

La IA ya no solo ayuda a las empresas. También puede ayudar a ejecutar un ataque.

La inteligencia artificial empieza a cambiar también el escenario de las amenazas digitales. **El pasado 14 de septiembre, la AEPD recibió la primera notificación de una brecha de datos personales en España en la que el ataque habría sido ejecutado mediante un agente de IA.**

Según la información comunicada a la Agencia, el agente habría iniciado la búsqueda de vulnerabilidades, una vez conseguido acceder al sistema y, una vez dentro, analizado de forma autónoma la aplicación hasta encontrar nuevas vías que le permitieron modificar datos personales y acceder a facturas. La AEPD advierte de que se trata de una primera notificación y que los hechos deberán ser objeto del correspondiente análisis.

¿Qué cambia con los agentes de IA?

La utilización de IA en ataques no es nueva. Ya se emplea para crear phishing, analizar código, suplantar identidades o buscar vulnerabilidades.

La diferencia está en la **capacidad agéntica**: un agente puede recibir un objetivo, planificar tareas, utilizar herramientas, interpretar resultados y adaptar sus siguientes acciones con una intervención humana limitada.

Para las empresas, esto significa que algunos escenarios de ataque pueden ser **más rápidos, automatizados y difíciles de contener**.

Por eso, conviene revisar:

- **Vulnerabilidades:** ¿cuánto tardamos en identificar y corregir una vulnerabilidad crítica?
- **Identidades:** ¿qué cuentas, credenciales y API keys tienen acceso a nuestros sistemas?
- **Permisos:** ¿un acceso comprometido permite llegar a más información de la necesaria?
- **Detección:** ¿somos capaces de detectar comportamientos anómalos con la velocidad suficiente?
- **Proveedores:** ¿qué controles de seguridad aplican las empresas que tienen acceso a nuestros datos?

La IA no crea nuevas amenazas, pero **puede acelerar y amplificar técnicas de ataque que ya conocemos**.

Binaura – Grupo Monlex ayuda a las organizaciones a revisar estos escenarios desde una perspectiva de seguridad y protección de datos, identificando vulnerabilidades, accesos y riesgos antes de que se conviertan en un incidente.

Porque si los atacantes pueden automatizar sus movimientos, **nuestra capacidad de detectar y responder también tiene que estar preparada para hacerlo a esa velocidad**.

Si deseas más información o asesoramiento, puedes contactar con su equipo escribiendo a: info@binaura.es