五大热门安全趋势

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	The 5 Most Hotly Contested Security Trends and Questions		
原文作者	大卫·比森（David Bisson）	**原文发布日期**	2022 年 1 月 5 日
作者简介	大卫·比森是一位信息安全记者。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/debatable-the-5-most-hotly-contested-security-trends-and-open-questions/		
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	企业基于假设推动与网络安全相关的决策。《福布斯》指出：“风险评估、预算需求和优先事项都是假设性辩论的结果，并受到内部压力和政治的影响。企业安全专家和高管都在不断寻求安全解决方案或方法，但这些解决方案或方法都需要投入资金且都存在风险。”因此，在网络安全方面存在一些开放性问题，这些问题决定着企业在未来几年内可以采取哪些策略。在本文中，我们将分析正在塑造网络安全领域的五个问题。		
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。		

五大热门安全趋势

大卫·比森

2022年1月5日

企业对网络安全工作采取刻板的立场，是一件很糟糕的事情。如今，数字威胁形势不断演变，如果企业局限于一种观点，就会导致风险增加，无法防御其他数字威胁。

实际上，企业基于假设推动与网络安全相关的决策。《福布斯》指出：“风险评估、预算需求和优先事项都是假设性辩论的结果，并受到内部压力和政治的影响。企业安全专家和高管都在不断寻求安全解决方案或方法，但这些解决方案或方法都需要投入资金且都存在风险。”

因此，在网络安全方面存在一些开放性问题，这些问题决定着企业在未来几年内可以采取哪些策略。在下文中，我们将分析正在塑造网络安全领域的五个问题。

1. 口令是否弊大于利?

微软等科技公司放弃口令的原因有三个。首先，他们正在寻求单点登录（SSO）等技术，这些技术不会像传统的基于口令的身份保护那样影响员工的体验和生产力。其次，通过无口令身份验证，企业更容易保护其授权账户免受暴力破解、撞库等依赖猜测弱口令的攻击。第三，企业选择采用多因子身份验证（MFA）等控制措施，以限制攻击者利用泄露口令执行恶意操作。

但是，无口令身份验证也是存在风险的。举例来说，指纹读取器、生物识别扫描器等安全措施提供了新的攻击目标，攻击者可能会通过这些目标来访问用户数据。此外，无口令身份验证也无法使企业和用户免受网络钓鱼攻击、诈骗和身份窃取攻击。

因此，企业需要了解无口令身份验证的优势和风险，以便妥善保护用户。

2. 防火墙是否能够为零信任服务?

答案很微妙。传统防火墙无法保护企业免受渗透网络的威胁，因此无法为零信任服务。

但下一代防火墙（NGFW）可以。NGFW可以充当分段网关，利用网络访问工具、微分段、Web应用程序防火墙等工具，以此来补充零信任策略。分段网关在网络的中心（而

非边界）运行。这样一来，它们可以提供对数据访问的洞察力，信息安全团队可以利用这些信息识别潜在攻击。

3. 网络靶场能否为企业提供帮助?

2020 年，新冠疫情爆发，且发生了 Colonial Pipeline 等严重的攻击事件，企业被迫迅速迁移到远程/混合办公。因此，企业对网络靶场的需求不断增加。需要注意的是，并非每个企业都需要长期的网络靶场。有些企业无法负担构建和维护网络靶场的费用。

话虽如此，网络靶场确实有其优势。例如，通过网络靶场，企业可以提高其安全团队的协同水平和经验。安全团队可以沉浸在真实的攻击场景中，探索真实的响应方法。此外，网络靶场还可以帮助企业满足美国国家标准与技术研究院（NIST）和其他机构制定的合规标准和要求。

企业需要注意，并非每个网络靶场都“生而平等”。因此，他们需要确定哪种类型的网络靶场适合其安全需求。这样一来，他们就可以构建和维护适合他们的解决方案。

4. 安全专家是否需要走传统的职业道路?

完全不需要。信息安全人员源于各种背景，例如在线玩扑克、服兵役和音乐学院等。这些经验有助于为其工作提供信息，能够为安全社区提供新视角，从而保护企业的系统和数据。这就是说，任何人都可以在网络安全领域开创自己的事业。

5. 开发人员可以做些什么来确保企业的安全?

企业在“谁负责安全”方面缺乏凝聚力。例如，许多安全专家不信任开发人员编写安全代码的能力。同时，开发人员觉得他们没有获得适当的指导来保护企业的安全。

这说明企业的数字防御缺乏明确性。例如，在 GitLab 最近进行的一项调查中，大约三分之一的安全人员表示他们为安全负责。近 30%的受访者表示，企业中的每个人都应对安全负责；而 21%的受访者表示开发人员应为安全负责。

显然，企业需要采取一些措施。与几年前相比，如今大多数开发人员发布软件和应用程序的速度更快了。这说明开发人员在“为企业安全做贡献”方面有更多的机会。

关键是，安全专家和开发人员可以合作实现代码安全。其中一种方法是，通过无缝的、

API 消费模型公开他们提供的服务。这样一来，开发人员更容易将安全性融入软件开发生命周期。

此外，企业应为其开发人员提供安全意识培训。除非开发人员了解他们面临的安全风险，否则就无法成为 DevSecOps 合作伙伴。考虑到这一点，企业可以将 DevSecOps 视为培养协作和包容性安全文化的契机。

网络安全是不断变化的

本文所讨论的问题可能在几年内都不会被公开讨论，但它们确实能够为企业提供一些思路。幸运的是，安全行业是一个社区，该社区将会继续探索这些问题。

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