Akamai Security

INTRODUÇÃO

Rupesh Chokshi

Vice-presidente Sênior e Gerente Geral de Segurança de Aplicações

Em reuniões com clientes e eventos do setor, e em quase todos os dias, quando leio as notícias, uma coisa fica clara para mim: ao realizarmos a promessa da nova era da IA, precisamos estar cientes dos desafios de segurança que ela está criando.

Já foi possível perceber alguns exemplos graves do que acontece quando a IA não recebe a devida proteção. Talvez, o exemplo mais famoso de manipulação mal-intencionada da IA seja o que ocorreu em Watsonville, na Califórnia, quando um homem convenceu o chatbot de uma concessionaria Chevrolet a lhe vender um Chevy Tahoe novo por US$ 1. Meses depois, em fevereiro de 2024, um tribunal canadense considerou a Air Canada responsável pelas informações erradas que seu chatbot baseado em IA havia dado a um cliente.

Mas esses são apenas alguns exemplos iniciais. É bem possível que, neste exato momento, empresas no mundo todo estejam introduzindo novas vulnerabilidades de IA em seus ambientes, sem nem perceber. Os custos podem ser significativos, não só para a reputação e os resultados financeiros, mas também em multas por não conformidade e em enormes investimentos que muitas empresas já fizeram para implementar a IA.

Recentemente, em uma consulta de rotina, meu médico perguntou se poderia usar um agente de IA para fazer anotações. Durante a consulta, conversamos sobre outros assuntos também, como meus planos para o fim de semana e as escolhas universitárias da milha filha, entre outras coisas, além das minhas questões de saúde. E eu fiquei me perguntando para onde aquelas informações estavam indo. Será que o médico sabia? Será que ocorreu uma possível violação de confidencialidade?

Esses são os tipos de perguntas que estão sendo feitas em salas de conferência e reuniões de diretoria em todo o mundo. Será que estamos usando a IA com segurança? Estamos construindo a IA de maneira segura? E se essas perguntas não estiverem sendo feitas, elas precisam ser! A IA gerou uma onda de otimismo e inovação. Porém, ela traz consigo um novo universo de vulnerabilidades de segurança cibernética, para as quais as soluções de segurança existentes não estão preparadas. Já é possível perceber a existência de uma tensão natural entre duas partes:

- Diretores de IA e suas equipes de desenvolvimento, que estão se apressando para implantar novas aplicações de IA e modelos de negócios.
- Diretores de Segurança da Informação, que vivem tentando encontrar soluções para ameaças que eles ainda nem conheçam.