Latinoamérica: falta de regulación incrementa vulnerabilidades del sector asegurador

Boletín N°: 42

May 27, 2025 LATINOAMÉRICA

Latinoamérica avanza hacia su consolidación como la región de seguros que más rápido se está expandiendo y que más beneficios reporta en el mundo. Este año está marcado por una probable desaceleración económica regional, la adopción de nuevas tecnologías, un panorama regulatorio básico en materia de ciberseguridad que se espera evolucione y la adaptación a un entorno global incierto, escenario que implica un ambiente inseguro que los cibercriminales tratarán de aprovechar.

Vulnerabilidades

El gran volumen de datos confidenciales y financieros que manejan las aseguradoras las convierte en un objetivo atractivo para los ciberdelincuentes, según Oswaldo Palacios, especialista en ciberseguridad para Latinoamérica de Akamai, quien destaca que el sector asegurador posee bases de datos con información personal identificable (PII), es decir, datos personales, números de la seguridad social, detalles de ingresos, información sobre propiedades y mucho más. Además, en sus bases de datos almacenan información sobre empresas y tienen una visión general de sus activos.

Al caer en manos indebidas, esta información podría utilizarse para cometer diversas actividades fraudulentas. De ahí que los robos de identidad, el fraude financiero y la extorsión que sufre este sector se produzcan a través de sofisticados ciberataques, colocando al ransomware como principal amenaza, seguido de los ataques de denegación de servicio (DDoS). “La complejidad de los sistemas y procesos de las aseguradoras las puede exponer a más vulnerabilidades explotables; brechas en la seguridad de la red, protocolos de cifrado débiles, autenticación de usuarios o dispositivos no securizados, facilitan el acceso no autorizado o el robo de información sensible a los cibercriminales”, señala Palacios.

Sector asegurador

Un estudio del Instituto Ponemon revela que el sector asegurador es el segundo más vulnerable a los ciberataques, con un 85% de las aseguradoras sufriendo un ciberataque el año pasado.

Las consecuencias de una vulnerabilidad pueden ser devastadoras para las aseguradoras. Por si fuera poco, un ciberataque puede dañar la reputación de una compañía de seguros, lo que genera una pérdida de confianza y lealtad de los clientes. También pueden enfrentarse a fuertes multas y sanciones por no proteger los datos de los

clientes y los asegurados pueden emprender acciones legales contra las compañías que no protejan su información personal y financiera.

Fortalecer las estrategias de ciberseguridad y normativas

El mercado de ciberseguridad en el sector asegurador alcanzará los 10.600 millones de dólares en 2025, con una tasa de crecimiento anual compuesta (CAGR) del 10,7% entre 2020 y 2025, según GlobalData. Aunque representa una inversión significativa, es urgente avanzar hacia un marco regulatorio más sólido y fortalecer las estrategias de ciberseguridad para proteger los datos de los clientes y prevenir pérdidas financieras.

Palacios añade que “en América Latina, las regulaciones sobre ciberseguridad para aseguradoras avanzan de forma desigual entre los países. El sector asegurador en Latinoamérica cumple con regulaciones básicas, lo que significa que su estrategia de seguridad digital incorpora lo mínimo necesario e insuficiente para hacer frente a ciberataques cada vez más sofisticados, generando así un ambiente vulnerable y poniendo en riesgo las operaciones diarias”.

En la actualidad las diversas regulaciones de los distintos países de Latinoamérica piden a las aseguradoras implementar mecanismos de seguridad para datos personales, así como tener políticas de seguridad, continuidad de negocio y protección contra incidentes cibernéticos. La adaptación a estas normativas no sólo implica cumplir con las disposiciones legales, sino también modernizar la infraestructura tecnológica para garantizar la seguridad y la privacidad de los datos de los clientes.

Microsegmentación

En ese sentido, la microsegmentación debe convertirse en una herramienta cada vez más importante para los equipos de TI del sector asegurador, que se enfrentan al reto de mantener las políticas de seguridad y el cumplimiento en consonancia con el rápido ritmo de cambio de los actuales centros de datos dinámicos, entornos de nube y de nube híbrida.

“La implementación de la microsegmentación reduce en gran medida la superficie de ataque en entornos con un conjunto diverso de modelos de implementación y una alta tasa de cambio”, asegura el experto. Añade que “incluso cuando los procesos de desarrollo e implementación de aplicaciones de estilo DevOps están en constante cambio, una plataforma de microsegmentación puede proporcionar visibilidad continua y garantizar que las políticas de seguridad estén al día mientras se añaden y actualizan las aplicaciones”.

La microsegmentación ayuda a las empresas de seguros a reforzar su estrategia de cumplimiento normativo, incluso cuando comienzan a utilizar los servicios en la nube de manera más amplia, y también simplifica enormemente las auditorías.

Fuente

Fuente: Todo Riesgo

Enlace:
https://www.todoriesgo.com.ar/akamai-latinoamerica-regulacion-vulnerabilidades-sector-

asegurador/