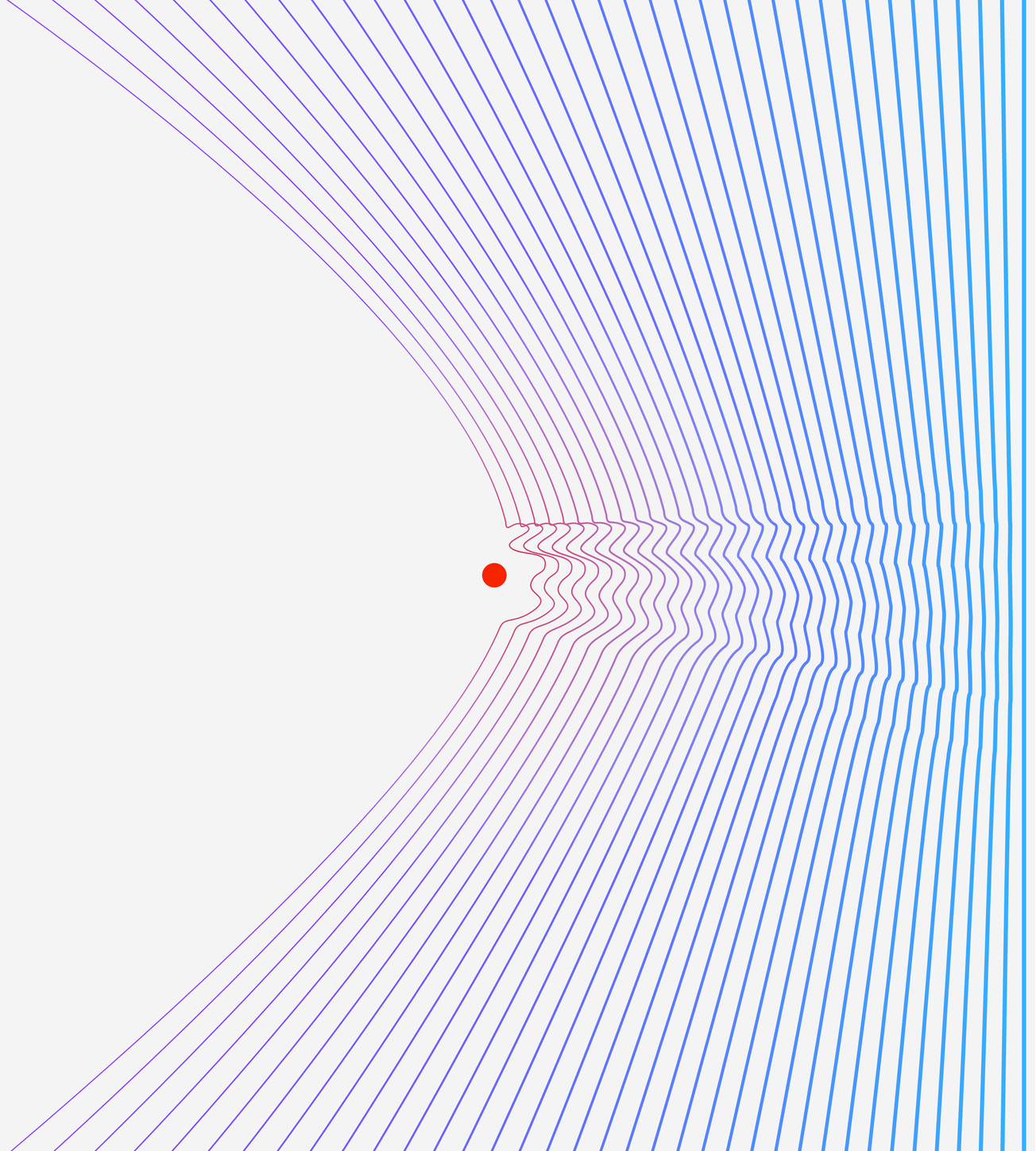
