

Las brechas de seguridad de datos cuestan a las empresas una media de 4,24 millones de dólares por incidente, según el informe Cost of Data Breach de IBM

- La adopción de la IA, la nube híbrida y el enfoque de confianza cero redujeron los costes de las brechas de seguridad
- Las filtraciones de datos en el sector sanitario fueron las más costosas, con 9,23 millones de dólares por incidente, un aumento de 2 millones de dólares con respecto al año anterior
- Casi el 20% de las organizaciones estudiadas informaron que el trabajo remoto fue un factor importante en la filtración de datos

29 de Julio, 2021 – IBM Security ha anunciado los resultados de un estudio mundial en el que se constata que las violaciones de datos ahora cuestan a las empresas encuestadas 4,24 millones de dólares de media por incidente, el coste más alto en los 17 años de historia del informe. Basado en un análisis en profundidad de las violaciones de datos experimentadas por más de 500 organizaciones, el estudio sugiere que los incidentes de seguridad se han vuelto más costosos y difíciles de contener debido a los drásticos cambios operativos durante la pandemia, con un aumento de los costes del 10% en comparación con el año anterior. A su vez, el tiempo de respuesta para detectar y contener estas filtraciones fue de 287 días (212 para detectar, 75 para contener), lo que supone una semana más que el informe del año anterior.

Las conclusiones de este informe sugieren que la seguridad en las empresas puede haber quedado en un segundo plano, después de los cambios informáticos que han tenido que implementar para facilitar el trabajo remoto o dar el salto al cloud.

El informe anual *Cost of a Data Breach Report*, realizado por Ponemon Institute y patrocinado y analizado por IBM Security, ha identificado las siguientes tendencias entre las organizaciones estudiadas:

“ Aunque los costes de estas filtraciones alcanzaron un récord el año pasado, el informe también mostró signos positivos sobre el impacto de las tácticas de seguridad modernas, como la IA, la automatización y la adopción de un enfoque de zero trust, que pueden dar sus frutos en la reducción del coste de estos incidentes más adelante ”

- **Impacto del trabajo a distancia:** El cambio rápido a las operaciones remotas durante la pandemia parece haber conducido a violaciones de datos más costosas. Las filtraciones costaron más de un millón de dólares más de media en aquellas asociadas al trabajo a distancia, en comparación con las filtraciones que no estaban relacionadas con ello (4,96 frente a 3,89 millones de dólares)[1].
- **Aumento en los costes de las filtraciones en el sector sanitario:** Los sectores que se enfrentaron a grandes cambios operativos durante la pandemia (atención sanitaria, comercio minorista, hostelería y fabricación/distribución de productos de consumo) también experimentaron un aumento sustancial de los costes de las filtraciones de datos con respecto a años anteriores. Las filtraciones de datos en el sector sanitario fueron las más caras (9,23 millones de dólares), seguidas del sector financiero (5,72 millones de dólares) y del farmacéutico (5,04 millones de dólares). Aunque los costes totales fueron menores, el comercio minorista, los medios de comunicación, la hostelería y el sector público experimentaron un gran incremento de costes en comparación con el año anterior.
- **El robo de contraseñas compromete los datos de usuarios y empresas:** El robo de credenciales de usuario fue la causa más común de las filtraciones en el estudio realizado. Al mismo tiempo, los datos personales de los clientes (como el nombre, el correo electrónico o la contraseña) fueron el tipo de

información más comúnmente expuesta en las filtraciones de datos: el 44% de las filtraciones incluían este tipo de datos. La combinación de estos factores podría provocar un efecto espiral, ya que las filtraciones de nombres de usuario/contraseñas proporcionan a los atacantes una ventaja para futuras filtraciones de datos.

- **El uso de herramientas tecnológicas redujo los costes:** La adopción de la IA, los análisis de seguridad y el cifrado fueron los tres principales factores atenuantes que demostraron reducir el coste de una filtración, ahorrando a las empresas entre 1,25 y 1,49 millones de dólares en comparación con las que no hicieron un uso significativo de estas herramientas. En el caso de las filtraciones de datos relacionadas con el entorno cloud, las organizaciones que habían implementado un enfoque de nube híbrida tenían menores costes de filtración de datos (3,61 millones de dólares) que las que tenían un enfoque principalmente de nube pública (4,80 millones de dólares) o principalmente de nube privada (4,55 millones de dólares).

"El aumento de los costes de las brechas de datos es otro gasto añadido para las empresas a raíz de los rápidos cambios tecnológicos durante la pandemia", ha señalado Chris McCurdy, vicepresidente y director general de IBM Security. "Aunque los costes de estas filtraciones alcanzaron un récord el año pasado, el informe también mostró signos positivos sobre el impacto de las tácticas de seguridad modernas, como la IA, la automatización y la adopción de un enfoque de zero trust, que pueden dar sus frutos en la reducción del coste de estos incidentes más adelante".

