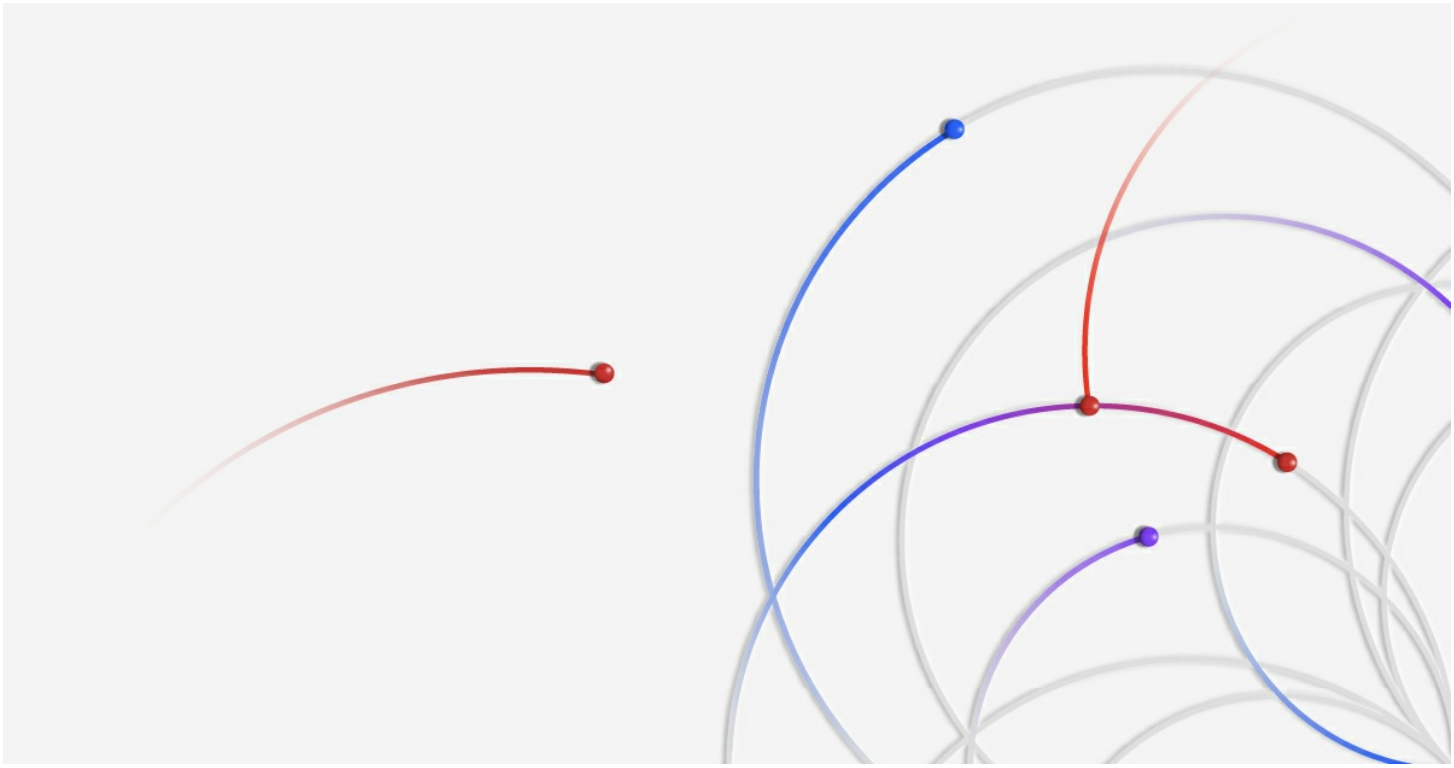
Anuncios

El aumento de las interrupciones causadas por las filtraciones de datos eleva los costes de las brechas a nuevos máximos, según un estudio de IBM

El robo de propiedad intelectual se disparó; más de un tercio de las filtraciones involucraron 'shadow data' (datos en la sombra). Sin embargo, el uso de la IA y la automatización redujo el coste de las brechas de datos en 1,88 millones de dólares



CAMBRIDGE, Massachusetts, 30 de julio de 2024 -- IBM (NYSE: IBM) ha publicado hoy su informe anual Cost of Data Breach Report, que revela que el coste medio global de una filtración de datos alcanzó los 4,88 millones de dólares en 2024, una cifra que se incrementa a medida que las brechas se vuelven más disruptivas y aumentan aún más las exigencias de los equipos de seguridad. Los costes de las filtraciones aumentaron un 10% con respecto al año anterior, el mayor salto anual desde la pandemia, ya que el 70% de las organizaciones vulneradas informaron que la violación causó interrupciones significativas o muy significativas.

