

简译版

提高网络弹性：让企业事半功倍

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	Cyber Resilience: Doing More with Less		
原文作者	托斯汀·乔治 (Torsten George)	原文发布日期	2020 年 4 月 22 日
作者简介	托斯汀·乔治是 Centrifify 的安全专家。		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/cyber-resilience-doing-more-less		
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。 		

提高网络弹性：让企业事半功倍

托斯汀·乔治

2020 年 4 月 22 日

“新冠”疫情迫使企业安全团队需要用更少的资源提供更多的服务。

这绝对不是一件简单的事。威胁行为者正充分利用这些特殊时期，通过网络钓鱼、勒索软件和撞库攻击等手段，发起新一轮的网络攻击。VMware Carbon Black 威胁研究人员的数据显示，仅勒索软件一项攻击在过去一个月就激增了 148%。同时，许多企业被迫裁员并推迟了计划的 IT 安全项目。现在比以往任何时候都需要将重点放在能够确保最大收益的防御策略上。因此，企业精打细算过紧日子的同时，应该关注可以在哪些方面提高网络弹性。

根据 ESG 的研究，62% 的企业准备在 2020 年增加网络安全支出。事实上，32% 的受访者表示，他们将投资于使用 AI / ML 进行威胁检测的网络安全技术，然后是数据安全 (31 %)，网络安全 (30%) 和云应用程序安全 (27%)。显然，这些优先事项已经颠倒过来了，新常态要求对传统安全策略进行彻底的重新思考。

为了提高当前条件下的网络弹性，至关重要的是，应重点关注黑客战术、技术和程序（通常称为 TTP）环境中的安全控制措施的有效性。在减少人员和削减预算的情况下，这种方法可以帮助安全领导者防御网络敌人的攻击。根据对威胁行为者的 TTP 分析，在不增加使用资源的情况下，以下五个最佳实践可以提高网络弹性：

1. 为员工和 IT 管理员建立安全的远程访问.....

为了保持运营，在“新冠”疫情期间，企业被迫开启 100% 的远程工作模式。尽管最初的重点是提高员工的工作效率，让他们能够正常的工作。但是企业现在应该重新审视其远程访问部署，以确保拥有关键权限的员工和 IT 管理员帐户免受威胁行为者的侵害。例如，超级用户应结合身份访问区域、多因子身份验证和最小特权，减少使用 VPN 访问。

2. 避免上当（网络钓鱼）

最终，与利用现有漏洞（甚至是零日漏洞）相比，通过网络钓鱼攻击窃取有效凭证并使用它们访问网络更容易、风险更低、效率更高。根据 Barracuda Networks 的数据，自 2 月底

以来，网络钓鱼邮件的数量增加了 6 倍以上。因此，网络安全防御需要适应这一现实。用户教育和加强组织的身份验证系统是两个基本步骤，可以最大限度的降低与网络钓鱼和随后针对数据泄露的网络攻击相关的风险。

3. 加强多因子身份验证

显然，威胁行为者不再通过“入侵”设备来执行可导致数据泄露的攻击。相反，他们只通过利用薄弱的、默认的、被盗的或以其他方式受到破坏的凭证来登录账户。多因子身份验证（MFA）仍然是增强组织现有访问控制的最可靠选择。使用 MFA 取代和（或）补充用户名和密码身份验证，极大地提高了执行网络攻击的门槛和成本，这就是其被攻击的概率接近于零的原因。如果您尚未实施 MFA，那么现在是时候去实施了。否则，您可能需要考虑通过提高身份验证级别（如美国国家标准技术研究院（NIST）SP 800-63A 定义）来提高安全性。

4. 提高针对勒索软件的基础架构防御能力

如上所述，勒索软件攻击在过去两个月里急剧增加，目前还看不到缓解的迹象。也没有针对每种现有勒索软件变种的广谱免疫工具。但是，遵循基本的最佳实践，包括实施安全意识计划、定期备份数据以及应用最小特权访问权限，可以最大程度地降低企业受到勒索软件威胁的风险。

5. 实施最小特权

说到违规事件，最终其实都是人为因素导致的。实际上，Forrester Research 估计有 80% 的安全漏洞涉及受损的特权凭证。很明显，对人为因素实施更好的控制，能够显著改善数据泄露预防工作的效果。对于超级用户和 IT 管理员来说，基于足够、即时特权访问管理（JIT PAM）的最小特权访问是最佳实践。最小特权是指只向 IT 管理员提供在一定时间内执行某个任务所需的权限，实施最小特权是应对许多安全事件的最佳策略。

随着企业缩减 IT 预算，以应对当前健康危机导致的经济紧缩，安全团队需要用更少的资源提供更多的服务。重点关注作为安全边界的身份验证对于缓解网络威胁来说是一种行之有效的有效的方式。

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 endpoint 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，“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>