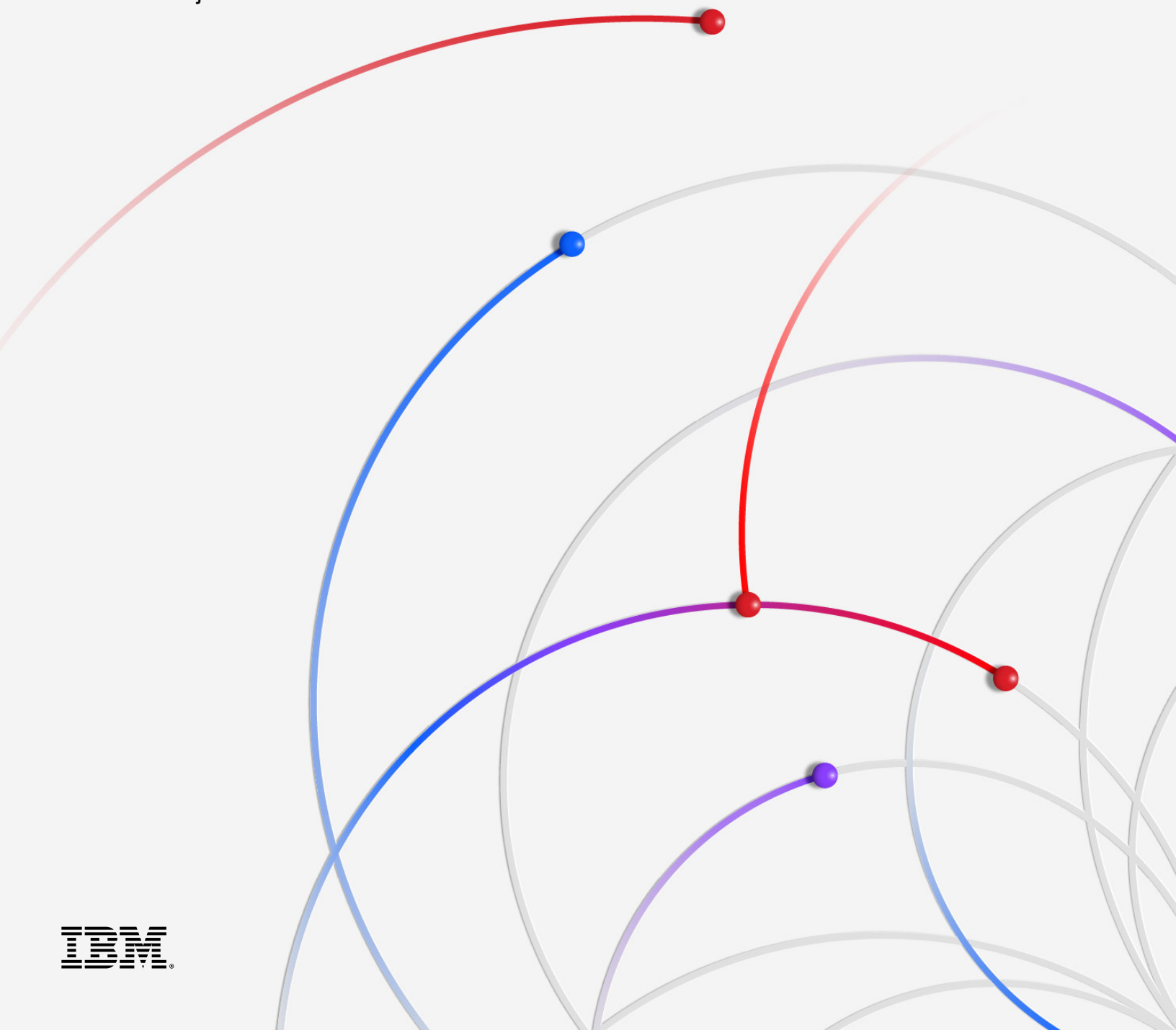
Informe Cost of a Data Breach 2024

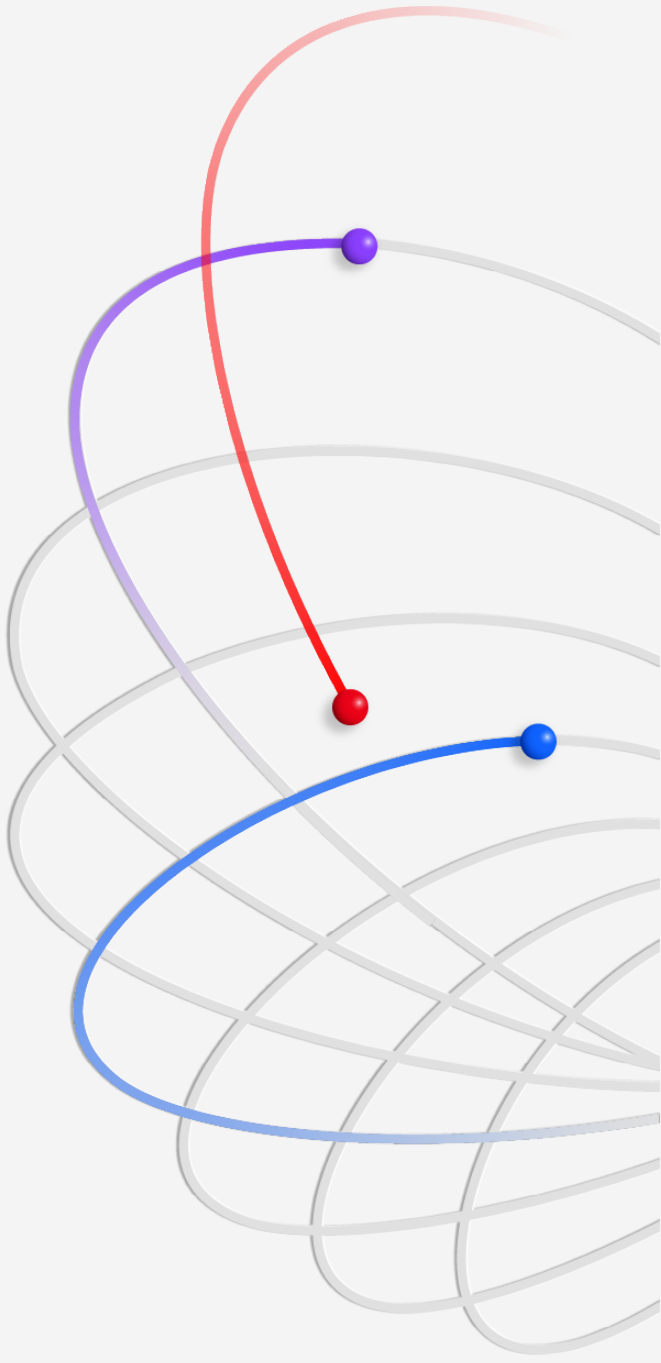
Resumen ejecutivo



IBM

Índice

Resumen ejecutivo



El informe Cost of a Data Breach anual proporciona a los responsables de TI, gestión de riesgos y seguridad pruebas oportunas y cuantificables para orientarles en su toma de decisiones estratégicas. También les ayuda a gestionar mejor sus perfiles de riesgo y sus inversiones en seguridad. El informe de este año, que es el decimonoveno de la serie, refleja la transformación provocada por los cambios tecnológicos, como el aumento de los datos ocultos, que son datos que residen en fuentes de datos no gestionadas, y el alcance y los costes de la interrupción del negocio provocada por las vulneraciones de datos.

Durante la investigación del informe (realizada de forma independiente por Ponemon Institute y patrocinada, analizada y publicada por IBM) se estudió a 604 organizaciones afectadas por vulneraciones de datos entre marzo de 2023 y febrero de 2024. Los investigadores analizaron organizaciones de 17 sectores, en 16 países y regiones, y vulneraciones que oscilaban entre 2100 y 113 000 registros comprometidos. Para obtener información sobre el terreno, los investigadores del Ponemon Institute entrevistaron a 3556 líderes empresariales de equipos directivos y de seguridad que conocían de primera mano los incidentes de vulneración de datos en sus organizaciones.

El resultado es un informe de referencia que los líderes empresariales y de seguridad pueden utilizar para reforzar sus defensas de seguridad e impulsar la innovación, especialmente en torno a la adopción de la IA en la seguridad y la seguridad de sus iniciativas de IA generativa.