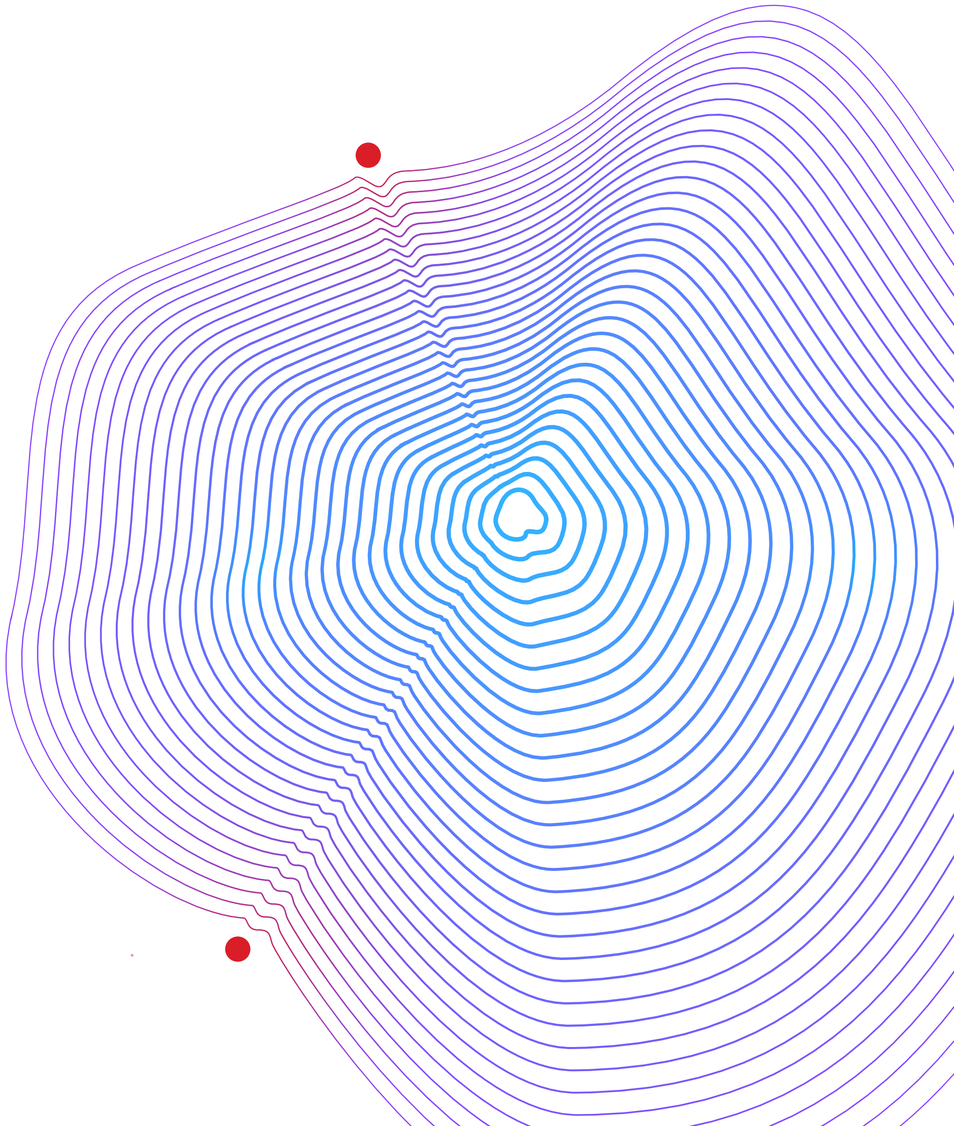
IBM® **Security**

