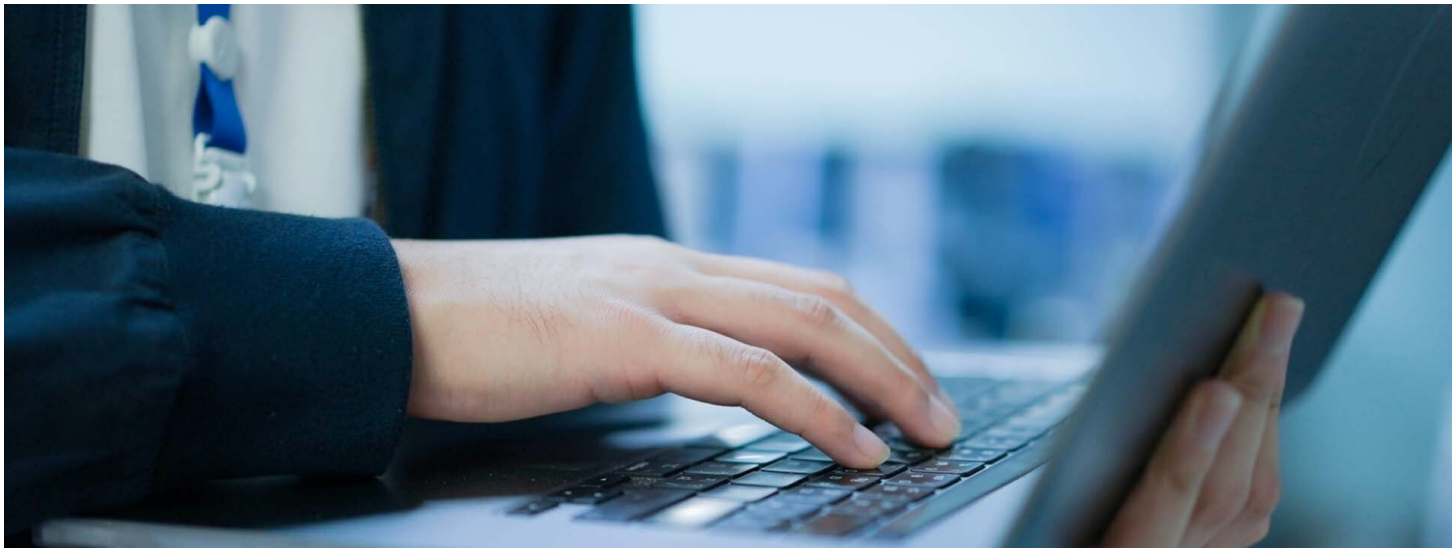
Comunicados

IBM Security: Los costos ocultos de las brechas de datos aumentan los gastos para las empresas

• El estudio, realizado por el Ponemon Institute, calcula por primera vez el costo que tienen las "mega infracciones", una cifra que asciende a $350 millones de dólares.



CAMBRIDGE, Massachusetts - 11 jul 2018: IBM (NYSE: IBM) Security anunció hoy los resultados de un estudio global que examina el impacto financiero de una violación de datos en los resultados de una empresa. El estudio descubrió que los costos ocultos en las brechas de datos, como la pérdida de negocios, el impacto negativo en la reputación y el tiempo empleado en la recuperación, son difíciles y costosos de administrar. Por ejemplo, encontró que un tercio del costo de las "mega infracciones" (más de 1 millón de registros perdidos) se derivan del negocio perdido.

De IBM Security y dirigido por el Ponemon Institute, el *Estudio sobre el Costo de una Brecha de Datos* de 2018 descubrió que el costo promedio de una violación de datos a nivel mundial es de $3.86 millones de dólares, un aumento del 6.4% con respecto al informe de 2017. Basado en entrevistas de profundidad a cerca de 500 compañías que experimentaron una violación de datos, el estudio analiza cientos de factores de costos que rodean una violación, desde investigaciones técnicas y recuperación hasta notificaciones, actividades legales y regulatorias, y el costo de pérdida de negocios y reputación.

Este año, por primera vez, el estudio también calculó los costos asociados con "mega infracciones" que van de 1 millón a 50 millones de registros perdidos, proyectando que estas brechas les cuestan a las compañías entre $40 millones y $350 millones de dólares, respectivamente.

"Si bien las brechas de datos más mediáticas a menudo informan pérdidas en millones, estas cifras son muy variables y a menudo se centran en unos pocos costos específicos que se cuantifican fácilmente", dijo Wendi Whitmore, líder mundial de IBM X-Force Incident Response and Intelligence Services (IRIS). *"La verdad es que hay muchos gastos ocultos que deben tenerse en cuenta, como daños a la reputación, rotación de clientes y costos operativos. Saber dónde están los costos y cómo reducirlos puede ayudar a las empresas a invertir sus recursos de manera más estratégica y a reducir los enormes riesgos financieros en juego".*

Calculando el costo de una “mega infracción”

En los últimos 5 años, la cantidad de “mega infracciones” (infracciones de más de 1 millón de registros) casi se ha duplicado, desde solo 9 en 2013, a 16 mega brechas en 2017. Debido a la pequeña cantidad de “mega infracciones” en el pasado, el *Estudio sobre el Costo de una Brecha de Datos* analizó históricamente infracciones de alrededor de 2,500 a 100,000 registros perdidos.

