DIARIO FINANCIERO®

Fecha: 30/05/2025 Audiencia: 48.450 Sección: ECONOMIA
Vpe: $5.987.402 Tirada: 16.150 Frecuencia: DIARIO
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 80,44%

STEFAN DEUTSCHER
LÍDER GLOBAL DE CIBERSEGURIDAD DE BCG

PABLINA SALINAS

"Los atacantes son más eficientes usando la IA que los defensores"

■ Aseguró que a nivel mundial las organizaciones no están "muy bien preparadas", que los cibercriminales llevan la delantera y que en Latinoamérica la baja inversión en ciberseguridad la convierte en un "objetivo blando".

POR MARCO ZECCHETTO

La inteligencia artificial (IA) está cambiando el panorama de la ciberseguridad. La aparición de "ataques como servicio" en la *dark web*, la proliferación de herramientas como *deepfakes* (videos, imágenes o audios generados que imitan la apariencia y el sonido de una persona) están ampliando las posibilidades y la superficie de ataque, encendiendo las alertas en las organizaciones.

Esas son algunas de las alertas que abordó con **DF** el socio y director de Boston Consulting Group (BCG), líder global de ciberseguridad y gestión de riesgos TI, Stefan Deutscher, quien afirmó que los atacantes están haciendo un uso más eficiente de la IA que las organizaciones para defenderse, y que estas últimas "no están muy bien" preparadas.

Señaló que las amenazas no se limitan a vulnerabilidades técnicas, sino que se amplifican por errores humanos y organizacionales, destacando que en Chile y la región, la inversión en ciberseguridad es menos de la mitad del promedio mundial, lo que podría los convierte en un "objetivo más blando" para los atacantes.

– ¿Qué diferencias hay entre este ciclo de ciberseguridad con uso de IA y los anteriores?

– Hay dos diferencias clave. La primera es la velocidad. La IA puede ser usada por los atacantes como una explosión, ya que permite que el tiempo de preparación (de los ataques) se reduzca masivamente. Y los adversarios utilizan cada vez más algoritmos apoyados en IA para ajustar sus ataques para lograr atravesar las defensas del objetivo. Además, hay ofertas de "ataque como servicio" en la *dark web*, con garantía de devolución si no funciona.

Lo segundo, es que hemos entrenado a la IA para comportarse como los humanos, lo que hace que sea casi imposible distinguir, por ejemplo, un correo legítimo de uno falso generado por IA. Eso se vuelve aún más complejo con los *deepfakes* de audio y video. Actualmente las organizaciones no están muy bien preparadas.

– ¿La balanza está inclinada a favor de los cibercriminales? ¿Van por delante de las organizaciones y la regulación?

– Hoy los atacantes son más eficientes en el uso de la IA que los defensores. A menudo el desarrollo tecnológico supera el ritmo del pensamiento regulador, y sólo cuando los reguladores se dan cuenta de que está pasando algo, empiezan a estructurar y regular, pero estos también están actualizando y modernizando su aproximación a la tecnología, y comienzan a mirar más hacia el futuro.

Respecto de las organizaciones, aquellas más maduras son relativamente saludables en sus defensas cibernéticas y pueden seguir protegiéndose, así que no es una carrera armamentística perdida. Pero ahora mismo creo que los atacantes van por delante.

> "Chile invierte un 0,08% del PIB en ciberseguridad, menos de la mitad del 0,17% del gasto promedio mundial".

– ¿Qué sectores son los principales objetivos?

– Históricamente eran bancos, aseguradoras y telecomunicaciones, pero han endurecido bastante su panorama informático y otras industrias se han vuelto blancos más fáciles, como bienes industriales, de consumo y retail. Pero ahora, casi todo el mundo es un objetivo. En Latinoamérica vemos muchos ataques a la administración pública, proveedores de servicios de TI (tecnologías de la información) y comercio electrónico.

– ¿Cuáles son los puntos de entrada más comunes?

– Vemos que un 22% de las ciberamenazas se deben a vectores de ataque y problemas tecnológicos, mientras que el 78% restante ocurre por errores humanos, de procesos o de la organización. También hay problemas cuando se usan sistemas antiguos que ya no se pueden actualizar. Además, vemos un crecimiento en los ataques a terceros, como proveedores o socios de las cadenas de suministro de las empresas.

Inversión y futuro

– ¿Cuánto invierte la región en ciberseguridad?

– El gasto promedio global se sitúa en torno al 0,17% del PIB (Producto Interno Bruto). En Chile es 0,08%, en consonancia con otros países de la región. Otros gastan cuatro veces más: Reino Unido, 0,35%; Singapur, 0,33%; Estados Unidos, 0,32%; Canadá, 0,28%. Esto puede acabar convirtiendo a Latinoamérica en un objetivo más blando para los ciberataques.

– ¿Qué potenciales amenazas observa para los próximos 12 a 24 meses?

– Hay cinco cosas que me preocupan. Primero, los ataques potenciados por IA, tanto para evadir su detección como para engañar a usuarios legítimos y llevarlos a cometer acciones indeseables. Segundo, ataques a dispositivos IoT (internet de las cosas), que crecen en uso, pero son históricamente inseguros y, por lo general, técnicamente limitados en recursos. Tercero, ataques a infraestructura OT (tecnología de operaciones), que está cada vez más conectada a redes y expuesta a internet, pero es difícil de proteger, como sistemas de agua, energía o tránsito. Cuarto, la computación cuántica, una tecnología emergente y en rápida evolución, pero es una amenaza silenciosa que puede romper un tipo de criptografía que hoy protege el tráfico en internet, e incluso, las formas tradicionales de criptografía están en riesgo de ser borradas por el poder de los computadores cuánticos en los próximos tres a siete años.

La última no es un vector de ataque, sino una vulnerabilidad sistémica: la falta de talento calificado. Faltan 320 mil expertos en ciberseguridad en Latinoamérica, y entre cuatro a cinco millones a nivel global.