Akamai Security

INTRODUCCIÓN

Rupesh Chokshi

Vicepresidente sénior y director ejecutivo de Seguridad de aplicaciones

En las reuniones con los clientes y los eventos del sector, y casi todos los días cuando leo las noticias, me ha quedado claro algo: a medida que cumplimos la promesa de la nueva era de la IA, debemos ser conscientes de los desafíos de seguridad que está creando.

Ya hemos visto algunos ejemplos destacados de lo que sucede cuando la IA no está correctamente bloqueada. En el que posiblemente sea el incidente más famoso de la manipulación maliciosa de la IA, un hombre convenció a un chatbot de un concesionario de Chevrolet de Watsonville, California, para que le vendiera un nuevo Chevy Tahoe por 1 $. Meses más tarde, en febrero de 2024, un tribunal canadiense declaró a Air Canada responsable de la desinformación que su chatbot con tecnología de IA había dado a un consumidor.

Estos son solo un par de ejemplos iniciales, por supuesto. En este momento, es posible que empresas de todo el mundo estén introduciendo involuntariamente nuevas vulnerabilidades de IA en sus entornos. Los costes pueden ser significativos, para su reputación, para sus resultados, en términos de sanciones de cumplimiento y para las grandes inversiones que tantos han realizado en la implementación de la IA en primer lugar.

Recientemente, en un chequeo médico, mi médico me preguntó si podía usar un agente de IA para tomar notas. Esa conversación se extendió más allá de mi salud, a los planes de fin de semana, a las elecciones universitarias de mi hija y mucho más. Me preguntaba a dónde iba esa información. ¿Acaso el médico lo sabía? ¿Había tenido lugar una posible infracción de la HIPAA?

Este es el tipo de preguntas que se hacen en salas de conferencias y reuniones de juntas directivas de todo el mundo. ¿Estamos utilizando la IA de forma segura? ¿La estamos construyendo de forma segura? Y si no se están formulando estas preguntas, tienen que empezar a hacerse. La IA ha creado una ola de optimismo e innovación. Sin embargo, trae consigo todo un nuevo ámbito de vulnerabilidades de ciberseguridad, y las soluciones de seguridad existentes no están bien equipadas para gestionarlas. Ya hemos visto surgir una tensión natural entre dos partes:

- Los directores de IA y sus equipos de desarrollo se apresuran a implementar nuevas aplicaciones de IA y modelos de negocio.
- Los directores de seguridad de la información (CISO) se quedan preguntándose cómo protegerse contra amenazas que ni siquiera conocen aún.