

«La IA no solo mejora la productividad; también está haciendo más sofisticados los ciberataques»

ZUCCHETTI SPAIN La creciente importancia del dato está transformando la forma en que las empresas operan, toman decisiones y protegen su información. Para analizar este escenario hablamos con Mikel Lorente, director de I+D de Zucchetti Spain, compañía tecnológica especializada en 'software' empresarial, que destina el 15% de su facturación a la investigación, desarrollo e innovación para la evolución de sus soluciones empresariales en sus centros de I+D+i locales

¿Es la IA beneficiosa o causará más daño que alegrías al ser humano en un futuro?

La IA representa un gran desafío para la seguridad de los datos, pero también una ventana de oportunidad para el crecimiento empresarial. La tecnología aporta una alta productividad, sobre todo en tareas repetitivas o en las que hay mucha información pública.

La aplicación de IA al desarrollo bien ejecutado puede ser muy provechosa, pero es probable que en un periodo se hagan desarrollos con carencias técnicas y de seguridad. Ya se conocen casos en los que el texto en un email incluye instrucciones maliciosas para manipular un sistema de IA ('prompt injection') que abre la puerta a que un agente (mal diseñado) le entregue credenciales al atacante.

Este año 2026 estará marcado por el uso de agentes de IA que hacen cosas por ti con tus credenciales. No obstante, no debemos dejar de prestar atención a los riesgos que esto supone.

¿Cómo está afectando la IA a los usuarios y a las empresas en términos de privacidad y protección de datos?

Muchos usuarios y pequeñas empresas están subiendo información sensible a IAs públicas sin ser conscientes del riesgo. Las organizaciones más maduras ya trabajan en entornos privados.

La mejor opción para minimizar riesgos es integrar la inteligencia artificial en los procesos de gestión empresarial, con soluciones de empresa que ya la incorporan de forma nativa, como Sol-micro ERP.

¿Cómo cree que afectará la computación cuántica a la seguridad de las contraseñas actuales?

Por ahora el acceso a la computación cuántica está controlado, pero una vez sea accesible todas las contraseñas actuales van a ser vulnerables y habrá que sustituirlas por sistemas de cifrado resistentes a la computación cuántica.



Mikel Lorente, director de I+D de Zucchetti Spain.

En términos generales, los usuarios primamos la comodidad o la usabilidad frente a la seguridad y estas suelen ser inversamente proporcionales. Hoy la seguridad no depende solo de la contraseña, sino del modelo de protección completo.

¿Cuál es la importancia de los datos para el futuro de la tecnología? ¿Somos conscientes de sus aplicaciones por parte de las empresas y los riesgos que lleva su cesión para la ciberseguridad?

Los datos representan la base sobre la

que descansan la revolución digital y tecnologías como la IA y el 'big data', pero todavía existe poca cultura del dato y de ciberseguridad en empresas y sociedad.

No digo que no sea adecuado ceder los datos, pero sí hay que plantearse a quién, para qué, durante cuánto tiempo los van a tener, cómo voy a poder recuperarlos si quiero... y pensar que quien los recoge recibe un activo que para él tiene un valor económico.

¿La IA está ayudando más a defenderse o a atacar?

Ambas cosas. La IA permite mejorar la detección de anomalías y prevenir incidentes, pero al mismo tiempo está facilitando ataques más automatizados y sofisticados, como el 'ransomware' basado en IA. Por eso, la ciberseguridad debe evolucionar al mismo ritmo que la digitalización.

Los ciberataques son cada vez más frecuentes y sofisticados. Dinero, prestigio e información son los tres daños que nos pueden causar los ciberdelincuentes. Pero... ¿cuándo un ciberataque es realmente peligroso?

Los ciberataques pueden tener un impacto devastador en las empresas, sobre todo en las pymes. No solo por el riesgo que supone el robo de datos, sino por el tiempo que transcurre hasta que las empresas logran recuperarse, lo cual puede suponer grandes pérdidas económicas y un gran daño reputacional.

La IA está volviendo más sofisticados los ciberataques, por ejemplo con 'ransomware' basado en IA o como servicio (RaaS), 'malware' sin archivos ('fileless') y el notable incremento de identidades no humanas en la red.

En Zucchetti valoramos la ciberseguridad como un factor estratégico de la digitalización. Por ello, contamos con una unidad especializada en Sistemas y Ciberseguridad orientada a proteger el dato y garantizar la continuidad del negocio.

MUNDO DIGITAL

«Los ciberataques pueden tener un impacto devastador en las empresas, sobre todo en las pymes»

«Todavía existe poca cultura del dato y la ciberseguridad, tanto en empresas como en la sociedad»