Cybersecurity reference guide

用户手册

目录

简介

简介

本指南旨在提供一个通用基准，并作为 Axis 制作的网络安全相关材料的参考。这些是基于 NIST、SANS、ISO 和 RSA 会议的简化描述、模型和结构，以及来自网络安全社区内各个组织的材料。

Axis 其他资料的链接：

- *axis.com/about-axis/cybersecurity*
- *help.axis.com/cybersecurity-qna*
- *axis.com/support/cybersecurity/resources*
- *help.axis.com/axis-security-development-model*
- *axis.com/support/cybersecurity/vulnerability-management*

网络安全的定义

部分基于 NIST 的定义：

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。

组织类型

不同的组织拥有不同的资产、资源、暴露和网络成熟度。在遵循建议的做法时，*CIS 控制（以前称为关键安全控制）* 定义了三种组织概况。

- SANS 实施组 1 (IG1)

  在大多数情况下，IG1 企业通常是中小型企业，其专门用于保护 IT 资产和人员的 IT 和网络安全专业知识有限。

- SANS 实施组 2 (IG2)

  IG2 企业雇用负责管理和保护 IT 基础设施的人员。这些企业通常支持多个部门，这些部门根据工作职能和任务不同具有不同的风险概况。小型企业单位可能有法规遵从性负担。

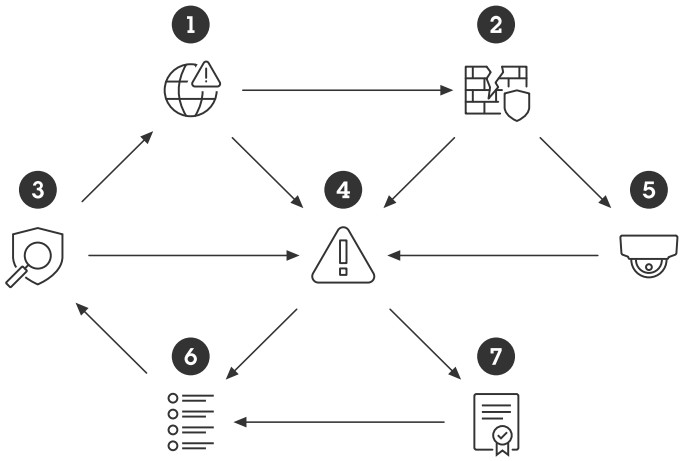
- SANS 实施组 3 (IG3)

  IG3 企业通常会聘用专门从事网络安全各方面工作（如风险管理、渗透测试、应用安全）的安全专家。IG3 资产和数据包含受监管和合规性监督的敏感信息或功能。

术语

术语

术语图显示了本文档中讨论的特定网络安全关键术语之间的关系。



- (1) 威胁开发(2) 漏洞暴露（5）资产并不断增加（4）风险
- （4）风险影响（7）政策并显示（6）要求
- （6）要求予以解决在(3)安全控制，这里不断面对(1) 威胁同时减轻（4）风险

