简译版

未使用身份是一项日益严重的安全威胁

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	Unused identities: A growing security threat		
原文作者	多森·巴·诺亚（Dotan Bar Noy）	**原文发布日期**	2021 年 12 月 13 日
作者简介	多森·巴·诺亚是 Authomize 公司的首席执行官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/12/13/unused-identities/		
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	企业管理员向各种“身份”授予访问权限，但之后通常会丧失对这些身份的可见性，导致这些身份处于暴露状态。这属于“管理不善”，这种风险会随着此类“无用户账户”的增加而增加。如果企业能够实施一些基本的安全措施，就能降低此类风险。		
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。		

未使用身份是一项日益严重的安全威胁

Help Net Security

2021 年 12 月 13 日

2021 年 5 月上旬，输送东海岸 45%燃油的管道运营商 Colonial Pipeline 宣布他们遭到了黑客攻击。

在参议院国土安全和政府事务委员会作证时，该公司总裁兼首席执行官乔·布朗特（Joe Blount）表示，黑客通过一个被盗用的旧 VPN 账户入侵了他们的网络。

该事件几乎囊括了所有的安全要素问题：

- 被盗数据中包含凭证
- VPN 账户未设置多因子身份验证保护
- 攻击者利用（很可能不受监控的）老旧服务入侵公司网络

被盗账户很可能是 IT 团队早前创建的保留配置文件。不幸的是，他们把该账户遗忘了，在切换到不同系统时没有关闭该账户，导致该账户能够访问新系统。

他们的错误凸显了一个常见问题：企业管理员向各种“身份”授予访问权限，但之后通常会丧失对这些身份的可见性，导致这些身份处于暴露状态。这属于“管理不善”，这种风险会随着此类“无用户账户”的增加而增加。如果企业能够实施一些基本的安全措施，就能降低此类风险。

眼不见心不烦，但仍有风险

根据我们的内部研究，企业有 6%的用户账户处于非活动状态。但是，它们不被使用并不意味着不会遭到攻击。如果攻击者获得对这些账户的访问权限（尤其是在账户不受监控的情况下），就可以利用这些账户访问企业的资产。

这些账户可能属于已离职的前员工，也可能属于已经改变角色且不再使用这些账户的人员。

这些问题必须要解决。企业可以采用“身份治理和管理”（IGA）工具，在“加入者、

移动者、离开者”生命周期管理框架下很好地解决此类问题。

然而，在管理不善的空组和机器人身份等领域，这些工具也存在盲点。上述两个领域都存在可以使用甚至滥用的权限。

虽说企业的空组并不多，但是这些空组通常可以访问数千个文件，这为黑客窃取数据或在不被发现的情况下造成破坏提供了足够大的窗口。

在机器人身份领域，情况也很糟糕。机器人身份是用于执行各种任务的服务账户，因此具有一系列权限——在某些情况下甚至包括管理员权限。据 Forrester 估计，“非人类”身份的数量在去年翻了一番。

如何识别、监控和补救

控制身份和资产授权的第一步是了解企业拥有哪些“身份”。首先，企业应扫描所有 XaaS 环境（即 SaaS、IaaS 和 PaaS），并清点哪些“身份”有权访问哪些资产。

这涉及从这些不同环境中提取数据，将数据规范化为一个可行的模型，然后将其与企业的身份提供商（IDP)（如 OktaPing、Azure AD 或 Google）的身份相关联。

这样做的目的是了解身份和资产之间的关系，对各种因素进行评估，包括它们的使用情况以及它们是否合适，以满足企业的策略/需求。

举例来说，企业是否存在对“至少 60 天未使用的资产”具有访问权限的身份？如果存在，则应撤销这些身份的访问权限。一旦企业开始更深入地分析其授权，就会发现他们对各种“身份”的授权过多了，有些权限一开始就不应该授予。

弄清楚拥有哪些“身份”之后，企业应着手修复多年来积累的错位授权问题，并制定实施计划。

比如，如果看到有风险的授权弹出窗口，应拒绝。如果发现空组，应将其关闭。对于不经常使用的机器人身份，也应该这样处理。

如果企业的权限配置过程是自动化的，则企业应将其撤销，未来需要时再将其启动。

为了有效地消除“未使用身份”带来的风险，企业需要过渡到一种“摄取数据、监控违规行为并不断进行补救”的状态。

当前的定期检查标准可能会让审计员满意，但如果企业想继续执行足够的安全标准，这还远远不够。

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