El informe de este año comienza con dos novedades importantes. En primer lugar, el coste medio mundial de la vulneración de datos aumentó un 10 % con respecto al año anterior, alcanzando los 4,88 millones de dólares, lo que supone el mayor incremento desde la pandemia. La interrupción de la actividad empresarial y la atención al cliente, así como la corrección tras la vulneración, determinaron este aumento de los costes. Cuando se les preguntó cómo estaban afrontando estos costes, más de la mitad de las organizaciones afirmaron que los estaban repercutiendo a los clientes. Hacer que los clientes asuman estos costes puede ser problemático en un mercado competitivo que ya se enfrenta a la presión de la inflación sobre los precios.

En segundo lugar, en lo que respecta a la defensa, los investigadores también descubrieron que la aplicación de la IA y la automatización de la seguridad está dando sus frutos, reduciendo los costes de las vulneraciones una media de 2,2 millones de dólares en algunos casos. Las soluciones de IA y automatización están reduciendo el tiempo necesario para identificar y contener una vulneración y los daños resultantes. Dicho de otro modo, los defensores que no cuenten con la ayuda de la IA y la automatización tardarán más tiempo en detectar y contener una vulneración, y verán aumentar los costes en comparación con quienes utilizan estas soluciones.

Como hemos visto en todo el sector, es habitual que los equipos de ciberseguridad carezcan de personal suficiente. El estudio de este año reveló que más de la mitad de las organizaciones que sufrieron vulneraciones se enfrentaban a una grave escasez de personal de seguridad, un déficit de cualificación que aumentó en dos dígitos con respecto al año anterior. Esta falta de personal de seguridad capacitado aumenta a medida que se amplía el panorama de las amenazas. Se espera que la continua carrera por adoptar la IA generativa en casi todas las funciones de la organización traiga consigo riesgos sin precedentes y ejerza aún más presión sobre estos equipos de ciberseguridad.

Este informe ofrece información y recomendaciones basadas en la investigación para ayudar a reducir los posibles daños financieros y de reputación derivados de una vulneración de datos.

Novedades en el informe de 2024

Cada año seguimos desarrollando el informe Cost of a Data Breach para que queden reflejadas las nuevas tecnologías, las tácticas emergentes y los acontecimientos recientes. En la investigación de este año se analizan por primera vez los siguientes aspectos:

- Si las organizaciones sufrieron interrupciones operativas a largo plazo, como la imposibilidad de tramitar pedidos de venta, el cierre completo de las instalaciones de producción o la ineficacia de los servicios de atención al cliente
- Si la vulneración incluía datos almacenados en fuentes de datos no gestionadas, también conocidos como datos ocultos
- En qué medida las organizaciones utilizan la IA y la automatización en cada una de las cuatro áreas de las operaciones de seguridad: prevención, detección, investigación y respuesta
- La naturaleza de los ataques de extorsión, como ataques de extorsión y ransomware o de extorsión y exfiltración de datos únicamente
- El tiempo que se tarda en restaurar los datos, sistemas o servicios a su estado anterior a la vulneración
- Cuánto tardaron las organizaciones en notificar la vulneración si estaban obligadas a hacerlo
- Si las organizaciones que recurrieron a las fuerzas del orden tras un ataque de ransomware pagaron el rescate

Principales conclusiones

Las principales conclusiones aquí descritas se basan en el análisis realizado por IBM de los datos de investigación recopilados por el Ponemon Institute.

4,88 millones de dólares

Coste total promedio de una vulneración
El coste medio de una vulneración de datos pasó de 4,45 millones de dólares en 2023 a 4,88 millones de dólares, lo que supone un aumento del 10 % y el mayor incremento desde la pandemia. Este incremento se debió al aumento del coste de la pérdida de negocio, incluyendo el tiempo de inactividad operativa y la pérdida de clientes, y al coste de las respuestas posteriores a la vulneración, tales como la dotación de personal de los servicios de atención al cliente y el pago de multas más altas. En conjunto, estos costes ascendieron a 2,8 millones de dólares, el importe combinado más alto por pérdida de negocio y actividades posteriores a la vulneración en los últimos 6 años.

2,2 millones de dólares

Ahorro de costes gracias al uso generalizado de la IA en la prevención
Dos de cada tres organizaciones estudiadas declararon que están implementando IA y la automatización de la seguridad en su centro de operaciones de seguridad, lo que supone un 10 % más que el año anterior. Cuando se implementa ampliamente en los flujos de trabajo de prevención (gestión de la superficie de ataque (ASM), red-teaming y gestión de la posición), las organizaciones reducen los costes de vulneración una media de 2,2 millones de dólares en comparación con aquellas que no utilizan IA en los flujos de trabajo de prevención. Este hallazgo supuso el mayor ahorro de costes revelado en el informe de 2024.

