Akamai Security

INTRODUCTION

Rupesh Chokshi

Senior Vice President et General Manager,
Application Security

Lors de réunions avec les clients et d'événements du secteur, et presque tous les jours lorsque je lis les actualités, une chose est devenue claire pour moi : alors que nous répondons aux promesses qui vont avec cette nouvelle ère de l'IA, nous devons être conscients des défis de sécurité qu'elle pose.

Nous avons déjà vu des exemples très médiatisés de ce qui se passe lorsque l'IA n'est pas correctement verrouillée. Dans l'un des incidents les plus célèbres de manipulation malveillante de l'IA, un homme a convaincu le chatbot d'un concessionnaire Chevrolet de Watsonville, en Californie de lui vendre une Chevrolet Tahoe pour 1 $. Quelques mois plus tard, en février 2024, un tribunal canadien a conclu qu'Air Canada était responsable des informations erronées que son chatbot basé sur l'IA avait données à un consommateur.

Bien sûr, il ne s'agit là que de premiers exemples. Actuellement, les entreprises du monde entier peuvent introduire involontairement de nouvelles vulnérabilités de l'IA dans leurs environnements. Les coûts peuvent être importants : pour votre réputation, pour vos résultats, en termes de pénalités réglementaires et pour les très gros investissements réalisés par de nombreuses personnes au démarrage de l'IA.

Récemment, lors d'un bilan, mon médecin m'a demandé s'il pouvait utiliser un agent d'IA pour prendre des notes. Au-delà de ma santé, cette conversation a couvert les projets de week-end, les choix universitaires de ma fille et bien plus encore. Je me suis demandé où ces informations allaient. Mon médecin lui-même le savait-il ? Une violation potentielle de la loi HIPAA a-t-elle eu lieu ?

Ces questions ressemblent à celles qui sont posées dans les salles de conférence et les réunions du conseil d'administration dans le monde entier. Utilisons-nous l'IA en toute sécurité ? La construisons-nous en toute sécurité ? Et si ces questions n'ont pas été posées, elles doivent l'être. L'IA a généré une vague d'optimisme et d'innovation. Mais elle apporte avec elle un tout nouveau domaine de vulnérabilités en matière de cybersécurité, que les solutions de sécurité existantes ne sont pas bien équipées pour gérer. Nous avons déjà constaté l'émergence d'une tension naturelle entre deux parties :

- les responsables de l'IA et leurs équipes de développement qui se précipitent pour déployer de nouvelles applications d'IA et de nouveaux modèles commerciaux ;
- les responsables de la sécurité des systèmes d'informations qui se demandent comment se protéger contre les menaces qu'ils ne soupçonnent peut-être même pas.