Informe sobre el costo de una filtración de datos 2023

Resumen Ejecutivo



Índice



01

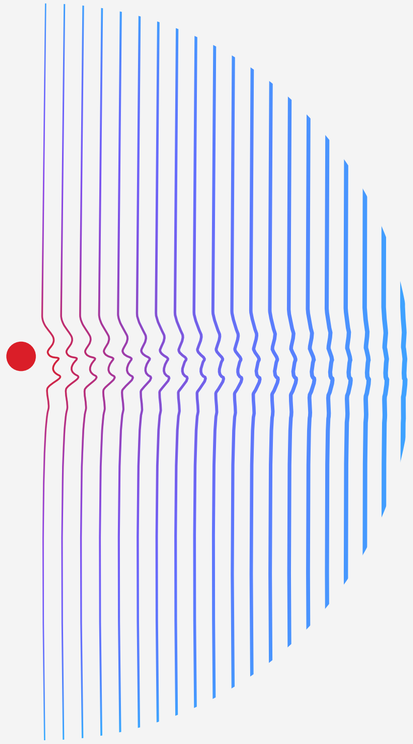
Resumen ejecutivo

El Informe sobre el costo de una filtración de datos dota a los líderes de TI, gestión de riesgos y seguridad con evidencia cuantificable para ayudarlos a administrar mejor sus inversiones en seguridad, perfil de riesgo y procesos de toma de decisiones estratégicas. La edición 2023 representa el 18.º año consecutivo de este informe.

La investigación de este año, realizada de forma independiente por Ponemon Institute y patrocinada, analizada y publicada por IBM® Security, estudió 553 casos de filtración de datos entre marzo de 2022 y marzo de 2023.

El periodo mencionado en este informe se refiere al año en que se publicó el informe, no necesariamente al año en que ocurrieron las filtraciones. Las filtraciones estudiadas ocurrieron en 16 países y regiones y en 17 industrias diferentes.

A lo largo de este informe, examinaremos las causas raíz y las consecuencias tanto a corto como a largo plazo de las filtraciones de datos. También analizaremos los factores y tecnologías que permitieron a las empresas limitar las pérdidas, así como los que provocaron un aumento de los costos.



Novedades en el informe de 2023

Cada año, seguimos perfeccionando el Informe sobre el costo de una filtración de datos para que coincida con nuevas tecnologías, tácticas emergentes y sucesos recientes. Por primera vez, la investigación de este año analiza:

- Cómo se identifican las filtraciones: ya sea que lo hagan los propios equipos de seguridad de una organización, un tercero o el atacante
- El impacto que tiene involucrar a las autoridades policiales en un ataque de ransomware
- La efectividad de las guías de referencia sobre ransomware y los flujos de trabajo
- Los costos específicos asociados con multas reglamentarias
- Si y como planean las empresas aumentar las inversiones en seguridad como resultado de una filtración
- El impacto de las siguientes estrategias de mitigación:
  - Inteligencia en materia de amenazas
  - Vulnerabilidad y gestión de riesgos
  - Gestión de la superficie de ataque (ASM)
  - Proveedores de servicios de seguridad gestionados (MSSP)

Dado que el costo de una filtración sigue en alza, la información contenida en este documento es esencial para ayudar a los equipos de seguridad y de IT a gestionar mejor el riesgo y limitar las posibles pérdidas. El informe se divide en las siguientes secciones:

- Resumen ejecutivo con las principales conclusiones, así como las novedades de la edición de 2023.
- Análisis detallado, incluidos los costos de las filtraciones por región geográfica o industria
- Recomendaciones de seguridad de expertos de IBM® Security, con base en los resultados de este informe

02

Principales conclusiones

Las principales conclusiones que se describen aquí se basan en el análisis que hizo IBM® Security de los datos que recopiló Ponemon Institute en la investigación. Los importes de los costos en este informe se especifican en dólares estadounidenses (USD).

USD 4,45 millones

Costo total promedio de una filtración
El costo promedio de una filtración de datos alcanzó un máximo histórico de USD 4,45 millones en 2023. Esto representa un aumento de 2.3 % respecto del costo reflejado en 2022, que fue de USD 4,35 millones. Considerando una perspectiva de largo plazo, el costo promedio aumentó un 15.3 % respecto de los USD 3,86 millones reflejados en el informe de 2020.

