简译版

行为分析：深入了解“内部人员威胁”

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	Behavior Analysis: Getting an Inside Track on Insider Threats		
原文作者	Kacy Zurkus	原文发布日期	2019 年 7 月 2 日
作者简介	Kacy Zurkus 是一名网络安全和信息安全自由撰稿人。https://securityboulevard.com/author/kacy-zurkus/		
原文发布单位	Security Boulevard		
原文出处	https://securityboulevard.com/2019/07/behavior-analysis-getting-an-inside-track-on-insider-threats/		
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。		

行为分析：深入了解“内部人员威胁”

Kacy Zurkus

2019 年 7 月 2 日

了解人类行为可以帮助企业更好地识别和消除恶意内部人员。

无论是已毕业的学生进入校园，使用恶意 U 盘破坏学校的计算机，还是被认为“可信”的员工对企业造成损害；“内部人员威胁”（insider threat）越来越受企业关注。

但是，企业真正担心的是什么，或者是谁呢？目前，企业对内部人员威胁的定义还比较模糊——是那些为了获取经济利益从事犯罪活动的恶意员工？心怀不满的员工？为了个人利益而泄露敏感数据的员工？还是不小心点击了网络钓鱼链接的倒霉鬼员工呢？

根据今年 RSA 大会上公布的一项调查，恶意内部人员是大中型企业最关注的问题。对 671 名受访者的调查显示，用户错误是最严重的内部人员威胁。

在最近的一篇博文中，SANS 安全意识主管兰斯·施皮策（Lance Spitzner）写道，“在与企业或企业高管讨论内部人员威胁时，我们首先要弄清楚内部人员威胁是什么。”

只有弄清楚企业的各类内部人员威胁，才能有效地搜寻经常被忽视的告警迹象。

识别内部人员威胁

有些行为应该纳入企业的“必须监控”清单。但是，许多公司的安全团队缺乏相应的技能，难以确定某些行为发生的根本原因。而相比于通过行为分析创建的模式，这些原因有时会是更好的信标。

Flashpoint 公司内部人员威胁首席顾问艾力克·雷基（Eric Lackey）分享了一个案例。“一家客户公司正在起诉一名前高管。该高管在任职期间向公司的竞争对手提供内部信息，之后竞争对手开办了自己的太阳能公司。公司对该高管的计算机进行取证调查，发现他向其个人电子邮件账户发送了敏感数据。”雷基解释道。此外，该高管还创建了以竞争对手命名的 PPT 演示文稿。

“这是公司数据遭窃的典型案例。对于内部人员来说，公司数据唾手可得——员工可以下载公司数据并将其上传到个人云盘或 U 盘，或者通过电子邮件将其发送出去。这可不

是一两个文件的问题。”雷基说。

公司动辄丢失数百个文件，而他们只能在事后才会发现——这是因为，公司未能有效地监控此类行为，导致此类行为通常能够持续数月。

经常被忽视的告警迹象

既然公司在监控用户的行为，为何还会被恶意内部人员泄露数百个文件之多呢？

雷基说，这是因为企业经常忽视某些告警迹象。“内部人员威胁计划是人类行为和网络领域相交的学科，其最终目标是预测恶意行为。”

这就是企业需要重新考虑“必须监控”行为列表的原因。这些行为包括在专业网络和社交媒体网站上的活动，以及访问异常和趋势等。“许多企业专注于用户行为分析工具，或用户活动监控工具和端点解决方案，但他们并不一定向这些检测工作投入足够的人力。”他指出。

人类行为问题的解决方案

企业应对员工开展识别风险行为的培训。例如，将某人的数据泄露行为与他过去三个月一直在寻找新工作的事实联系起来（即，将工具收集到的所有数据整合起来），可以了解他实施某种行为的前因后果。

“例如，许多公司依赖于数据丢失防护（DLP）解决方案。DLP 是一种非常出色的工具，但是也有点老旧了。”雷基说。识别文件名和文件中的关键字是一种不错的办法，但是许多内部人员威胁计划没有考虑到：查看监控屏幕的分析师，并没有看到发送数百个文件的员工在发送文件之前经历了什么。即使他们发现员工在发送包含关键字的文件，也无法确定这是否是一种威胁——因为他们没有看到此人实施该行为的前因后果。

为了了解事件全局并创建成功的内部人员威胁计划，企业需要挑选出具备相关技能，能够监控和分析人类行为的员工。

“企业务必要对员工进行培训。”雷基说，“企业的员工拥有不同的技能，我们应将这些技能组合起来。例如，有的员工具备反间谍技能，有的员工具备审计或反欺诈技能。他们可以展开合作，互通关键信标。”

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，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、超过十五亿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（APT）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，已连续五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