由企业内部人员的失误造成的独特安全挑战难以根除

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	Inadvertent Insider Threats Present a Unique Challenge to Organizations		
原文作者	莉萨·迈尔斯（Lysa Myers）	**原文发布日期**	2020年3月13日
作者简介	莉萨·迈尔斯是ESET的安全研究员。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/inadvertent-insider-threats-present-a-unique-challenge-to-organizations/		
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。		

由企业内部人员的失误造成的独特安全挑战难以根除

莉萨·迈尔斯

2020 年 3 月 13 日

根据最新的《 2020 X-Force 威胁情报指数》，2019 年因违规而暴露的记录超过 85 亿条，其中 86%是由资产配置不当引起的。这些问题只影响了 2018 年违规记录的一半，正如 2017 年的报告所述，当年 29 亿条记录中，有 70%是由于配置不当造成的。

这些统计数据展现了因内部人员的失误给企业带来的威胁。虽然我们可以将内部人员的失误想象为粗心的员工点击了不可靠的电子邮件，但我们不能局限于此，因为还有很多种类的不良安全行为。可以说，更大的安全事故来源是人们在内网中创建了具有超级权限的云服务器。

未经监控的添加会增加内部人员失误带来的风险

驾驶一辆经过精心设计、充满创新安全特性、并经过定期测试、在碰撞场景中表现良好的汽车，您能有多安全？如果这辆车在设计过程中没有经过测试来验证法定的安全性能是否得到了正确的使用，您会有不同的感受吗?

资产（含服务器和其他企业设备）配置不当，就好像在制造车间的每个人都为最终的汽车产品添加了意想不到的部件，并希望得到最好的结果。由于没有对这个过程进行监控，所以无法知道一个部分会对其他部分产生什么影响，也无法知道最终产品会如何危及驾驶员的生命。

在人们经常实施影子 IT[1]措施的环境（包括充满敏感客户信息的整个数据库）中，无法验证我们的环境是否真正安全。随着越来越多的行业需要遵守使用“合理”安全措施的规定，如果企业因资产配置不当而发生违规，它们可能会被处以巨额罚款。

我认为我们不仅需要具有安全意识，还需要改善安全态势，以应对内部人员带来的威胁风险。由于服务器配置不当而导致的违规事件的增加进一步证明，安全专家需要学习新方法来应对因内部人员的失误引起的威胁。

[1] 译者注：影子 IT 是指未经授权在公司和组织机构内部创建和应用的 IT 解决方案和系统。

期望与现实

根据 McAfee 去年发布的《云采用和风险报告》，大多数接受调查的企业自己云服务的使用状况：他们认为其环境中仅使用了 30 种云服务。然而，报告发现，平均每个组织机构实际使用了将近 1900 种独特的云服务，且存储在云中的所有文件中有 20%包含敏感数据，这一数字同比增长了 53%。

对于安全从业人员，这些统计数据自然会引发一些问题：谁在什么时间使用了什么类型的云服务？这些服务由谁创建和维护？创建的目的是什么？它们是否可以在更安全的环境中被复制？大概这些并不是在 IT 或安全部门的支持和监督下创建的资产。

在您的环境中回答这些问题的最佳方法是与组织机构中的人员进行持续对话。使用网络的人对于这些问题最为了解，重要的是，他们要乐于告诉您其正在使用的产品和服务，尤其是那些涉及敏感数据的产品和服务。

然而，沟通只是一个开始。您可以也应该采取其他步骤来确定和缓解内部人员威胁。

实施流量监控与拦截

虽然开放的通信环境可以带来各种重要的好处，但您还应该检查网络流量，以确定企业环境中是否经常使用云服务。了解在您的环境中哪些类型的流量是正常的，可以帮助您看到什么时候出了问题，无论是由于人们正在创建未经批准的云服务，还是由于犯罪分子正在从您的网络中窃取数据。

很多企业都会阻止员工访问网关上流行的云服务，但要小心，如果不先与您的员工讨论就这样做，则有可能将影子 IT 进一步推向地下，而不是让它曝光。

为云服务创建可接受的安全使用策略

如果企业已有严重的影子 IT 问题，那么花时间开发一个可接受的、涵盖云服务的使用策略可能有点像把挤出的牙膏塞回牙膏管中。尽管如此，延迟推出彻底的策略总比根本不推出要好。在创建云服务之前，您必须制定相应的规则来说明明应该采取的步骤。这将有助于您确保可以根据适当的预定义安全设置监视和评估这些设备和服务。

确保这些策略除了禁止员工执行的操作之外，还包括可以积极采取的措施。如果您建立

了不遵守策略的惩罚规定，那必须采取一种方法让员工不会因为害怕承担后果而瞒报自己的失误或者发现的事故。

评估云服务的风险

在确定环境中的云服务时，下一步应对其进行彻底检查。无论您是只检查服务是否使用了可用的最佳安全设置，还是将其迁移到一个已批准的平台，您都必须按照流程，以确保随着时间的推移它们仍然是安全的。

如果您尚未进行风险评估，那么现在是开始的好时机。对企业所有的云服务进行风险评估。人们可能会想当然地认为云服务提供商会采取安全措施，但如果我们做出降低自身安全性的更改，那我们就不能期望他们来阻止我们搬起石头砸自己的脚。

一些云服务提供商正试图通过提供扫描配置不当的服务来做到这一点，但很可能有人在没有完全理解这些警告的情况下就点击了这些警告，从而使关键数据处于危险之中。

云服务为疏忽的内部人员提供了一种在我们的防御系统中制造漏洞的新方法。如果安全人员和组织机构其他成员之间的沟通不畅，使得影子 IT 措施不受限制地泛滥，那将使我们的工作更加困难。使用合适的工具和自动检测技术可以在很大程度上帮助我们了解我们所处的环境，但加强内部安全人员与其他业务人员的沟通和交流，不仅仅让业务人员知道如何做，还让他们知道为什么要那样做，对于确保企业资产安全同样重要。

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，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万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，“您们也是国家队，虽然您们是民营企业”。

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