Akamai 客户案例

金融公司发现并保护 API

一家银行通过发现隐藏 API，评估和抵御 API 风险，以及满足法规要求，保护了公司的数字化方案。

获得全面的监测能力 | 改善安全态势 | 保护数字化计划

金融服务业正在迅速开展数字化转型，以在不断发展的市场中保持竞争力。借助人工智能和大数据分析等数字功能，金融机构能够提供创新型产品，降低成本，并为客户带来更加个性化的高效服务。

与此同时，数字化转型也伴随着更大的网络攻击风险。为应对这一日益严重的问题，网络安全现已成为所有数字化转型战略的重要组成部分。金融服务公司必须确保其系统安全且具有恢复能力，以保护客户的数据和资产免遭恶意攻击。

亚洲一家著名的商业银行很快找到了 Noname Security（现已被 Akamai 收购），来帮助加强其 API 安全态势。API 漏洞数量已达到惊人水平；Tech Wire Asia 指出，“如今，每 13 起网络事件中就有 1 起可归因于 API 安全问题。”他们还强调，“API 漏洞每年会给企业造成高达 750 亿美元的损失。”

考虑到我们的客户拥有超 7000 亿美元的总资产、5000 多家企业客户并享有全球知名的财富管理声誉，尽快解决所有 API 漏洞迫在眉睫。

Financial Services

位置

亚洲

行业

金融服务

解决方案

Akamai API Security

Akamai

需要更全面地监测 API 及其风险

该机构已经部署了一个 API 管理平台来进行身份验证和流量控制，但对这个平台能不能阻止 API 滥用和网络攻击心存怀疑。尽管 API 网关提供了急需的基本 API 安全控制，但遗憾的是，它们不足以全面保护企业免受 API 特定的威胁。

例如，受损的对象级别授权（常称为 BOLA），它会伪装成正常 API 流量流向网关。API 请求和响应之间缺少语境感知，这使得 BOLA 攻击能够逃过检测并访问关键的后端服务。这一缺陷不仅会使企业容易受到 BOLA 漏洞的攻击，还会招致其他攻击和业务逻辑滥用。

其监测能力还有一个局限性——无法维持准确的 API 清单。与大多数大型企业一样，该银行也面临着其环境中存在未知 API 的难题。现实情况是：企业管理着数千个 API，其中许多 API 并非通过 API 网关一类的代理进行路由。这些 API 称为流氓 API 或僵尸 API。这些 API 可能是由前员工部署，或者是在企业充分重视 API 安全性之前部署的。不管它们因何存在，银行的 API 网关都无法监测到这些 API，所以很容易低估银行真正拥有的 API 数量。

加强部署以迎接 API 安全挑战

该企业部署了综合性 Noname API Security Platform（现为 Akamai API Security 的一部分），其中包括用于 API 态势管理、运行时保护和跨环境测试的解决方案。客户的安全态势呈指数级提升，因为他们现在能够检测并修复世界上最隐蔽的一种威胁媒介的攻击漏洞了。

现在可以在平台内发现并揭示未知 API，从而实现全面监测，并抵御风险。Akamai API Security 可对敏感数据进行分类以帮助满足 GDPR、HIPAA 等法规要求，因而大幅缓解了该机构的 API 蔓延情况，提高了合规性。

该银行现在能够实时阻止攻击并保护客户的数据资产。运行时保护解决方案可以智能地检测潜在威胁并确定其优先级，同时持续监测 API 活动。通过与 Web 应用程序防火墙、API 网关、安全信息和事件管理、信息技术服务管理和其他工作流工具相集成，我们的平台可支持以手动、半自动或自动方式修复威胁。

结果

API 已迅速成为黑客首选的攻击媒介，攻击没有丝毫减缓的迹象。例如，2022 年，我们看到“针对金融服务业的攻击数量同比增长 257%”。在 Akamai API Security 的助力下，该金融服务公司将能够未雨绸缪，避免成为受攻击对象，并抵御这一波来势汹汹的攻击。特别是，客户的安全团队将更明确地了解 API 带来的风险，并能够创建更安全的系统。

扫码关注，获取最新云计算、云安全与CDN前沿资讯

©2024 Akamai Technologies | 支持 | 发布时间：2024 年 8 月