51%

Porcentaje de organizaciones que planean aumentar las inversiones en seguridad como resultado de una filtración.
Si bien los costos de las filtraciones de datos siguieron al alza, las opiniones de quienes participaron en el informe se dividieron casi equitativamente en cuanto a si planean aumentar las inversiones en seguridad en consecuencia de una filtración de datos. Las áreas principales identificadas para realizar inversiones adicionales incluyeron: planificación y pruebas de la respuesta a incidentes (IR), capacitación de los empleados y tecnologías para la detección de amenazas y de respuesta ante estas.

USD 1,76 millones

El efecto de utilizar ampliamente IA y automatizar la seguridad en el impacto financiero que conlleva una filtración.
Se demostró que la IA y la automatización de la seguridad son inversiones importantes para reducir costos y minimizar el tiempo que consume identificar y contener las filtraciones. Las organizaciones que utilizaron estas capacidades ampliamente dentro de su enfoque redujeron, en promedio, 108 días el tiempo que les llevaba identificar y contener la filtración. También informaron que los costos de una filtración de datos se redujeron USD 1,76 millones en comparación con los de las organizaciones que no las utilizaron.

1 de 3

Número de filtraciones identificadas por los propios equipos o herramientas de seguridad de una organización Solo una tercera parte de las empresas descubrió la filtración de datos a través de sus propios equipos de seguridad, lo que pone de manifiesto la necesidad de mejorar la detección de amenazas. El 67 % de las filtraciones fueron notificadas por un tercero benévolo o por los propios atacantes. Cuando los atacantes revelaron una filtración, a las organizaciones les costó casi un millón de dólares más en comparación con la detección interna.

USD 470.000

Costo adicional experimentado por organizaciones que no involucraron a las autoridades en un ataque de ransomware
La investigación de este año muestra que excluir a las autoridades policiales de los incidentes de ransomware provocó costos más elevados. Mientras que el 63 % de los encuestados afirmó que involucró a las autoridades policiales, el 37 % que no lo hizo también pagó un 9,6 % más y experimentó un ciclo de vida de la vulneración 33 días más largo.

53,3%

Desde 2020, los costos de la filtración de datos en el sector de la atención médica han aumentado 53,3 %
El sector salud extremadamente regulado ha observado un incremento considerable en los costos derivados de la filtración de datos desde 2020. Por 13.° año consecutivo, esta industria reportó las filtraciones de datos más costosas, a un costo promedio de USD 10,93 millones.

82%

El porcentaje de filtraciones que involucraron datos almacenados en la nube: entornos públicos, privados o múltiples.
Los entornos en la nube fueron blancos frecuentes para los ciberataques en 2023. Los atacantes a menudo obtuvieron acceso a diversos entornos, donde 39 % de las infiltraciones abarcaron múltiples entornos e incurrieron en un costo superior al promedio de USD 4,75 millones.

USD 1,68 millones

Reducción de costos gracias a los altos niveles de adopción de DevSecOps.
Las pruebas de seguridad integradas en el proceso de desarrollo de software (DevSecOps) mostraron un ROI considerable en 2023. Las organizaciones con alta adopción de DevSecOps ahorraron USD 1,68 millones en comparación con aquellas cuya adopción fue baja o nula. En comparación con otros factores de mitigación de costos, DevSecOps demostró la mayor reducción de costos.

USD 1,49 millones

Reducción de costos logrado por organizaciones con altos niveles de planificación y pruebas de respuesta a incidentes (RI).
Además de ser una inversión prioritaria para las organizaciones, la planificación y las pruebas de IR se revelaron como una táctica muy eficaz para contener el costo de una filtración de datos. Las organizaciones con altos niveles de planificación y pruebas de IR ahorraron USD 1,49 millones en comparación con aquellas con niveles bajos.

