LITORALPRESS

Fecha: 21-06-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **Inteligencia Artificial comienza a ganar terreno en Chile para detectar y combatir ciberamenazas**

Pág. : 32
Cm2: 627,2

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

Inteligencia artificial comienza a ganar terreno en Chile para detectar y combatir ciberamenazas

POR MARCO ZECCHETTO

Expertos señalaron que sectores como banca, seguros y proveedores de servicios esenciales ya usan IA integrada en sistemas de monitoreo, detección y respuesta ante amenazas.

El avance y desarrollo de nuevas tecnologías como la Inteligencia Artificial (IA) tiene una doble cara. Por una parte, ha propiciado la sofisticación de la ciberdelincuencia, donde el blanco muchas veces son empresas y, por otro, ha puesto a disposición de las organizaciones nuevos modelos y herramientas para detectar estas amenazas y proteger su información y sistemas.

En ese contexto, el *managing director & partner* de Boston Consulting Group (BCG), Julián Herman, indicó que uno de los factores que ha cambiado el panorama de la ciberseguridad y ha llevado a una mayor preocupación por adoptar soluciones en las compañías locales, ha sido el auge de la IA generativa (producción de texto, imagen u otro, a partir de contenido existente).

"Ahí es donde hemos visto que, por un lado, han aumentado bastante los eventos de seguridad. Ha habido muchas filtraciones de datos principalmente por temas de mal uso o desconocimiento. La gente ocupa Chat GPT de código abierto y sube cosas que no debería, pero también esta tecnología ha generado una mayor sofisticación de los ataques", afirmó Herman.

En una línea similar, el socio líder de Cyber Risk en Deloitte, Nicolás Corrado, comentó que las empresas están utilizando principalmente modelos de IA conocidos y previamente probados, e indicó que es clave que estas tengan la precaución de que los sistemas que implementen sean privados, seguros y confidenciales.

"Mucha gente está probando, armando o programando el código de un sistema a través de IA generativa abierta, y cuando lo hacen, no se dan cuenta de que la información puede quedar expuesta", afirmó.

IA integrada

Corrado señaló que hoy las compañías en Chile están empleando en gran medida "IA embebida", es decir, aquella integrada en los productos o soluciones de ciberseguridad que ya tienen o que adquieren.

Por ejemplo, están adoptando sistemas de detección y respuesta administrada (MDR, por su sigla en inglés), los que incorporan tecnologías como el análisis de comportamiento e IA para detectar amenazas y generar respuestas.

También se está implementando IA en soluciones de detección y respuesta de red (NDR, por su sigla en inglés), lo que permite a las compañías detectar virus, *ransomware* (código malicioso) y diferentes tipos de amenazas.

> La IA generativa se está utilizando para acelerar respuestas ante un riesgo, pero alertaron que los modelos de código abierto pueden dejar información "expuesta".

Corrado comentó que además se está incorporando IA en las herramientas de gestión de información y eventos de seguridad (SIEM, en inglés), las que a través de tecnologías de análisis de comportamiento de usuarios y entidades permiten detectar patrones y cualquier cambio anómalo de forma rápida y sin interacción humana.

"En este último campo -monitoreo y respuesta ante incidentes- empezamos a ver que entre las soluciones aparece la IA generativa para que los analistas puedan preguntar en forma directa lo que están buscando y acelerar procesos de *threat hunting* (caza de amenazas) o análisis forense", indicó el ejecutivo de Deloitte.

Por otro lado, comentó que muy pocas empresas maduras en niveles de ciberseguridad están creando sus propias IA para realizar inteligencia de ciberamenazas -recopilación de información sobre las amenazas o ciberdelincuentes-, detectar fugas de información o cambios en comportamientos de usuarios o en la red.

Directorios e industrias

Según Herman de BCG, la preocupación por la ciberseguridad y la incorporación de este tipo de herramientas ha ido tomando peso dentro de los directorios nacionales, siendo incluso uno de los temas más discutidos.

"En los últimos directorios que me ha tocado estar, el tema de ciberseguridad y de uso de herramientas más sofisticadas basadas en IA, está dentro de la agenda y es algo que en los próximos tres, cuatro o seis meses va a estar mucho más extendido en las organizaciones locales", afirmó Herman.

Comentó que, en los últimos cuatro años, la banca y las compañías de seguros se han enfocado en fortalecer sus capacidades en ciberseguridad, las que son hasta ahora, "las principales industrias del país que han ido adoptando estas tecnologías", dijo el socio de BCG.

También ha visto una creciente adopción y preparación en el uso de estos sistemas en los servicios esenciales asociados a *utilities*, como proveedores de agua, gas y electricidad.

En tanto, Corrado señaló que el retail está más avanzando en esta materia, y que, en el caso de la minería, esta industria "viene trabajando mucho con IA en sus centros de operación remota", y "un poco" en aplicaciones de ciberseguridad, porque "están más acostumbrados a la parte de gobierno de datos, IA y automatización".

Añadió que, más allá de la adopción de estas tecnologías, la capacidad de poder internalizarlas y hacer un uso eficaz en las organizaciones, dependerá del nivel de "madurez" y capacidades en ciberseguridad que estas tengan.*