简译版

克服打补丁的挑战：自动化是关键

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	Want to overcome patching challenges once and for all? Automation is the key		
原文作者	Vijay Kurkal	**原文发布日期**	2019 年 10 月 30 日
作者简介	Vijay Kurkal 是 Resolve Systems 首席运营官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/10/30/overcome-patching-challenges/		
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。		

克服打补丁的挑战：自动化是关键

Vijay Kurkal

2019 年 10 月 30 日

英国的网络安全威胁形势非常复杂。企业面临的不再是“网络攻击是否会发生”的问题，而是“何时发生”的问题。根据最近的 Beaming 报告，在 2019 年第二季度，每 50 秒就有一家英国企业遭受网络攻击。

同时，英军国防参谋长最近表示，由于外部网络威胁，该国“每天都处于战争中”。有趣的是，据分析公司 Gartner 预测，到 2020 年，在被利用的漏洞中，99%仍将是安全和 IT 专家已知的漏洞。鉴于此，我们不难理解英国企业为何将打补丁作为重中之重了。

不幸的是，正如 CISO 所了解的那样，即使许多企业购买了补丁工具，打补丁仍然一个难题。问题的根源并非部署补丁，而是必须考虑的其他众多因素，例如：补丁对性能的影响、软件的不同版本、对相关应用程序的影响、准确了解真正需要打补丁的内容、批准和通知以及更换窗口等；更不用说打补丁后进行验证，以确保补丁不会无意间破坏关键业务系统了。此外，补丁监管还需进行大量的文档记录和跟踪。所有这些因素使补丁管理成为一个看似无法克服的挑战。

因此，越来越多的企业开始寻求自动化补丁方法。这是因为实施自动化方法能够增强安全性，促进合规性，实现最长的正常运行时间和服务交付，还能够缓解 IT 团队面临的补丁挑战。

打补丁还是不打补丁

在当今复杂且通常独立的 IT 环境中，修复特定漏洞可能会引入另一个漏洞，或意外导致服务中断或性能问题。正是这种固有的复杂性导致了许多企业延迟打补丁或不打补丁。而另一方面，英国企业遭受的网络攻击比去年增加了 40%，造成的损失超过 20 万英镑，因此不打补丁是很愚蠢的。

出于许多原因的考量，企业不应忽视打补丁。最重要的是，在当今的商业环境中，数据隐私的重要性不可低估。在技术发展的历史中，现阶段的典型特征是：我们非常重视企业对客户信息的处理。

GDPR 等数据隐私法规对企业的行为准则产生了重大影响。发生数据泄露事件，导致员工和客户数据泄露的公司，可能会遭受巨额罚款。强大而有效的补丁策略有助于公司符合此类数据隐私法规的要求——最终成为一家应客户需要而非因法规要求，而遵守良好行为规范的公司。

考虑到最近的重大数据泄露规事件，如果企业未能定期为系统打补丁，就会面临更高的网络攻击风险。定期打补丁是不可避免的，因此企业需要诸如自动化之类的新型解决方案来应对这一艰巨的任务。

打补丁涉及风险决策

打补丁如此困扰 CISO 和 IT 团队的一个原因是：打补丁涉及风险决策。打补丁意味着要打破某些内容，而不打补丁意味着存在安全漏洞。因此，企业需要决定部署哪些补丁。当然，打补丁时可能会遇到安装故障或导致服务中断。很多方面都可能会出现问题。

幸运的是，企业可以采取简单的解决办法：自动化。自动化方法可以接管艰难的“决策步骤”，减轻 IT 团队的压力。自动化的补丁解决方案可以自动调查最适合每个系统的补丁，交叉引用之前的成功补丁，决定整个补丁管理流程，并自动执行打补丁后的验证和测试。将手动步骤减少到最低程度，有助于减少人为错误并确保有效的补丁部署。

打补丁需要大量时间

另一个棘手的问题是，打补丁非常耗时——永无止境的补丁周期需要端到端的编排和全面的系统监控。选择、部署和验证补丁需要大量的时间，有时在整个环境中安装所需的补丁可能要花费数月的时间。打补丁需要执行多个步骤，这可能会造成补丁延迟——因为 IT 团队试图为数千个易受攻击的服务器打补丁，而每次打补丁都必须手动执行特定步骤。

这正是自动化方法如此具有吸引力的原因。除了加快决策速度以外，自动化还能以可控地方式将补丁同时应用到多个漏洞中，从而显著加速打补丁的速度并消除失败风险。

使用自动化解决方案编排繁琐的补丁任务，还意味着员工可以腾出精力来处理更高价值的战略性工作，便于 IT 领导为业务创新和增长做出重要决策。另一个不可避免的现实问题是，打补丁后需要进行测试和验证，这使打补丁的过程更加漫长。部署补丁时，可能会出现安装失败的情况，从而导致服务中断或其他新问题。此外，打补丁可能会导致系统不稳定，

并对相关应用程序的性能产生负面影响。

自动化方法可以接管整个打补丁过程，包括验证阶段。该方法可以自动执行运行状况检查，识别和记录问题，并快速解决打补丁前后的问题。它还可以自动执行耗时的变更管理程序记录——这些记录令 IT 专家颇为头疼，但对于补丁监管和合规性至关重要。因此，该方法能够减轻 IT 团队在打补丁后的负担，使他们能够继续处理下一个紧迫的任务。

成功、有效的补丁就是在人工判断和自动化之间找到最佳结合点。虽然人工监督有助于完成打补丁过程中一些最关键的阶段，但自动化可以简化和执行介于两者之间的所有步骤，将整个打补丁过程所需的时间从几天缩短到几分钟。

采用自动化方法的企业，不仅能够改善运营效率和资源分配，还能够改善安全状况和合规性。

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，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、超过十五亿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