Comunicados

Informe de IBM: Los consumidores pagan el precio de las filtraciones de datos

A nivel mundial, 60% de las empresas afectadas aumentaron los precios de sus productos o servicios después de una filtración de datos.

En América Latina, el costo promedio de una filtración de datos aumentó casi un 15% comparado con el año anterior, alcanzando el récord de USD 2.09 millones de dólares.

América Latina, 16 de agosto de 2022 - IBM Security publicó su informe anual Cost of a Data Breach Report[1], que revela que las filtraciones de datos son más costosas y tienen mayor impacto que nunca, con un **costo promedio de USD 2.09 millones de dólares en América Latina, el mayor costo** en la historia del informe para las organizaciones encuestadas.

En la región, con un aumento de los costos por filtraciones de datos de casi un 15% comparado con el año anterior, los hallazgos sugieren que estos incidentes también pueden estar contribuyendo al aumento de los precios en bienes y servicios. De hecho, el 60% de las organizaciones a nivel global incrementaron los precios de sus productos o servicios debido a una filtración, en un momento en el que el costo de los bienes ya se está disparando en todo el mundo por la inflación, los problemas de la cadena de suministro, entre otros.

Por otro lado, el **tiempo promedio en la región para identificar y contener una filtración de datos fue de 331.5 días en 2022**, una reducción de casi 25 días en comparación con el año anterior. Además, la perpetuidad de los ciberataques también está arrojando luz sobre el "efecto perseguidor" que las filtraciones de datos están teniendo en las empresas, ya que el informe de IBM revela que el 83% de las organizaciones a nivel mundial experimentaron más de una filtración de datos en su vida.

Por duodécimo año consecutivo, los participantes de la industria de salud sufrieron las filtraciones más costosas de todos los sectores a nivel mundial, seguida por los servicios financieros. **En América Latina, las industrias que observaron el mayor costo por registro en una filtración son salud (USD 128), servicios financieros (USD 124) y el sector servicios (USD 111).**

Además, el **45% de las empresas en América Latina tienen un nivel de adopción maduro de Zero**

Trust (enfoque de Confianza Cero). Esta estrategia es importante ya que, globalmente, entre las organizaciones con una implementación madura de Zero Trust en su arquitectura de seguridad y aquellas que recién están comenzando, la diferencia de costos en la filtración fue de más de USD 1.5 millones de dólares.

El informe “Cost of a Data Breach 2022” -patrocinado y analizado por IBM Security, realizado por Ponemon Institute- se basa en un análisis en profundidad de las filtraciones de datos reales experimentadas por 550 organizaciones a nivel mundial -66 empresas de América Latina[2]- entre marzo de 2021 y marzo de 2022.

Entre los hallazgos globales, se destacan:

Infraestructura crítica

- El ransomware y los ataques destructivos representaron el 28% de las filtraciones en las organizaciones de infraestructuras críticas estudiadas, lo que pone de manifiesto que los atacantes buscan fracturar las cadenas de suministro globales que son la columna vertebral de la economía.
- El costo global promedio de una filtración de datos para estas organizaciones fue de USD 4.82 millones de dólares, mayor que el promedio mundial (USD 4.35 millones de dólares).
- Casi el 80% de las organizaciones de infraestructuras críticas no adoptaron estrategias Zero Trust, por lo que el costo medio de las filtraciones de datos aumenta hasta los USD 5.4 millones de dólares, un incremento de 24% en comparación con las que sí lo hacen.
- Además, en el 17% de las infracciones, un socio comercial se vio inicialmente comprometido, lo que pone de manifiesto los riesgos de seguridad que plantean los entornos de confianza excesiva.

No es rentable pagar el rescate:

- Las víctimas del ransomware del estudio que optaron por pagar el rescate sólo vieron una disminución de USD 630.000 dólares en el costo promedio de la filtración en comparación con aquellas que no lo hicieron, sin incluir el costo del rescate.
- Si se tiene en cuenta el elevado precio de los rescates (mayor a USD 800.000 dólares)[3], el costo financiero puede ser aún mayor, lo que sugiere que la acción de pagar el rescate, por si sola, no es una estrategia eficaz; mientras que además podrían estar financiando inadvertidamente futuros ataques con el capital que sería útil para esfuerzos de corrección y recuperación, e incluso se podría incurrir en posibles delitos federales.
- IBM Security X-Force descubrió que la duración de los ataques de ransomware descendió 94% en los últimos 3 años -pasó de 2 meses a menos de 4 días- por lo que los equipos de seguridad tienen menos margen de acción.
- En el caso de filtraciones de datos causadas por ransomware y ataques destructivos, el tiempo promedio para identificar y contener es significativamente mayor que la media global. Para un ransomware fue de 49 días más y en ataques destructivos fue de 47 días más, frente al promedio global de 277 días.