风险

网络安全就是随着时间的推移管理风险。风险无法消除，只能减轻。有时人们会混淆这些术语：风险、资产、威胁、漏洞或负面影响

RFC 4949 互联网安全术语将风险定义为一种损失预期，表示为特定威胁利用特定漏洞产生特定有害结果的概率。

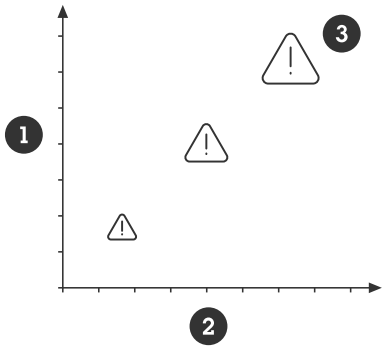
常用的简写形式是风险 = 概率 x 影响

该公式用于确定风险的优先级。RFC 定义包括“特定”一词，表示威胁、漏洞和有害结果。应该单独看待每个威胁，从最有可能发生且负面影响最大的威胁开始。

讨论风险时的一个挑战是概率因素。事情可能会发生，也可能不会发生。对手利用漏洞的概率通常取决于漏洞被利用（暴露）的容易程度以及对手利用该漏洞的潜在利益。

可以用这两个维度来绘制风险图：将风险发生的概率作为一个轴，将风险（如果发生）的影响作为另一个轴。这样就可以清楚地了解每个风险的潜在影响以及您需要给予的优先级。

术语



1 可能性从低到高
2 负面影响从低到高
3 风险级别从低到高

攻击价值 = 攻击利益 – 攻击成本

添加保护会增加攻击成本，从而降低概率。攻击成本与攻击成功所需的时间、资源、技能和复杂程度有关。被抓住的风险或其他负面后果也是攻击成本的一部分。

风险评估是分析网络空间风险的过程，与实物保护相同。需要考虑的问题如下：

1. 想要保护什么?
2. 想要保护其免受谁的侵害?
3. 产生负面影响的概率是多少?
4. 如果失败，后果有多严重?
5. 应该实施哪些策略来降低风险?

实施任意类型的保护或安全控制措施都会产生某种类型的成本。组织的财政资源都有限。如果不知道风险是什么，就很难估计保护预算。您总是需要接受风险，但这个决定必须是深思熟虑的基于风险的决定。

估算对每种资产类型的潜在负面影响既困难又复杂。在许多情况下，估算是主观的，影响分析往往被低估。使用 ISO 27000 影响模型和名称类型（即有限、严重、重度或灾难性）可以帮助您快速了解情况，从而帮助您确定优先级。它提供了一种简单的方法，根据从负面影响中恢复所需的时间来估算，从而确定一个更精确的值，即：

- 有限 = 从几小时到几天
- 严重 = 从几天到几周
- 重度 = 从几周到几个月
- 灾难性 = 从几个月到几年，如果有的话

资产

实物保护的重点是保护人和实物，而网络安全保护侧重于保护数据资产和计算机资源。主要有三个方面：

- 保密性：信息或资源的披露
- 完整性：信息或资源的破坏或篡改
- 可用性：信息和资源的可访问性

术语

这些方面也被称为 CIA 三要素。操作技术 (OT) 通常会优先考虑可用性，而那些使用信息技术 (IT) 的人通常会优先考虑安全性。在保密性、完整性和可用性之间找到适当的平衡往往具有挑战性。

需要对资产和资源进行分类，以确定适当的保护级别。就负面影响而言，并非全部数据资产和计算机资源都一样。它们通常分为以下几类：

- 公共：资产以公众消费者为目标。或者，如果向公众披露，负面影响是限。
- 私有：资产为特定/选定组所特享。通常，负面影响仅限于特定组织（如公司或家庭）内部。
- 受限：资产为组织内选定个人所特享。

视频系统中的实时视频可归类为公共，既指一般公众，也指组织内的公众。但在大多数情况下，实时视频被归类为私有，即仅特定组织单位可以访问。同时，在大多数情况下，录制的视频被归类为受限，因为可能存在非常敏感的场景。凭证和配置也是应归类为受限的数据。

威胁

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。

攻击不会凭空出现。对系统及其资产进行破坏总有一些动机。攻击可以分为机会攻击或目标攻击。在网络安全中，攻击者也被称为可能怀有恶意的对手。

今天的大多数攻击都是机会攻击：仅仅因为有机可乘而发生的攻击。在许多情况下，外部机会攻击者甚至不知道受害者是谁。这些攻击者会使用低成本的攻击载体，如网络钓鱼和探测。在这些情况下，他们没有决心在失败的攻击上花费时间和资源；他们迅速转向下一次尝试。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。更难防范的是目标攻击，那些有特定目标、针对特定系统的攻击者。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。