USD 1,44 millones

Aumento en los costos de filtración de datos para organizaciones con un sistema de seguridad con altos niveles de complejidad.
Las organizaciones que reportaron un sistema de seguridad con poca o nula complejidad observaron un costo promedio de filtración de datos de USD 3,84 millones en 2023. Aquellas con un sistema de seguridad con un alto nivel de complejidad reportaron un costo promedio de USD 5,28 millones, lo que representa un aumento del 31, 6%.

USD 1,02 millones

Diferencia promedio en los costos entre las filtraciones que tomaron más de 200 días en ser detectadas y resueltas y aquellas que tomaron menos de 200 días.
El tiempo necesario para identificar y contener las filtraciones, conocido como el ciclo de vida de la vulneración, sigue siendo esencial para el impacto financiero global. Las filtraciones que toman menos de 200 días para ser identificadas y contenidas le cuestan a las organizaciones USD 3,93 millones. Aquellas para las que toma más de 200 días cuestan USD 4,95 millones, una diferencia del 23 %.

03

Recomendaciones para ayudar a reducir el costo de una filtración de datos

En esta sección, IBM® Security describe las medidas que pueden tomar las organizaciones para ayudar a reducir los impactos económicos y de reputación de una filtración de datos. Nuestras recomendaciones incluyen enfoques de seguridad exitosos que están asociados con menores costos y menos tiempo para identificar y contener filtraciones.

1. Integre seguridad en cada etapa del desarrollo y la implementación del software, y realice pruebas con regularidad.
2. Modernice la protección de datos en la nube híbrida.
3. Utilice IA y automatización de seguridad para aumentar la velocidad y precisión.
4. Fortalezca la resiliencia conociendo su superficie de ataque y practicando IR.

1

Integre seguridad en cada etapa del desarrollo y la implementación del software, y realice pruebas con regularidad.

Los requisitos reglamentarios continúan siendo más complicados, especialmente a medida que la tecnología se entrelaza más con las actividades cotidianas y el software se vuelve más rico y complejo. Un enfoque de DevSecOps, el principal mitigador de costos en un análisis especial de 27 factores en el informe de 2023, será esencial para incorporar seguridad en cualquier herramienta o plataforma de la que dependa una organización para interactuar con su fuerza laboral o sus clientes.

Las organizaciones de todo tipo deben buscar garantizar que la seguridad esté a la vanguardia del software que están desarrollando, así como del software comercial listo para usar que están implementando. Los desarrolladores de aplicaciones deben continuar acelerando la adopción de los principios de seguridad por diseño y seguridad predeterminada para garantizar que la seguridad sea un requisito fundamental que se considere durante la fase de diseño inicial de los proyectos de transformación digital y no simplemente se aborde después del hecho. Los mismos principios se están aplicando a los entornos en la nube para favorecer el desarrollo de aplicaciones nativas de la nube que realmente se esfuerzan para proteger la privacidad del usuario y minimizar las superficies de ataque.

Las pruebas de aplicación o las pruebas de penetración desde la perspectiva de un atacante también pueden brindar a las organizaciones la oportunidad de identificar y corregir vulnerabilidades antes de que se conviertan en filtraciones. Ninguna tecnología o aplicación será completamente segura, y agregar más funciones introduce nuevos riesgos. Probar las aplicaciones de manera continua puede ayudar a las organizaciones a identificar nuevas vulnerabilidades.

2

Modernice la protección de datos en la nube híbrida

Los datos se están creando y compartiendo, así como se está accediendo a ellos, a una escala sin precedentes en entornos multinube. La rápida adopción de nuevas aplicaciones y servicios en la nube está agravando el riesgo de “datos en la sombra” —datos confidenciales que no se rastrean ni controlan—, lo cual aumenta los riesgos de seguridad y cumplimiento normativo. La mayoría (82 %) de las filtraciones de datos estudiadas en este informe involucraron datos almacenados en entornos de nube, y el 39 % de las filtraciones incluyeron datos que abarcaban varios tipos de entornos. El costo y el riesgo de estas filtraciones de datos se ven agravados por una matriz de regulaciones en constante evolución y severas sanciones por incumplimiento.

