2022 年能够推动网络安全的两项举措

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	Two initiatives that can move the needle for cybersecurity in 2022		
原文作者	阿肖克·桑卡尔（Ashok Sankar）	**原文发布日期**	2022 年 2 月 2 日
作者简介	阿肖克·桑卡尔是 ReliaQuest 产品和解决方案营销副总裁。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/02/02/initiatives-cybersecurity/		
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		
摘要	2022 年，企业应更全面地审视他们的安全计划，改善基本安全实践，例如调整安全指标或采用新的安全方法等。虽然在新的一年里，网络攻击很可能会大幅增加，但是希望更多的企业能够更好地应对威胁。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

2022 年能够推动网络安全的两项举措

阿 肖 克 · 桑 卡 尔

2022 年 2 月 2 日

众所周知，2021 年对于网络安全专家来说是艰难又压力重重的一年。新冠疫情驱动的远程/混合办公模式，以及勒索软件威胁的加剧，促使企业重新评估他们的安全策略。今年也不例外，随着攻击者利用新的攻击向量来渗透企业网络，企业面临的威胁会进一步增加。因此，企业必须做好充分的准备来应对威胁。

为应对威胁，公司必须建立一种更标准化的方法来衡量安全有效性。不幸的是，很多企业缺乏这样的方法。在 2022 年，他们需要对其安全方法进行调整。此外，零信任策略的采用率将迅速增加。虽然目前，只有不到一半的安全领导者将零信任原则作为其安全战略的一部分；但是到 2022 年底，这一比例将超过 50%。

在下文中，我们将深入探讨企业可以采取的一些措施。

1. 建立有效的安全指标

2021 年发生了多起严重的网络攻击事件。今年，企业应考虑重置其安全计划。首先，企业应制定可行的标准化安全指标。缺乏与企业业务相关的框架以及定制方法，是企业无法实施有效安全计划的主要原因。此外，只有三分之一的网络领导者认为其安全团队使用了正确的指标。没有正确的指标，网络领导者就难以向高管阐明问题，最终导致沟通不畅和安全投资减少。

今年，企业应考虑针对下述问题制定可操作的指标。

- **准备程度：**对攻击的准备程度如何？衡量这一点的最佳方法各不相同，但是有效的方法可确保正确的安全控制措施到位并发挥作用。这需要安全团队实施攻击模拟演习，以识别应该解决的故障或差距。
- **工具的效力：**多年来，企业在各种安全工具和技术上投入了数百万美元。但是许多工具处于休眠状态、未充分利用或未优化。安全和运营团队应确保这些工具是有效的并予以优化。

- **运营差距：**安全团队应利用领先的框架（例如 Cyber Kill Chain 和 MITRE ATT & CK）来衡量覆盖率并识别差距。通过了解每种技术的检测性质和级别，安全团队可以了解他们的漏洞并优化投资。

- **风险情况：**网络安全计划的主要目的是保护企业免受网络风险。企业应优先考虑他们最关心的风险、威胁类型和可能的攻击向量，并了解他们可以采取哪些保护措施。

- **检测、解决和遏制攻击的平均时间：**跟踪检测、解决和遏制恶意攻击所需的时间，可以帮助企业确定安全流程中最需要关注和优化的步骤。

使用这些指标作为基线，能够显著改善公司的安全状况。重要的是，企业应不断地更新这些指标，以适应不断变化的网络安全状况。确定了安全指标之后，企业就可以更具战略性地考虑安全问题，包括采用诸如零信任等新方法。

进一步理解零信任策略

“零信任”是 2021 年的热门术语之一。然而，业界对于它的影响以及如何利用这种安全模型仍然感到困惑。只有不到一半的安全领导者表示，他们正在考虑实施零信任原则。今年，更多的企业将会采用零信任策略。

企业不应将零信任策略视为单一的解决方案。本质上看，零信任策略旨在重新思考企业的安全问题并跨越安全孤岛，是需要持续监控的安全范式的进一步演变。鉴于此，在 2022 年，企业应进一步理解并采用零信任策略。

2022 年，远程办公将继续存在，企业的数据和资产无法受到企业防火墙的保护，因此更多的企业将会采用零信任框架。当然，企业也可以让员工使用 VPN。但是，VPN 很容易被黑客入侵。

2022 年，企业应更全面地审视他们的安全计划，改善基本安全实践，例如调整安全指标或采用新的安全方法等。虽然在新的一年里，网络攻击很可能会大幅增加，但是希望更多的企业能够更好地应对威胁。

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，目前，安天的威胁检测引擎为全球超过八十万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