Con base en el análisis de 11 compañías que experimentaron una “mega infracción” en los últimos dos años, el informe de este año usa modelos estadísticos para proyectar el costo de brechas que van desde 1 millón hasta 50 millones de registros comprometidos. Los hallazgos clave incluyen:

- El costo promedio de una violación de datos de 1 millón de registros comprometidos es de casi $40 millones de dólares.
- En 50 millones de registros, el costo total estimado de una infracción es de $350 millones de dólares.
- La gran mayoría de estas infracciones (10 de 11) se debieron a ataques maliciosos y criminales (a diferencia de fallas técnicas o errores humanos).
- El tiempo promedio para detectar y contener una “mega infracción” fue de 365 días, casi 100 días más que una brecha de menor escala (266 días).

Para “mega infracciones”, la categoría de gasto más grande tiene que ver con los costos asociados con la pérdida de negocios, que se estimó en casi $118 millones por brechas de 50 millones de registros, casi un tercio del costo total de una infracción de este tamaño. IBM analizó los costos informados públicamente de “mega infracciones” de alto perfil y descubrió que las cifras informadas a menudo son menores que el costo promedio encontrado en el estudio. Es probable que esto se deba a que los costos informados públicamente a menudo se limitan a los costos directos, como la tecnología y los servicios para recuperarse de la infracción, los honorarios legales y reglamentarios y las reparaciones a los clientes.

¿Cómo afecta el costo promedio de una violación de datos?

Durante los últimos 13 años, el Instituto Ponemon ha examinado el costo asociado con las infracciones de datos de menos de 100,000 registros y ha constatado que los costos han aumentado a lo largo del tiempo. El costo promedio de una violación de datos fue de $3.86 millones en el estudio de 2018, en comparación con $3.50 millones en 2014, lo que representa un aumento neto de casi 10% en los últimos 5 años.

El estudio también examina los factores que aumentan o disminuyen el costo de la infracción, descubriendo que los costos se ven muy afectados por la cantidad de tiempo dedicado a contener una violación de datos, así como las inversiones en tecnologías que aceleran el tiempo de respuesta.

- El tiempo promedio para identificar una violación de datos en el estudio fue de 197 días, y el tiempo promedio para contener una violación de datos una vez identificado fue de 69 días.
- Las empresas que contuvieron un incumplimiento en menos de 30 días ahorraron más de $1 millón de dólares en comparación con las que tardaron más de 30 días ($3,09 millones frente a un total promedio de $4,25 millones de dólares).

La cantidad de registros perdidos o robados también afecta el costo de una infracción, con un costo promedio

de $148 dólares por pérdida o robo. El estudio examinó varios factores que aumentan o disminuyen este costo:

- Tener un equipo de respuesta a incidentes fue el principal factor de ahorro de costos, reduciendo el costo en $14 por registro comprometido.
- El uso de una plataforma de inteligencia artificial para la ciberseguridad redujo el costo en $8 por pérdida o robo de registro.
- Las compañías que indicaron una "prisa para notificar" tuvieron un costo más alto por $5 por registro perdido o robado.

Este año, por primera vez, el informe examinó el efecto de las herramientas de automatización de seguridad que utilizan inteligencia artificial, aprendizaje automático, análisis y orquestación para aumentar o reemplazar la intervención humana en la identificación y contención de una violación. El análisis encontró que las organizaciones que implementaron ampliamente las tecnologías de seguridad automatizadas ahorraron más de $1.5 millones de dólares en el costo total de una infracción ($2.88 millones de dólares, en comparación con $4.43 millones de dólares para aquellos que no implementaron la automatización de seguridad).

"El objetivo de nuestra investigación es demostrar el valor de las buenas prácticas de protección de datos y los factores que marcan una diferencia en lo que paga una empresa para resolver una violación de datos", dijo el Dr. Larry Ponemon, presidente y fundador de Ponemon Institute. *"Si bien los costos de las brechas de datos han aumentado constantemente a lo largo de la historia del estudio, vemos signos positivos de ahorro de costos mediante el uso de tecnologías más nuevas, así como una planificación adecuada para la respuesta a incidentes, lo que puede reducir significativamente estos costos".*

Para más información, visita: https://costofadatabreach.mybluemix.net

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 IBM X-Force® de renombre mundial, permite a las organizaciones administrar los riesgos de forma efectiva y defenderse contra amenazas emergentes. IBM opera una de las organizaciones de investigación, desarrollo y distribución de seguridad más amplias del mundo, supervisa 35 mil millones de eventos de seguridad por día en más de 130 países y ha obtenido más de 8,000 patentes de seguridad en todo el mundo. Para obtener más información, visite www.ibm.com/security, siga IBMSecurity en Twitter o visite el blog de IBM Security Intelligence.

Contacto(s)

Fernanda Martínez

External Communications IBM México (55) 4448 1923 fer.martinez@mx1.ibm.com