权的客户端才能从安讯士设备接收视频流。
- *边缘存储加密*（SD卡）
- *边缘记录密码加密导出*（SD卡、网络共享），从AXIS OS 10.10开始。这意味着可以导出经过密码加密的记录，增加了安全共享敏感视频数据的可能性，而无需手动加密导出的记录。

4.5 事件报告

安讯士对在我们的产品和服务中发现的安全事件或漏洞提供事件报告。

- 安讯士是通用漏洞披露 (CVE) 编目权威机构之一。这意味着安讯士遵循行业良好做法，以透明的方式管理和应对我们产品和服务中已发现的漏洞，从而降低客户的暴露风险。安讯士还可以为新发现的漏洞分配CVE编号，并将这些漏洞报告到*www.cve.org*网站。安讯士*漏洞管理政策*发布在axis.com上。
- 可以*在此*自由订阅，接收安讯士安全通知。
- 新版AXIS OS推出安全补丁和错误修复。AXIS Camera Companion、AXIS Camera Station、AXIS Device Manager、AXIS Device Manager Extend以及Milestone XProtect和Genetec Security Center等第三方VMS也突出显示更新设备软件的可用性。
- 安讯士致力于实现与公司相关的网络攻击的透明度，并将根据瑞典相关当局提供的指南报告此类事件。

4.6 隐私方面的考虑

安讯士在网上发布其*隐私政策*和声明，其中概述收集哪些个人数据（例如，从“我的安讯士”在线账户收集的数据）以及如何使用这些数据。

安讯士还发布了与其信息安全管理系统有关的*网络安全框架和实践*，并且已通过ISO/IEC 27001认证。安讯士ISO/IEC 27001证书的范围涵盖内部IT基础设施和服务的开发与操作。ISO 27001是国际公认的标准，为如何通过有效的风险管理保护和管理企业信息提供指导。

符合*ISO/IEC 27001*即意味着，安讯士使用了国际公认的流程和良好做法来管理其用于向客户和合作伙伴提供支持和服务的内部信息基础设施和系统。

此外，安讯士还帮助客户解决监控中有关捕捉视频和音频方面的隐私问题。解决方案包括：

- 安讯士摄像机中的静态隐私遮罩以及*AXIS Live Privacy Shield*软件应用中的动态隐私遮罩
- 基于边缘的分析功能，如*AXIS People Counter*应用或*AXIS P8815–2 3D People Counter*，它们仅采集和存储统计数字数据，不处理个人身份信息。
- *热成像摄像机*
- *雷达产品*
- *AXIS Camera Station*中的视频编辑工具，用于遮罩目标或非关注区域
- 安讯士视频监控产品中的*默认禁用音频功能*

有关隐私解决方案的更多信息，请访问*axis.com/solutions/privacy–in–surveillance*

4.7 供应链安全

确保从组件供应商到客户的供应链安全，对于防止安全漏洞的出现非常重要。

在解决网络安全问题时，安讯士采用了一种产品*生命周期方法*。我们致力于降低风险，这不仅体现在从组件到成品的整个供应链中，还体现在分销和实施过程中，以及服务和退役阶段。

以下是安讯士解决供应链安全问题的一些方法：

- 安讯士直接从战略供应商处采购关键组件。我们与生产合作伙伴密切合作。我们监控生产流程，全天24小时不间断获取数据，开展实时分析，保证透明度。了解*安讯士供应链安全*。
- 通过Axis Edge Vault实现内置设备安全，从而通过以下功能保障安讯士设备的完整性：
  - **签名操作系统**：确保所安装的AXIS OS是安讯士正版。它还能保障打算安装在设备上的新的AXIS OS也经过安讯士签名。
  - **安全启动**：使设备能够检查操作系统是否具有安讯士签名。如果操作系统未经授权或者已被篡改，则会中止启动过程，并且设备会停止运行。将签名操作系统、安全启动和恢复设备出厂设置结合在一起，可以防止在设备运输过程中试图进行修改。
  - **安讯士设备ID**符合IEEE 802.1AR标准，可在网络上实现安全设备识别和加载。安讯士设备ID保存在设备的安全密钥库（安全元件、TPM、TEE）中。
  - **加密文件系统**保护存储在文件系统中的客户特有的配置和信息，防止在设备未使用时（比如，在将设备从系统集成商运往最终客户时），这些配置和信息遭到提取或篡改。
  - 此外，安讯士支持**签名视频**，使观察员能够验证从设备导出的视频是否被篡改。这在调查或诉讼中尤其重要。更多信息，请访问*axis.com/solutions/edge–vault*。
- 从axis.com下载的软件提供校验和，通过校验和可以验证文件的完整性。
- ETSI认证：运行AXIS OS 11或更高版本的150多款安讯士产品已通过*ETSI EN 303 645网络安全标准*认证。ETSI是欧洲电信标准协会的简称。这些要求涵盖设备本身，包括支持安全密钥存储等基于硬件的安全功能，以及默认启用HTTPS和无默认密码等默认安全功能。另一个方面涉及生命周期管理，如规定设备安全更新的支持期。其他方面还包括在软件开发中采用减少漏洞风险的方法；制定透明的漏洞管理政策；以及支持个人数据处理方面的良好做法。这些要求考虑有助于确保认证产品在整个生命周期内具有基准安全级别的行业良好实践。该标准与《欧洲网络安全复原力法案》、《欧洲无线电设备指令》以及世界各地的其他标准和立法密切保持一致。

4.8 培训和指导

安讯士为员工、合作伙伴和客户提供有关网络安全良好实践的信息和培训。其中包括以下方面：

- 内部安全意识和培训：安讯士开发了安全意识课程，持续培训员工如何避免和减轻企业面临的安全威胁。安讯士人员都必须接受这种意识培训。根据个人的企业角色和职责，为开发人员和系统所有者提供额外的安全培训。
- *安讯士学院培训*：为客户提供的培训课程包括有关网络安全和*安讯士应对该问题的方法*的在线课程。
- 在线提供*强化配置指南*，针对：
  - *AXIS OS*
  - *AXIS Camera Station*
  - *安讯士网络交换机*
- *AXIS OS安全扫描仪指南*：安讯士建议对安讯士设备运行安全扫描，检查它们是否受到漏洞或配置不良的影响。“AXIS OS安全扫描器指南”就如何纠正某些扫描结果提供建议，并概述常见的“假警报”。
- *Axis OS取证指南*：对于在周围网络上以及在安装有安讯士设备的IT基础设施上发生网络安全攻击时，需要对安讯士设备进行取证分析的人员，此指南提供相关的技术建议。

有关安讯士和网络安全的更多信息，请访问*安讯士网络安全门户*。

关于 Axis Communications

Axis 通过打造解决方案，不断提供改善 以提高安全性和业务绩效。 作为网络技术 公司和行业领导者，Axis 提供视频监控解决方案， 访问控制、对讲以及音频系统的相关产品和服务。 并通过 智能分析应用实现增强，通过高品质培训提供支持。

Axis 在 50 多个国家/地区拥有约 4,000 名敬业的员工 并与全球的技术和系统集成合作伙伴合作 为客户带来解决方案。 Axis 成立于 1984 年，总部 在瑞典隆德