“零信任”现状的几点思考

在区块链、人工智能、物联网等新技术的深入发展应用、远程办公日趋常态化，以及企业数字化转型不断加速的背景下，传统基于边界的网络安全防护已无法满足数字化时代的安全要求，零信任作为无边界趋势下的新安全理念，成为应对复杂网络威胁、保障业务连续性的全新突破口。

文丨**周鸣爱** 赛迪智库网络安全研究所工程师

一、零信任

网络攻击日益复杂，网络边界逐渐泛化，零信任认知度不断提升。疫情大爆发后，远程办公成为许多企业的办公常态，Facebook、Twitter 等企业甚至允许部分员工实行永久远程办公。加之区块链、移动互联、人工智能等新技术的发展，互联网已渗透到经济社会的各行各业，越来越多的企业进入数字化转型发展的新阶段，网络安全问题也日益复杂，安全威胁逐步升级，安全边界逐步被打破，传统基于边界的安全架构已不再“安全”，零信任逐渐成为网络安全界关注的焦点。2018 年 Gartner 的一次网络研讨会中 70% 的参会人听说过零信任，23% 不了解零信任，只有 8% 在计划零信任项目。而 Dimensional Research 对 1009 名 IT 安全人员的调查显示，零信任是大多数组织的主要安全优先事项。One Identity 的调查结果显示，75% 的组织认为零信任对于加强整体网络安全非常重要。此外，美国国家安全局、国防部、国防工业基地和拜登政府的《网络安全行政令》都迫切要求实施零信任架构。美国国防部和联邦政府将零信任技术列入关键性的新一代安全体系计划，

作为无边界趋势下的新安全理念，成为许多行业高度关注并寄予厚望的焦点。Illumio 公司近期的一项调查显示，98% 的英国商业领袖和 IT 决策者已开始或计划在他们的组织中实施零信任战略。ISMG 发布的《2022 年零信任策略报告》显示，绝大部分人认为零信任对降低网络安全风险非常重要，46% 的受访者认为零信任是 2022 年最重要的安全实践。当前，整个网络安全行业对零信任认知度不断提升，然而零信任在具体解决方案上却依然滞后。Forrester 的一项调查显示，仅有 6% 的企业能够全面部署零信任；30% 的企业表示只是局部部署了零信任；还有 63% 的企业目前的零信任项目只是在评估或者计划阶段。

“从来不信任，始终在校验”是零信任的核心思想。零信任的产生起初是由于发现传统基于边界的网络安全架构设计存在缺陷，传统安全网络架构通常认为内部网络绝对可信，实际上却充满威胁，当过度滥用信任，发现信任其实是安全最致命的弱点。“零信任”颠覆了传统网络安全架构中以网络为边界，将网络内部认为可信的安全范式，将安全不仅仅定义在防护网络边界上。在零信任模型下，任何用户（包括进入内部网络）都不应被信任，需在整个网络中标识用户并对设备登录进行身份认证，而不仅仅是在网络边界上进行身份验证，应把防护边界缩小到单个资源组，不再根据位置对系统授予完全可信的权限。但这并不意味着将抛弃传统 VPN 技术，而是引导安全体系架构从以“网络为中心”走向“以身份为中心”，增强以身份为中心的安全访问控制。

二、零信任“认知度高，采用滞后”的原因

兼容性问题是采用零信任最大的障碍。零信任解决方案需要集成并兼容目前已部署的基础设施及相关系统，将云端和本地网络环境全部覆盖并确保应用层的安全。然而，在边缘不断扩展的网络中采用零信任新型架构极具挑战。例如，国内较早探索零信任架构的企业在做零信任内部落地过程中，由于不断收缩内网权限，矫枉过正，在部署时安装大量客户端且各终端环境复杂，也遇到了兼容性问题；华为 HiSec 零信任安全解决方案是通过厂商的终端安全产品实现全面终端环境感知，终端承载着企业数据的生产、使用和流转，但是终端的多样性及环境的复杂性也带来了兼容性难题。

遗留系统和底层技术与零信任原则相互冲突。一方面，零信任的一个基本原则是对所有资源的访问都需要经过身份验证，而遗留应用程序、基础设施和操作系统没有最小权限或横向移动的概念，也没有动态允许基于上下文使用进行修改的身份验证模型，无法通过零信任感知。另一方面，组织内采用的传统底层技术也有可能违反零信任模型，如 Win10 操作系统采用的 P2P 技术，使得对等系统间可共享 Windows 更新以节省带宽资源，这种系统权限的横向移动基本上是不受控制的，但零信任却不允

许未授权的横向移动的出现；再如，需要点对点操作的ZigBee等网络协议及mesh网络技术均基于密钥或者密码，并不涉及身份验证修改的动态模型。

高投入低产出阻碍零信任架构替换进程推进。零信任部署过程中往往需要对原有系统进行重建，组织重新建设一套零信任系统以满足当前业务需求，需要极大的人力、预算、时间和资源的投入，这使得诸多组织望而却步。如Google作为零信任的领头者，从专线网络及VPN访问模式迁移至零信任模式整整用了长达六年的时间。美国国家安全电信咨询委员会《零信任和可信身份管理报告》指出，零信任是一项变革性工作，政府及相关组织需要承诺至少十年的投入，包括零信任认知度提升和对组织技术架构重新设计的相关工作。此外，零信任会涉及多种安全设备、业务系统及网络，且基于微分割和细粒度边界规则，零信任系统的运维难度及工作量均高于常规运维的工作量。

三、几点思考

加快制定出台零信任政策标准，推动零信任大规模落地。当前，零信任还没有统一的解决方案，各组织均基于自身技术基础及实践经验开展零信任规划和部署，无法开展规模化、兼容性强的落地实施。建议加强政策引导，推动零信任相关标准的制定及实施，以此推动厂商间进行技术协作、开放接口、深挖落地场景，加速零信任全面落地。

着力解决零信任技术瓶颈，加强网络安全防护能力。软件定义边界、身份权限管理、微隔离是零信任的三大核心技术，这三大技术在不同的应用场景中落地存在较大差异，还需要一些辅助技术的加持，对技术要求较高，且与现有的网络架构、资源配置、应用系统所采用的技术密切相关，部署落地具有一定的复杂性。目前对零信任的采用还处于起步探索阶段，需加大对零信任技术的研究，重点突破与部分常用安全技术及现有安全产品、方案的兼容适配。此外，应加快对区块链、大数据、人工智能等新技术场景下解决方案的探索研究，逐步实现零信任大规模落地部署，提升网络安全防护能力。

推动开展局部零信任部署，助力零信任全局化逐步落地实施。推动相关组织在保障业务可用性的前提下，选择从非关键网络资源进行“零信任”升级改造，形成多种灵活的零信任解决方案。后续，再对关键网络资源实施零信任访问控制，并逐渐实现全局化的零信任部署。例如，用户身份认证、设备身份认证、最低权限访问作为零信任应用和服务的三个重点领域，可按逐步增加用户、设备、数据及应用的粒度进行细化和扩展，实现精细安全的访问控制。

责任编辑：杜玢翰 dubh@staff.ccidnet.com