A raíz de estos desafíos, obtener visibilidad y control de los datos distribuidos en la nube híbrida debe ser una prioridad para las organizaciones de todo tipo y debe centrarse en el cifrado sólido, la seguridad de los datos y las políticas de acceso a los datos. Las empresas deben buscar tecnologías para reforzar la seguridad de los datos y el cumplimiento normativo que funcionen en todas las plataformas para proteger los datos a medida que se mueven a través de bases de datos, aplicaciones y servicios implementados en entornos de nube híbrida. Las soluciones de supervisión de la actividad de los datos pueden ayudar a garantizar que se implementen los controles adecuados mientras se aplican activamente estas políticas, como la detección temprana de actividad sospechosa y el bloqueo de amenazas contra almacenes de datos cruciales en tiempo real.

Además, las tecnologías más nuevas, como la gestión de las posturas de seguridad de los datos, pueden ayudar a encontrar datos desconocidos y confidenciales en la nube, incluidos recursos estructurados y no estructurados dentro de los proveedores de servicios en la nube, las propiedades de software como servicio (SaaS) y los data lakes. Esto puede ayudar a identificar y mitigar las vulnerabilidades en las configuraciones, derechos y flujos de datos subyacentes del almacén de datos.

A medida que las organizaciones siguen avanzando en las operaciones híbridas multinube, es esencial desplegar estrategias sólidas de gestión de identidades y accesos (IAM) que incluyan tecnologías como la autenticación multifactor (MFA), con especial atención a la gestión de cuentas de usuario privilegiadas que tienen un nivel de acceso elevado.

3

Utilice IA de seguridad y automatización para aumentar velocidad y precisión
El informe de 2023 arrojó que solo el 28 % de las organizaciones utilizó ampliamente IA de seguridad y automatización en sus operaciones, lo que significa que muchas organizaciones tienen una buena oportunidad para mejorar su velocidad, precisión y eficiencia. El amplio uso de IA de seguridad y automatización generó una reducción de costos de filtración de datos de casi USD 1,8 millones, así como ayudó a reducir el tiempo para identificar y contener una filtración más de 100 días para estas organizaciones en comparación con las que no hicieron uso de estas.

Los equipos de seguridad pueden beneficiarse de tener IA de seguridad y automatización integradas en sus conjuntos de herramientas. Por ejemplo, integrarlas en las herramientas de detección de amenazas y respuesta a estas puede ayudar a los analistas a detectar nuevas amenazas con mayor precisión y contextualizar y priorizar las alertas de seguridad de manera más eficaz. Estas tecnologías también pueden automatizar partes del proceso de investigación de amenazas o recomendar medidas para acelerar la respuesta. Además, las soluciones de verificación de identidad y seguridad de datos con tecnología de IA pueden ayudar a impulsar una postura de seguridad proactiva al identificar transacciones de alto riesgo, protegerlas con mínima fricción del usuario y relacionar comportamientos sospechosos de manera más efectiva.

Al aplicar IA dentro de sus operaciones de seguridad, busque tecnologías que ofrezcan casos de uso confiables y maduros con precisión, efectividad y transparencia comprobadas para eliminar posibles sesgos, puntos ciegos o desviaciones. Las organizaciones deben planificar un modelo operativo para la adopción de IA que respalde el aprendizaje continuo a medida que evolucionan las amenazas y las capacidades tecnológicas.

Las organizaciones también pueden beneficiarse de un enfoque que integre estrechamente las principales tecnologías de seguridad para facilitar los flujos de trabajo y la capacidad de compartir información a través de conjuntos de datos comunes. Los directores de seguridad de la información (CISO) y los líderes de operaciones de seguridad (SecOps) también pueden utilizar los informes de inteligencia sobre amenazas para ayudarse a reconocer patrones y tener visibilidad de las amenazas emergentes.

