LITORALPRESS

Fecha: 16-06-2025
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: ATAQUES SOFISTICADOS MARCAN EL PRIMER SEMESTRE EN CHILE

Pág. : 26
Cm2: 687,9

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

ATAQUES SOFISTICADOS MARCAN EL PRIMER SEMESTRE EN CHILE

En alza están los ciberataques en el sector corporativo, con el *ransomware* liderando dentro de las modalidades. Y aunque la evolución en técnicas y el uso de herramientas como IA dan cuenta del perfeccionamiento de los ciberdelincuentes, las empresas siguen al debe en dar prioridad a este tema.

POR MACARENA PACULL M.

El primer semestre de 2025 dejó en evidencia que la ciberseguridad es una creciente preocupación para las empresas en Chile, ya que son uno de los principales blancos a nivel regional de los ataques cibernéticos. Según el Reporte de Ciberseguridad 2025 de Entel Digital, los sectores más afectados en el país son infraestructura TI (21%), banca y finanzas (17%), y agricultura y ganadería (13%), siendo el *ransomware* la amenaza predominante.

Según explica el analista de seguridad del Equipo Global de Investigación y Análisis para América Latina de Kaspersky, Leandro Cuozzo, desde la telemetría de la empresa se observa que Chile asciende al tercer lugar regional en esta modalidad de ataque, luego de Brasil y México, y que particularmente en el país, las ciberamenazas más comunes son el *ransomware* avanzado y de doble extorsión, el *phishing* hiperpersonalizado, ataques con *deepfakes*, *infostealers* y troyanos bancarios.

El *phishing* marca una tendencia: el país ocupa el quinto lugar en el número absoluto de usuarios afectados, dice Cuozzo, detrás de Brasil, México, Colombia y Perú, lo que se correlaciona con el tamaño de cada mercado. "Sin embargo, al observar el porcentaje de usuarios impactados sobre el total, Chile lidera la región con un 27%, seguido de Perú (25%), Colombia (24%) y Brasil (23%), evidenciando una alta tasa de exposición relativa", apunta.

En términos generales, "la alta digitalización de su economía, la madurez de su infraestructura tecnológica y su creciente relevancia regional hacen que Chile se mantenga como un objetivo interesante para actores maliciosos, especialmente cuando se trata de ataques dirigidos y de alto impacto", asevera.

Un ejemplo reciente que agrega el consultor senior en ciberseguridad de Mainsoft, Sebastián Campos, es el grupo de atacantes FunkSec, surgido en diciembre de 2024: en lo que va de año "se ha vuelto rápidamente uno de los grupos más temidos, precisamente por su aprovechamiento de inteligencia artificial".

Errores comunes

A juicio del gerente comercial de ITQ Latam, Camilo Vidal, muchas empresas chilenas siguen cometiendo errores en sus estrategias, lo que las hace más vulnerables. Resalta la falta de conciencia y capacitación, con el factor humano como "el eslabón más débil". Además, muchas organizaciones no tienen un inventario completo y actualizado de sus activos de TI (hardware, software, aplicaciones, datos), "ni una visibilidad clara de lo que ocurre en su red", dice. Por otro lado, menciona los planes de respuesta a "incidentes inmaduros o inexistentes" y la falta de enfoque en el respaldo y la recuperación. "Es vital tener copias de seguridad robustas, segregadas y probadas regularmente", enfatiza.

El impacto de la ley

La Ley Marco de Ciberseguridad es una de las normas clave en línea con los ciberataques, pues, además de crear la Agencia Nacional de Ciberseguridad, obliga a los operadores críticos a reportar incidentes, explica la directora del magíster en Gestión de Tecnologías de la Información y Telecomunicaciones, de Ingeniería UNAB, Mailyn Calderón. Sin embargo, "aunque el marco elevó las exigencias, su aplicación es desigual", asegura.

La académica alude a la Radiografía de la Ciberseguridad en Directorios de Chile 2024, del Instituto de Directores, que reveló que el 65% de ellos no entiende el impacto práctico de la Ley 21.663, y el 55% desconoce sus sanciones. "Así, muchas pymes siguen sin planes formales de respuesta pese al récord de 27.600 millones de intentos de ataque en 2024", dice.

Con todo, el principal obstáculo estructural del ecosistema chileno sigue siendo la escasez de capital humano especializado, plantea Calderón. "Sin suficiente talento para implementar las obligaciones legales y las buenas prácticas, el país continuará expuesto, aunque el marco regulatorio avance", puntualiza.