LITORALPRESS

Fecha: 28-07-2025
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: La inteligencia artificial impulsa la innovación y los riesgos en APIs y aplicaciones web

Pág. : 44
Cm2: 477,9
VPE: $ 659.967

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

La inteligencia artificial impulsa la innovación y los riesgos en APIs y aplicaciones web

El auge de la inteligencia artificial está revolucionando el desarrollo de aplicaciones y APIs, pero también intensifica los riesgos de ciberseguridad. Un nuevo estudio revela un alza explosiva en los ataques automatizados, especialmente en América Latina, donde la digitalización avanza más rápido que la protección.

La inteligencia artificial (IA) y las interfaces de programación de aplicaciones (APIs) se han convertido en dos pilares imprescindibles en la transformación digital. A medida que un mayor número de organizaciones de Latinoamérica adoptan estas tecnologías, la superficie de ataque de vulnerabilidades se amplía. Según el estudio "Estado de la seguridad de API y aplicaciones 2025: cómo cambia la IA el panorama digital" de Akamai, se destaca que tan solo en 2024 se observaron más de 311.000 millones de ataques a API y aplicaciones web a nivel global, lo que representa un aumento interanual del 33% relacionado con la rápida adopción de servicios en la nube, arquitecturas de microservicios y aplicaciones con inteligencia artificial.

"Actualmente, vemos que la inteligencia artificial no solo está acelerando la innovación, sino que, lamentablemente, también está siendo aprovechada por ciberdelincuentes. El aumento del uso de la IA ha coincidido con un incremento significativo de los ataques a APIs, ya que los ciberdelincuentes están utilizando herramientas de IA para el reconocimiento, la explotación y la automatización de amenazas", comenta Jairo Parra, experto en Seguridad de Akamai.

El impacto en América Latina

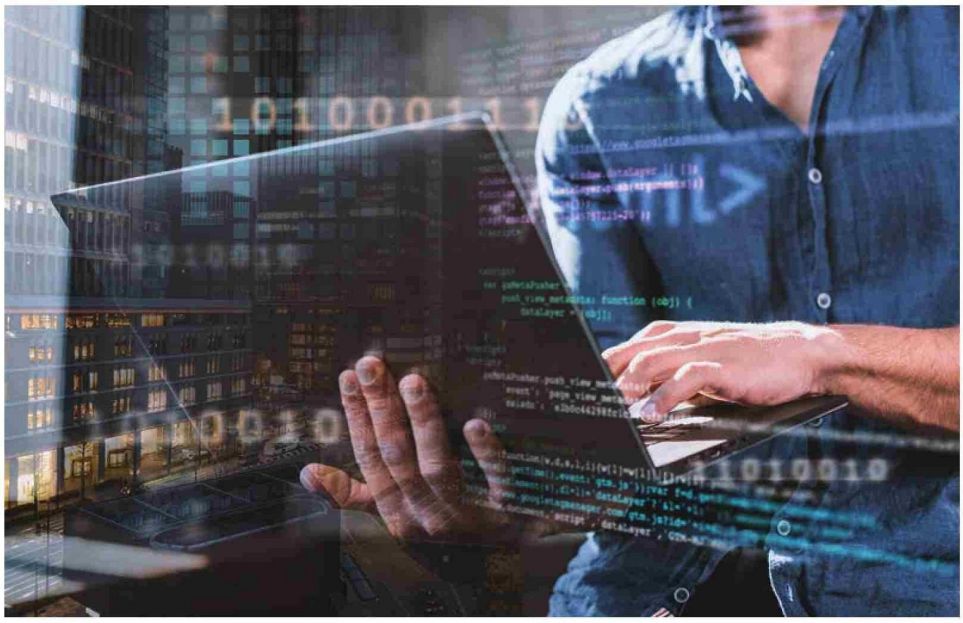
Según el mencionado estudio, América Latina se ha convertido en un objetivo prioritario para la ciberdelincuencia debido a la rápida digitalización y la creciente interconectividad de esta región. "En países como México, Brasil, Colombia y Argentina, el avance de la digitalización ha sido impresionante. Pero

LITORALPRESS

Fecha: 28-07-2025
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: La inteligencia artificial impulsa la innovación y los riesgos en APIs y aplicaciones web

Pág. : 45
Cm2: 425,8
VPE: $ 588.091

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida



muchas organizaciones aún carecen de visibilidad total de sus APIs, lo que las convierte en objetivos atractivos", añade el experto.