4

Fortalezca la resiliencia conociendo su superficie de ataque y practicando IR. Comprenda su exposición a los ataques más relevantes para su industria y organización, y priorice su estrategia de seguridad en consecuencia. Las herramientas como ASM o técnicas como la simulación de adversarios pueden ayudar a que las organizaciones obtengan una perspectiva fundamentada en los atacantes y aprovecharla para incorporarla en su perfil y vulnerabilidades particulares, que incluyen las vulnerabilidades que se pueden explotar fácilmente.

Además, se ha demostrado que contar con un equipo que ya esté versado en los protocolos y herramientas adecuados para responder a un incidente reduce significativamente los costos y el tiempo para identificar y contener la filtración. La planificación y pruebas de RI no solo resultaron ser uno de los 3 principales mitigadores de costos que arrojó el informe de 2023, sino que los datos también demostraron que las organizaciones que utilizaron en gran medida estas tácticas defensivas redujeron sus costos de filtración en USD 1,49 millones en comparación con las organizaciones que las utilizaron poco o no las utilizaron en absoluto, y resolvieron incidentes 54 días más rápido. Forme un equipo especializado en RI, elabore guías de referencia sobre RI y pruebe regularmente los planes de RI en ejercicios de simulación, tal como en un entorno cibernético controlado. Contar con un proveedor de RI bajo una iguala puede ayudar a acelerar el tiempo para responder a una filtración.

Por último, las organizaciones deben buscar implementar prácticas de segmentación de redes para limitar la propagación de los ataques y la magnitud de los daños que pueden causar, reforzando la resiliencia general y reduciendo los esfuerzos de recuperación.

Las recomendaciones de prácticas de seguridad tienen fines informativos y no garantizan resultados.

04

Acerca de Ponemon Institute e IBM® Security

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

Ponemon Institute mantiene estrictas normas de confidencialidad de datos, privacidad y ética en la investigación y no recopila ninguna información de identificación personal (PII) de individuos ni información identificable de empresas en la investigación empresarial. Asimismo, las estrictas normas de calidad garantizan que no se planteen preguntas extrañas, irrelevantes ni inadecuadas.

IBM® Security
IBM® Security ayuda a proteger a las empresas y gobiernos más grandes del mundo con una cartera integrada de productos y servicios de seguridad infundidos con capacidades dinámicas de IA de seguridad y automatización. Esta cartera, respaldada por la mundialmente reconocida investigación de IBM® Security X-Force, permite que las organizaciones prevean amenazas, protejan los datos a medida que se mueven y respondan con velocidad y precisión sin contener la innovación empresarial. Miles de organizaciones confían en IBM como su socio para evaluar, elaborar estrategias, implementar y gestionar transformaciones de seguridad.

IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo; supervisa más de 150 mil millones de eventos de seguridad cada día en más de 130 países; y se le han concedido más de 10.000 patentes de seguridad en todo el mundo.

Si tiene preguntas o comentarios sobre este informe de investigación, incluso si quiere solicitar autorización para citarlo o reproducirlo, no dude en ponerse en contacto por carta, teléfono o correo electrónico:

Ponemon Institute LLC
A/A: Research Department
2308 US 31 North
Traverse City
Michigan 49686 EE. UU.
+1.800.887.3118
research@ponemon.org

Obtenga más información sobre cómo mejorar su postura de seguridad

Visite ibm.com/security.

Únase a la conversación en la Comunidad de IBM Security.

Dé los siguientes pasos

Soluciones de IA para ciberseguridad
Acelere los tiempos de respuesta de seguridad e impulse la productividad.
Más información

Soluciones de detección y respuesta a amenazas
Capacite a los equipos de seguridad para que superen las amenazas con velocidad, precisión y eficiencia.
Más información

Soluciones de seguridad en la nube
Integre la seguridad en su camino a la multinube híbrida.
Más información

Soluciones contra el ransomware
Gestione los riesgos y vulnerabilidades de ciberseguridad para minimizar el impacto del ransomware.
Más información

