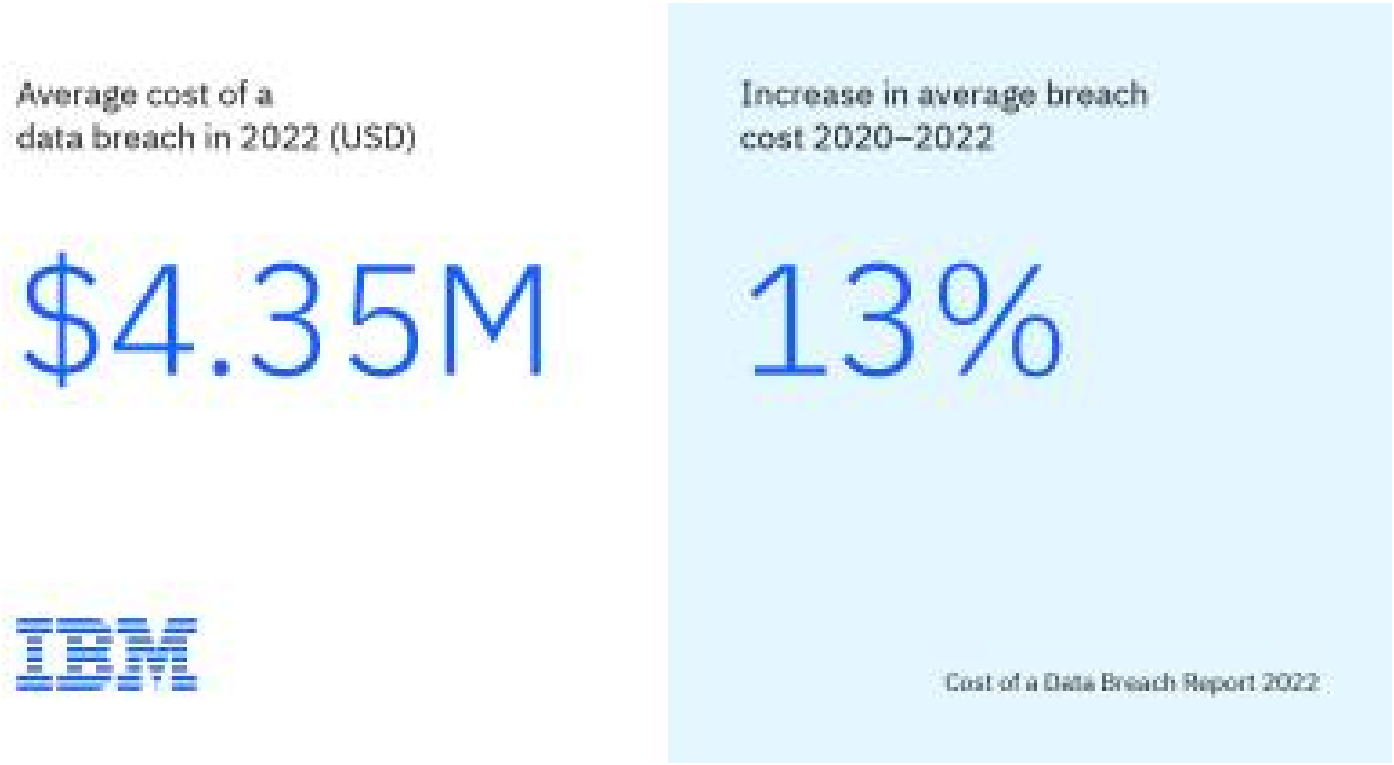
Anuncios

Según el nuevo informe Cost of Data Breach 2022 de IBM, los consumidores pagan el precio de las brechas de datos, que alcanzan su nivel más alto

El 60% de las empresas afectadas aumentaron los precios de sus productos después de una brecha de datos

La gran mayoría de las infraestructuras críticas van rezagadas en la adopción del plan de zero trust



CAMBRIDGE, Mass., 27 de julio de 2022 – IBM Security ha publicado hoy el informe anual Cost of a Data Breach[1] que revela que las filtraciones de datos son más costosas y tienen mayor impacto que nunca y que, el coste medio global de una brecha de datos ha alcanzado un máximo histórico de 4,35 millones de dólares para las organizaciones encuestadas.