26,2 %

Crecimiento de la escasez de habilidades cibernéticas
Más de la mitad de las organizaciones víctimas de vulneraciones se enfrentan a altos niveles de escasez de personal de seguridad. Este problema representa un aumento del 26,2 % con respecto al año anterior, una situación que se corresponde con una media de 1,76 millones de dólares más en costes por vulneraciones. Incluso cuando una de cada cinco organizaciones afirma haber utilizado algún tipo de herramienta de seguridad de IA generativa (que se espera que ayude a eliminar la vulneración al impulsar la productividad y la eficiencia), esta carencia de habilidades sigue siendo un desafío.

1 de cada 3

Porcentaje de vulneraciones de datos ocultos
El 35 % de las vulneraciones afectaron a datos ocultos, lo que demuestra que la proliferación de datos está dificultando su seguimiento y protección. El robo de datos ocultos se correlacionó con un 16 % de aumento del coste de la vulneración. Los investigadores descubrieron que el almacenamiento de datos en distintos entornos era una estrategia de almacenamiento común, responsable del 40 % de las vulneraciones. Estas vulneraciones también tardaron más tiempo en identificarse y contenerse. Por el contrario, los datos almacenados en un solo tipo de entorno se vulneraron con menos frecuencia, tanto si se trataba de un cloud público (25 %) como de un entorno local (20 %) o un cloud privado (15 %).

4,99 millones de dólares

Coste medio del ataque de un usuario interno negligente
En comparación con otros vectores, los ataques de usuarios internos negligentes generaron los costes más elevados, con una media de 4,99 millones de dólares. Otros vectores de ataque costosos fueron el compromiso del correo electrónico empresarial, el phishing, la ingeniería social y las credenciales robadas o comprometidas. Es posible que la IA generativa contribuya a la creación de algunos de estos ataques de phishing. Por ejemplo, la IA generativa facilita más que nunca la producción de mensajes de phishing gramaticalmente correctos y plausibles incluso a los no angloparlantes.

46 %

Porcentaje de vulneraciones de datos personales de clientes
Casi la mitad de las vulneraciones afectaron a información de identificación personal (PII) de clientes, que puede incluir números de identificación fiscal (NIF), correos electrónicos, números de teléfono y direcciones particulares. Los registros de propiedad intelectual (PI) ocuparon un cercano segundo lugar (43 % de las vulneraciones). El coste de los registros de propiedad intelectual aumentó considerablemente con respecto al año pasado: 173 dólares por registro en el estudio de este año, frente a los 156 del informe del año pasado.

1 millón de dólares

Ahorro de costes cuando las fuerzas del orden intervienen en ataques de ransomware
Dos tercios de las organizaciones que sufrieron ataques de ransomware e involucraron a las fuerzas de seguridad no pagaron el rescate. Esas organizaciones también acabaron reduciendo el coste del ataque en una media de casi un millón de dólares, si se excluye el coste de cualquier rescate pagado. Involucrar a las fuerzas de seguridad también ayudó a acortar el tiempo necesario para identificar y contener las vulneraciones de 297 a 281 días.

