El Longino
Soy del Norte
Fecha: 28/01/2025 Audiencia: 10.800 Sección: OPINION
Vpe: $267.971 Tirada: 3.600 Frecuencia: 0
Vpe pág: $515.658 Difusión: 3.600
Vpe portada: $515.658 Ocupación: 51,97%

VÍCTOR PAREDES CH.
Gerente Comercial en
TLine Chile S.A.

Protección de datos en Chile: judicialización y persecución de los ciberdelitos

Este 28 de enero se celebra a nivel internacional el Día de la Protección de Datos, que nació con el objetivo de poder informar y concientizar sobre los derechos que tienen las personas sobre sus datos, y así promover las mejores prácticas de privacidad y protección de la información.

Pero ¿qué entendemos por datos privados o sensibles o privados? Y ¿cuál es la diferencia y propósito respecto de los datos abiertos?

Cuando nos referimos a datos privados o sensibles, estos corresponden a toda información relevante para una persona, compañía o institución, ya sea esta información comercial, financiera u operacional. En el último tiempo, la información de identificación personal ha tomado gran relevancia por la nueva ley de protección de datos y las estandarizaciones creadas para el tratamiento y protección de este tipo de información.

Hoy el mundo se rige prácticamente por el IoT y la IA. En cuanto al IoT lo tenemos presente en miles de formas y convivimos con ellos casi sin darnos cuenta, generando información de alto valor para las compañías, e incluso han escalado a una posición altamente relevante para el negocio de éstas, ya que han apalancado la transformación de las operaciones y sus negocios.

De ahí la importancia de contar con una estrategia de protección de datos apropiada, que permitirá un mayor grado de confianza para el negocio, su continuidad y crecimiento.

Sin embargo, esto trae consigo riesgos para los usuarios y organizaciones, al estar expuestos a ciberataques. Este riesgo dependerá de la exposición de cada entidad; phishing, malware y robo de identidad, son solo algunos de los ciberdelitos más frecuentes. Estas son las formas de ataque más comunes a las que están expuestas las personas y en donde la práctica más utilizada es la ingeniería social. Para una compañía, en tanto, se agregan los ataques dirigidos; DDoS o denegación de servicio, explotación de vulnerabilidades y otros mecanismos con la intención de contaminar con los temidos malware del tipo Ransomware, el cual ya no solo encripta y solicita pago por el rescate, sino que hoy también se enfocan en el robo de información y la venta y reventa de ésta, como otro mecanismo para generar ingresos.

Hoy en día, los sectores más vulnerables al ataque de correos fraudulentos para el robo de información (fishing), siguen siendo el financiero, retail y gubernamental. Sabemos que la orientación de los ataques en los dos primeros es el lucro correspondiente al rescate de la información encriptada por Ransomware y en otros casos la re-venta de esta información en la Deep web. Para el caso del sector gubernamental, el robo de información es el principal objetivo dado que es el mayor controlador y procesador de información de identificación personal, algo muy preciado por los ciberatacantes.

En la actualidad la Inteligencia Artificial también está siendo aplicada por los ciberatacantes, lo que ha llevado a una proliferación de ataques más sofisticados y de mayor precisión.

Chile ha dado pasos importantes para fortalecer la ciberseguridad a través de la creación de un marco legal sólido, junto a un desarrollo de estrategias y participación en iniciativas internacionales.

Hoy contamos con una Ley Marco de Ciberseguridad e Infraestructuras Críticas, un CSiRT y una recientemente inaugurada Agencia Nacional de Ciberseguridad (ANCI). Esto nos posiciona entre los países de Latinoamérica con mayor avance en esta área. Sin embargo, países como Brasil, México y Uruguay avanzan muy rápidamente, en tanto que el resto lo hace en forma muy paulatina, lo que ha permitido a los ciberatacantes tener foco en nuestra región.

Este panorama ha permitido que las estrategias de ciberseguridad sean prioridad en la mayor parte de los negocios, sean o no web. Para la industria, esto exige la entrega de servicios de protección de datos y continuidad operacional como son BaaS, DRaaS además de SoCaaS, análisis de vulnerabilidades y otros servicios complementarios como parchado y concientización.

Este 2025 el desafío que tienen las organizaciones se debe enfocar en robustecer la protección de datos en entornos Cloud o multicloud, la aplicación y ejecución efectiva de buenas prácticas de seguridad y protección de datos, y la normalización de sistemas mediante la adopción de estándares de protección de datos, además de optar a certificaciones que avalen la gestión de la información.

Chile avanza en la línea correcta, pero necesitamos fortalecer los aspectos judiciales y la persecución de los delitos informáticos.