La pérdida de negocio y los costes de respuesta a clientes y terceros posteriores a la filtración impulsaron el aumento interanual de los costes, ya que los daños colaterales de las filtraciones de datos no han hecho más que intensificarse. Los efectos disruptivos que las violaciones de datos están teniendo en las empresas no solo están aumentando los costes, sino que también están alargando las secuelas que provoca una filtración, ya que la mayoría de las pocas empresas que consiguen recuperarse por completo (12%) tarda más de 100 días en hacerlo.

> *"Las empresas están atrapadas en un bucle continuo de filtraciones, contención y respuesta a las consecuencias. Este ciclo ahora, a menudo, incluye inversiones en fortalecer las defensas de seguridad y trasladar los costes de las filtraciones a los consumidores, lo que convierte a la seguridad en el nuevo coste de hacer negocios"*

El informe 'Cost of Data Breach 2024´se basa en un análisis en profundidad de las violaciones de datos reales experimentadas por 604 organizaciones de todo el mundo entre marzo de 2023 y febrero de 2024. La investigación, realizada por Ponemon Institute, y patrocinada y analizada por IBM, ha sido publicada durante 19 años consecutivos y ha estudiado las filtraciones sufridas por más de 6.000 organizaciones, convirtiéndose en un referente de la

industria.

Algunas de las principales conclusiones del informe de IBM `Cost of Data Breach 2024´ son:

- **Equipos de seguridad con poco personal:** un mayor número de organizaciones se enfrentó a una grave escasez de personal en comparación con el año anterior (aumento del 26%) y observó un coste promedio de 1,76 millones de dólares más alto en filtraciones que aquellas con problemas de personal de seguridad insuficiente o poco capacitado.
- **La prevención impulsada por IA da sus frutos:** dos de cada tres organizaciones estudiadas están implementando la IA y automatización de seguridad en su centro de operaciones de seguridad (SOC). Cuando estas tecnologías se utilizaron de manera amplia en los flujos de trabajo de prevención, las organizaciones incurrieron en una media de 2,2 millones de dólares menos en costes de infracción en comparación con las empresas que no utilizaban estas tecnologías en estos flujos de trabajo, los mayores ahorros de costes revelados en el informe de 2024.
- **Deficiencias en la visibilidad de datos:** el 40% de las violaciones involucraron datos almacenados en múltiples entornos, incluida la nube pública, la nube privada y en las instalaciones. Estas brechas costaron más de 5 millones de dólares de promedio y tardaron más tiempo en identificarse y contenerse (283 días).

“Las empresas están atrapadas en un bucle continuo de filtraciones, contención y respuesta a las consecuencias. Este ciclo ahora, a menudo, incluye inversiones en fortalecer las defensas de seguridad y trasladar los costes de las filtraciones a los consumidores, lo que convierte a la seguridad en el nuevo coste de hacer negocios", ha señalado Kevin Skapinetz, vicepresidente de Estrategia y Diseño de Productos de IBM Security. "A medida que la IA generativa se integra rápidamente en las empresas, expandiendo la superficie de ataque, estos gastos pronto se volverán insostenibles, lo que obligará a las empresas a reevaluar las medidas de seguridad y las estrategias de respuesta. Para salir adelante, las empresas deben invertir en nuevas defensas impulsadas por la IA y desarrollar las habilidades necesarias para abordar los riesgos y oportunidades emergentes que presenta la IA generativa".

La escasez de personal de seguridad elevó los costes de las brechas

Más de la mitad de las organizaciones estudiadas tuvieron una escasez de personal grave o de alto nivel el año pasado y, como resultado, experimentaron costes de filtraciones significativamente más altos (5,74 millones de dólares para niveles altos frente a 3,98 millones de dólares para niveles bajos o nulos). Esto llega en un momento en el que las organizaciones están compitiendo por adoptar tecnologías de IA generativa (gen AI), que se espera que introduzcan nuevos riesgos para los equipos de seguridad. De hecho, según un estudio global del IBM Institute for Business Value, el 51% de los líderes empresariales encuestados estaban preocupados por los riesgos impredecibles y las nuevas vulnerabilidades de seguridad que surgían, y el 47% estaban preocupados por los nuevos ataques dirigidos a la IA.

Los crecientes desafíos de personal pronto podrían verse aliviados, ya que más organizaciones declararon que planean aumentar los presupuestos de seguridad en comparación con el año pasado (63% frente a 51%), y la capacitación de los empleados surgió como una de las principales áreas de inversión planificadas. Las organizaciones también planean invertir en planificación y pruebas de respuesta a incidentes, tecnologías de detección y respuesta a amenazas (por ejemplo, SIEM, SOAR y EDR), gestión de identidades y accesos y herramientas de protección de seguridad de datos.