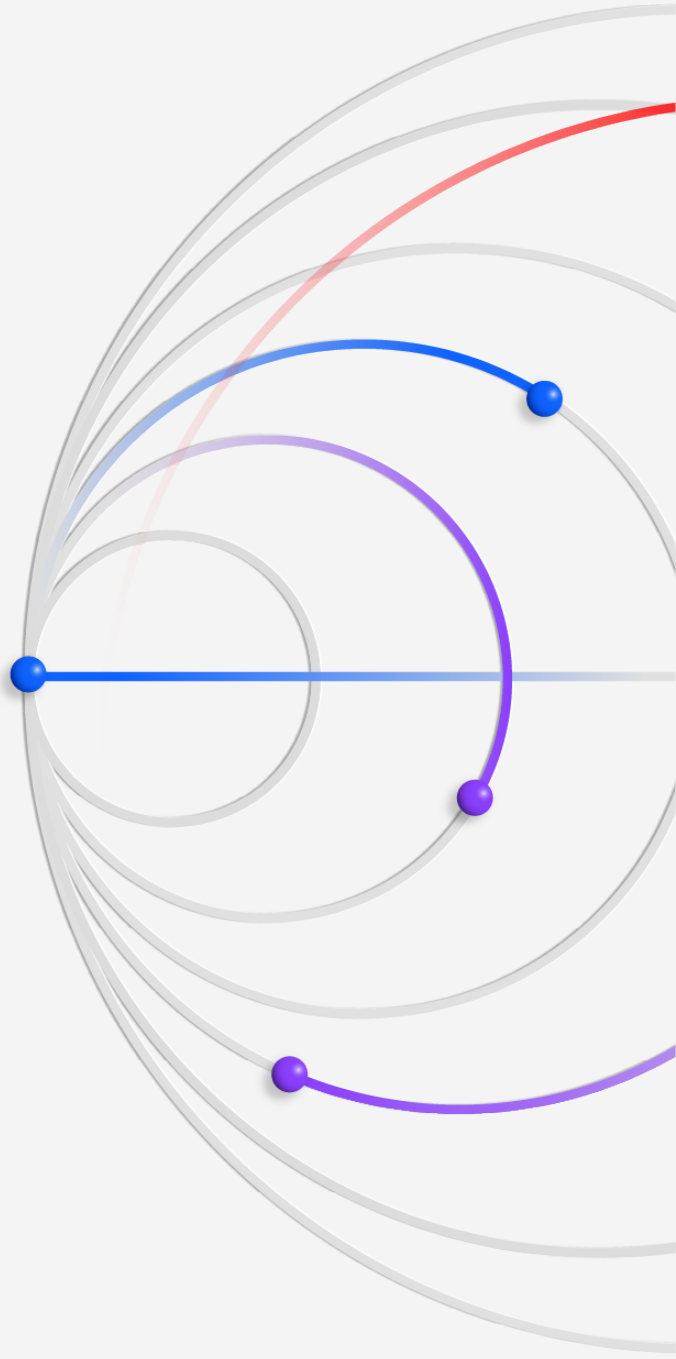
292

Días para identificar y contener las vulneraciones relacionadas con el robo de credenciales
Las vulneraciones que implicaban el robo o el compromiso de credenciales fueron las que más tardaron en identificarse y contenerse (292 días) de todos los vectores de ataque. Los ataques similares que implicaban aprovecharse de los empleados y del acceso de los empleados también tardaron mucho tiempo en resolverse. Por ejemplo, los ataques de phishing duraron una media de 261 días, mientras que los ataques de ingeniería social tardaron una media de 257 días.

830 000 dólares

El mayor aumento medio de costes de todos los sectores
El sector industrial experimentó el aumento más costoso de todos, con una subida media de 830 000 dólares por vulneración con respecto al año pasado. Este aumento de los costes podría reflejar la necesidad de que las organizaciones industriales se preparen para una respuesta más rápida, ya que las organizaciones de este sector son muy sensibles al tiempo de inactividad operativa. Aun así, el tiempo necesario para identificar y contener una vulneración de datos en las organizaciones industriales fue superior a la media del sector, con 199 días para identificarla y 73 días para contenerla.

Recomendaciones para ayudar a reducir el coste de una vulneración de datos



Nuestras recomendaciones incluyen enfoques de seguridad eficaces que se asocian a una reducción de los costes y de los tiempos para identificar y contener las vulneraciones de datos.

Conozca su panorama informativo

La mayoría de las organizaciones distribuyen datos a través de múltiples entornos, incluyendo repositorios de datos locales, clouds privados y clouds públicos. Sin embargo, muchas organizaciones tienen inventarios de datos incompletos o desactualizados, lo que retrasa los esfuerzos para descubrir qué datos han sido vulnerados y cuán sensibles o confidenciales son. Estos retrasos pueden complicar la respuesta y aumentar el coste de una vulneración.

Los equipos de seguridad deben asegurarse de tener una visibilidad completa de todos estos entornos para poder monitorizar y proteger los datos de forma continua, independientemente de dónde residan. Las organizaciones pueden aplicar la gestión de la posición de seguridad de datos (DSPM) y otras soluciones, como la gestión de identidades y acceso y ASM, en todos estos entornos para ofrecer una protección sistemática y completa.