Soluciones de gestión de identidades y acceso
Conecte a cada usuario, API y dispositivo con cada aplicación de forma segura.
Más información

Servicios de respuesta a incidentes y detección de amenazas
Gestione y responda de forma proactiva a las amenazas de seguridad.
Más información

Soluciones de seguridad y protección de datos
Proteja los datos y simplifique el cumplimiento normativo en nubes híbridas.
Más información

Gestión de la superficie de ataque
Gestione la expansión de su espacio digital y mejore la resiliencia cibernética de su organización rápidamente.
Más información

Soluciones de gestión unificada de endpoints
Amplíe su fuerza laboral móvil protegiendo y gestionando cualquier dispositivo.
Más información

Servicios de gobernanza, riesgo y cumplimiento
Aumente la madurez de la ciberseguridad con un enfoque integrado de gobernanza, riesgo y cumplimiento.
Más información

Programe una consulta individual
Reúnase con un experto de IBM Security X-Force para hablar sobre sus necesidades.
Más información

Solicite un taller sobre detección y estructura de IBM® Security
Obtenga ayuda para modernizar su programa de seguridad.
Más información

Alfonso Nápoles Gandara 3111
Col. Parque corporativo de Peña Blanca
C.P. 01210
México D.F.
IBM Corporation
New Orchard Road
Armonk, NY 10504

Producido en los
Estados Unidos de América
Julio de 2023

Este documento está vigente a partir de la fecha inicial de publicación, pero IBM puede modificarlo en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

Todos los ejemplos de clientes citados o descritos se presentan como ilustración de la forma en que algunos clientes han utilizado los productos de IBM y los resultados que pueden haber obtenido. Los costos medioambientales y las características de rendimiento reales variarán en función de las configuraciones y condiciones de cada cliente. No es posible garantizar resultados esperados, puesto que los resultados de cada cliente dependerán por completo de los sistemas y servicios solicitados por este. LA INFORMACIÓN INCLUIDA EN ESTE DOCUMENTO SE PROPORCIONA “TAL CUAL” SIN NINGUNA GARANTÍA, EXPRESA O IMPLÍCITA, INCLUSO SIN NINGUNA GARANTÍA DE COMERCIABILIDAD, IDONEIDAD PARA UN PROPÓSITO PARTICULAR NI GARANTÍA O CONDICIÓN DE NO INFRACCIÓN. Los productos de IBM están amparados de acuerdo con los términos y condiciones de los acuerdos bajo los cuales se proveen.

Declaración de buenas prácticas de seguridad: la seguridad del sistema de TI implica proteger los sistemas y la información a través de la prevención, detección y respuesta al acceso indebido dentro y fuera de su empresa. El acceso no autorizado puede resultar en la alteración, destrucción, apropiación indebida o mal uso de la información o puede derivar en daños o mal uso de sus sistemas, incluso para su uso en ataques a otros. Ningún sistema o producto de TI debe considerarse completamente seguro y ningún producto, servicio o medida de seguridad por sí solo puede ser completamente eficaz para prevenir el uso o acceso no autorizado. Los sistemas, productos y servicios de IBM están diseñados para ser parte de un enfoque de seguridad legal e integral, que necesariamente implicará procedimientos operativos adicionales y pueden requerir otros sistemas, productos o servicios para ser más eficaces. IBM NO GARANTIZA QUE LOS SISTEMAS, PRODUCTOS O SERVICIOS SEAN INMUNES A LA CONDUCTA MALICIOSA O ILEGAL DE CUALQUIER PARTE, O QUE SU EMPRESA SEA INMUNE A DICHAS CONDUCTAS.

El cliente es responsable de garantizar el cumplimiento de las leyes y regulaciones que le sean aplicables. IBM no brinda asesoría legal ni representa ni garantiza que sus servicios o productos asegurarán que el cliente cumpla con las leyes o regulaciones. Las declaraciones sobre la dirección e intención futuras de IBM están sujetas a cambios o eliminaciones sin previo aviso, y representan solo metas y objetivos.