漏洞管理对企业的重要性

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 importance of vulnerability management for your organization		
原文作者	迈克尔·米特尔（Michael Mittel）	**原文发布日期**	2021 年 12 月 2 日
作者简介	迈克尔·米特尔是 RapidFire Tools 公司的总裁。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/12/02/importance-vulnerability-scanning/		
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	对抗潜在攻击的一个重要方法是实施漏洞扫描，以检测网络、应用程序和安全漏洞并对其进行分类。通过漏洞扫描，企业可以识别已知漏洞、编码错误、数据包构造异常和对敏感数据访问的错误配置，进而评估攻击者可能利用哪些弱点。		
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。		

漏洞管理对企业的重要性

迈克尔·米特尔

2021 年 12 月 2 日

现实世界中，“入室盗窃”是指犯罪分子通过打开的窗户、未上锁的门、打开的车库等轻松进入房屋，并实施盗窃。而在电子世界中，攻击者伺机寻找网络漏洞，以便能够访问他们想要的数据。相较于大型企业来说，中小型企业（SMB）用于安全工作的资源更少，因此是更受犯罪分子青睐的攻击目标。

漏洞扫描

如果你聘请家庭安全专家，他们通常会从外到内地检查房子内外的每个窗户、门和入口。他们的工作是确保所有可能的进入方式都是安全的，并消除弱点。

漏洞扫描与上述检查非常相似，是指从内外部寻找企业网络的入口点。通过漏洞扫描，企业可以识别其薄弱点，赶在网络犯罪分子有机会利用它们并对企业织造成严重破坏（可能造成数百万美元的损失）之前消除或修复这些薄弱点。

美国国家标准与技术研究院（NIST）建议，无论企业的网络规模或类型如何，应至少每季度进行一次漏洞扫描。对于依赖计算机网络持续可用性进行常规操作的企业来说，应至少每月进行一次漏洞扫描；对于收集和/或处理个人或敏感数据的企业来说，应更加频繁地进行漏洞扫描。

如果将所有直接和间接成本（包括停机时间、罚款、诉讼、通知和对信息泄露人士的身份保护）加起来，一次内部人员数据泄露可能会造成约 768 万美元的损失。很显然，内部人员威胁也是非常严重的，企业不能仅考虑外部网络攻击。数据泄露不仅会造成经济损失，还会造成声誉损失和客户流失。

对抗潜在攻击的一个重要方法是实施漏洞扫描，以检测网络、应用程序和安全漏洞并对其进行分类。通过漏洞扫描，企业可以识别已知漏洞、编码错误、数据包构造异常和对敏感数据访问的错误配置，进而评估攻击者可能利用哪些弱点。

定期扫描

虽然 NIST 建议企业进行定期扫描，但是 RapidFire Tools 最近进行的一项调查发现，33%的企业并没有进行任何定期漏洞扫描。不幸的是，即使 IT 专家了解这些风险，但是他们往往受到预算限制——大约 60%的受访者表示，如果漏洞扫描的成本能够降低一些，他们会更频繁地进行扫描并检查资产的安全性。

虽然漏洞扫描无法让企业免受网络攻击，但它能够增加另一层保护，有助于阻止攻击者。鉴于一次攻击可能会造成超过 700 万美元的损失，IT 专家应将漏洞扫描作为其整体网络安全支出计划中的一个关键项目，并对其分配预算。

最近的调查还发现，几乎三分之一的企业没有执行漏洞扫描，因为这些企业的 IT 专家认为漏洞扫描过于复杂和耗时。对于承担多种职责的 IT 专家，最好将漏洞扫描外包给托管服务提供商 （ MSP ），以确保以经济高效的方式保护企业系统，并且不会妨碍日常任务。无法外包漏洞扫描的内部 IT 团队，应考虑那些通过自动创建票证简化扫描过程，并轻松设置自定义告警的解决方案，以避免误报和其他可能阻碍漏洞识别的“噪音”。

实施漏洞管理计划可帮助企业评估和保护其网络。该计划包括检测、评估和缓解系统和软件的安全漏洞，其关键在于漏洞检测。如果无法检测到漏洞，就无法修复漏洞。漏洞未被发现的时间越长，造成的损害就越大。

随着针对 SMB 的网络攻击不断增加，企业需要采取主动的网络安全方法，其中一个关键方法就是漏洞管理。

不要成为下述一员

- 52%的 SMB 报告说凭证是他们最容易泄露的数据
- 83%的 SMB 数据泄露是出于经济动机
- 22%的 SMB 在未建立威胁防御计划的情况下转移到远程办公
- 50%的 SMB 所有者承认他们没有为员工提供网络安全培训
- 58%的企业表示员工无视网络安全指令
- 42%的 IT 领导者认为，他们的静态数据丢失防护工具只能检测到一半的威胁事件。

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