Factores y vectores en la filtración de datos:

- Las credenciales comprometidas continúan siendo la causa más común de una filtración (19%), con un costo promedio de USD 4.5 millones de dólares. También tienen el ciclo de vida más largo: 327 días para

identificar y contener.

- El phishing fue la segunda (16%) y la más costosa, con un promedio de USD 4.91 millones de dólares en las organizaciones estudiadas. BEC (Business Email Compromise) alcanza 6% y es la segunda causa más costosa con USD 4.89 millones de dólares.
- Tres factores principales que amplifican el costo de la filtración: complejidad del sistema de seguridad, migración a la nube y fallas de compliance.
- Tres principales mitigadores de costos: uso de plataforma de Inteligencia Artificial para seguridad, DevSecOps y formación del equipo de Respuesta a Incidentes.

Profesionales, Automatización e IA en seguridad son clave para el ahorro de costos multimillonarios:

- Las organizaciones que desplegaron completamente la automatización y la IA en seguridad incurrieron en un costo promedio menor y lograron un ahorro de 65.2% frente a las que no -el mayor ahorro de costos observado en el estudio. Además su tiempo de detección y contención es menor: 2.5 meses más rápido.
- El 62% de las organizaciones admitió no tener suficiente personal para cubrir las necesidades relacionadas con la seguridad, lo que se traduce en una media de USD 550.000 dólares más en costos de filtraciones frente a las que sí cuentan con los recursos profesionales.
- El 73% de las empresas tiene planes de Respuesta a Incidentes, pero el 37% no lo prueba regularmente. Se observa un ahorro del 58% en costo promedio por filtración de datos para las organizaciones que tienen equipo de Respuesta a Incidentes y prueban periódicamente su plan.
- El 44% de las organizaciones utilizan tecnologías XDR (Extended Detection and Response) y acortaron el ciclo de vida de las filtraciones en casi un mes. Además ahorraron una media de USD 400.000 dólares.

Ventaja de la nube híbrida:

- Un significativo 43% de las organizaciones estudiadas están en las primeras etapas o no han empezado a aplicar prácticas de seguridad para proteger sus entornos de nube.
- Ahorro y Rapidez. Las empresas con entornos maduros de seguridad en la nube ahorraron 16% en el costo promedio para las filtraciones de datos. Además, son capaces de detectar y contener más rápido: 40 días menos que el promedio global.
- Las empresas que adoptaron la nube híbrida notaron costos menores (USD 3.8 millones de dólares en promedio) en comparación con aquellas con un modelo de nube exclusivamente pública (USD 5.02 millones de dólares) o privada (USD 4.24 millones de dólares).
- De hecho, las organizaciones con un entorno de nube híbrida fueron capaces de identificar y contener las filtraciones de datos 15 días más rápido que la media global de 277 días.

"Las empresas necesitan poner sus sistemas de seguridad a la ofensiva y vencer a los atacantes. Es hora de impedir que el adversario consiga sus objetivos y empezar a minimizar el impacto de los ataques. Cuanto más intenten las empresas perfeccionar su perímetro en lugar de invertir en la detección y la respuesta, mayor será el número de filtraciones de datos que pueden provocar aumentos en el costo de vida", comentó Charles Henderson, Director Global de IBM Security X-Force. "Este informe muestra que las estrategias correctas y las tecnologías adecuadas pueden ayudar a marcar la diferencia cuando las empresas son atacadas".

Recursos adicionales:

- *Para descargar el informe completo "Cost of a Data Breach 2022" visite: https://www.ibm.com/security/data-breach.*
- *Inscríbase al webinar en español de "Cost of a Data Breach 2022", el 25 de agosto de 2022, a las 8:00 a.m. ET, aquí.*
- *Puede leer más sobre los hallazgos del reporte en IBM Security Intelligence en el blog.*

Acerca de IBM Security

IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad empresarial. La cartera, respaldada por la investigación de renombre mundial de IBM Security X-Force®, permite a las organizaciones gestionar eficazmente los riesgos y defenderse de las amenazas emergentes. IBM cuenta con una de las organizaciones de investigación, desarrollo y servicios de seguridad más amplias del mundo, supervisa más de 150 mil millones de eventos de seguridad por día en más de 130 países y ha obtenido más de 10.000 patentes de seguridad en todo el mundo. Para más información, consulte https://www.ibm.com/security, siga a @IBMSecurity en Twitter o visite el blog IBM Security Intelligence.

---

[1] Cost of a Data Breach Report 2022, realizado por Ponemon Institute, patrocinado y analizado por IBM.

[2] América Latina representa una muestra de 66 empresas de Argentina, Brasil, Chile, Colombia y México.

[3] Según Sophos alcanzó los USD 812.000 dólares en 2021.