

简译版

特权用户可能成为企业最大的安全漏洞

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 - Why Your Most Privileged Users Could Be Your Biggest Security Weakness		
原文作者	Ronan O'Connor	原文发布日期	2019 年 4 月 25 日
作者简介	Ronan O'Connor 是 IBM Europe 的数字营销经理。 https://securityintelligence.com/author/ronan-oconnor/		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/posts/zero-trust-why-your-most-privileged-users-could-be-your-biggest-security-weakness/		
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	<ul style="list-style-type: none"> 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。 		

特权用户可能成为企业最大的安全漏洞

Ronan O'Connor

2019 年 4 月 25 日

企业的安全基础设施旨在保护企业免受恶意威胁。但是，如果攻击者窃取了用户凭证并访问企业的系统，可能会导致企业数据泄露，以及随之而来的声誉损失、运营中断和经济损失。

但是，并非所有访问都“生而平等”。如果企业的某位特权用户的身份信息遭窃，会导致什么后果呢？特权帐户管理（PAM）可以密切监控最敏感的帐户，有助于防范最危险的数据泄露事件。

保护特权帐户至关重要

在大多数数据泄露事件中，攻击者通过网络钓鱼、恶意软件等攻击向量来感染用户帐户和特权帐户。一旦攻击者在网络中创建了据点，就能查找并劫持特权帐户，然后冒充合法用户在企业的网络中横向移动。

此时，恶意活动就开始了。攻击者会在受感染的网络中搜索有价值的数据，如个人信息（PII）、知识产权和财务数据；然后利用这些信息执行金融诈骗等犯罪活动。

保护关键数据意味着保护最有价值的用户——这就是研究公司 Gartner 将 PAM 列为《2019 年十大安全项目》之一的原因。其他项目包括检测和响应、云安全状态管理，企业电子邮件感染等。该公司在 2018 年就将 PAM 列入了十大安全项目清单。

Centrify 公司的研究进一步证明了 PAM 的重要性。其研究指出，74% 的数据泄露涉及未经授权地访问特权帐户。如果说特权访问是最有成效的攻击方法，为何还有这么多公司未采取措施来防止特权滥用呢？

采用“零信任”模型解决特权滥用问题

如果企业希望一劳永逸地解决特权滥用问题，应考虑采用“零信任”（zero trust）策略。《福布斯》指出，采用“永不信任，永远验证”的方法有助于发展数字商业模式。要实现零信任架构，企业必须采用“不断验证”的策略。这意味着创建这样一个环境：在知道访问者

的身份之前，阻止所有访问。

由于网络犯罪分子针对特权用户，因此企业应考虑放弃传统的“城堡护城河”（castle-and-moat）方法，在用户对网络进行初始访问后限制其在内部系统中移动的能力。网络中的默认连接是一种严重的漏洞，攻击者会不断尝试利用这种漏洞。

传统的防火墙充当内外部活动之间的屏障。要迁移到零信任环境，企业必须创建更细粒度的边界，包括单独分割的应用、数据库和基础设施的其他关键部分。

第一步是定义企业的策略，而非技术。企业应确定如何推进该策略，如何将该策略应用于企业的基础设施，然后寻找适当的工具来执行该策略。

这是为了创建可以保护企业中最有价值的用户和系统的体系。企业需要知道，如果不通过监控特权用户来减轻其风险，这些用户可能成为企业最大的安全漏洞。为这些用户创建以验证为中心的安全系统，是降低风险的好办法。

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>