2024 年 API 安全影响研究

金融服务行业

API 事件频发。了解金融服务业如何应对这一重要安全问题，以及您的企业可以采取哪些措施来确保安全。

去年，有 88.7% 的金融服务公司遭受过 API 攻击。这些 API 主要是帮助他们处理数据以及使客户和合作伙伴能够使用他们的重要服务。随着各种创新的攻击手法不断涌现，攻击者得以入侵未受保护的 API，进而访问其中的数据来窃取敏感的个人信息和财务信息（包括帐户余额和交易记录等）。

面对由此带来的压力，安全团队正在想方设法寻找应对之道。然而，应对新的攻击媒介并非易事。尤其是 API 之类的媒介，一旦配置错误或存在业务逻辑漏洞就极易被攻击者发现并加以利用。

这一结论从何而来？为了解企业在应对 API 威胁方面的经历，Akamai 对 1,200 多名 IT 和安全专业人士（包括首席信息安全官、应用安全人员等）展开了调研。

我们对金融服务业受访者的调研结果进行了筛选总结，结果表明，他们认为 API 安全事件的主要影响包括“监管机构的罚款”和“团队/部门的压力倍增”。考虑到参与调研的金融服务业从业者表示，他们平均需要花费 832,800 美元来处理 API 安全事件，这一数字不仅比所有八个受调研行业的平均水平高出 40%，而且高于任何其他行业，上述这些相互关联的后果也就不难理解了。

继续阅读，通过 2024 年 API 安全影响研究获取行业深入见解。

攻击加剧，监测能力下降

在所有行业中，有 84% 的企业表示曾遭遇过 API 安全事件，但金融服务业的企业遭受攻击的频率明显高于平均水平，达到 88.7%。调研表明，导致这些攻击事件的漏洞主要有两个：网络防火墙未能有效拦截威胁（占比 26.5%），以及大语言模型 (LLM) 等生成式 AI 工具自身的 API 存在安全漏洞（占比 23.2%）。

尽管 API 威胁日益凸显，频繁的安全事件、高昂的修复成本和监管罚款等先例比比皆是，但我们的研究表明，许多金融服务团队仍然没有充分重视 API 安全。事实上，在企业未来一年的网络安全优先事务中，API 安全防护仅排名第九，占比只有 18.5%。

对于金融行业来说，准确区分 API 活动是真实合规还是恶意欺诈仍然是一项巨大的挑战，尤其是在全面了解 API 带来的诸多风险方面。在调研中，尽管有 73.5% 的金融服务业受访者表示其企业已建立完整的 API 清单，但仅有 28.5% 的受访者能够明确知晓哪些 API 会返回敏感数据，这些敏感数据包括个人身份信息 (PII) 以及持卡人信用记录、大型商业银行客户财务记录等数据。

88.7% 的金融服务公司在过去 12 个月内曾遭遇过 API 安全事件

在拥有完整 API 清单的金融服务公司中，
只有 28.5% 的公司知晓哪些 API 会返回敏感数据

过去 12 个月内，金融服务公司遭遇的 API 安全事件造成的经济损失高达 **832,800** 美元

三大影响

1. 安全团队**压力倍增**
2. 监管机构的**罚款**
3. **信任和声誉损失**

来源：
Akamai，“API 安全影响研究”，2024 年

Akamai

试想一下，如果金融服务提供商的某个部门或子公司部署了一个影子 API，但未得到公司中央 IT 或安全团队的配合或监督，结果会怎样？该 API 可能会发生以下情况：

- 设计上允许返回客户的交易数据，但缺乏适当的授权控制，并且未经过充分的错误配置测试
- 被新版本的 API 取代后未及时停用，因此仍持续暴露在互联网环境中
- 绕过传统工具的监测，这些工具无法检测未受管控的 API
- 被网络犯罪分子用以访问真实客户的帐户，进而窃取客户资产

这一设想并非空穴来风。LexisNexis® Risk Solutions 在其《2023 年欺诈的真实成本研究》报告中指出，50% 的欺诈损失可以追溯到新帐户的开设滥用，即欺诈者大规模滥用 API 来开设帐户。此外，我们的设想也反映了现实生活中 IT 和安全领域公认的 API 事件的主要成因。

API 事件对合规性、业务成本及团队压力的影响

根据 Gartner® 2024 年 5 月发布的《API 保护市场指南》*，“当前的数据表明，平均而言，API 漏洞导致的数据泄露量至少是一般安全漏洞的 10 倍以上。”因此，广受关注的 PCI DSS v4.0 标准增加了关于 API 安全的要求并不令人意外。新版标准明确要求企业在发布 API 前必须验证 API 代码，定期进行漏洞扫描，并确保基于 API 的组件的安全使用。尤其是在 API 每天支持数百万笔金融交易的行业中，这一点尤为重要。

一旦失去监管机构的信任，企业势必会面临更严格的监管审查，给本已疲于应对合规性要求的安全团队造成更大的工作压力，并可能面临高额的罚款。

综上所述，不难看出，金融服务公司对于 API 威胁可能造成的后果有着深刻的认识。在本次调研中，我们首次向来自三个不同国家的受访者征询其企业在过去 12 个月内因 API 安全事件所造成的经济损失估值。

	金融服务行业	所有行业的平均值
美国	$832,800	$591,404
英国	£297,189	£420,103
德国	€604,405	€403,453

问题 3：如果您的企业曾遭遇过 API 安全事件，据您估计，这些事件造成的累计经济损失总额是多少？请包括所有相关费用，例如系统修复、停机时间、法律费用、罚款和任何其他相关费用。

* Gartner《API 保护市场指南》，2024 年 5 月 29 日。GARTNER 是 Gartner, Inc. 和/或其附属机构在美国和全球的注册商标和服务标志，已获许可用在本文中。保留所有权利。

主动保护 API 安全，降低风险和压力

针对金融服务公司的 API 攻击正在迅速升级，其范围、规模、复杂性以及造成的经济损失不断扩大。这其中包括由生成式 AI 驱动的爬虫程序攻击，这类攻击具备快速学习和适应能力，能够轻松绕过传统 API 安全工具和其他外围防御措施。许多金融服务业的安全团队已经切身体会到这些威胁所带来的财务和人力影响。然而，即便企业意识到了 API 威胁的严重性，他们仍然面临一个亟待解决的问题：如何应对这些威胁？

立即采取有效措施，加强对 API 及其传输数据的安全防护，从而帮助您的企业保护收入来源，并减轻安全团队的运营压力。除了采取这些措施外，还应注重提升团队对高级 API 威胁的认知水平，以及防御这些威胁所需的技术能力，这将有助于维护客户和董事会对您的企业的信任。

如需阅读完整报告，并了解 API 可见性与保护的最佳实践，请下载**《2024 年 API 安全影响研究》**。

准备好与我们探讨您的挑战，以及 Akamai 将如何为您提供帮助了吗？

申请定制化的 Akamai API Security 演示

为帮助企业应对本文中介绍的各种 API 安全威胁，Akamai 专门设计了一系列解决方案，旨在降低与之相关的风险：

- Akamai API Security，此解决方案能够发现 API、评估其风险态势、分析其行为模式，并阻止威胁潜藏到企业内部。
- Akamai Account Protector，此解决方案能够实时监控用户行为并适应不断变化的风险状况，从而抵御开户滥用。

Akamai

Akamai 安全部门致力于为您的应用程序提供全方位安全防护，从而助力您的业务发展，确保实现卓越的性能和流畅的客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：25 年 03 月。

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