Impacto del trabajo a distancia y del cambio a la nube en las violaciones de datos

El proceso de adaptación al trabajo a distancia fue un factor significativo en la respuesta a la violación de datos. Casi el 20% de las organizaciones estudiadas informaron que el trabajo remoto fue un factor importante en la filtración de datos, las cuales que acabaron costando a las empresas 4,96 millones de dólares (casi un 15% más que la filtración media).

Por otro lado, las empresas del estudio que experimentaron una brecha de seguridad durante su proceso de migración a la nube tuvieron un coste un 18,8% superior a la media. En este aspecto, las que ya estaban en una fase más madura de adopción de la nube fueron capaces de detectar y responder a los incidentes con mayor eficacia: 77 días más rápido de media que las que estaban en la fase inicial de adopción.

Las credenciales comprometidas son un riesgo creciente

El informe también hace hincapié en la vulneración de credenciales, un problema en el que los datos de los consumidores expuestos (incluidas las contraseñas) pueden utilizarse para propagar otros ataques. De hecho, el 82% de los encuestados admite que reutiliza sus claves de acceso en distintas cuentas, lo que representan tanto la causa como el efecto principal de las filtraciones de datos y supone un riesgo añadido para las empresas.

Casi la mitad (44%) de las filtraciones analizadas expusieron datos personales de los clientes, como el nombre, el correo electrónico, la contraseña o incluso los datos sanitarios, lo que representa el tipo de registro más comúnmente vulnerado en el informe. El informe también destaca que las contraseñas filtradas fueron el método de ciberataque más común, representando el 20% de las violaciones estudiadas. Además, las filtraciones a partir de credenciales comprometidas fueron las que más tardaron en detectarse, con una media de 250 días para identificarlas (frente a los 212 de la filtración media).

Las empresas que se modernizaron tuvieron menores costes por violación de datos

Las organizaciones que no implementaron ningún proyecto de transformación digital para modernizar sus

operaciones comerciales durante la pandemia registraron costes más altos a causa de las filtraciones. En concreto, de 750.000 dólares más, un 16,6% más alto que la media.

Por otro lado, las empresas estudiadas que adoptaron un enfoque de seguridad de zero trust estaban mejor posicionadas para hacer frente a las violaciones de datos, con un coste por brecha de 3,28 millones de dólares, 1,76 millones menos que no habían puesto en marcha este enfoque.

El informe también reveló que las organizaciones con una estrategia de automatización de la seguridad "totalmente desplegada" tuvieron un coste medio por infracción de 2,90 millones de dólares, mientras que las que no tenían automatización experimentaron más del doble de ese coste, con 6,71 millones de dólares.

A su vez, la inversión en equipos y planes de respuesta a incidentes también redujeron los costes de las violaciones de datos entre las empresas estudiadas. Las compañías que contaban con un equipo de respuesta y que ensayaron su plan de respuesta a incidentes, tuvieron un coste medio de violación de 3,25 millones de dólares, mientras que las que no contaban con ninguno de los dos, experimentaron un coste medio de 5,71 millones de dólares (lo que representa una diferencia del 54,9%).

Metodología y estadísticas adicionales sobre las violaciones de datos

El informe de 2021 sobre el coste de una filtración de datos de IBM Security y Ponemon Institute, se basa en un análisis en profundidad de las filtraciones de datos del mundo real de 100.000 registros o menos, experimentadas por más de 500 organizaciones de todo el mundo entre mayo de 2020 y marzo de 2021. El informe tiene en cuenta cientos de factores de coste implicados en los incidentes de violación de datos, desde las actividades legales, reglamentarias y técnicas, hasta la pérdida de valor de la marca, de los clientes y de la productividad de los empleados.

Para descargar una copia del informe 2021 Cost of a Data Breach, visite: ibm.com/databreach

Inscríbase en el webinar 2021 Cost of a Data Breach Report el 12 de agosto a las 11 AM ET, aquí: ibm.biz/CODBwebinar

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 suministro de seguridad más amplias del mundo, supervisa más de 150.000 millones de eventos de seguridad al 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](https://twitter.com/IBMSecurity) en Twitter o visite el blog [IBM Security Intelligence](https://ibm.com/security/intelligence).

[1] Coste medio de 4,96 millones de dólares para los encuestados en los que el trabajo a distancia era un factor, frente a 3,89 millones de dólares cuando el trabajo a distancia no era un factor.

For further information: Patricia Torralba IBM Comunicación Tlf.- 637 804 148 patricia.torralba@es.ibm.com