Hackeando el tiempo con IA

El `Cost of Data Breach Report´ también revela que el 67% de las organizaciones implementaron inteligencia artificial y automatización de seguridad, lo que supone un aumento de casi el 10% con respecto al año anterior y, el 20% declaró que utilizaba algún tipo de herramientas de seguridad de IA generativa. Las organizaciones que emplearon la inteligencia artificial y la automatización en seguridad detectaron y contuvieron ampliamente un incidente, en promedio, 98 días más rápido que las organizaciones que no utilizan estas tecnologías. Al mismo tiempo, el ciclo de vida promedio mundial de las violaciones de datos alcanzó un mínimo histórico en los últimos 7 años, 258 días, frente a los 277 días del año anterior, lo que revela que estas tecnologías pueden estar ayudando a recuperar el tiempo de los equipos de defensa al mejorar las actividades de mitigación y corrección de amenazas.

Los ciclos de vida más cortos de las brechas también se pueden atribuir al aumento de la detección interna: el 42% de las violaciones fueron detectadas por el propio equipo o herramientas de seguridad de una organización, en comparación con el 33% del año anterior. La detección interna acortó el ciclo de vida de la filtración de datos en 61 días y ahorró a las organizaciones casi 1 millón de dólares en costes de filtración en comparación con los revelados por un atacante.

La falta de seguridad de los datos almacenados impulsa el robo de propiedad intelectual

Según el informe de 2024, el 40% de las violaciones involucraron datos almacenados en múltiples entornos y más de un tercio de las brechas involucraron *shadow data* (datos almacenados en fuentes de datos no administradas), lo que destaca el creciente desafío con el seguimiento y la protección de datos.

Estas brechas en la visibilidad de los datos contribuyeron al fuerte aumento (27%) del robo de propiedad intelectual (PI). Los costes asociados con estos registros robados también aumentaron casi un 11% con respecto al año anterior, alcanzando los 173 dólares por registro. La propiedad intelectual puede volverse aún más accesible a medida que las iniciativas de IA generativa acerquen éstos y otros datos altamente confidenciales más cerca de la superficie. Dado que los datos críticos son cada vez más dinámicos y activos en todos los entornos, las empresas tendrán que reevaluar los controles de seguridad y acceso que los rodean.

Otros hallazgos clave del IBM `Cost of Data Breach 2024´ incluyen:

- **Las credenciales robadas encabezaron los vectores de ataque iniciales –**con un 16%, las credenciales robadas/comprometidas fueron el vector de ataque inicial más común. Estas brechas también tardaron más en identificarse y contenerse, con casi 10 meses.
- **Se pagan menos rescates cuando las fuerzas del orden están involucradas –**al involucrar a las fuerzas del orden, las víctimas de *ransomware* ahorraron en promedio casi 1 millón de dólares en costes de violación en comparación con aquellos que no lo hicieron (ese ahorro excluye el pago del rescate para aquellos que pagaron). La mayoría de las víctimas de *ransomware* (63%) que involucraron a las fuerzas del orden también pudieron evitar pagar un rescate.
- **Las organizaciones de infraestructuras crítica experimentan los costes de filtración más altos –**las organizaciones sanitarias, de servicios financieros, industriales, tecnológicas y energéticas incurrieron en los mayores costes de infracción en todos los sectores. Por 14º año consecutivo, los participantes del sector sanitario fueron testigos de las infracciones más costosas de todas las industrias, con un coste medios de infracción que alcanzó los 9,77 millones de dólares.

- **El coste de las filtraciones recae sobre los consumidores –**El 63% de las organizaciones declararon que este año aumentarían el coste de los bienes o servicios a causa de las filtraciones de datos, un ligero aumento con respecto al año pasado (57%), lo que marca el tercer año consecutivo en que la mayoría de las organizaciones estudiadas declararon que tomarían esta medida.

Fuentes Adicionales

- Descarga una copia del IBM Cost of Data Breach 2024.
- Regístrese en el seminario web IBM Security Cost of a Data Breach 2024 el martes 13 de agosto de 2024 a las 11:00 a.m. ET.
- Lea más sobre los principales hallazgos del informe en esteblog de IBM Security Intelligence.

Acerca de IBM

IBM es un proveedor líder de nube híbrida global e inteligencia artificial, así como experiencia en consultoría. Ayudamos a clientes en más de 175 países a capitalizar los conocimientos de sus datos, optimizar los procesos comerciales, reducir costos y obtener una ventaja competitiva en sus industrias. Más de 4.000 entidades gubernamentales y corporativas en áreas de infraestructura crítica, como servicios financieros, telecomunicaciones y atención médica, confían en la plataforma de nube híbrida de IBM y Red Hat OpenShift para llevar a cabo sus transformaciones digitales de manera rápida, eficiente y segura. Las innovaciones revolucionarias de IBM en IA, computación cuántica, soluciones en la nube específicas de la industria y consultoría ofrecen opciones abiertas y flexibles a nuestros clientes. Todo esto está respaldado por el compromiso a largo plazo de IBM con la confianza, la transparencia, la responsabilidad, la inclusión y el servicio. Visite ibm.com para obtener más información.

For further information: Camila Cuetos, Dpto. Comunicación, camila.cuetos2@ibm.com

---