Ciberdelincuencia: un costo anual superior a los diez billones de dólares para la economía mundial

Por staff de redacción Infosecurity Mexico

En el mundo actual, el cibercrimen representa una carga económica que supera los diez millones de dólares anuales, un fenómeno que demanda atención constante y estratégica. EL creciente números de datos almacenados a nivel global, estimado en más de doscientos zettabytes[1]para el 2025, plantea un desafío monumental en términos de seguridad cibernética. Estos datos incluyen información alojada en infraestructuras de TI públicas y privadas, en servicios públicos, centros de datos en la nube, en dispositivos informáticos personales como PC, portátiles, tabletas y teléfonos inteligentes, además de su aplicación en el Internet de las Cosas (IoT).

Actualmente, cerca de 5 mil millones de personas acceden y almacenan datos en dispositivos digitales y en la nube. Se estima que, para el año 2029, el noventa por ciento de la población mundial, es decir, siete mil quinientos millones de personas, estará en línea y generará datos. En 2020, ya había tres mil quinientos millones de usuarios de teléfonos inteligentes que utilizaban internet. Este crecimiento se acelerará con la tecnología 5G, esperando que alcance los dos mil seiscientos millones de suscriptores para el 2025.

Este ascenso vertiginoso en el uso y almacenamiento de datos conlleva riesgos significativos en materia de ciberseguridad. Los ciberataques pueden perturbar, dañar e incluso destruir empresas por ataques a su infraestructura de TI. Simplemente, el costo medio de una filtración de datos es superior a los 4 millones de dólares[2]; el precio incluye descubrir y responder a la infracción, el tiempo de inactividad, la pérdida de ingresos y el daño a la reputación de la empresa y marca.

Una encuesta[3] revela que casi el treinta y uno por ciento de cuatro mil trecientos treinta y dos líderes empresariales a nivel global consideran la ciberseguridad como una de las principales prioridades de inversión para sus organizaciones en el 2023, superando a la gestión de datos, análisis de datos (25%), IA y ML[4] (20%), por citar algunos.

Algunos ciberataques pueden ser aún más costosos. Los ataques de ransomware han exigido rescates de hasta 40 millones de dólares[5], y los ataques al correo electrónico empresarial (BEC) han costado hasta 47 millones de dólares a las víctimas en una sola sesión[6].

Los daños no se limitan a pérdidas financieras, ya que los ataques que comprometen la información de identificación personal (PII) de los clientes pueden resultar en la pérdida de confianza de los clientes, sanciones regulatorias y acciones legales. Se estima[7], que el cibercrimen costará a la economía mundial 10.5 billones de dólares al año desde 2022 hasta 2025.

Para mitigar estos riesgos, los expertos en seguridad de la información recomiendan las siguientes medidas:

---

[1] https://n9.cl/abjux
[2] https://n9.cl/cqgw9
[3] https://n9.cl/6940d
[4] Inteligencia Artificial y “Machine Learning”
[5] https://n9.cl/qh5qv
[6] https://n9.cl/ct4it
[7] https://n9.cl/izvnr

1. Cifrar los datos: cualquier dato que pueda causar daño financiero o a la reputación de una organización, si fuera expuesto o manipulado, debe cifrarse. Esto significa convertir un archivo de texto legible en un texto incomprensible, es decir, cifrado; implica modificar datos legibles de forma aleatoria. Requiere una clave criptográfica y un conjunto de valores matemáticos acordados por el emisor y el destinatario.
2. Realizar una copia de seguridad y recuperación: la mayoría de los ciberintrusos pasan desapercibidos durante lapsos prolongados, por ello las organizaciones deben realizar copias de seguridad de manera que les permitan restaurar los datos a su estado original antes de un ataque, sea que tengan sus datos en la nube, en un centro de datos o en otros dispositivos.
3. Establecer una política transparente: las organizaciones no sólo deben cumplir con leyes como la LFPDPPP o la LGPDPPSO[8], sino que tienen que transmitirlo de manera proactiva a los consumidores y usuarios, que cada vez conocen más acerca de cómo se almacenan y administran sus datos. Por ello las organizaciones deben demostrar abiertamente su compromiso.
4. Contemplar una póliza de seguro: el ransomware podría estar cubierto por pólizas de ciberseguro, que normalmente reembolsan los daños por pérdida de datos, incluso si una organización es (involuntariamente) negligente o imperfecta en sus prácticas de respaldo. Desde luego, cada institución aseguradora solicita requisitos diferentes, y habría que evaluarlos.
5. Contratar expertos: se debe contar con especialistas disponibles contractualmente en todo momento (ya sea que pertenezcan a la propia planta laboral, contratistas o a través de proveedores), con una profunda experiencia en la materia en todos los aspectos de la seguridad de los datos (legal, técnico, operativo y de recuperación ante desastres).

La ciberseguridad es esencial tanto en la nube como en los dispositivos personales, ya que un pequeño descuido puede tener consecuencias graves para una organización. Consultar con expertos, como los que se presentarán en Infosecurity Mexico, es una oportunidad única para conocer las últimas tendencias y mejores prácticas de protección.

[8] https://n9.cl/p7qul