Con un aumento de los costes de las brechas de casi un 13% en los dos últimos años, los resultados sugieren que estos incidentes también pueden estar contribuyendo al aumento de los costes de los bienes y servicios. De hecho, el 60% de las organizaciones encuestadas aumentaron los precios de sus productos o servicios debido a la filtración, en un momento en el que el coste de los bienes ya se está disparando en todo el mundo debido a la inflación y a los problemas de la cadena de suministro.

" "Las empresas tienen que 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 violaciones que pueden provocar aumentos del coste de la vida", comentó Charles Henderson, Director Global de IBM Security X-Force. "Este informe muestra que las estrategias correctas junto con las tecnologías adecuadas pueden ayudar a marcar la diferencia cuando las empresas son atacadas". ”

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 estudiadas han experimentado más de una brecha de datos en su vida. Otro factor que aumenta con el paso del tiempo son los efectos posteriores de las filtraciones en estas organizaciones, que persisten mucho tiempo después de que se produzcan: casi el 50% de los costes de las brechas se producen más de un año después de la misma.

El informe “Cost of Data Breach 2022” se basa en un análisis en profundidad de las brechas de datos reales experimentadas por 550 organizaciones a nivel mundial entre marzo de 2021 y marzo de 2022. El estudio, patrocinado y analizado por IBM Security, y realizado por el Instituto Ponemon, ha identificado las siguientes tendencias en las organizaciones estudiadas:

- **Las infraestructuras críticas se quedan atrás en zero trust –** Casi el 80% de las organizaciones de infraestructuras críticas estudiadas no adoptan estrategias zero trust, lo que hace que el coste medio de las brechas aumente hasta los 5,4 millones de dólares, un incremento de 1,17 millones de dólares en comparación con las que sí lo hacen. De estas brechas, el 28% de las mismas fueron ataques de ransomware o destructivos.
- **No es rentable pagar –** Las víctimas de ransomware del estudio que optaron por pagar el rescate solo vieron una disminución de 610.000 dólares los costes medios de la brecha en comparación con los que decidieron no pagar, sin incluir el coste del rescate. Si se tiene en cuenta el elevado coste de los pagos de los rescates, el coste financiero puede ser aún mayor, lo que sugiere que pagar simplemente el rescate puede no ser una estrategia eficaz.
- **Inmadurez de seguridad en las nubes-** El 43% de las organizaciones estudiadas están en las primeras etapas o no han empezado a aplicar prácticas de seguridad en sus entornos de nube, observando más de 660.000 dólares de media en costes de brechas que las organizaciones con seguridad madura en sus entornos de nube.
- **La IA y la automatización de la seguridad son claves en el ahorro de costes multimillonarios –** Las organizaciones que desplegaron completamente IA de seguridad y automatización incurrieron en una media de 3,05 millones de dólares menos en costes de brechas en comparación con las organizaciones analizadas que no han desplegado la tecnología, lo que supone el mayor ahorro de costes observado en el estudio.

"Las empresas tienen que 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 violaciones que pueden provocar aumentos del coste de la vida", comentó Charles Henderson, Director Global de IBM Security X-Force. "Este informe muestra que las estrategias correctas junto con las

tecnologías adecuadas pueden ayudar a marcar la diferencia cuando las empresas son atacadas".

Exceso de confianza en las organizaciones de infraestructuras críticas

La preocupación por los ataques a las infraestructuras críticas parece haber aumentado en todo el mundo durante el último año y, las agencias de ciberseguridad de muchos gobiernos han instado a incrementar la vigilancia contra los ataques disruptivos. De hecho, el informe de IBM revela que el ransomware y los ataques destructivos representaron el 28% de las brechas en las organizaciones de infraestructuras críticas estudiadas, lo que pone de manifiesto cómo los actores de las amenazas buscan fracturar las cadenas de suministro globales que dependen de estas organizaciones. Esto incluye a empresas de servicios financieros, industriales, de transporte y sanitarias, entre otras.

A pesar de la llamada a la cautela y, un año después de que la Administración Biden emitiera una orden ejecutiva sobre ciberseguridad centrada en la importancia de adoptar un enfoque de zero trust para reforzar la ciberseguridad de la nación, según el informe, sólo el 21% de las organizaciones de infraestructuras críticas estudiadas adoptaron un modelo de seguridad zero trust. Además, el 17% de las infracciones en las organizaciones de infraestructuras críticas se debieron a que un socio comercial se vio inicialmente comprometido, lo que pone de manifiesto los riesgos de seguridad que plantean los entornos de confianza excesiva.

