

简译版

中小企业增强防御需了解五件事

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	5 Things Every SMB Should Know to Strengthen Defenses		
原文作者	Ashley Arbuckle	原文发布日期	2019 年 5 月 23 日
作者简介	Ashley Arbuckle 担任思科全球安全客户体验副总裁兼总经理。		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/5-things-every-smb-should-know-strengthen-defenses		
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。 		

中小企业增强防御需了解五件事

Ashley Arbuckle

2019 年 5 月 23 日

根据美国商业改善局（BBB）的数据，在北美企业中，小企业占 97% 以上，这令人很惊讶。好消息是，在所有网络攻击中，只有不到一半是针对中小企业的；而坏消息是，当中小企业遭受攻击时，他们大多都无法生存下去。但是，中小企业可以采取的措施来改变这一点。

在本月初的“全国小企业周”之后，中小企业高管是时候了解以下五件事情了，以便做好准备并增强防御。

1. 中小企业是很有吸引力的目标

根据 BBB 的数据，43% 的攻击针对中小企业；而《2018 年威瑞森数据泄露调查报告》发现，58% 的中小企业遭遇了数据泄露事件——这说明攻击的成功率很高。除了直接从中小企业窃取数据之外，攻击者还将中小企业作为跳板，以渗透到更大的企业中，执行更大规模的攻击活动。攻击者觊觎每一个可能的攻击机会，并寻求最大的回报，这意味着他们会继续将中小企业作为攻击目标。

2. 攻击的影响可能是毁灭性的

对于中小企业来说，从网络攻击中恢复会很困难且成本高昂，甚至是不可能的，具体取决于攻击的性质和范围。中小企业不太可能拥有多个办公地点或业务部门，其核心系统通常更加互联。当这些企业遭受攻击时，威胁可以快速、轻松地从网络传播到其他系统，带来毁灭性的影响。当 BBB 向北美的小企业主询问：“如果永久性地失去对核心业务数据的访问权限，你的企业还能支撑多久”时，约三分之一的受访者表示他们还可以支撑三个月以上，而超过一半的受访者则表示，他们只能支撑不到一个月。

3. 中小企业最关心的网络威胁

思科对 26 个国家/地区的 1816 家中小企业进行了调查，发现受访者最关心的威胁如下：

- 针对员工的攻击，如精心设计的网络钓鱼活动。
- 高级持续性威胁，如未出现过的高级恶意软件。

- 勒索软件。这类威胁尤其严重，因为中小企业无法承受停机和失去对关键数据的访问权限，因此更倾向于支付赎金。

4. 中小企业还面临其他威胁

尽管中小企业担心勒索软件威胁，但是随着越来越多的攻击者将注意力转向挖矿（cryptomining，窃取计算能力以挖掘加密货币并由此创收），此类威胁逐渐减弱。当挖矿软件进入企业环境时，会降低系统的性能，而且通常意味着企业还会遭受其他类型的威胁。此外，企业的内部威胁也在增加，没有任何企业可以避免这一点。但这并不意味着每家企业都有员工恶意地将企业暴露在风险之中，员工或承包商的粗心大意通常是主要原因。

5. 增强防御的建议

有很多方法（包括人员、流程和工具）可以帮助企业改善网络安全。以下是其中一些建议。

- 关注外包和云安全**

与大型企业一样，中小企业也面临着网络安全人才短缺问题，因此许多企业希望通过外包和云策略来增强防御。这两者都是帮助企业充分利用有限资源的有效手段。但是，如果公司认为外包提供商或云合作伙伴能够提供他们缺乏的所有功能，那公司就会遇到麻烦。中小企业应了解外包提供商提供的分析和监控服务的范围，以及云提供商提供的安全控制措施的种类和影响。

- 强化安全流程**

对安全实践进行全面审查有助于企业识别其防御中的弱点。可能是由于人才缺乏，审查流程在中小企业中并不普遍，但是，这些流程可以大大减轻员工的负担。通过审查安全实践，中小企业可能会发现他们需要增强或添加以下策略：一致的访问权限管理和职责划分、网络分段、口令管理、备份关键数据并确保备份不易受攻击，以及持续的员工安全意识培训等。

- 寻求整合工具**

在考虑新工具时，中小企业要避免增加要管理的供应商数量。企业应选择一个开放式平台，以便在共享数据和威胁情报时简化与工具的整合，而非挣扎于各自产生告警的单个产品，因为这种产品难以识别导致最大风险的威胁。这种平台还可以提供自动化功能，从不同的安

全产品中提取数据，并将它们聚合到易于阅读的单一面板中，这样可以节省大量的时间和精力，同时提供更好的可见性和可控性。

即使中小企业没有足够的资源进行全面的安全评估和审核，渐进性的改变也比没有改变强。要记住，随着威胁形势和攻击面的不断演变，企业必须不断审查并改进其安全措施。

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>