容器的错误配置会导致严重的安全问题

非官方中文译文·安天技术公益翻译组 译注

简译版

文档信息			
原文名称	Misconfiguration a Top Security Concern for Containers		
原文作者	Kevin Townsend	原文发布日期	2018 年 11 月 14 日
作者简介	Kevin Townsend 是 SecurityWeek 的签约作家。		
原文发布单位	SecurityWeek		
原文出处	https://www.securityweek.com/misconfiguration-top-security-concern-containers		
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。		

容器的错误配置会导致严重的安全问题

Kevin Townsend

2018 年 11 月 14 日

尽管越来越多的企业开始在 DevOps 中使用容器（container），但他们对其安全性还是很担忧。在一项新调查中，35%的受访者认为他们的公司没有对容器安全进行充分的投资，另有 15%的受访者则认为公司没有认真对待容器安全问题。

该调查由 StackRox 公司发起，受访者是来自各公司的 230 名 IT 员工（其中有将近一半受访者的主要职责是 IT 安全）。超过 45%的受访者来自员工人数超过 10,000 人的大公司，58%的受访者来自金融科技或技术行业。StackRox 在其报告《容器安全现状》中指出，尽管容器和 Kubernetes 的使用量激增，但是大多数企业都未做好保护云应用的准备。（译者注：kubernetes，简称 K8s，是一个开源的，用于管理云平台中多个主机上的容器化的应用。）

Docker 是最受欢迎的容器，有 189 位受访者使用。Kubernetes 由谷歌开发，是目前最受欢迎的容器编排器，有 122 位受访者使用。Docker Swarm 排在第二位，有 93 位受访者使用，这些受访者主要来自员工人数达到 5000 人或更多的大型公司。

40%的受访者在混合环境中（本地和云端）运行容器，28%只在云端运行，另有 32%只在本地运行。那些在云端运行容器的受访者中，118 位使用 AWS，56 位使用 Azure，39 位使用 Google Cloud Platform。“考虑到谷歌在容器使用和 Kubernetes 方面的行业领导地位，这个排名有点出乎意料。”该报告评论道，“但是考虑到我们的调查对象大多是大型企业，这一点也可以理解。”

54%的受访者最担心的是编排器的错误配置，包括 Docker 容器和 Kubernetes 编排器。StackRox 产品副总裁邓韦琏（Wei Lien Dang）指出，“最严重的‘容器攻击’包括特斯拉 AWS 挖矿事件和 Shopify 元数据泄露事件。这两个问题都源于编排器的错误配置。”

2018 年 2 月，RedLock 公司披露，特斯拉在 AWS 服务器中运行的 Kubernetes 容器被劫持并用于挖矿。发现该问题后，特斯拉在一天内锁定了其服务器。这并不是说 Kubernetes 不安全，而是访问容器的操作过于复杂——而这正是受访者担心错误配置的原因。

“Kubernetes 平台面临的安全挑战，不是被直接访问、登录并攻击。”邓韦琏解释道，

“而是在于，Kubernetes 经常意外地配置已经暴露的内容（例如仪表板），或者其元数据是可访问的，这些错误配置会导致攻击的发生。”

DevOps 对容器的支持，以及 DevOps 不一定有安全团队参与，也加剧了容器的安全风险。

“最常使用容器和配置 Kubernetes 的团队是 DevOps 团队。”他继续道，“安全团队应该参与制定保护基础设施的策略和指南。任何容器安全解决方案都应该将安全性纳入 DevOps 的考量——利用 DevOps 的工具和流程提供安全监督和指导。”

StackRox 公司认为，像许多强大的平台一样，Kubernetes 最好配备一个抽象层。这个安全抽象层能够识别配置错误，发现诸如不必要的开放通讯端口或路径等风险。

在评论调查结果时，调查和咨询公司 CyberEdge Group 的联合创始人兼首席运营官马克·布查德（Mark Bouchard）说：“在每一次基础设施变革浪潮中，大部分安全风险都是人为错误导致的——容器和 Kubernetes 基础设施也是如此。该基础设施的安全工具应该自动标记整个生态系统中最明显的配置错误，这一点至关重要。”

“StackRox 不仅能帮助企业进行资产管理——也就是识别已部署的容器，还能保护容器和 Kubernetes 环境。”邓韦琏解释道，“StackRox 容器安全平台能够保护映像并评估构建过程中的风险，强化环境并减少部署阶段的攻击面，在运行时能够发现和阻止恶意活动。StackRox 平台、Kubernetes 以及容器生态系统之间的紧密集成，能够保证整个生命周期的安全。”

容器最好由安全团队管理。对容器安全性的担忧，应该推动公司的 DevOps 转变为 Security DevOps。

“DevOps 的影响以及容器化和 Kubernetes 的快速发展，使得应用开发更加无缝、高效和强大。然而，我们的调查结果显示，在企业的容器策略中，安全仍然是一项重大挑战。”StackRox 首席执行官卡马尔·沙（Kamal Shah）指出，“容器为 DevOps 和安全团队之间的协作提供了桥梁，但它们也带来了独特的风险。如果不对这些风险加以控制，可能会给企业带来真正的损害。”

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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、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有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

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厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，为捍卫国家主权、安全和发展利益提供了有力支撑。

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的发言代表，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*