Los equipos de seguridad deben prestar especial atención a los entornos híbridos y los clouds públicos. El 40 % de las vulneraciones de datos afectaron a datos almacenados en varios entornos, y cuando los datos vulnerados se almacenaron en clouds públicos, el coste medio de la vulneración fue de 5,17 millones de dólares. Es imprescindible que los equipos de seguridad conozcan en profundidad los riesgos y controles específicos de cada servicio cloud que emplean.

La gestión de datos en distintos entornos se complica aún más por el impacto de los datos no gestionados. Más de un tercio de las vulneraciones de datos están relacionadas con datos ocultos. Los equipos de seguridad deben asumir ahora que sus organizaciones tienen fuentes de datos no gestionadas. Los datos sin cifrar, incluidos los de las cargas de trabajo de IA, agravan aún más el riesgo. Las estrategias de cifrado de datos deben tener en cuenta los tipos de datos, su uso y dónde residen para reducir el riesgo en caso de vulneración.

Refuerce las estrategias de prevención con IA y automatización

La adopción de modelos de IA generativa y aplicaciones de terceros en toda la organización, así como el uso continuo de dispositivos del Internet de las cosas (IoT) y aplicaciones SaaS, están ampliando la superficie de ataque y sometiendo a presión a los equipos de seguridad.

La aplicación de la IA y la automatización en apoyo de las estrategias de prevención de la seguridad (incluidas las áreas de ASM, red-teaming y gestión de la posición) puede abordarse a menudo mediante servicios de seguridad gestionados. En el estudio de este año, las inversiones en IA de las organizaciones que aplicaron la IA y la automatización a la prevención de la seguridad tuvieron la mayor repercusión en comparación con otras tres áreas de seguridad: detección, investigación y respuesta. Ahorraron una media de 2,22 millones de dólares con respecto a las organizaciones que no implementaron IA en tecnologías de prevención.

Dé prioridad a la seguridad en la adopción de la IA generativa

Aunque las organizaciones están avanzando rápidamente con la IA generativa, solo el 24 % de las iniciativas en dicha materia están protegidas. La falta de seguridad amenaza con exponer los datos y los modelos de datos a vulneraciones, lo que podría socavar los beneficios que los proyectos de IA generativa pretenden ofrecer.

A medida que aumenta la adopción de la IA generativa, las organizaciones necesitan un marco para proteger los datos, los modelos y el uso de la IA generativa, además de establecer controles de gobierno de la IA. Tendrán que asegurar los datos de entrenamiento protegiéndolos de robos y manipulaciones. Las organizaciones pueden utilizar la detección y la clasificación de datos para detectar los datos confidenciales utilizados en el entrenamiento o el ajuste. También pueden implantar controles de seguridad de los datos mediante el cifrado, la gestión del acceso y la monitorización del cumplimiento.

Con la IA generativa, las organizaciones no solo se enfrentan al riesgo y al crecimiento de los datos ocultos, sino también a los modelos ocultos. Las organizaciones deben ampliar la gestión de la posición a los propios modelos de IA para proteger los datos de entrenamiento de IA confidenciales, obtener visibilidad del uso de modelos de *IA no autorizados u ocultos,* y del uso indebido de la IA o la fuga de datos.

Para garantizar la seguridad del desarrollo de modelos de IA generativa es necesario buscar vulnerabilidades en la canalización, reforzar las integraciones y aplicar políticas y accesos. Para proteger el uso de los modelos de IA generativa es necesario que los equipos de seguridad vigilen las entradas maliciosas, como las inyecciones de instrucciones, y las salidas que contengan datos confidenciales. También deben implementar soluciones de seguridad de IA que puedan detectar y responder a ataques específicos de IA, como el envenenamiento de datos, la evasión de modelos y la extracción de modelos. También es esencial desarrollar guías de estrategias para denegar el acceso y poner en cuarentena y desconectar los modelos comprometidos.

Con la proliferación del panorama de amenazas debido a la IA generativa y otras iniciativas de TI, es necesario ofrecer formación en seguridad a los profesionales no relacionados con la seguridad, incluidos los científicos e ingenieros de datos que trabajan en equipos de IA.

