

CINCO RIESGOS DE LA IA EN LA FILTRACIÓN DE INFORMACIÓN EMPRESARIAL

- Entre octubre de 2023 y octubre de 2024, se bloquearon 9.3 millones de ataques de malware en empresas peruanas, incluyendo 38 millones de intentos de phishing y alrededor de 17,000 ataques de ransomware.
- Es importante que las organizaciones adopten medidas proactivas para prevenir incidentes de seguridad y refuercen sus sistemas ante amenazas emergentes.

Lima, 10 de abril 2025

El avance de la inteligencia artificial (IA) ha traído innumerables beneficios a las empresas, pero también ha abierto nuevas puertas para los ciberdelincuentes. En la actualidad, los ataques dirigidos a grandes corporaciones son cada vez más sofisticados, aprovechando la IA para cometer fraudes, acceder a información confidencial y manipular datos estratégicos.

Un informe de Kaspersky reveló que, entre octubre de 2023 y octubre de 2024, se bloquearon 9.3 millones de ataques de malware en empresas peruanas, incluyendo 38 millones de intentos de phishing y alrededor de 17,000 ataques de ransomware. Estas cifras subrayan la creciente amenaza que enfrentan las organizaciones en el país y la necesidad urgente de fortalecer las estrategias de ciberseguridad.

En este contexto, la ciberseguridad corporativa se convierte en una prioridad para mitigar los riesgos y proteger la información empresarial. José Díaz, Gerente de Producto-Seguridad y Vigilancia del Grupo EULEN Perú, destaca la importancia de que las organizaciones adopten medidas proactivas para prevenir incidentes de seguridad y refuercen sus sistemas ante amenazas emergentes.

1- Suplantación de identidad

Las herramientas de IA pueden generar videos, audios e imágenes falsificadas con una precisión sorprendente. Esto permite a los ciberdelincuentes suplantar la identidad de directivos o empleados clave para engañar a terceros y obtener acceso a información sensible o realizar transferencias fraudulentas.

2- Automatización de ataques de phishing

Los correos electrónicos fraudulentos han evolucionado gracias a la IA. Los atacantes pueden generar mensajes altamente personalizados y difíciles de detectar, imitando el lenguaje y estilo de comunicación de la empresa. Esto aumenta la probabilidad de que empleados desprevenidos compartan credenciales o descarguen archivos maliciosos.

3- Explotación de vulnerabilidades en sistemas

Los algoritmos de IA pueden analizar grandes volúmenes de datos en poco tiempo, identificando debilidades en los sistemas de seguridad de las empresas. Los ciberdelincuentes pueden utilizar esta tecnología para descubrir y explotar fallos en la infraestructura digital, accediendo a bases de datos o manipulando información crítica.

El Grupo EULEN, empresa familiar multinacional con la matriz en España, avalado por la experiencia de más de 57 años en el mercado y consolidado como líder internacional en la prestación de servicios generales a empresas y administraciones públicas, que cuenta con más de 7 000 clientes en 11 países, y emplea a más de 90 000 personas en modalidad de planilla.

En el 2002 inicia sus operaciones en Perú, contando con una oficina central en Lima y dos delegaciones en las provincias de Arequipa y Trujillo, además de oficinas administrativas en todos los departamentos del Perú. Cuenta con más de 7.500 empleados y ofrece servicios de limpieza, seguridad física, seguridad electrónica, mantenimiento, servicios auxiliares, jardinería, Facility Management, Facility Services y trabajo temporal a más de 300 clientes de primer nivel en todo el país.

Para más información:

Liseth Ruiz
Analista de prensa

993014844

[www](http://www.eulen.com)   

4- Espionaje corporativo automatizado

La IA facilita el análisis masivo de información pública y privada, permitiendo a los atacantes obtener inteligencia de mercado de manera más eficiente. Desde el rastreo de correos electrónicos filtrados hasta la extracción de datos sensibles en redes sociales y foros.

5- Manipulación de información empresarial

Los ataques basados en IA no solo buscan robar datos, sino también alterarlos. La manipulación de registros financieros, la creación de documentos falsos y la difusión de noticias falsas pueden afectar la reputación y estabilidad de una empresa, generando desconfianza en clientes e inversionistas.

Para hacer frente a estos desafíos, las compañías deben fortalecer sus estrategias de ciberseguridad con tecnología avanzada, capacitación constante a sus colaboradores y una regulación estricta del acceso a la información. "Sin duda, la combinación de tecnología avanzada y concienciación humana representan una sinergia clave para proteger la información empresarial en la era digital", concluye Díaz, gerente del producto de seguridad en la compañía de prestación de servicios.

El Grupo EULEN, empresa familiar multinacional con la matriz en España, avalado por la experiencia de más de 57 años en el mercado y consolidado como líder internacional en la prestación de servicios generales a empresas y administraciones públicas, que cuenta con más de 7 000 clientes en 11 países, y emplea a más de 90 000 personas en modalidad de planilla.

En el 2002 inicia sus operaciones en Perú, contando con una oficina central en Lima y dos delegaciones en las provincias de Arequipa y Trujillo, además de oficinas administrativas en todos los departamentos del Perú. Cuenta con más de 7.500 empleados y ofrece servicios de limpieza, seguridad física, seguridad electrónica, mantenimiento, servicios auxiliares, jardinería, Facility Management, Facility Services y trabajo temporal a más de 300 clientes de primer nivel en todo el país.

Para más información:

Liseth Ruiz
Analista de prensa

993014844