

La AEPD recibe la primera notificación de una brecha de datos personales causada por un agente de IA

La utilización autónoma de agentes de IA introduce una nueva superficie de riesgo que debe incorporarse a los análisis de seguridad y a los protocolos de gestión de brechas.

La Agencia Española de Protección de Datos (AEPD) ha recibido la primera notificación de una brecha de datos personales causada por un ataque ejecutado mediante un agente de inteligencia artificial. Según la información comunicada por la organización afectada, el agente habría sido capaz de identificar vulnerabilidades, acceder a sistemas, modificar datos personales y consultar información contenida en facturas.

La relevancia del incidente no radica tanto en la naturaleza de la brecha, sino en el elevado grado de autonomía del agente de IA utilizado para llevar a cabo el ataque. A diferencia de los sistemas de inteligencia artificial que se limitan a proporcionar información o asistencia, los agentes de IA pueden recibir un objetivo, planificar acciones, utilizar herramientas, interpretar resultados y adaptar su comportamiento de forma autónoma para alcanzar la finalidad encomendada.

La AEPD advierte de que esta nueva tipología de amenaza debe ser tenida en cuenta en los análisis de riesgos asociados a los tratamientos de datos personales. La capacidad de estos agentes para actuar con rapidez, escalar ataques y adaptarse dinámicamente a las medidas de defensa puede incrementar significativamente el impacto potencial de los incidentes de seguridad. Asimismo, adquieren una especial relevancia la correcta gestión de credenciales, permisos de acceso y privilegios de los sistemas utilizados por las organizaciones.

La Agencia recuerda que, en caso de producirse una brecha de seguridad, continúan siendo plenamente aplicables las obligaciones previstas en el Reglamento General de Protección de Datos (RGPD). En particular, deberá evaluarse si el incidente supone un riesgo para los derechos y libertades de las personas afectadas y, cuando proceda, notificarse a la autoridad de control en el plazo máximo de 72 horas desde que la organización tenga conocimiento de la brecha.

ER-0623 / 2015

Las circulares de **Escura** tienen carácter meramente informativo, resumen disposiciones que por carácter limitativo propio de todo resumen pueden requerir de una mayor información. La presente circular no constituye asesoramiento legal.

©La presente información es propiedad de **Escura** quedando prohibida su reproducción sin permiso expreso.

La comunicación de la AEPD no supone la creación de una nueva categoría jurídica de brecha de seguridad. Sin embargo, sí pone de manifiesto que los agentes de inteligencia artificial deben ser considerados una nueva superficie de riesgo dentro de las estrategias de ciberseguridad y protección de datos de las organizaciones.

¿Qué implica para las organizaciones?

Este incidente constituye una señal de alerta para las empresas que utilizan tecnologías de inteligencia artificial o que pueden verse expuestas a ataques apoyados en este tipo de herramientas. En este contexto, resulta recomendable revisar:

- Los análisis de riesgos y, en su caso, las evaluaciones de impacto en materia de protección de datos.
- Los sistemas de gestión de identidades, credenciales y privilegios de acceso.
- Las medidas de monitorización, detección y respuesta ante incidentes.
- Los procedimientos internos de gestión y notificación de brechas de seguridad.
- Las políticas corporativas de utilización y gobierno de herramientas de inteligencia artificial.

Recomendación de Escura

Desde Escura recomendamos revisar los análisis de riesgos, las medidas de seguridad y los procedimientos de gestión de incidentes para evaluar específicamente la exposición de la organización a amenazas derivadas del uso de agentes de inteligencia artificial. Asimismo, resulta conveniente verificar que los protocolos de respuesta y notificación de brechas permiten cumplir adecuadamente las obligaciones impuestas por el RGPD en un entorno en el que la IA puede actuar no solo como herramienta empresarial, sino también como instrumento para la ejecución de ataques cada vez más sofisticados.

ER-0623 / 2015

Las circulares de **Escura** tienen carácter meramente informativo, resumen disposiciones que por carácter limitativo propio de todo resumen pueden requerir de una mayor información. La presente circular no constituye asesoramiento legal.

©La presente información es propiedad de **Escura** quedando prohibida su reproducción sin permiso expreso.