CARLOS SEISDEDOS, CEO DE MAGNETO INTELLIGENCE:

"Los sistemas tradicionales contra la ciberdelincuencia no están funcionando"

Según el ejecutivo, debemos ocupar ciberinteligencia proactiva y "ser capaces de ver antes de que ocurra; porque la amenaza que conoces, no te sorprende".

FERNANDO VIAL

En el marco del Cybertech South America 2025, celebrado en "El Mercurio", Carlos Seisdedos, CEO de Magneto Intelligence, abordó la importancia de la ciberinteligencia proactiva como herramienta fundamental para la defensa de empresas y organizaciones. En un contexto donde los ciberataques aumentaron 14,5% en América Latina y el Caribe, y que solo en Chile se registraron 27.600 millones de intentos de ataques informáticos en 2024, la anticipación se vuelve crucial, aseguró.

Según el ejecutivo, lo primero es identificar las principales amenazas, que dividió en seis: grupos estatales (APT); operadores del cibercrimen ("cada vez más profesionalizados"); activistas y "hacktivistas"; crimen organizado ("que diversifica sus actividades hacia lo digital"); competidores ("que subcontratan cibercriminales para difamar") y, "de manera crucial", la amenaza interna o "insider", donde empleados venden credenciales o facilitan información confidencial.

Además, Seisdedos mencionó vectores amplificadores como las tensiones geopolíticas, la cadena de suministro, la desinformación y la inteligencia artificial, que actúan como catalizadores del impacto de los ciberataques, sin olvidar el impacto legal y regulatorio, que genera multas y sanciones a las empresas víctimas.

HYPO PHOTOS

SEISDEDOS DETALLÓ EN SU PRESENTACIÓN QUE EN CHILE se registraron 27.600 millones de intentos de ataques informáticos en 2024.

CAMBIO DE PARADIGMA

Sin embargo, para el CEO de Magneto Intelligence, "los sistemas tradicionales que se están utilizando en la lucha contra la ciberdelincuencia no están funcionando (...). Entonces, lo que se propone es hacer un cambio de paradigma de ese enfoque".

Y es que con 15 años combatiendo el crimen organizado y el terrorismo en el ámbito policial, el especialista se pregunta: "¿Por qué tenemos que esperar a que nos ataquen?". Por ello, abogó por aplicar un "plan B" proactivo, utilizando técnicas de ciberinteligencia para la recopilación de datos y anticiparse a los incidentes, como lo hace actualmente su empresa. "Magneto Intelligence se enfoca en el uso de identidades virtuales o 'avatares' desplegados en foros y plataformas como Telegram, donde se mueven los ciberdelincuentes. Estas identidades, con capacidad de monitorear miles de canales, permiten obtener información valiosa de manera temprana, como la venta de credenciales, técnicas de *exploits* o rangos de IP vulnerables".

Para concluir, Seisdedos resumió la esencia de la ciberinteligencia proactiva en "ser capaces de ver antes de que ocurra; porque la amenaza que conoces, no te sorprende".