Akamai 客户案例

体育传媒公司发现隐藏的 API 风险

建立完整 API 清单，并揭示易遭攻击者利用的错误配置

建立准确清单

发现缺少控制措施

发现 SQL 注入攻击

数字平台和应用程序正在借助 API 的力量彻底变革体育传媒行业。这些技术进步改变了直播活动的组织、宣传和体验方式，为艺人、活动组织者和观众创造了新的机会。

API 可以跨各种社交媒体渠道无缝共享活动信息、最新动态和门票链接，加大了宣传力度，也提高了门票销量。此外，API 也让直播活动的现场体验发生了变化。与移动应用程序和可穿戴设备的集成实现了个性化日程、交互式地图和实时通知等交互功能。

然而，值得注意的是，由于体育传媒行业涉及的数据和交易较为敏感，因此必须将 API 安全防护作为优先事项。API 安全控制在确保数据的完整性、机密性和可用性方面发挥着关键作用，也正因如此，这家世界知名的体育传媒企业与 Noname Security（现已被 Akamai 收购）展开了合作。

采用 API 安全防护

客户很清楚自己对 API 安全性的需求，但具体不确定应该从何处入手，以及应该优先考虑哪些方面。以往，他们主要关注于应用程序安全性，并认为 API 网关和 Web 应用程序防火墙等现有的工具足以保护 API 安全。但是，尽管此类工具可以提供某种程度上的基础保护，但由于设计所限，它们无法像专业 API 安全解决方案一样提供专业级的监测能力、实时安全防护和持续测试。大部分此类防护措施无法通过现有基础架构发挥功效。例如，API 安全防护的两个关键方面是身份验证和授权。完善的身份验证机制可确保只有授权用户或系统才能访问 API。

Sports and Media Company

位置

美国

行业

媒体和娱乐

解决方案

Akamai API Security

Akamai

发现漏洞

Akamai API Security 团队使用其“态势管理”和“运行时保护”模块，摸清了客户当前的 API 安全态势。待我们掌握了客户环境中的 API 准确清单，就能够发现各种现有的安全漏洞和配置错误了。

第一个发现是，客户是结构化查询语言注入 (SQLi) 的受害者。SQLi 是一种安全漏洞，当攻击者得以操纵 API 请求的输入参数来执行未经授权的 SQL 命令时，就会出现这种漏洞。SQLi 攻击得逞的后果可能非常严重。攻击者可能会未经授权访问敏感数据，修改或删除数据，甚至在底层数据库服务器上执行任意命令。

第二个发现是，客户缺少身份验证。如果不采取完善的身份验证机制，任何人都可以访问 API 端点，并可能检索或修改敏感数据。他们可能会修改或删除数据，导致数据完整性问题和关键信息丢失。而这可能会造成数据泄露、未经授权的信息泄露，甚至危及整个系统。

未来展望

现在客户已经完全掌控了生产中的 API，而他们一直在探索如何在生产前解决漏洞。为帮助企业发现和修复这些漏洞，Akamai API Security 纳入了主动测试机制，这是一种专门构建的 API 安全测试解决方案，它可以了解企业的独特业务逻辑，并全面监测其 API 特定的漏洞。主动测试可以帮助企业将 API 安全测试左移并嵌入到各个开发阶段。