简译版

实现策略自动化以消除配置错误

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	Policy automation to eliminate configuration errors		
原文作者	鲁维·基托夫（Ruvi Kitov）	**原文发布日期**	2021 年 10 月 15 日
作者简介	鲁维·基托夫是 Tufin 公司的首席执行官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/10/15/policy-automation/		
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	通过将策略自动化与事件响应计划或系统集成，企业可以提高“减少驻留时间”和“加快事件响应”的能力。如果企业能够实施基于策略的自动化方法，就会大大降低配置错误导致安全事件的风险。实施自动化解决方案，可以自动执行容易出错的重复性任务，并全天候监视企业环境，这有助于防止配置错误并在发生配置错误时迅速恢复。		
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。		

实现策略自动化以消除配置错误

鲁维·基托夫

2021 年 10 月 15 日

很多时候，重大的安全事件可以追溯到简单的配置错误。企业对网络和安全配置的更改和调整是不可避免的，这是管理其技术环境的必要步骤。但是，企业需要认识到，这些更改是有风险的，可能会产生意想不到的后果，包括服务中断、性能下降和意外停机，以及安全事件和违反合规性要求等等。

复杂的环境

从表面上看，配置错误似乎是很容易解决的问题——企业可以关注每次更改，并在每次进行更改时手动确保所有设置都是正确的。企业应制定更改策略，确保全体员工都遵守这些策略并根据这些策略检查所有的调整。许多企业采用“四眼原则”（Four Eyes principle）来减少错误——一个人设计并要求进行更改，第二个人批准该更改。有时候，还需要第三个人来实施该更改。

但是，说起来容易做起来难。问题在于，如今的大型企业都很复杂，在任何时候都有很多活动部分需要处理。此外，有很多团队能够进行更改和调整，这使得确保正确配置的难度呈指数级增长。更糟糕的是，有的团队会使用不同的语言。

对整个环境的可见性也是一个问题。如果企业希望查看并确保每项更改都符合安全策略，则需要查看每项更改或调整，和/或收到每项更改或调整的告警。即使企业具有完全的可见性，也无法手动审查和批准所有更改。

将所有需要考虑的变量加起来，这个工作量就非常庞大了——有太多的任务需要完成，有太多的潜在差距需要弥补。为了成功控制每一次更新、更改和添加的实施方式，并了解每项更改如何影响环境和其他已经“进行中”的更改，唯一的方法是采用自动化技术。

自动化带来敏捷性

“因为没有足够密切地关注配置和更改而导致安全事件发生”，没有人希望看到这种情况。但是，如果企业把大量时间都花在这个问题上，就会面临更大的问题。此外，让安全团

队处理简单重复性任务而非更具战略意义的活动，是对关键资源的浪费，尤其是有简单的解决方案时。要想完成大量的此类任务，关键是在配置和更改方面采用自动化方法。

企业可以将自动化技术应用于下述三个关键领域，以帮助控制配置更改。

自动化的更改分析和设计：企业需要知道，不存在“简单的配置更改”。即使看似最简单、最良性的更改也可能会导致错误。举例来说，假设你将一台主机添加到一个网络组以提供访问权限，并且你不知道该网络组被用在不同的地方来阻止流量。如果你不密切关注该网络组，就会忽略潜在的问题。像这样的简单问题可能会增加企业的攻击面，并使企业系统过度暴露，或者阻止对关键系统或服务的访问。这样一来，安全团队就需要花费大量时间进行故障排除并找出问题出在哪里，以降低安全事件发生的可能性。

通过为网络可见性添加自动化技术，安全团队可以及时了解整个企业的情况，并重点了解关键领域。这样一来，安全团队就可以查看最近的更改和请求以及潜在问题，并知道应该将精力放在哪些方面。

防护措施和策略合规性：通过采用自动化方法，企业可以根据安全策略和标准自动审查所有请求，了解它们对整体环境的潜在影响。企业还可以轻松实现合规性，或意识到更改可能会使合规性面临风险。企业可以确定变更要求或开发人员防护措施，以确保不会批准任何可能造成安全问题或影响正常操作的内容。

进行更改是否可能会导致问题？企业环境中是否还有其他元素需要调整以支持更改？自动化方法可以回答这些问题，能够自动批准或拒绝请求，或将更改标记为需要直接审查和调整以保持合规性。

自动报告、记录和审计：所有更改、返工配置和请求都应进行记录。对于安全团队的成员来说，仅此一项任务就可能让他们精疲力竭。因此，企业应寻求自动化工具来维护可访问且可操作的审计信息。全面的审计跟踪应包括更改配置的设备或平台、更改的确切时间、配置详细信息、涉及的人员（请求者、批准者、实施者）以及更改情境（例如项目或应用程序）。

该措施的目标是持续改进企业的安全策略、管理流程，并持续减少攻击面。要想取得成功，唯一的方法是从过去吸取教训并应用这些教训。企业要想拥有更强大的安全态势，审计和更改记录是关键。

预防问题并加速恢复

专家们认为，事件响应期间或发现错误时，大部分恢复时间实际上是用于弄清楚更改了哪些配置、何时、为什么以及由谁更改的。如果企业已经设置了这些控制流程并采用了自动化技术，那么在发生危机时，企业能够很快获得必要的信息，然后就可以迅速回滚任何更改、阻止攻击事件并加快恢复。

此外，通过将策略自动化与事件响应计划或系统集成，企业可以提高“减少驻留时间”和“加快事件响应”的能力。如果企业能够实施基于策略的自动化方法，就会大大降低配置错误导致安全事件的风险。

实施自动化解决方案，可以自动执行容易出错的重复性任务，并全天候监视企业环境，这有助于防止配置错误并在发生配置错误时迅速恢复。

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