2024 年 API 安全影响研究

零售与电子商务行业

您的同行如何看待和面对日益增长的 API 威胁

驱动零售和电子商务企业数字化举措的 API 正面临攻击。攻击者不断翻新手段，利用未受保护的 API 窃取信用卡数据、盗用忠诚计划资金，并发起凭证填充攻击等多种恶意行为。安全团队正在感受到这些攻击造成的影响，迫切希望找到改进办法。然而，面对新的攻击媒介，尤其是因配置错误或业务逻辑漏洞而极易被发现并加以利用的 API，团队感到压力倍增。

我们是如何了解到这一点的？Akamai 针对 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，以了解他们对 API 相关威胁的见解。

本简报针对贵行业的情况进行了筛选，其结果表明，在过去的 12 个月里，有 68% 的受访者称曾遭遇 API 安全事件。这些事件带来了哪些影响？同行们给出的最常见回答有团队压力增大以及在高级管理层和董事会中声誉受损。考虑到报告中提到的成本，这一回答是可以理解的。零售和电商专业人士称，他们为处理所遭遇的 API 事件，产生的成本高达 526,531 美元。

继续阅读，以获取 2024 年 API 安全影响研究的行业洞察。

尽管攻击频发，可见性却在下降

虽然大多数零售和电商领域的受访者都曾遭遇过 API 安全事件，但他们的平均比例为 68%，低于所有八个受访行业 84% 的平均水平。与此同时，您的同行在未来 12 个月内的首要安全优先事项是“防御由人工智能驱动的攻击”和“保护 API 免受攻击者的侵害”。

将 API 保护作为优先事项是否能预防攻击？零售和电商公司的安全团队可能已经意识到 API 保护的重要性，并采取了相应措施减少事件的发生频率。然而，我们的调查结果也表明，这些团队并未能完全察觉所有的 API 滥用实例。

对于零售和电商公司来说，区分正常 API 活动与恶意或欺诈行为仍然充满挑战。与此同时，风险的可见性也是一大难题。尽管 67% 的同行表示他们拥有完整的 API 清单，但在这一部分人中，*只有 29%* 知道在众多的 API 中哪些会返回敏感数据，这包括个人身份信息 (PII) 或信用卡详细信息。

设想一下，如果业务部门部署了一个 API，但没有零售商中央 IT 部门或安全团队的协作或监管，会发生什么情况。该 API 可能会发生以下情况：

- 在没有适当授权控制的情况下，构建了返回客户数据的功能，且没有充分测试是否存在错误配置
- 旧版本被新版本替代后未及时停用，因此仍持续暴露在互联网环境中
- 由于传统工具检测不到不受管的 API，因此未能被察觉
- 被欺诈者利用，访问真实客户的忠诚账户并兑换现金

68% 的零售/电子商务公司在过去 12 个月内经历了 API 安全事件[1]

在拥有完整 API 清单的零售/电子商务公司中，**只有 29%** 了解哪些 API 会返回敏感数据[1]

$526,531 = 过去 12 个月内，零售/电商公司遭遇 API 安全事件所造成的财务影响[1]

三大影响：[1]

1. 团队的**压力倍增**
2. 为解决问题而**产生的成本**
3. 部门在高层领导和/或董事会中的**声誉受损**

44% 的针对商业组织的网络攻击瞄准了 API[2]

来源：
1. Akamai，“API 安全影响研究”，2024 年
2. Akamai 互联网现状 (SOTI)，“潜伏在阴影之中：攻击趋势揭示了 API 威胁”，2024 年

Akamai

这一设想并非空穴来风。据 LexisNexis® Risk Solutions“2023 年度欺诈事件的真实成本研究”(2023 True Cost of Fraud™Study) 显示，50% 的欺诈损失可追溯至新帐户开设滥用，即欺诈者大规模滥用 API 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。

零售/电子商务安全团队报告的 API 事件的主要原因

1. LLM 等生成式 AI 工具中的 API——**24.7%**
2. API 意外暴露于互联网——**24.0%**
3. API 配置错误——**22.0%**
4. Web 应用程序防火墙没有进行拦截——**21.3%**
5. API 网关没有进行拦截——**20.7%**
6. API 编码错误导致的漏洞——**20.0%**
7. 知名的技术工具/服务——**20.0%**
8. 网络防火墙没有进行拦截——**18.7%**
9. 授权漏洞——**17.3%**
10. 从互联网下载的软件解决方案——**16.7%**
11. API 身份验证控制缺失——**16.0%**
12. 中层软件解决方案——**14.7%**
13. 不受管 API（例如僵尸 API）——**13.3%**

问：您认为您所在的企业发生 API 安全事件的原因是什么？（最多选择 3 项）；受访人数为 1,207 人

API 事件对合规性、业务成本以及团队压力造成的影响

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。”[3]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。公司及其监管机构需要掌握传输的数据类型，这不仅限于自己的 API，还包括合作伙伴和供应商的 API，这无疑增加了电子商务第三方风险管理的挑战。

失去监管机构的信任可能会导致监管机构加大审查力度，让本就负担沉重的团队需要拿出更多精力满足合规要求。且可能面临高额的罚款。考虑到成本问题，显然零售和电子商务公司非常清楚 API 威胁带来的财务后果。我们首次要求来自三个国家或地区的受访者分享他们在过去 12 个月内经历的 API 安全事件的预计财务影响。

[3] 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，已获许可在本文中使用。保留所有权利。

	零售/电子商务	行业平均水平
美国	$526,531	$591,404
英国	£258,815	£420,103
德国	€348,467	€403,453

问：如果您经历过 API 安全事件，这些事件的累计总财务影响估值是多少？请包括所有相关费用，如系统维修、停机时间、法律费用、罚款以及其他相关费用。（受访人数为 1,207 人）

尽管财务损失数额巨大，但受访者明确强调，API 造成的影响远超财务层面的范畴。当被问及 API 安全事件的最大影响时，我们的零售和电子商务的受访者强调，最主要的影响不是财务损失，而是人力影响，团队面临的巨大压力和焦虑。

API 安全事件对零售和电子商务公司的五大影响

1. 团队/部门的压力倍增——28.7%
2. 为解决问题而产生的成本——28.0%
3. 损害了部门在高层领导和/或董事会中的声誉——25.3%
4. 导致企业加强了对团队/部门的内部审查——23.3%
5. 监管机构的罚款——25.3%

问：API 安全事件给您的企业带来了哪些成本和/或影响（如果有）？（最多选择 3 项）；受访人数为 1,207 人

后续步骤：通过积极的 API 安全防护降低风险和压力

针对零售和电子商务公司的 API 攻击正在迅速升级，其范围、规模和复杂性不断扩大。这包括生成式 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。许多同行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，即便企业意识到了这些威胁的重要性，问题仍然摆在眼前：我们该如何应对这些威胁？

现在采取措施更好地保护您的 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，并了解监测和保护 API 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 安全演示服务

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯

Akamai Security 可为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。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：2024 年 11 月。