通过“抗沌工程”增强云基础设施的弹性恢复能力

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	Embrace chaos to improve cloud infrastructure resilience		
原文作者	Josh Stella	原文发布日期	2019 年 6 月 5 日
作者简介	Josh Stella 是 Fugue 公司的首席技术官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/06/05/improve-cloud-infrastructure-resilience/		
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。		

通过“抗沌工程”增强云基础设施的弹性恢复能力

Josh Stella

2019 年 6 月 5 日

在借助“抗沌工程”（译者注：chaos engineering，抗沌工程是在分布式系统上进行实验的学科，目的是建立对系统抵御生产环境中失控条件的能力以及信心，最早由 Netflix 及相关团队提出）提高云基础设施的弹性恢复能力方面，美国视频巨头 Netflix 可谓是领军者。正是通过这种方法，该公司确保了用户能够不中断地收看科幻惊悚电视剧《怪奇物语》（Stranger Things）。除了 Netflix，越来越多的公司（包括耐克、亚马逊和微软等）也开始利用抗沌工程对其云基础设施进行压力测试，以应对各种不可预测的云事件，例如云资源丢失或整个区域的云服务掉线等。

这使他们能够创建高弹性恢复能力的云基础设施环境，并确保可靠的应用交付。此外，他们还能够创建一个模型，并遵循该模型来增强云计算服务和 API 的安全性。

导致云数据泄露的首要原因是基础设施配置错误，无论这些错误是由人为失误、CI/CD 流水线的策略缺失，还是攻击者造成。在传统的扫描和告警工具发现配置漏洞之前，现代云威胁就可以利用自动化技术来查找和利用这些漏洞。为了更主动地查找漏洞并防止这些威胁造成损害，企业需要模拟真实的配置错误，以便在漏洞被利用之前加以识别。（译者注：CI，Continuous Integration，持续集成；CD，Continuous Delivery/Continuous Deployment，持续交付/持续部署。）

如果企业已经大规模地使用云，就会非常熟悉诸如持续监控所有者未明的资源、配置错误和人为失误（如在维护工作完成后留下太多访问权限）等风险。

事实上，即使企业尚未将大部分 IT 系统迁移到云端，他们也很有可能是熟悉这些风险的。这是因为，每次因 S3（译者注：S3，Simple Storage Service，简单存储服务，即可扩展的云存储，又称桶存储，是一种面向互联网的存储服务）配置错误导致数据泄露时，这些风险都会登上新闻头条。这些风险的根本原因通常在于企业自身，即他们未能获取关于云配置的所有详细信息。

这听起来很“混沌”，的确如此。然而，恢复措施正是接受这种混沌。

企业无法消除混沌。混沌会一直存在，而唯一的防御措施就是增强弹性恢复能力。无论损害的来源或性质如何，真正具有弹性的云系统都能够恢复。要想实现弹性恢复能力，企业需创建一个“已知良好的”（known-good）系统来持续监控自身，并在发生损害时自动恢复到已知良好状态。

在云共享责任模型中，安全团队的主要职责是保护服务配置层。云服务通过 API 相互通信；较新的服务则使用 ID 来配置访问权限，而不再使用旧的 IP 地址空间确认方法。安全团队通过“软件定义网络”（SDN）和安全组配置来定义网络边界。与数据中心不同，网络边界基本安全状态的配置更改是通过 API 实现的，而且出于各种原因会发生大量更改。安全团队的目标是对这些服务进行配置，使其在面对不可预测的损害（混沌）时具有弹性恢复能力。

企业需要一种机制，将对云配置的破坏更改恢复为安全配置。有几种方法可以实现这一目标。其中一种方法是编写特定的恢复脚本，但这需要企业预测何时、会出现什么问题；但是，满足这些条件，往往是不切实际的。

因此，更有效的方法是实现自我恢复配置，即获得已知良好的基准并使用知道如何恢复所有可变更改的引擎。此外，采用自动化的流程可以减轻安全团队人工监控和手动恢复潜在破坏更改的工作负担。

企业需定期测试这些自动化流程以确定它们能否正常运作。在这方面，企业需要关注的是身份和访问管理策略或安全组定义被更改时会发生什么，而非计算资源在删除后是否会再次出现。此外，企业还需测试 S3 存储桶配置、VPC/网络配置、口令策略等。弹性安全策略需要涵盖攻击者可能尝试利用的所有漏洞。

要想将弹性恢复能力引入云安全基础设施，企业可以从小处着手，例如先关注单个资源类型（如 S3 存储桶或安全组），然后采用更强大的工具来覆盖更大的范围。

企业需要一种模拟混沌的方法。在这方面，没有任何现成的工具，但是企业可以轻松通过控制台人工操作，或通过执行更改的脚本自动执行。通过这两种方法，企业就可以向云开发或测试环境中引入混沌。企业特别要关注弹性恢复能力的完整性（即所有更改是否都能得到恢复）；此外，企业应将平均恢复时间（MTTR）控制在几分钟内，而非几小时或几天。

通过云安全抗沌工程，企业可以确保云安全工作涵盖所有关键云资源，例如网络配置、

安全组规则、身份和访问管理以及资源访问策略；并在所有配置错误事件中启用自动恢复。此外，这还有助于企业符合相关法律、行业法规和政策，如 GDPR、HIPAA、NIST 800-53、PCI、CIS 基准，以及企业内部安全策略等。

混沌是安全界的常态，而唯一的防御措施就是增强弹性恢复能力——包括云计算服务和 API 的配置和安全性。

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*