Akamai Security

はじめに

Rupesh Chokshi

アプリケーションセキュリティ担当、Senior Vice President 兼 General Manager

顧客とのミーティングや業界イベント、ほぼ毎日のニュースで、あることが明確になりました。それは、AI の新時代を実現する上で、私たちはセキュリティ上の課題を認識する必要があるということです。

AI への適切なロックダウンが行われていない場合にどんな事態がもたらされるのか、世間の注目を集めた事例がすでにいくつか確認されています。おそらく最も有名な悪性の AI 操作インシデントは、カリフォルニア州ワトソンビルに住む男性がシボレーのディーラーのチャットボットを説得し、新車のシボレー・タホを 1 ドルで販売することに同意させたことです。数か月後、2024 年 2 月には、AI を搭載した Air Canada のチャットボットが消費者に誤情報を提供したことについて、カナダの裁判所が Air Canada の法的責任を認めました。

もちろん、これらは初期の頃のほんの一例に過ぎません。現在、世界中の企業が、新たな AI の脆弱性を無意識のうちに自社環境に取り入れている可能性があります。これは、評判、収益、コンプライアンス違反の罰則、そして多くの企業が AI を最初に導入する際に行った大規模な投資に対する莫大なコストになり得ます。

最近、検診で、医師から AI エージェントを使ってメモを取ってよいか尋ねられました。そのときの会話は、健康に関する話にとどまらず、週末の予定や娘の大学選びなど、さまざまなトピックに及びました。そこで私は、この情報はいったいどこへ送られるのだろうと疑問に思いました。そもそも、あの医者は知っていたでしょうか？ HIPAA に違反していた可能性はないでしょうか？

世界中の会議室や取締役会で、AI を安全に使用できているか、安全に構築できているか、という質問が投げかけられています。そのような質問を受けていないとすれば、質問されるべきです。AI は楽観主義と革新の波を生み出してきました。しかし、この技術はサイバーセキュリティの新たな脆弱性をもたらしており、既存のセキュリティソリューションでは十分に対処できないものとなっています。すでに、当事者である次の 2 者の間に自然な緊張が生まれています。

- 新しい AI アプリケーションとビジネスモデルの導入を急務とする AI の最高責任者とその開発チーム
- まだ認識さえしていない脅威をどうすれば阻止できるのか考えあぐねている CISO