Mejore su formación en ciberrespuestas

La forma en que una organización reacciona y se comunica durante y después de una vulneración (con la dirección de la empresa, los reguladores y los clientes) importa más que nunca. El 75 % de aumento del coste medio de las vulneraciones en el estudio de este año se debió al coste de la pérdida de negocio, incluido el tiempo de inactividad, la pérdida de clientes y pedidos, y la captación de nuevos clientes. También se incluyeron las actividades de respuesta tras la vulneración, como la creación de un servicio de asistencia técnica para el cliente, la monitorización del crédito de los clientes afectados y el pago de multas. La lección: invertir en la preparación de la respuesta posterior a la vulneración puede ayudar a reducir los costes.

Las organizaciones deben complementar la capacidad de respuesta técnica con una planificación estratégica para cubrir el impacto en el negocio, proteger a los clientes y mantener la continuidad operativa. Fomentar el gobierno y tomar decisiones con antelación puede ayudar a los ejecutivos a prever la gestión de una interrupción importante del negocio y hacer más eficientes las acciones que beneficiarán a la organización en caso de ataque.

Para mejorar su capacidad de hacer frente a ataques de gran impacto, las organizaciones pueden participar en ejercicios de simulación de crisis de alcance cibernético con el fin de desarrollar la memoria muscular para responder a las vulneraciones. En estos ejercicios pueden participar tanto los equipos de seguridad como los directivos, de modo que toda la organización mejore su capacidad para detectar, contener y responder a las vulneraciones. Los responsables de seguridad deben trabajar con antelación con las funciones empresariales de toda la organización y con los equipos de comunicación para elaborar planes de respuesta y ponerlos a prueba. Con la proliferación del panorama de amenazas debido a la IA generativa y otras iniciativas de TI, es necesario ofrecer formación en seguridad a los profesionales no relacionados con la seguridad. Entre estos profesionales se incluyen los científicos e ingenieros de datos que trabajan en equipos de machine learning e IA y aquellos encargados de la continuidad de las cargas de trabajo de IA en recursos locales y cloud.

Al invertir en la preparación de la respuesta, las organizaciones pueden ayudar a reducir los efectos costosos y disruptivos de las vulneraciones de datos, respaldar la continuidad de las operaciones y ayudar a preservar sus relaciones con los clientes, socios y otras partes interesadas clave. Además, el ensayo de la respuesta tranquiliza a los empleados y reduce el estrés, la angustia y las fricciones internas, ya que un equipo directivo bien preparado se encarga de gestionar, controlar y comunicar las fases agudas de un ataque.

Acerca de IBM y el Ponemon Institute

Ponemon Institute

Fundado en 2002, el Ponemon Institute es una institución dedicada a la investigación y formación independiente que fomenta el avance de las prácticas responsables de gestión de la privacidad y la información dentro de las empresas y el gobierno. Nuestra misión es realizar estudios empíricos de alta calidad sobre temas cruciales que afectan a la gestión y la seguridad de la información confidencial sobre personas y organizaciones.

El Ponemon Institute mantiene estrictas normas de confidencialidad de datos, privacidad e investigación ética y no recopila ninguna información de identificación personal (PII) ni información de identificación de empresas en la investigación empresarial. Además, las estrictas normas de calidad garantizan que no se hagan preguntas extrañas, irrelevantes o inadecuadas a las personas.

Si tiene preguntas o comentarios sobre este informe de investigación, incluidas las solicitudes de autorización para citar o reproducir el informe, póngase en contacto con nosotros por correo postal, teléfono o correo electrónico:

Ponemon Institute LLC
Departamento de investigación
1-800-887-3118
research@ponemon.org

IBM

IBM es un proveedor líder mundial de cloud híbrido, IA y servicios empresariales que ayuda a clientes de más de 175 países a capitalizar la información de sus datos, agilizar los procesos empresariales, reducir costes y obtener una ventaja competitiva en sus sectores. Todo ello respaldado por el legendario compromiso de IBM con la confianza, la transparencia, la responsabilidad, la inclusión y el servicio. Para obtener más información, visite www.ibm.com/es-es.

Obtenga más información sobre cómo mejorar su posición de seguridad:
Visite ibm.com/es-es/security

Únase a la conversación
en la comunidad de IBM Security

IBM España, S.A.
Santa Hortensia, 26-28
28002 Madrid
IBM Corporation
New Orchard Road
Armonk, NY 10504

Producido en los Estados Unidos de América
Julio de 2024