零信任安全模型

维基百科，自由的百科全书

零信任安全模型（英語：Zero trust security model），也称**零信任架构**、**零信任网络架构**、**ZTA**、**ZTNA**等，还有时称为**无边界安全**（perimeterless security），此概念描述了一种IT系统设计与实施的方法。零信任安全模型的主要概念是“从不信任，总是验证”，即不应默认信任设备，即使设备已经连接到经许可的网络（例如公司局域网）并且之前已通过验证。大多数现代企业网络结构复杂，包含众多相互连接的区域、云服务以及基础设施，以及与远程和移动环境的连接、非常规IT连接（例如物联网设备）。零信任原则是因传统的方法（如在名义上的“企业边界”内信任设备，或者设备通过VPN进行连接）不切合企业网络的环境复杂性。零信任提倡相互认证，包括在不考虑位置的前提下检查设备身份和完整性，以及基于设备身份和设备状况的置信度来结合用户身份验证，提供对应用程序和服务的访问许可。[1]

目录

背景

1994年4月，Stephen Paul Marsh在其斯特灵大学计算机安全专业的博士论文中提出了“零信任（zero trust）”一词。Marsh的研究将“信任”视作可以用数学描述的有限事物，断言“信任”的概念超越了道德、伦理、合法性、正义和判断等人为因素。[2]

2003年的Jericho Forum强调了为组织IT系统定义边界的挑战性，讨论了当时称为“去边界化”的趋势。2009年，Google实施了一种名为BeyondCorp的零信任架构。Forrester Research的分析师John Kindervag在2010年使用术语“零信任模型”表示更严格的公司内部网络安全计划和访问控制。[3] [4]

2019年，英国国家网络安全中心（NCSC）建议网络架构师考虑对新增IT部署采用零信任措施，尤其是计划大量使用云服务时。[5]

原则和定义

2018年， NIST和NCCoE的网络安全研究人员在美国开展的工作促成了“SP 800-207，零信任架构”的发布。[6][7]此刊物将零信任（ZT）定义为“一组概念和想法”，旨在面对“受损”（遭侵入）的网络时，减少信息系统和服务中准确执行、为每个请求进行访问权限决策时的不确定性。零信任架构（ZTA）是企业的网络安全计划，利用零信任概念并包含组件关系、工作流程规划和访问策略。

NCSC[5]采用了一种替代但保持一致的举措来确定零信任架构背后的关键原则：

1. 一种足够强的用户身份源
2. 用户身份验证
3. 机器身份认证
4. 额外上下文，例如策略合规性和设备健康状况
5. 访问一个应用的授权策略
6. 应用程序中的访问控制策略

参见

- 信任，但要核实（俄罗斯谚语）

参考资料

1. Mutual TLS: Securing Microservices in Service Mesh. The New Stack. 2021-02-01 [2021-02-20].（原始内容存档于2021-03-13）（美国英语）.
2. Stephen Marsh, Google Scholar, 2021-03-03 [2021-03-03],（原始内容存档于2018-12-01）
3. Akamai Bets on 'Zero Trust' Approach to Security. www.wsj.com. [2022-02-17].（原始内容存档于2022-02-18）（英语）.
4. Forrester Pushes 'Zero Trust' Model For Security. www.darkreading.com. [2022-02-17].（原始内容存档于26 August 2021）（英语）.
5. Network architectures. www.ncsc.gov.uk. [2020-08-25].（原始内容存档于2021-01-21）（英语）."Network architectures"（页面存档备份，存于互联网档案馆）. *www.ncsc.gov.uk*. Retrieved 2020-08-25.
6. Zero Trust Architecture | NCCoE. www.nccoe.nist.gov. [2020-08-25].（原始内容存档于2021-04-22）.
7. Rose, Scott; Borchert, Oliver; Mitchell, Stu; Connelly, Sean. Zero Trust Architecture (PDF). nvlpubs.nist.gov. NIST. [2020-10-17].（原始内容 (PDF)存档于2021-04-21）.