LITORALPRESS

Fecha: 14-06-2025
Medio: El Heraldo
Supl. : El Heraldo
Tipo: Noticia general
Título: **Ciberataques contra bancos en Chile han aumentado un 30% en dos años**

Pág. : 5
Cm2: 458,4
VPE: $ 916.876

Tiraje: 3.000
Lectoría: 6.000
Favorabilidad: No Definida

Ciberataques contra bancos en Chile han aumentado un 30% en dos años

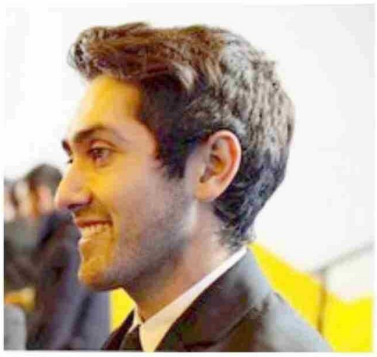
Durante los últimos años, conforme al informe "Cyber Threat Landscape" de Trellix, Chile se ha posicionado como el segundo país más atacado de Sudamérica, con más de un millón de ciberamenazas detectadas en los primeros meses de este año. Los ataques más comunes, según el mismo análisis, incluyen ransomware, inyecciones SQL y explotación de vulnerabilidades en API bancarias. La banca es el sector más golpeado, representando el 30,2 % de los ataques en el país.

De acuerdo al reciente informe Security Report 2025 de Check Point Software Technologies, los Ciberataques contra bancos en Chile han aumentado un 30% en dos años. El estudio también alerta sobre este crecimiento en comparación al 2023, siendo el área financiera el objetivo principal de los ciberdelincuentes.

Este contexto, se debe a la digitalización acelerada y la dependencia de servicios en la nube, se ha ampliado la superficie de ataque, exponiendo vulnerabilidades tanto en en aplicaciones web como en sistemas de autenticación. Para mitigar estos riesgos, las instituciones financieras han comenzado a implementar medidas como autenticación multifactor, inteligencia artificial para detección de amenazas y firewalls avanzados para proteger apps y datos sensibles. Sin embargo, la sofisticación de los embates continúa al alza.

Ante este panorama, el experto de Ionix asegura que los bancos nacionales también han optado por intensificar sus esfuerzos en educación y concientización de sus clientes, desarrollando campañas informativas acerca de los riesgos de estafas y amenazas. Otras regulaciones clave, explica, son el uso de firewalls de última generación y sistemas de monitoreo continuo que previenen irrupciones antes de que provoquen daños.

La colaboración entre instituciones bancarias y organismos de seguridad también ha sido fundamental, facilitando el intercambio de información sobre amenazas y fortaleciendo la capacidad de respuesta del sector financiero.



Sebastián de la Fuente, gerente de Producto de Ionix Latam.

El impacto de estos ataques no solo se traduce en pérdidas económicas, sino también en una creciente preocupación por la confianza del consumidor. La respuesta de los bancos ha sido reforzar sus estrategias de ciberseguridad con soluciones avanzadas, como sistemas de seguridad de aplicaciones web y sistemas de detección de amenazas en tiempo real. Sin embargo, la velocidad con la que evolucionan las amenazas exige una adaptación constante y una mayor inversión en tecnologías de prevención.

Sin embargo, la creciente sofisticación de las arremetidas y la falta de acciones de seguridad adecuadas en muchas organizaciones siguen siendo obstáculos significativos para mitigar estos riesgos.

Mientras que dichas entidades expanden su digitalización, los ciberdelincuentes han perfeccionado sus métodos para vulnerar sistemas de autenticación y filtrar datos sensibles. La protección de la infraestructura online se ha vuelto un desafío recurrente, ante el cual la resiliencia tecnológica es esencial para garantizar la estabilidad del sistema financiero.