Akamai 客户案例

财富 100 强饮料零售商妥善保护 API 和数据

通过识别关键 API 漏洞以及修复之前的欺诈、滥用和盗用造成的损害，帮助保护客户数据

应用程序编程接口（简称 API）使得零售商可以为客户构建端到端的个性化体验，同时简化运营。要将一瓶饮料交付到消费者手上，整个过程会涉及许多变量，包括库存数据、订单提交、位置数据、付款甚至还有激励计划，这些变量都是由 API 传递的。API 将零售商、合作伙伴及客户连接起来组成生态系统，彻底变革了购物体验。但是，API 始终与敏感数据相伴，这也使得风险并存。

虽然消费者喜欢新的数字化零售体验，但他们也经常会担心个人信息是否得到了妥善保护，这是理所当然的。网络犯罪分子将 API 作为首选攻击媒介的情况日益普遍。由此，一家财富 100 强零售饮料公司找到 Noname Security（现为 Akamai 的公司），请求解决其 API 安全环境中的漏洞。

不断增长的 API 使用量带来的挑战

经过初步交流得知，该公司对于无法在全球范围内实施行之有效的 API 治理和安全措施这一情况，表达出深切的担忧。为了收集证据，公司公开委托了一项漏洞赏金计划，结果发现有一个巨大的漏洞存在，有近 1 亿用户的姓名、地址、电子邮箱和电话号码存在被泄露的风险。幸运的是，这是一项赏金计划，上述问题没有造成伤害就得到了解决。

Retail Beverage Company

位置

美国

行业

零售业、旅游业和酒店业

解决方案

Akamai API Security

重要影响

- 每天保护数十亿次 API 调用
- 每秒保护 5,000 个请求
- 发现并解决了 200 多个问题

Akamai

公司对生产 API 也没有足够的监测和监控能力，导致公司无法充分评估风险，并且其 Apigee 数据未能提供上下文详细信息（例如，数据类型、用户行为、基准、漏洞取证）。由于存在这些 API 漏洞，欺诈、滥用和盗用随之而来，进而导致了零售商运营成本攀升。

强化 API 安全态势

Noname API Security Platform（现已包括在 Akamai API Security 中）能够清点客户的 API 并提供行为分析、实时攻击检测和漏洞管理，包括特定于 API 的应用程序开发测试。由此，客户能够检测到现有控制措施疏漏的 API 攻击并加以修复。应用程序安全（简称 AppSec）团队则能够提高效率并改进高风险问题的优先级排序功能。

Akamai 还支持每个引擎高达 5 万个 API 且没有操作延迟。客户以我们的平台为核心，开发出了全球 API 安全程序。公司现在可以全面监测其 API 清单以及与上下文相关的 API 详细信息。此外，公司获得了现有工具无法提供的可以指导行动的情报。这使高效的 API 漏洞管理和实时威胁检测功能实现了经济高效。