Akamai Security

前言

Rupesh Chokshi

应用程序安全部高级副总裁兼总经理

无论是在客户会议和行业活动中，还是几乎每天读到相关的新闻时，我都清楚地认识到一件事：在我们履行对 AI 新时代的承诺时，也必须知道它所带来的安全挑战。

我们已经看到一些备受瞩目的示例，它们充分说明了当 AI 未得到妥善管控时会发生什么。有一起恶意 AI 操纵事件或许最为著名：一名男子说服了加利福尼亚州沃森维尔市一家雪佛兰经销商的聊天机器人，让其同意以 1 美元的价格向他出售一辆全新的雪佛兰 Tahoe 汽车。数月后的 2024 年 2 月，加拿大的一家法院裁定，加拿大航空公司的 AI 赋能聊天机器人向消费者提供了错误的信息，并需因此而承担责任。

当然，这些只是一些早期的示例。现在，世界各地的公司可能在不知不觉中将新的 AI 漏洞引入了其环境中。由此产生的损失是巨大的——这会损害您的声誉、影响您的利润、招致合规处罚，还会让许多公司最初在实施 AI 时投入的巨额资金付诸东流。

在最近的一次体检中，我的医生问我是否可以使用 AI 助手来做笔记。那次对话不仅谈到了我的健康状况，还谈到了周末计划、我女儿选择的大学等等。我当时就在想，这些信息会去向何处？医生知道吗？是否会发生潜在的 HIPAA 违规行为？

在世界各地的会议室和董事会会议中，都会有人提出这样的问题：我们是否正在以安全的方式使用 AI？我们是否正在以安全的方式构建它？即使现在没有，也必须有人提出来。AI 掀起了一股乐观的浪潮，创新随处可见。但是，随之而来的还有一个全新的网络安全漏洞领域，而现有的安全解决方案无法有效应对。而且我们也已经看到，以下两个相关方之间自然而然地出现了一种紧张关系：

- 急于部署新的 AI 应用程序和业务模式的首席人工智能官及其开发团队
- 那些不知道如何防范威胁，甚至可能根本不了解这些威胁的首席信息安全官们