零信任模型的实现、误解和策略

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Zero Trust creator talks about implementation, misconceptions, strategy		
原文作者	泽尔卡·佐尔兹（Zeljka Zorz）	**原文发布日期**	2021年4月6日
作者简介	泽尔卡·佐尔兹是Help Net Security总编辑。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/04/06/john-kindervag-zero-trust/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	大约十几年前，约翰·金德瓦格（John Kindervag）提出了“零信任”安全模型。零信任模型能够确保，只有在正确的环境下，正确的人员或资源才能从正确的设备上正确访问正确的数据和服务。本文概述了零信任模型的有效性、存在的误解以及实现方法。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

零信任模型的实现、误解和策略

泽尔卡·佐尔兹

2021 年 4 月 6 日

大约十几年前，约翰·金德瓦格 （John Kindervag）提出了“零信任”安全模型。约翰·金德瓦格是 Forrester Research 副总裁兼安全与风险团队首席分析师，他花了多年的时间进行基础研究，最终建立了一种新的信任模型，一种新的网络安全方法以及一种旨在防止日益严重的数据泄露的安全策略。

在随后的几年中，零信任模型赢得了众多拥护者。这有充分的理由：随着移动设备、BYOD、IoT、云计算、远程工作（以及对公司资源的远程访问）的广泛采用，企业边界逐渐消亡，这大大扩大了企业的攻击面。因此，企业的防御措施必须全面覆盖用户、资产和资源。

零信任模型是否有效？

正如 MobileIron 联邦首席技术官比尔·哈罗德（Bill Harrod）所总结的那样，“零信任模型能够确保，只有在正确的环境下，正确的人员或资源才能从正确的设备上正确访问正确的数据和服务。”

举例来说，上个月，黑客攻击了安全初创公司 Verkada 的建筑大楼。他们声称获得了 Cloudflare 办公室中 Verkada 监控探头的访问权限，可由此感染 Cloudflare 首席执行官的笔记本电脑，从而感染其公司网络。Cloudflare 公司的首席技术官很快否认了这一说法。

“我们不信任我们的公司网络；我们使用诸如 Cloudflare Access 之类的产品来控制对资源的访问。即使攻击者能够访问公司网络中的计算机，也只是与连接到我们公司的 WiFi 网络有一样的效果。重要的不是网络，而是访问控制。”他解释说。

“当然，如果我们一直使用旧的城堡-护城河式网络（公司网络中的任何内容和人员都受到信任），结果可能会大有不同。这就是零信任模型如此强大的原因。疫情期间，零信任模型使我们所有人都可以居家办公——即使攻击者能够进入办公室网络，也无法获得进一步的访问权限。”

为了进一步证明该模型的有效性，金德瓦格指出，零信任策略已广泛部署在世界上一些最安全的环境中。例如，最近美国国家安全局（NSA）为零信任策略提供了指南。

这并不是说，零信任策略仅对至关重要的大型组织有用。金德瓦格说，全球规模最大和最小的组织都可以实施零信任策略，该策略有助于抵御勒索软件攻击和数据泄露等可怕的网络灾难。

“零信任模型专注于受保护的内容，因此它会阻止不属于‘5W+1H 分析法’的流量。这意味着到 C&C 节点的出站流量（勒索软件和数据泄露的运作方式）会被自动阻止。当恶意软件试图对互联网上的 C&C 节点执行 ping 操作时，控制系统中没有规则允许建立该会话。因此，数据不会被泄露，勒索软件也不能交换密钥。”他解释说。

实施零信任策略

目前，ON2IT 网络安全战略高级副总裁致力于使各种规模的组织更轻松地访问和使用零信任策略。金德瓦格建议组织遵循以下五个部署步骤来构建“零信任”网络。

1. 定义保护面：需要保护什么？

2. 映射业务流程：系统如何协同工作？

3. 构建环境：控制措施尽可能靠近保护面，以便定义微边界。

4. 创建零信任策略（采用 5W+1H 分析法，即回答：谁[who]能够访问某些网络和资源[what]，何时[when]、何地[where]、为什么[why]访问，以及如何[how]访问）

5. 监控和维护环境：收集监控数据，执行机器学习和分析，并自动执行策略中的响应措施。

金德瓦格说：“自从我创建零信任模型以来，其战略概念从未改变，我只是逐渐完善了一些术语。”

“我之前说五步部署模型的第一步是‘定义数据’，现在将其完善为‘定义保护面”。基于对攻击面的理解，我提出了‘保护面’这一概念：组织的攻击面很庞大，并且一直在增长和扩大，这使得组织难以进行保护。相比之下，保护面小了几个数量级，而且很容易理解。”

实施零信任模型的组织应避免哪些陷阱？金德瓦格提出了两点：（1）认为零信任是二

次元的（要么对一切实施零信任，要么对一切都不实施零信任）；（2）在未创建策略的情况下部署产品（从而造成虚假的安全感）。

“零信任策略是增量的。它一次建立一个保护面，可以以迭代、无中断的方式完成保护面的创建。”他解释说。

他建议，组织首先要为最不敏感/最不重要的保护面创建零信任网络（以学习、实践并减少干扰性错误），然后逐渐为更重要的保护面实施零信任网络。

他补充说，在设计零信任网络时，组织应专注于业务成果，确保从内到外进行设计，确定谁需要访问资源，并检查和记录第 7 层的所有流量，以便制定第 7 层策略声明。

消除误解

金德瓦格指出了一个常见的误解：零信任策略使系统“受信任”，因此等同于身份验证和多因子身份鉴别（MFA）。

他说，零信任策略消除了对数字系统的信任，因为‘信任’就是一个可以利用的漏洞。

“零信任策略需要身份属性信息，这些信息在第 7 层策略中通过 MFA 进行验证。如果零信任等同于 MFA（许多供应商都这样认为），那么 Snowden 和 Manning 攻击就都不会发生了——他们拥有非常强大的 MFA 和身份验证解决方案，但是没有在身份鉴别后查看数据包。”

最后，他强调说，许多供应商已重新定义了零信任，以粉饰其产品的局限性，但是现实情况是，没有什么“零信任产品”。

他说：“有些产品在零信任环境中运行良好，但是如果有供应商向你兜售他们的‘零信任’产品，很明显地说明他们不了解这一概念。”

“如果你想聘请托管服务提供商来帮助你实施零信任策略，请询问他们将零信任定义为产品还是策略。而他们问你的第一个问题应该是‘你想要保护什么’。”

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com