Prensa Capgemini
Luis Antón / Ángeles García Molero
Tel: +34 91 657 70 00

Miriam Sarralde / Jorge Majada
Tel: +34 696 005 743 / +34 648 96 31 67
Email: miriam.sarralde@trescom.es
jorge.majada@trescom.es

La IA y Gen IA están transformando la ciberseguridad de la mayoría de las organizaciones

Si bien la Gen IA acentúa los puntos débiles, más de la mitad de las organizaciones también prevén una detección de amenazas más rápida y una mayor precisión gracias a su uso

Madrid, 19 de noviembre de 2024 – El nuevo informe del Instituto de Investigación de Capgemini, «Nuevas defensas, nuevas amenazas: Qué aportan la IA y la Gen IA a la ciberseguridad», publicado hoy, revela que, si bien están surgiendo nuevos riesgos para la ciberseguridad debido a la proliferación de la IA y la IA generativa (Gen IA), estas tecnologías representan un cambio transformador a la hora de reforzar las estrategias de ciberdefensa a largo plazo para predecir, detectar y responder a las amenazas. Dos tercios de las organizaciones están dando prioridad a la IA en sus operaciones de seguridad.

Según el informe, aunque las organizaciones consideran la IA como una tecnología clave para reforzar sus estrategias de seguridad, la creciente adopción de la Gen IA en diversos sectores[1] conlleva una mayor vulnerabilidad. La Gen IA introduce tres grandes áreas de riesgo para las organizaciones: ataques más sofisticados con más adversarios, la expansión de la superficie de ciberataques y un aumento de las vulnerabilidades en todo el ciclo de vida de las soluciones Gen IA personalizadas. Estos riesgos también se ven agravados por el uso indebido de la IA y la Gen IA por parte de los empleados, lo que puede aumentar significativamente el riesgo de filtración de datos.

Dos de cada tres organizaciones desconfían de una mayor exposición a las amenazas

Casi todas las organizaciones encuestadas (97%) reconocen haber sufrido infracciones o problemas de seguridad relacionados con el uso de Gen IA en el último año. La Gen IA también conlleva riesgos adicionales, como por ejemplo la creación de alucinaciones, la generación de contenidos sesgados, dañinos o inapropiados, y los *prompt injection attacks*[2]. Dos de cada tres organizaciones (67%) están preocupadas por la intoxicación de datos y la posible filtración de datos confidenciales a través de los conjuntos de datos de entrenamiento utilizados para entrenar los modelos de Gen IA.

Además, la capacidad de Gen IA para generar contenidos falsos de gran realismo está planteando riesgos adicionales: más de dos de cada cinco organizaciones encuestadas (43%) afirmaron haber sufrido pérdidas económicas derivadas del uso de *deepfakes*.

Casi 6 de cada 10 empresas creen que necesitan aumentar su presupuesto de ciberseguridad para reforzar sus sistemas de defensa en consecuencia.

1 Casi una cuarta parte (24%) de las organizaciones ha habilitado capacidades de IA Generativa en algunas o la mayoría de sus funciones y ubicaciones, según el informe del Instituto de Investigación de Capgemini "Aprovechar el valor de la IA generativa, 2ª edición: Casos de uso en todos los sectores" de julio de 2024.

2 Se trata de utilizar entradas maliciosas para manipular los modelos de IA y Gen IA, comprometiendo su integridad.

La IA y la Gen IA son primordiales para detectar y responder a los ataques

Según el informe, en el que se encuestó a 1.000 organizaciones[3] que han pensado en la IA para la ciberseguridad o que ya la utilizan, la mayoría confía en ella para reforzar la seguridad de sus datos, aplicaciones y cloud, debido a la capacidad de la tecnología para analizar rápidamente grandes cantidades de datos, identificar patrones y predecir posibles infracciones.

Más del 60% de ellos informó de una reducción de al menos el 5% en el tiempo de detección, y casi el 40% señaló que su tiempo de corrección se redujo en un 5% o más tras implantar la IA en sus centros de operaciones de seguridad (SOC).

