简译版

增强网空防御的三种方法

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	3 Ways to Strengthen Your Cyber Defenses		
原文作者	克里斯·哈伦贝克（Chris Hallenbeck）	**原文发布日期**	2020年3月4日
作者简介	克里斯·哈伦贝克是Tanium公司美洲区首席信息安全官。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/risk/3-ways-to-strengthen-your-cyber-defenses/a/d-id/1337145		
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	• 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。		

增强网空防御的三种方法

克里斯·哈伦贝克

2020 年 3 月 4 日

安全领域专业人员承受着很大的压力。这是可以理解的：根据网络保险公司 Hiscox 的数据，在过去 12 个月里，有 61%的美国和欧洲企业遭受了网空攻击，高于 2018 年的 45%，而且数据泄露的种类繁多，而且数量也出现增长。攻击的频率也在上升，同一时期内报告遭到四次或四次以上攻击的公司数量从 20%上升到 30%。

随着网空攻击越来越多，越来越复杂，黑客也更加灵活，企业的首席信息安全官（CISO）必须采取更多措施来建立全面的安全策略，以保护关键资产，监控影响，保证企业能够从任何意外攻击或破坏中恢复。建立防御系统还需要从根本上转变思维。安全和 IT 部门的领导者应该认真审视自己的工作方式，问问自己：企业的安全态势真的坚如磐石吗？注意到那些经常会导致违规事件的 IT 安全基础信息了吗？应该采取哪些核心的基本措施，以确保在尽可能的向前发展的前提下，尽最大可能减小遭到网空攻击的风险。

以下 3 个基本措施将有助于增强企业的网空防御。

1. 及时修补漏洞，不要拖延

许多组织机构未能及时修补其硬件和软件中的漏洞。我们与弗雷斯特咨询公司（Forrester Consulting）进行的最新研究表明，修补 IT 漏洞可能需要 28 到 37 个工作日。当这些安全漏洞被公开时，恶意行为者可以更轻松地进行攻击，从而为大量破坏性攻击铺平道路。因为企业不及时修补漏洞，则会造成系统的破坏或者数据泄露，便无法安全运行或保护其数据（或客户的数据）。

黑客可以并且将会利用任何可用的漏洞来攻破网络、破坏运营、窃取数据或勒索赎金。每天都有新的漏洞被发现。例如，今年 1 月，美国国家安全局向微软通报了一个漏洞。最重要的是这个漏洞将允许攻击者启用远程代码执行功能。（微软很快修复了该漏洞，该漏洞影响了 Windows 10 和 Windows Server 2016/2019。）此外，尽管有人认为 Mac 和 iOS 更安全，但苹果一直在应对 iOS 设备的“越狱”问题，这些问题会造成安全漏洞，而且这些漏洞并不总是那么容易修复。

但面临风险的不只是操作系统和主流程序。例如，Adobe FrameMaker 存在内存损坏漏洞，成功利用后可能导致任意代码执行。

由于每天都会发现此类和许多其他的漏洞，安全团队必须实时了解其 IT 企业。他们需要观察到所有计算设备和端点，并且他们必须具有快速修补其硬件和软件中的漏洞并监视其环境的能力。为此，统一的端点管理平台是一种能够更快地监视和修补系统的有效方法，也会降低违规和破坏的可能性。

2. 改善 IT 和安全运营之间的关系

去年发生的事件也证明了其他基础概念面临着挑战。我们的研究发现，IT 决策者有一种错误的自信：80%的人认为他们可以根据漏洞扫描的结果采取行动，但只有不到一半（49%）的人认为他们能够全面了解其环境中的所有硬件/软件资产，包括服务器、笔记本电脑、台式机和容器。

我们发现，当 IT 团队与安全和运营团队更紧密地协同工作时，总体可视性会显著提高，而且他们能够更好地使用可操作的共享数据集保护整个企业。在 IT 决策者中，与那些拥有良好伙伴关系的人相比，那些与安全团队关系紧张的人（40%）在保持可见性和 IT 安全方面更加困难。当这两个团队不能协同工作时，事情就会失败，错误就会产生，违规是不可避免的，整个组织机构就会处于危险之中。他们所需要做的就是在目标、关注领域和工具上达成一致。

3. 工具整合

我们看到的组织机构所犯的最大错误之一就是采用的工具数量激增。通常情况下，当问题出现时，企业就会获得一种补救工具来解决问题。这种方法常常导致工具堆积如山，难以大规模管理和监测。仅用于提升安全性，我们的研究表明，仅在过去两年中，IT 团队平均获得了五个的新工具。

IT 主管需要退后一步，积极评估所有工具。他们应该确定组织机构需要实现的能力及其可交付的成果，这将有助于他们更清晰地了解其网络，并确定可以在两个团队中合并的工具。最终形成一个更高效、更明智的管理环境，这将有助于企业取得积极的业务成果。

始终保持警惕

IT 团队在迈入新的十年之际，将继续面临巨大的挑战。恶意行为者比以往任何时候都更加复杂，而许多企业仍在与紧张的内部关系、未修补的漏洞和缺乏全面的端点可见性作斗争。通过以上三步骤采取的积极行动，组织机构可以以更大的灵活性和信心来应对威胁。

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，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*