网络安全问答

用户手册

有关其他问题和答案，请访问 Axis *FAQ 数据库*。

一般性问题

什么是网络安全?

网络安全是保护计算机系统和服务免受网络威胁。网络安全实践包括防止损坏和恢复计算机、电子通信系统和服务、有线和电子通信以及存储信息的过程，以确保其可用性、完整性、安全性、真实性、保密性和不可否认性。

网络安全是指在更长的时间内管理风险。风险无法消除，只能减轻。

管理网络安全通常涉及什么?

网络安全涉及产品、人员、技术和正在进行的过程。

因此，它将涉及**识别**和评估组织的各个方面，包括对设备、系统、软件和固件进行盘点；确定关键任务目标；记录程序和安全政策；应用风险管理策略并持续进行与资产相关的风险评估。

它将涉及实施安全控制和措施，以**保护**您已确定为网络攻击重点的数据、设备、系统和设施。

它还将涉及开发和实施帮助您**侦测**网络攻击的活动，以便您能够及时采取行动。例如，这可能涉及安全信息和事件管理 (SIEM) 系统或安全编排、自动化和响应 (SOAR) 系统，该系统管理来自网络设备和管理软件的数据，聚合关于异常行为或潜在网络攻击的数据，并分析该数据以提供实时警报。Axis 设备支持 SYS 日志和远程 SYS 日志，它们是 SIEM 或 SOAR 系统的主要数据源。

网络安全管理还包括制定和实施程序，以在发现网络安全事件时作出**反应**。您应考虑当地法规和内部政策，以及披露网络安全事件的要求。Axis 提供 *Axis OS 取证指南*，帮助您了解 Axis 设备在网络安全攻击期间是否受到了破坏。

制定和实施活动，以维持恢复能力计划，**恢复**或重置因网络安全事件而受损的能力或服务，也很重要。例如，*AXIS 设备管理应用程序*通过支持还原点，可以轻松重置 Axis 设备，这些还原点是在某个时间点保存的系统配置的“快照”。在没有相关恢复点的情况下，该工具可以帮助将设备恢复到其默认状态，并通过网络推出保存的配置模板。

网络安全风险是什么?

网络安全风险（如 RFC 4949 互联网安全术语所定义）是一种损失预期，表示为特定威胁利用特定漏洞并产生特定有害结果的可能性。

为长期实现充分的风险降低，必须定义明确的系统政策和流程。建议的方法是根据定义明确的 IT 保护框架（如 ISO 27001、NIST 或类似标准）进行工作。虽然这项任务对于小型企业来说可能是巨大的，但即使是很少的政策和流程文档也远远优于什么也不做。

有关如何评估风险并确定其优先级的信息，请参见*网络安全参考指南*。

威胁是什么?

威胁可以定义为可能危及或损害您的资产或资源的东西。一般来说，人们倾向于将网络威胁与恶意黑客和恶意软件联系起来。事实上，负面影响往往是由于意外、无意的滥用或硬件故障造成。攻击可以分为机会攻击或目标攻击。现在，大多数的攻击都是机会攻击：攻击的发生只是因为存在机会之窗。此类攻击将使用低成本的攻击载体，如网络钓鱼和探测。应用标准级别的保护将减轻与机会攻击相关的大多数风险。

更难防范的是有特定目标的特定系统的攻击者。目标攻击使用与机会攻击者相同的低成本攻击载体。不过，如果初始攻击失败，他们会更加坚定，愿意花费时间和资源来使用更复杂的方法来实现目标。对他们而言，这在很大程度上取决于价值的多少。

最常见的威胁是什么？如何应对?

故意或意外误用系统

合法访问系统的人是系统最常见的威胁之一。他们可以访问未经授权的服务。他们可能会窃取或故意伤害系统。人们也会犯错误。在试图修复问题时，他们可能会无意中降低系统性能。个人也容易

受到社会工程的影响；也就是说，让合法用户泄露敏感信息的伎俩。个人可能会丢失或替换关键部件（门禁卡、电话、笔记本电脑、文档等）。人们的计算机可能受到威胁，也可能无意中感染了恶意软件。

建议的保护措施包括：具有定义的用户账户策略和流程，具有足够的访问验证方案，具有随时间推移管理用户账户和权限的工具，减少暴露，以及网络意识培训。

AXIS 通过*强化配置指南*，以及*设备和视频管理软件来帮助应对这种威胁*。

物理篡改和破坏

物理上暴露的设备可能被篡改、被盗、断开、重定向或切割。

建议的保护措施包括将网络设备（例如，服务器和交换机）放置在锁定区域，安装摄像机使其难以接近，在物理暴露时使用受保护的外壳，以及保护墙壁或导管中的电缆。

Axis 通过设备*保护外壳*、防篡改螺钉、能够加密 SD 卡的摄像机、摄像机视图篡改侦测和打开外壳侦测，帮助应对这一威胁。

利用软件漏洞

基于软件的产品都有可能被利用的漏洞（已知或未知）。大多数漏洞的风险很低，这意味着很难利用，或者负面影响有限。偶尔也会有被发现并可被利用的漏洞，从而产生重大的负面影响。MITRE 托管一个大型的 CVE（常见漏洞和风险）数据库，以帮助他人降低风险。

建议的保护措施包括：有一个连续的修补过程，帮助减少系统中已知漏洞的数量；尽可能减少网络暴露，以便更难探测和利用已知漏洞，以及提供补丁并对发现的关键漏洞保持透明的人员。