Las empresas que pagan el rescate no consiguen una "ganga"

Según el informe de IBM, las empresas que pagaron rescates tuvieron 610.000 dólares menos en los costes medios de las brechas respecto a las que optaron por no pagar, sin incluir el importe del rescate pagado. Sin embargo, cuando se tiene en cuenta el pago medio de un rescate, que según Sophos alcanzó los 812.000 dólares en 2021, las empresas que optan por pagar el rescate podrían incurrir en unos costes totales más elevados además de ser responsables de financiar futuros ataques de ransomware a otras empresas con un capital que podría destinarse a financiar nuevos esfuerzos de remediación y recuperación.

La persistencia del ransomware, a pesar de los importantes esfuerzos mundiales para impedirlo, se ve alimentada por la industrialización de la ciberdelincuencia. IBM Security X-Force descubrió que la duración de los ataques de ransomware muestran un descenso del 94% en los últimos tres años: de más de dos meses a poco menos de cuatro días. Estos ciclos de vida de los ataques, cada vez más cortos, pueden dar lugar a ataques de mayor impacto, ya que los encargados de responder a los incidentes de ciberseguridad tienen muy pocas oportunidades para detectar y contener los ataques. Dado que el "tiempo hasta el rescate" se reduce a una cuestión de horas, es esencial que las empresas den prioridad a la comprobación rigurosa de las guías de respuesta a incidentes (IR) con antelación. Sin embargo, el informe afirma que hasta el 37% de las organizaciones que tienen planes de respuesta a incidentes no los prueban regularmente.

La ventaja de la nube híbrida

El informe también muestra que los entornos de nube híbrida son la infraestructura más frecuente (45%) entre las organizaciones participantes en el estudio. Con una media de 3,8 millones de dólares en costes de la filtración, las empresas que adoptaron un modelo de nube híbrida observaron menores costes de la misma en comparación con las empresas con un modelo de nube exclusivamente pública o privada, que experimentaron una media de 5,02 millones de dólares y 4,24 millones de dólares, respectivamente. De hecho, las empresas que adoptaron la nube híbrida fueron capaces de identificar y contener las violaciones de datos 15 días más rápido de media que la media global de 277 días.

El informe también destaca que el 45% de las brechas estudiadas se produjeron en la nube, lo que pone de relieve la importancia de la seguridad en la nube. Sin embargo, un significativo 43% de las organizaciones afirmaron que sólo están en las primeras etapas o no han comenzado a implementar prácticas de seguridad para proteger sus entornos de nube, observando mayores costos de violación[2]. Las empresas estudiadas que no aplicaron prácticas de seguridad en sus entornos en la nube necesitaron una media de 108 días más para identificar y contener una brecha de datos que las que aplicaron sistemáticamente prácticas de seguridad en todos sus dominios.

Otras conclusiones del informe incluyen:

- **El phishing se convierte en la causa más costosa de las brechas –** Mientras que las credenciales comprometidas siguieron siendo la causa más común de una brecha (19%), el phishing fue la segunda (16%) y la causa más costosa, con 4,91 millones de dólares de coste promedio en las organizaciones participantes en el estudio.
- **Los costes de las brechas del sector sanitario alcanzan cifras de dos dígitos por primera vez en la historia**– Por duodécimo año consecutivo, los participantes del sector sanitario fueron los que sufrieron las brechas más costosas de todos los sectores, ya que el coste medio aumentó en casi un millón de dólares hasta alcanzar la cifra récord de 10,1 millones de dólares.
- **Insuficiente personal de seguridad** – El 62% de las organizaciones admitió no tener suficiente personal para las necesidades que tienen relacionadas con la seguridad, lo que se traduce en una media de 550.000 dólares más en costes de brechas comparados con los que sí lo tienen.

Fuentes adicionales

- Para descargar una copia del informe 2022 Cost of a Data Breach, visite: https://www.ibm.com/security/data-breach.

- Inscríbase en el webinar 2021 Cost of a Data Breach Report el 3 de agosto a las 11 AM ET, aquí

Sobre 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 en Twitter o visite el blog IBM Security Intelligence.

For further information: Miguel Gimenez De Castro. Depto. Comunicación. Miguel.gimenezdc@ibm.com