简译版

边缘计算的安全注意事项

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	Edge Computing Security Dos and Don'ts		
原文作者	John Edwards	原文发布日期	2018 年 11 月 21 日
作者简介	John Edwards 是一名资深技术记者。https://www.networkcomputing.com/author/19274213		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/network-security/edge-computing-security-dos-and-donts/110375099		
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		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

边缘计算的安全注意事项

John Edwards

2018 年 11 月 21 日

在物联网环境中，“边缘计算”（Edge Computing）能够提供多种优势，但是有一点你肯定不希望“边缘化”——那就是边缘计算的安全性。

对于物联网设备集群收集到的数据，通过边缘计算可以显著提高汇集、处理和分析这些数据的效率。然而，为了保护物联网设备以及整个企业网络，实施完整和可靠的边缘计算安全措施至关重要。

计算分析公司 Edge Intelligence 首席技术官邓肯·保利（Duncan Pauly）表示，相比于集中环境（如云），边缘计算面临的安全风险有很大的不同。“在云环境中，你的所有数据可能位于一个或少数几个位置。”他解释道，“相比之下，在边缘计算环境中，数据是分散的，因此保护整个数据集会更加困难。”

由于边缘计算涉及分布式数据处理，因此边缘计算的保护比云的保护更具挑战性。“在边缘计算中，有很多运作方式不同的设备（通常是各种传感器和控制器）。”企业安全解决方案提供商 Positive Technologies 的网络安全弹性负责人利·安·加洛韦（Leigh-Anne Galloway）说，“每台设备都以自己的方式配置，这意味着不同的设备有不同的漏洞，这会导致许多问题。”加洛韦指出，虽然边缘计算是一项较新的技术，但是一些老问题仍然存在，包括弱登录凭证、零日漏洞、缺乏更新以及不太理想的网络架构等。

许多物联网用户错误地认为，边缘技术继承了私有数据中心和公有云的安全控制措施、流程和检查点。“现实情况是，所有环境中都存在物理边缘，而且经常对物理边缘进行远程管理和监控。”将于明年初开始运营的可编程边缘公司 Rafay Systems 的首席执行官兼联合创始人哈西卜·布达尼（Haseeb Budhani）指出。“边缘可能不像各机构已经习惯的公有云环境那样安全和可靠，”他警告说，“边缘客户必须以公有云环境作为安全标准，谨慎地审查供应商的安全架构和实践。”

最佳实践

网络安全服务公司 Mosaic451 高级安全工程师沙恩·麦克杜格尔（Shane MacDougall）发

现，任何边缘计算用户都可以采取的最佳安全实践是：为所有边缘节点配置与网络的其他部分相同级别的保护措施。“要记住，网络的安全性取决于最薄弱的环节。”他说，“因此，确保每台主机都被加固和打补丁，对于维护安全的环境至关重要。”

总部位于休斯顿的网络安全公司 SCIS Security 的副总裁兼信息安全顾问负责人丹尼斯·周（Dennis Chow）强调了持续监控和可见性的必要性。“预防是首要措施，检测是必要措施。”他说，“需要预防和检测的活动包括解密的网络流量、日志，以及其他近乎实时的监控功能。”

保利表示，边缘计算用户还需要确保：边缘计算环境中的所有数据（包括传输中的和保存的）都经过加密，所有通信都使用 SSL/TLS 协议，并采用多因子身份验证措施。“如果实施得当，这种方法能够降低对物理安全的依赖性，这是因为数据是加密的，要想访问数据还需要进行多因子身份验证。”

还有一点也很重要，边缘计算将越来越多地部署在数据中心以外的环境中，而这些环境无法保证物理安全。“在这些环境中，安全的数据加密和访问验证将变得越来越重要。”保利说。

最坏实践

边缘计算用户犯的最大错误之一是，他们认为传统的安全控制措施就能为设备提供足够的保护。“例如，他们仅使用杀毒软件和防火墙。这很可能意味着，他们已经是网络犯罪活动的受害者了，只是尚未找到证据。”特权访问管理技术提供商 Thycotic 的首席安全科学家约瑟夫·卡森（Joseph Carson）说。“企业的数据不只是通过互联网连接和防火墙流动，而是通过每一台边缘设备流动。这些设备相当于企业连接网络的‘门户’，因此，他们必须要保护每台设备。”他警告说。

边缘用户新手经常犯的另一个错误就是，将基于云的安全模型应用于边缘计算部署。“AWS 和谷歌各自拥有 20,000 名工程师。以 AWS 为例，每一名工程师保护着 56 个物理位置。”虚拟机安全技术提供商 NanoVMs 的首席执行官伊恩·艾伯格（Ian Eyberg）说，“假设你是一家零售商，想在 2000 个位置运行边缘计算（就像快餐连锁店 Chick-fil-A 做的那样），那么这 2000 个位置需要相同级别的安全性。但是，与大型公有云提供商不一样的是，你很可能没有 20,000 名工程师来保护这些位置。”

总结

“边缘计算将迎来一个全新的时代，这与我们通常所认为的网络安全和云架构有很大的不同。此外，它还会带来很多优势。”艾伯格总结道，“不幸的是，我们必须先经历一些严酷的教训。”

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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、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有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

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厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，为捍卫国家主权、安全和发展利益提供了有力支撑。

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的发言代表，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