常见对手（威胁行为者）

- 亲近的人：可能想窥探您个人生活的人
- 员工：或意外或故意滥用合法访问系统的人
- 恶作剧者：认为干扰计算机系统是一项令人愉快的挑战的人
- 黑客行动主义者：出于政治或意识形态动机攻击组织的人
- 网络犯罪分子：有意通过欺诈或出售有价值的信息赚钱的人
- 行业竞争对手：有意为其公司或组织获得经济优势的实体
- 网络恐怖分子：实施旨在引起惊恐或恐慌的攻击的人或实体，通常出于意识形态或政治原因
- 民族国家：采取行动以获取经济和政治利益或破坏关键信息系统的外国情报机构特工
- 个人：其动机可能与上述动机不同的单独行动的特定个人或群体。可能是一名调查记者、白帽黑客或类似人员。如果您优先考虑隐藏缺陷而不是修复缺陷，白帽黑客（又称道德黑客）可能会构成威胁。

漏洞

系统都会有漏洞。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、暴露、功能或人为错误造成。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、配置不当的系统或维护不善的系统——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

术语

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，可以通过补偿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，由于受害者没有时间保护系统，成功利用零日漏洞的风险会增加。

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暴露 (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。

政策

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。

安全控制

安全控制是用于规避、侦测、抵消或尽量降低实物财产、信息、电脑系统或其他资产安全风险所采取的保障措施或应对策略。部署安全控制的过程通常称为强化。

补偿安全控制是替代性保障措施，当无法应用佳选安全控制，或者佳选控制不可用或成本过高时，可以使用这些保障措施。

随着威胁、价值、漏洞和暴露随时间不断变化，需要对安全控制进行持续监控和更新。这就需要定义和遵循政策和流程。

SANS 研究所发布了一份 *CIS 控制列表*，这是一套按优先顺序排列的网络防御理想实践建议。为了展示安全控制的多样性，以下是完整列表。

- CIS 控制 #1：企业资产的库存和控制
- CIS 控制 #2：软件资产的库存和控制
- CIS 控制 #3：数据保护
- CIS 控制 #4：企业资产和软件的安全配置
- CIS 控制 #5：账户管理
- CIS 控制 #6：访问控制管理
- CIS 控制 #7：持续漏洞管理
- CIS 控制 #8：审核日志管理
- CIS 控制 #9：电子邮件和 Web 浏览器保护
- CIS 控制 #10：恶意软件防御
- CIS 控制 #11：数据恢复
- CIS 控制 #12：网络基础设施和管理
- CIS 控制 #13：网络监控和防御
- CIS 控制 #14：安全意识和技能培训
- CIS 控制 #15：服务提供商管理
- CIS 控制 #16：应用软件安全
- CIS 控制 #17：事件响应管理

术语

- CIS 控制 #18：渗透测试

*AXIS OS 强化指南*基于 CIS。

常见威胁的保护措施

通过了解和应对常见威胁，您可以降低大多数风险。

故意或意外滥用系统

在系统的可用性和安全性之间很难取得平衡。许多系统都是从便利性而非安全性的角度进行强化。这为故意或意外滥用提供了机会。合法访问系统的人是系统常见的威胁。

常见威胁示例：

- 个人可能会访问其未经授权访问的服务（如实时或录制的视频）
- 个人犯错
- 个人可能会尝试修复导致系统性能下降的问题
- 心怀不满的个人可能会故意破坏系统
- 个人容易受到社会工程学的影响
- 个人偷窃
- 个人可能会丢失或错放关键部件（访问卡、电话、笔记本电脑、文档等）。
- 个人的计算机可能会被入侵，无意中使系统感染恶意软件

常见建议的保护措施有：

- 明确的用户账户政策和流程
- 充分的访问身份验证方案
- 随时间推移管理用户账户和权限的工具
- 减少暴露
- 网络意识培训

Axis 如何帮助应对这一威胁：

- *AXIS OS 强化指南*介绍了设备常见威胁的常见安全控制
- *AXIS Camera Station 强化指南*介绍了视频系统的常见安全控制
- *AXIS Device Manager* 和 *AXIS Device Manager Extend* 帮助管理常见安全控制