AXIS 解决威胁的方法是：通过 *Axis Security Development Model*，旨在最大限度地减少 AXIS 软件中可被利用的漏洞；通过 *Axis Vulnerability Management Policy*，识别、修复并公布客户需要了解的漏洞，以便采取适当的行动。（截至2021年4月，*Axis 是 AXIS 产品的常见漏洞和风险编号机构*，允许我们根据 MITRE 公司的行业标准流程调整我们的流程。）AXIS 还提供*强化配置指南*，就如何减少曝光和增加控制以降低被利用的风险提出建议。Axis 为用户提供*不同的设备软件跟踪*，使 Axis 设备的操作系统保持更新。其中两个主要跟踪是：

1. 活动跟踪提供支持新特性和功能的设备软件更新，以及错误修复和安全补丁。
2. 长期支持 (LTS) 跟踪提供设备软件更新，支持错误修复和安全补丁，同时尽可能地降低与第三方系统不兼容的风险。

供应链攻击

供应链攻击是一种网络攻击，旨在通过针对供应链中不太安全的元素来损害组织。该攻击是通过破坏软件/操作系统/产品并引诱管理员将其安装在系统中实现的。产品在运送给系统所有者期间可能会受到损害。

建议的保护措施包括制定政策，仅安装来自可信和经验证来源的软件，通过在安装前将软件校验和（摘要）与供应商的校验和进行比较来验证软件完整性，检查产品交付是否存在篡改迹象。

Axis 以多种方式应对这一威胁。Axis 发布带有校验和的软件，以便管理员在安装之前验证其完整性。加载新的设备操作系统（OS）时，Axis 联网设备仅接受由 Axis 签名的设备软件。Axis 网络设备上的*安全引导*还确保只有 Axis 签名的 操作系统运行设备。每个设备都有一个单独的 Axis 设备 ID，这为系统提供了一种方法来验证该设备是否是真正的 Axis 产品。有关此类网络安全功能的详细信息，请参见白皮书 *Axis Edge Vault*。

有关威胁的更多详细信息，请参阅我们的*网络安全参考指南*。

什么是漏洞?

漏洞为攻击者提供攻击或访问系统的机会。它们可能是由缺陷、功能或人为错误造成的。恶意攻击者可能会试图利用已知漏洞，通常会结合一个或多个漏洞。大多数成功的破坏都是由于人为错误、配置不当的系统和维护不善的系统——通常是由于缺乏适当的政策、职责不明确和组织意识低下。

软件漏洞是什么?

设备 API（应用可编程接口）和软件服务可能存在漏洞或功能，可在攻击中被利用。没有供应商能保证产品没有瑕疵。如果已知缺陷，可以通过安全控制措施减轻风险。另一方面，如果攻击者发现一个新的未知缺陷，则风险会增加，因为受害者没有时间保护系统。

什么是通用漏洞评分系统 (CVSS)?

通用漏洞评分系统 (CVSS) 是对软件漏洞严重程度进行分类的一种方法。这是一个公式，它考虑了利用它的容易程度以及可能产生的负面影响。得分为 0–10 之间的值，10 表示最严重。您通常会在已发布的常见漏洞和风险 (CVE) 报告中找到 CVSS 编号。

Axis 使用 CVSS 作为确定软件/产品中已识别漏洞的严重程度的措施之一。

特定于 Axis 的问题

有哪些培训和指南可以帮助我更多地了解网络安全，以及我可以做什么来更好地保护产品和服务免受网络事件的影响?

通过*资源*网页，您可以访问强化指南（例如 *AXIS OS Hardening Guide*、*AXIS Camera Station Pro System Hardening Guide* 和 *Axis Network Switches Hardening Guide*）、策略文档等。Axis 还提供网络安全*电子学习*课程。

我可以在哪里查找设备的新操作系统?

转到*设备软件*并搜索您的产品。

如何轻松升级设备上的操作系统?

要升级设备软件，您可以使用 *Axis 视频或设备管理软件*。

如果 Axis 服务中断，如何通知我?

请访问 *status.axis.com*。

如何通知我发现的漏洞?

您可以订阅 *Axis 安全通知服务*。

Axis 如何管理漏洞?

请参见 *Axis 漏洞管理*。

Axis 如何减少软件漏洞?

阅读*让网络安全成为 Axis 软件开发不可或缺的一部分*一文。

Axis 如何在整个设备生命周期中支持网络安全?

访问*网络安全的生命周期方法*。

Axis 产品内置了什么网络安全功能?

阅读更多：

- *Axis Edge Vault*
- *AXIS OS*
- *支持整个设备生命周期的网络安全*

Axis 是否通过 ISO 认证，Axis 符合哪些其他与网络安全相关的法规?

是，AXIS 已通过 *ISO/IEC 27001:2023* 认证。公司拥有一套信息安全管理系统 (ISMS)，可满足软件、云服务和 IT 基础设施的开发和操作方面的要求。

Axis Communications UK Ltd. 通过了 Cyber Essentials（证书编号：IASME–CE–017710）和 Cyber Essentials Plus（IASME–CEP–004245）认证。

运行 *AXIS OS 11* 或更高版本的 Axis 设备已通过 *ETSI EN 303 645* 网络安全标准认证。AXIS OS 网络产品还获得了德国联邦信息安全办公室颁发的 IT 安全标签 (IT–Sicherheitskennzeichen)(*BSI – Bundesamt f ü r Sicherheit in der Informationstechnik*)。

有关 AXIS 网络安全合规性和认证的最新信息，请访问*Axis Trust Center*，了解更多详情。

Axis 如何帮助我公司遵守 NIS 2?

请参阅有关 *NIS 2* 的文章。

T10189380_zh

2025-09 (M5.2)