2024 年 API 安全影响研究

保险行业

API 事件频发。了解保险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。

当灾难来临时，无论是车祸还是商业设备损坏，投保人都要依靠数字服务来提交索赔并获得保险公司的援助。在这些服务背后，保险公司的 API 负责处理相关的敏感信息，这些信息以数据形式讲述着投保人的生活故事。

在保险行业中，客户的信任至关重要。然而，API 漏洞的存在，使得保险企业面临着日益严峻的安全挑战。

根据 Akamai 的全面调研，76.7% 的保险专业人士反映他们在过去 12 个月内遭遇过 API 事件。这些事件的财务影响尤为显著，仅美国保险机构为处理这些事件的平均支出就高达 625,634 美元。

但最令人担忧的或许是业务影响：“失去客户信任和客户流失”（占比 28%）成为保险公司遭遇 API 安全事件后最担心的问题。在客户可轻松转换保险服务提供商的竞争性市场中，这种声誉受损不仅会直接带来损失，而且还会产生长远的影响。

继续阅读，探索 2024 年 API 安全影响研究行业洞察。

在攻击不断增长的同时，监测能力仍然是一项关键挑战

API 攻击给保险公司造成了巨大的经济损失，其中美国保险公司遭受的损失（625,634 美元）超过了全行业的平均水平（591,404 美元）。导致这些事件发生的原因是什么？

保险行业安全团队表示，主要原因包括：

1. 不受管 API，如休眠 API 或“僵尸”API (22%)
2. 意外暴露到互联网的 API (21.3%)
3. 用于保护 API 的传统工具未能捕获威胁 (20%)
4. 授权漏洞 (19.3%)
5. API 错误配置 (18.7%)

很多企业都知道自己遭受 API 攻击的原因，但他们缺乏对关键风险指标的监测能力：API 在被调用时返回敏感数据的能力。虽然有 56.7% 的保险企业称拥有其 API 的完整清单（低于全行业平均水平 69.7%），但其中只有 20.7% 的企业知道哪些 API 会返回敏感数据。

对于处理受到严格监管的个人和财务数据的行业来说，这种监测能力不足对合规性及安全性带来了严重影响。

76.7% 的保险企业在过去 12 个月内经历过 API 事件

只有 20.7% 的保险企业知道哪些 API 会返回敏感数据，这在拥有完整 API 清单的保险企业中占比很低

625,634 美元，这是过去 12 个月内美国保险企业遭遇的 **API 安全事件造成的财务影响**

三大影响

1. 失去客户信任和客户流失 (28%)
2. 损害了部门在管理层中的声誉 (25.3%)
3. 解决事件所产生的成本 (24.7%)

来源：
Akamai 的 2024 年 API 安全影响研究

Akamai

我们注意到一些趋势导致保护 API 变得困难：

- **持续的 API 蔓延**：随着每项数字化计划的实施，API 都在成倍增加并不断发展，因此很难保持准确的清单。
- **不一致的标准**：很多保险公司都有多个开发团队，它们在各个业务部门内各自为政，并未采用统一的安全设计行动手册。
- **被忽视的风险**：API 会传输敏感的投保人数据，但大多数企业无法确定具体有哪些 API 会返回敏感信息。

试想一下，如果某个部门部署了 API，但没有安全团队采取合适的监管措施，那会发生什么情况？此类 API 可能在开发时未设置适当的管控措施便用于共享记录，或在系统升级后仍保持活跃状态，从而形成客户敏感数据的潜在暴露点。

API 事件如何对合规性、客户信任以及团队压力造成影响

显然保险公司非常清楚 API 威胁带来的财务后果。在我们的调查中，我们要求受访者分享他们在过去 12 个月内经历的 API 安全事件的预计成本：

	保险行业	所有行业平均值
美国	625,633.70 美元	591,404.01 美元
英国	493,000.50 英镑	420,103.18 英镑
德国	373,918.72 欧元	403,453.26 欧元

尽管财务影响巨大，但受访者明确强调，事件成本反映了收入和声誉方面的综合问题。当被问及他们所遭遇的 API 安全事件的最大影响时：

- 28% 的受访者认为是“失去客户信任和客户流失”
- 25.3% 的受访者认为是“损害了团队在管理层和董事会中的声誉”
- 24.7% 的受访者认为是“解决事件所产生的成本”

通过积极的 API 安全防护降低风险和压力

针对保险公司的 API 攻击正在迅速升级，其范围、规模、复杂性和造成的损失不断扩大。其中包括生成式 AI 驱动的爬虫程序攻击，它们能够迅速适应，并绕过传统的 API 安全工具和其他外围防御措施。同行业的许多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，即便企业了解了 API 威胁的严重性，他们仍然面临一个亟待解决的问题：我们该如何应对这些威胁？

立即采取措施以更好地保护您的 API 及其交换的数据，可以帮助您的企业保护收入，减轻安全团队的压力，同时维护董事会和客户的宝贵信任。这些措施包括增强团队对高级 API 威胁的了解，并发展防御这些威胁所需的能力。

如需阅读完整报告，并了解有关 API 监测与保护的最佳实践，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**：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**：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

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯

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，或者扫描上方二维码，关注我们的微信公众号。发布时间：2025 年 5 月。