Tres de cada cinco organizaciones encuestadas (61%) creen que la IA es esencial para responder eficazmente a las amenazas, ya que les permite aplicar estrategias de seguridad proactivas contra los cada vez más sofisticados ciberdelincuentes. Además, la misma proporción de encuestados prevé que Gen IA refuerce las estrategias de defensa proactiva a largo plazo, anticipando una detección más rápida de las amenazas. Más de la mitad de ellos también cree que la tecnología permitirá a los analistas de ciberseguridad concentrarse más en la estrategia para combatir amenazas complejas.

"El uso de IA y Gen IA ha demostrado hasta ahora ser un arma de doble filo. Si bien introduce riesgos sin precedentes, las organizaciones confían cada vez más en la IA para una detección más rápida y precisa de los problemas cibernéticos. La IA y Gen IA proporcionan a los equipos de seguridad nuevas y potentes herramientas para mitigar estos incidentes y transformar sus estrategias de defensa. Para garantizar que representan una ventaja clara frente a la sofisticación cambiante de las amenazas, las organizaciones deben mantener y priorizar la supervisión continua del panorama de la seguridad, crear la infraestructura de gestión de datos, los marcos y las directrices éticas necesarios para la adopción de la IA, y establecer sólidos programas de formación y concienciación de los empleados", subraya Marco Perira, Director Global de Ciberseguridad, Cloud y Servicios de Infraestructura de Capgemini.

Metodología

El Instituto de Investigación de Capgemini encuestó a 1.000 organizaciones que han considerado la IA para la ciberseguridad o que ya la están utilizando, en 12 sectores y 13 países de Asia-Pacífico, Europa y Norteamérica. Tienen unos ingresos anuales de 1.000 millones de dólares o más. La encuesta mundial tuvo lugar en mayo de 2024. Las organizaciones encuestadas representan una amplia gama de sectores, como automoción, productos de consumo, retail, banca, seguros, telecomunicaciones, energía y servicios públicos, aeroespacial y defensa, alta tecnología, fabricación de equipos industriales, farmacia y sanidad y sector público.

Acerca de Capgemini

Capgemini es un socio global de transformación empresarial y tecnológica, que ayuda a las organizaciones a acelerar su transición dual hacia un mundo digital y sostenible, al tiempo que crea un impacto tangible para las empresas y la sociedad. Es una organización responsable y diversa que cuenta con 340.000 profesionales en más de 50 países. Con una sólida trayectoria de más de 55 años, Capgemini cuenta con la confianza de sus clientes para liberar el potencial de la tecnología y dar respuesta a todas sus necesidades empresariales. Ofrece servicios y soluciones integrales aprovechando sus puntos fuertes, desde la estrategia y el diseño hasta la ingeniería, todo ello impulsado por sus capacidades líderes en el mercado en IA, Cloud y datos, combinadas con su gran experiencia en el sector y su propio ecosistema de socios. En 2023, el

[3] 1.000 organizaciones de 12 sectores y 13 países de Asia-Pacífico, Europa y Norteamérica, con ingresos anuales iguales o superiores a 1.000 millones de dólares.

Grupo registró unos ingresos globales de 22.500 millones de euros. Get The Future You Want | www.capgemini.com/es-es/

Acerca del Instituto de Investigación de Capgemini

El Instituto de Investigación de Capgemini es el grupo de expertos interno de Capgemini sobre todo lo digital. El Instituto publica investigaciones sobre el impacto de las tecnologías digitales en las grandes empresas tradicionales. El equipo se basa en la red mundial de expertos de Capgemini y trabaja en estrecha colaboración con socios académicos y tecnológicos. El Instituto cuenta con centros de investigación dedicados en India, Singapur, Reino Unido y Estados Unidos. Recientemente, ocupó el puesto número 1 en el mundo por la calidad de sus investigaciones realizadas por analistas independientes. Visítanos en https://www.capgemini.com/researchinstitute/