El informe resalta que entre enero de 2023 y junio de 2024 se registraron más de 108 mil millones de ataques a APIs en Latinoamérica, siendo los sectores del comercio electrónico, la banca digital y los medios los más afectados. Los comercios electrónicos, los procesadores de pagos, los bancos, las compañías de seguros, las empresas emergentes de tecnología financiera y los intercambios de criptomonedas son especialmente vulnerables a las amenazas que afectan a su infraestructura digital, especialmente a sus aplicaciones web y API.

Además, según Parra, los atacantes están utilizando la inteligencia artificial para identificar componentes vulnerables en APIs y desarrollar exploits personalizados, y para reducir tiempos de ejecución mediante bots de IA que explotan fallos a gran escala. También están saturando las APIs con tráfico masivo a través de bots inteligentes, como en los ataques DDoS automatizados, y llevan a cabo intrusiones de baja intensidad que operan por debajo de los umbrales de alerta habituales.

Akamai estima que los problemas de seguridad de las API cuestan a las organizaciones aproximadamente 87.000 millones de dólares al año y prevé que esta cifra podría superar los 100.000 millones en 2026 si no se actúa adecuadamente.

Por otro lado, las API basadas en IA han demostrado ser notablemente inseguras, ya que son accesibles externamente y una parte importante depende de mecanismos de autenticación inadecuados, lo que las hace susceptibles a ciberataques. Además, la integración de grandes modelos de lenguaje (LLM) en aplicaciones web ha abierto nuevos vectores de vulnerabilidad.

"Muchas organizaciones priorizan la rapidez en la implementación de soluciones con IA sin evaluar los riesgos de exposición. Esto deja puertas abiertas que los atacantes saben identificar con precisión". Este estudio revela que las APIs de las herramientas de IA generativa son la causa principal de los incidentes notificados por los equipos de seguridad del comercio electrónico y del sector retail.

Los atacantes están utilizando la inteligencia artificial para identificar componentes vulnerables en APIs y desarrollar exploits personalizados, y para reducir tiempos de ejecución mediante bots de IA que explotan fallos a gran escala.

¿Cuál es la solución para erradicar las amenazas de la IA?

El informe prevé un enorme crecimiento del mercado de API con IA: de 44.410 millones de dólares en 2025 se pasará a 179.140 millones en 2030, lo que supone una tasa de crecimiento anual compuesto del 32,2%.

En un panorama de amenazas en constante evolución, con técnicas de ataque cada vez más sofisticadas, la protección de las aplicaciones web y las API es un desafío esencial para las organizaciones. En este sentido, los sistemas avanzados de cortafuegos de aplicaciones web (WAF) basados en IA emergen como una defensa crucial, ya que mitigan muchos tipos de ciberataques en aplicaciones web y API. Sin embargo, las soluciones WAF deben adaptarse constantemente a medida que evolucionan las amenazas y cambian las aplicaciones.

Al utilizar estrategias de aprendizaje automático multicapa, los nuevos WAF pueden identificar patrones anómalos, aprender y adaptarse de forma continua, mejorar los tiempos de respuesta ante amenazas de día cero y prevenir proactivamente riesgos antes de que afecten a las organizaciones.

Por último, Jairo Parra opina que el volumen y la velocidad de los ataques hacen que las defensas tradicionales ya no sean suficientes. "Necesitamos inteligencia que actúe en tiempo real, y ahí es donde los WAF basados en IA marcan la diferencia. Mientras la IA transforma radicalmente la innovación tecnológica, también redefine el escenario de riesgos. Las empresas de todos los sectores deberían adoptar enfoques de seguridad más dinámicos e incorporar defensas basadas en IA que estén a la altura de esta nueva generación de amenazas automatizadas", concluyó. ChN

Artículo gentileza de Akamai.