物理篡改和破坏

从网络安全的角度来看，IT 系统的物理保护非常重要。

常见威胁示例：

- 物理上暴露的设备可能会被篡改
- 物理上暴露的设备可能会被盗
- 物理上暴露的电缆可能会被断开、重定向或切断

常见建议的保护措施：

- 将网络设备（如服务器和交换机）放置在锁定区域
- 将摄像机安装在不易触及的地方
- 物理暴露时使用保护外壳
- 保护墙壁或导管中的电缆

Axis 如何帮助应对这一威胁：

- 加密 SD 卡，阻止播放视频（如果一个未经授权的用户能够弹出 SD 卡）
- 摄像机视图篡改侦测
- 外壳打开侦测

利用已知软件漏洞

基于软件的产品都有可能被利用的漏洞。这些漏洞可以分为已知和未知两类。未知漏洞终会被发现；这只是时间问题。大多数漏洞的风险很低，这意味着它们很难被利用，或者负面影响有限。偶尔，会发现可被利用并可能造成重大负面影响的漏洞。MITRE 拥有一个大型 CVE（常见漏洞和暴露）数据库，以帮助人们降低风险。

常见建议的保护措施：

- 持续的修补过程，帮助减少系统中已知漏洞的数量。
- 尽量减少网络暴露，增加探测和利用已知漏洞的难度。
- 与可信赖的次级供应商合作，这些供应商根据尽量减少缺陷的政策和流程开展工作，有提供补丁的流程，并在发现关键漏洞时进行披露。

Axis 如何提供帮助：

- *Axis 安全开发模型*是一个框架，定义了 Axis 用于降低发布存在软件漏洞的产品的风险的流程和工具。
- *Axis 漏洞管理政策*涉及识别、修复和披露客户需要了解的漏洞，以便采取适当措施。自 2021 年 4 月起，Axis 已获准成为 Axis 产品的常见漏洞和暴露 (CVE) 编号机构 (CNA)，使我们能够调整流程以适应 MITRE Corporation 的行业标准流程。这反过来又有助于我们以更好的方式为客户提供支持。
- *Axis 强化指南*（如 *AXIS OS 强化指南*）就如何降低暴露和添加补偿控制以降低软件缺陷被利用的风险提出了建议。
- LTS（长期支持）固件版本使客户能够修补 Axis 设备的操作系统，同时尽量降低与第三方视频管理系统不兼容的风险。

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。它主要用于其他攻击载体（如社会工程学、网络钓鱼攻击和接口探测）因系统防护等级高而失败的情况。该攻击是通过破坏软件/固件/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。成功发动供应链攻击需要技能、时间和资源。

常见建议的保护措施有：

- 制定政策，仅安装来自受信任和经过验证的来源的软件。
- 在安装之前，通过将软件校验和（摘要）与供应商的校验和进行比较来验证软件的完整性。
- 交付时，检查包装或产品是否有篡改迹象。

常见威胁的保护措施

Axis 如何帮助应对这一威胁：

- Axis 软件发布时带有校验，使管理员能够在安装软件之前验证软件的完整性。
- Axis 设备中的签名固件确保安装的 AXIS OS 真正来自 Axis，并确保要在设备上下载和安装的全部新固件也由 Axis 签名。
- Axis 设备中的安全启动使设备能够检查固件是否具有 Axis 签名。如果固件未经授权或被篡改，引导过程将中止。
- 符合 IEEE 802.1AR 标准的 Axis 设备 ID 是设备独有的 Axis 供应商证书，为系统提供了一种验证外壳内硬件是否来自 Axis 的方法。
- SD 卡加密和文件系统加密防止在卡或设备被盗时提取存储的数据。

用户手册
Cybersecurity reference guide

版本 M3.2
日期：十一月 2023
零件号 T10201166