Akamai Security

INTRODUZIONE

Rupesh Chokshi

Senior Vice President e General Manager, Application Security

Durante le riunioni dei clienti e gli eventi di settore, praticamente ogni giorno quando leggo le ultime notizie, mi sono reso conto chiaramente che, se vogliamo tenere parola alla promessa di creare la nuova era dell'AI, dobbiamo essere consapevoli dei rischi che sta creando per la nostra sicurezza.

Abbiamo già osservato alcuni esempi significativi di cosa succede quando l'AI non viene bloccata correttamente. Come è successo in quello che viene probabilmente considerato il più famoso incidente di manipolazione dell'AI per scopi dannosi, un uomo ha convinto la chatbot di una concessionaria della Chevrolet a Watsonville in California a venderli una nuova Chevy Tahoe al prezzo di 1 dollaro. Alcuni mesi dopo questo evento, a febbraio 2024, un tribunale canadese ha condannato Air Canada perché ritenuta responsabile delle informazioni errate fornite ad un cliente dalla sua chatbot basata sull'AI.

Ovviamente, questi sono solo alcuni esempi iniziali. Al momento, le aziende di tutto il mondo potrebbero introdurre inconsapevolmente nuove vulnerabilità nei loro ambienti. I costi possono essere significativi in termini di danni alla reputazione, perdite di ricavi, sanzioni per mancata conformità e ingenti investimenti che molte aziende hanno effettuato nell'implementazione iniziale dell'AI.

Recentemente, durante una visita di controllo, il mio dottore mi ha chiesto se poteva usare un assistente basato sull'AI per prendere appunti. La conversazione sull'argomento è andata oltre il mio semplice stato di salute fino a parlare dei piani per il fine settimana, delle scelte universitarie di mia figlia e di molto altro. A quel punto mi sono chiesto dove sarebbero finite tutte quelle informazioni personali e se addirittura lo sapesse il dottore. Si poteva verificare una violazione dell'HIPAA?

Questi sono i tipi di domande che si sentono nelle sale conferenze e nelle riunioni aziendali in tutto il mondo, ma dobbiamo chiederci: "Stiamo usando l'AI in modo sicuro? Stiamo creando un'AI protetta?". Se non ci siamo fatti queste domande, dobbiamo farlo. L'AI ha creato un'ondata di ottimismo e innovazione, portando con sé, tuttavia, uno scenario completamente nuovo di vulnerabilità per la cybersecurity, che le soluzioni di sicurezza esistenti non sono in grado di gestire correttamente. Abbiamo già osservato l'emergere di una naturale tensione tra due componenti di questo panorama:

- I responsabili dell'AI e i loro team addetti allo sviluppo nell'urgenza di implementare le nuove applicazioni e i nuovi modelli aziendali basati sull'AI
- I CISO nel loro chiedersi come proteggersi da minacce di cui forse non sanno nulla