

简译版

## 识别、了解和打击内部威胁

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	Identifying, Understanding & Combating Insider Threats		
原文作者	Ilan Paretsky	原文发布日期	2019 年 2 月 12 日
作者简介	Ilan Paretsky 是 Ericom 公司的首席营销官。 <a href="https://www.darkreading.com/author-bio.asp?author_id=5131">https://www.darkreading.com/author-bio.asp?author_id=5131</a>		
原文发布单位	Dark Reading		
原文出处	<a href="https://www.darkreading.com/endpoint/identifying-understanding-and-combating-insider-threats/a/d-id/1333830">https://www.darkreading.com/endpoint/identifying-understanding-and-combating-insider-threats/a/d-id/1333830</a>		
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 <a href="https://bbs.antivy.cn">bbs.antivy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>		

## 识别、了解和打击内部威胁

Ilan Paretsky

2019 年 2 月 12 日

**企业肯定会关注来自外部的威胁。但是，你们准备好应对来自内部的威胁了吗？**

大多数（如果不是全部）企业都警惕地防范可能通过电子邮件、网站和其他已知和未知路径渗透端点系统的威胁。但是企业内部的威胁呢？更糟糕的是，那些你认为可以信任的员工呢？

### 什么是“内部威胁”？

“内部威胁”（Insider threats）远非单一种类的威胁。虽然我们倾向于认为，这是图谋报复的前雇员或承包商在寻找不义之财，但事实是，许多内部数据泄露完全是无意的。CA 公司的《2018 年内部威胁报告》指出，公司至少应该像担心恶意内部泄露事件（占有所有内部数据泄露事件的 47%）一样担心意外或无意的数据泄露事件（因用户疏忽或凭证泄露导致，占 51%）。

在过去的一年中，超过 50% 的企业遭受过内部攻击；而今年，预计 90% 的企业容易受到内部威胁。

在防止无意的数据泄露方面，用户教育是首要任务。企业应将安全培训作为入职流程的重要组成部分。当系统更新或新的流程或程序到位时，企业应开展教育和培训课程，这会减少由于错误或疏忽而导致内部攻击的可能性。

但是，如何预测内部的恶意攻击并防止它们及其造成的破坏呢？

### 识别早期告警迹象

企业主、IT 员工和网络安全专家必须始终警惕内部威胁的可能性。这是因为，保护数据免受特权人士的泄露，取决于对数据泄露事件的快速识别和响应。恶意内部人员占据上风——他们处于企业防御边界的内部。通过授权的系统访问，他们可以轻松获取敏感数据，了解企业的弱点，并轻松获取有价值的资产。《2018 年内部威胁报告》显示，正式员工（56%）和特权 IT 用户（55%）是企业最大的内部安全风险，其次是承包商（42%）。

## 关注不满意的员工

员工是否满意？请记住，不满意的员工很容易被诱惑。企业应密切关注员工并考虑他们的心态，这不仅仅是良好的人力资源实践，也是很好的网络安全策略。

因此，企业应与员工保持沟通。与他们会面、交谈，尝试了解他们对企业状态的看法。在事态升级为恶意网络活动之前解决问题，可以使公司免于因内部数据泄露而导致的麻烦。

## 员工离职后立即撤销其访问权限

可以访问公司网络和数据的前雇员构成了重大的安全威胁——那些被解雇的员工会带来特殊的风险。我们以 2014 年索尼影业公司黑客攻击为例。诺尔斯公司的研究人员发现，包括一名前雇员在内的六人组直接参与了此次攻击。而在攻击发生前的几个月，该雇员刚被解雇。这只是巧合吗？更像是复仇。

制定员工离职程序，并彻底、及时地执行这些程序。员工离职后立即通知 IT 部门，迅速撤销其对网络、数据和计算机设备的所有访问权限。

## 留意员工的经济危机

众所周知，内部泄露事件通常是出于经济动机和贪婪。无论是员工正在经历信贷紧缩、没有获得预期的晋升或加薪，还是面临健康危机或其他意外压力，都可能导致他们急需大笔资金。

除了构成网络安全威胁外，经济压力还会影响员工的工作效率和健康状况。人力资源专家应确保管理人员了解员工经济压力的迹象，并关注这些迹象可能导致的行为。

## 关注突发、不明原因的兴趣或行为变化

员工突然开始加班了？企业应关注不寻常的、无法解释的员工行为。员工突然有兴趣访问其当前任务之外的机密资料或信息了，企业应予以警惕，并调查出现这种变化的原因。企业不要盲目地信任员工，无论他们在公司中担任什么职位。

我们以爱德华·斯诺登为例。这位前中央情报局 (CIA) 特工和美国政府雇员逃离该国之前公布了有关政府监视的记录，直到今天他声称从未后悔过。

## 为员工分配最低权限

防范内部威胁的最佳实践包括：注意可疑或不稳定的行为；严格遵守员工离职程序；关注员工的不满情绪并予以解决。

现在，为了减少内部威胁的攻击面，越来越多的企业开始执行最低权限原则，以限制员工的权限。每位员工仅具备作业所需的系统和数据访问权限。同样，每个系统仅具备执行其指定职责所需的最低权限。

“零信任”（zero-trust）方法正是采用最低权限原则打击内部威胁，该方法不信任任何人或设备，无论他们是在网络边界内部还是外部。这要求对每个人和/或设备进行身份验证以访问资源。如果恶意代理进入系统，微分段（microsegmentation）可以阻止他们的传播。

这样一来，更少的员工会执行恶意行动，更少的帐户会被黑客入侵，更少的人会犯导致数据泄露的错误。

## 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>