LITORALPRESS

Fecha: 01-10-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: ENFOQUE INTEGRADO Y CAPAS DE SEGURIDAD: CÓMO PROTEGER LOS ACTIVOS FINANCIEROS DE LOS CIBERDELICUENTES

Pág. : 26
Cm2: 675,4
VPE: $ 5.985.103

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

DF
DIARIO FINANCIERO
SUPLEMENTO
SANTIAGO DE CHILE
MARTES 1 DE OCTUBRE DE 2024

ENFOQUE INTEGRADO Y CAPAS DE SEGURIDAD: CÓMO PROTEGER LOS ACTIVOS FINANCIEROS DE LOS CIBERDELINCUENTES

Ante la sofisticación de los ciberataques, las empresas con operaciones en Chile están redefiniendo estrategias y combinando acciones con tecnología avanzada. Aquí, varios expertos de la industria analizan las mejores prácticas.

POR ANDREA CAMPILLAY

Según cifras de la Policía de Investigaciones (PDI), en 2023 se investigaron 823 casos relacionados con delitos informáticos en el país, en un escenario donde, a medida que avanza la digitalización, las personas y empresas se enfrentan a nuevos retos para proteger su información sensible, especialmente aquella vinculada a datos financieros y patrimoniales que resulta atractiva para los ciberdelincuentes debido al valor potencial de su robo.

¿Qué están haciendo las empresas frente a eso? El subgerente de operaciones de ciberseguridad de Entel Digital, Eduardo Bouillet, observa que las firmas que operan en el país están fortaleciendo la protección de sus datos financieros mediante un enfoque "basado en capas de seguridad". Destaca tecnologías como la encriptación avanzada, la autenticación multifactor -que refuerza el control de acceso mediante la verificación en múltiples etapas- y el uso de firewalls de nueva generación (NGFW) que proporcionan una protección más robusta al filtrar amenazas y prevenir intrusiones complejas.

La gerente general para Sudamérica en Kaspersky, Andrea Fernández, explica que es importante tener en cuenta que la digitalización amplió la superficie de ataque y estos son "cada vez más complejos y avanzados", razón por la cual, a su juicio, la ciberseguridad de las empresas debe evolucionar en su enfoque para dar una respuesta rápida a los incidentes. "Hoy en día ya no solo hablamos del endpoint -cualquier dispositivo que proporcione un punto de entrada a los activos y aplicaciones de la empresa-, sino que ya hablamos del EDR (detección y respuesta de puntos de conexión), pero sobre esa capa también ya estamos hablando de XDR (detección y respuesta extendidas)", explica la experta, dando ejemplos de cómo esto permite "ser proactivo, más allá de las soluciones". No obstante, advierte que es importante añadir el uso de información de inteligencia que permita prevenir los ataques.

La implementación de sistemas de gestión de identidad y acceso que aseguran que solo el personal autorizado tenga acceso a la data financiera crítica y el monitoreo y análisis de seguridad en tiempo real son otras de las estrategias que las empresas locales están adoptando para proteger sus datos financieros, afirma el CEO de Unitti, Cristián López. Sobre este último punto, precisa que "muchas empresas están adoptando soluciones de monitoreo continuo que emplean inteligencia artificial y machine learning para detectar y responder a amenazas en tiempo real", a lo que se suma el uso de tecnologías emergentes como blockchain para asegurar transacciones y registros financieros y soluciones de nube segura que ofrecen una protección avanzada de datos.

"Es importante recalcar que, en ciberseguridad, la responsabilidad es compartida entre las instituciones financieras y los usuarios", complementa el gerente general de Tecnoera, Eduardo Castro, quien también detalla que fenómenos como el ransomware dirigido, ataques de phishing altamente personalizados y los llamados exploits de día cero de parte de los atacantes "ponen en riesgo incluso a aquellas empresas que tienen medidas de seguridad avanzadas".

34%
ES EL CRECIMIENTO ANUAL DEL NÚMERO DE VÍCTIMAS EN CHILE, SEGÚN EL ÚLTIMO REPORTE DE CIBERSEGURIDAD DE ENTEL DIGITAL, ACOMPAÑADAS DE CERCA DE 12 MILLONES DE ATAQUES ANUALES.

Los sectores más expuestos

El reporte de Ciberseguridad 2024 de Entel Digital muestra que el sector financiero es uno de los blancos más recurrentes para el robo de datos financieros debido a las grandes recompensas económicas que suelen ofrecer. "En 2023 se registraron 45 ataques a nivel global, principalmente utilizando ransomware y técnicas como phishing", detalla Bouillet.

Asimismo, Fernández asegura que en un reciente informe sobre el panorama de ciberamenazas en Latinoamérica elaborado por Kaspersky detectaron que entre agosto del 2023 y agosto del 2024, uno de los sectores más atacados fue el de gobierno. A eso suma el crecimiento de un fenómeno ahora conocido como ataque industrial, en sectores como la minería y manufactura. Otros blancos recurrentes son las áreas de salud y finanzas. Esta última, dice la experta, si bien es una de las más expuestas, también está entre las más protegidos pues sus empresas son las que más invierten en tecnología para su protección. "Otro sector que también está bajo ataque es el comercio minorista, debido al manejo de información de tarjetas de crédito y datos personales", añade Castro.

De igual manera, a los sectores de energía y de infraestructura crítica López los califica como vulnerables "debido a su importancia estratégica y el impacto económico que pueden tener los ataques".