

ESTUDIO SOBRE EL IMPACTO DE LA SEGURIDAD DE API DE 2024

Sector de los seguros

Los incidentes relacionados con las API aumentan. Descubra cómo el sector de los seguros está afrontando este importante problema de seguridad y qué puede hacer su organización para mantenerse a salvo.

Cuando se produce un incidente, desde un accidente en coche hasta daños que afectan al equipamiento empresarial, los titulares de las pólizas confían en los servicios digitales para abrir partes y recibir asistencia de sus proveedores de seguros. Para tramitar estos servicios, las API de las compañías de seguros deben gestionar información confidencial que representa la historia de la vida de un asegurado, contada en forma de datos.

En un sector en el que la confianza de los clientes resulta esencial, las compañías de seguros se enfrentan a un desafío de seguridad cada vez mayor: las vulnerabilidades de las API.

Según la exhaustiva encuesta de Akamai, el 76,7 % de los profesionales de los seguros han informado de incidentes relacionados con la seguridad de las API en los últimos 12 meses. Sin duda, el efecto en las finanzas resulta considerable, ya que las empresas de seguros gastan una media de 625 634 \$ en solucionar esos incidentes solo en Estados Unidos.

Pero quizás lo más preocupante son los efectos en las empresas: la "pérdida de la confianza de los clientes y pérdida de cuentas" (28 %) es la principal preocupación entre las compañías de seguros tras los incidentes en las API. En un mercado competitivo en el que los clientes pueden cambiar fácilmente de proveedor, este daño a la reputación puede tener efectos a largo plazo que van más allá de los costes inmediatos.

Siga leyendo para obtener información sobre el sector en el [Estudio sobre el impacto de la seguridad de API de 2024](#).

A pesar de que aumenta el número de ataques, la visibilidad sigue representando un gran problema

El coste financiero de los ataques a las API es considerable en el caso de las compañías de seguros, con costes en los Estados Unidos que alcanzan los 625 634 \$, y que superan la media del sector, que asciende a 591 404 \$. ¿Cuáles son las causas de estos incidentes?

Según los equipos de seguridad del sector de los seguros, entre las causas principales se encuentran:

1. API no gestionadas, como API inactivas o "zombis" (22 %).
2. API con exposición no intencionada a Internet (21,3 %).
3. Herramientas tradicionales que se utilizan para proteger las API y no son capaces de detectar las amenazas (20 %).
4. Vulnerabilidades de autorización (19,3 %).
5. Configuraciones incorrectas de API (18,7 %).

Muchas organizaciones son conscientes de las causas de los ataques que sufren sus API, pero no disfrutan de la visibilidad de un indicador de riesgo esencial: la capacidad de una API para devolver datos confidenciales cuando se la llama. Aunque el 56,7 % de las empresas de seguros afirman contar con un inventario completo de sus API (por debajo de la media del 69,7 % de todo el sector), solo el 20,7 % pueden identificar a las API que devuelven datos confidenciales.

Esta falta de visibilidad tiene importantes repercusiones en cuanto al cumplimiento de normativas y la seguridad, en un sector en el que se procesan datos personales y financieros muy regulados.



El **76,7 %** de las empresas de seguros han sufrido incidentes de las API en los últimos 12 meses.

Solo el **20,7 %** de las empresas de seguros tienen inventarios de API completos para saber qué API devuelven datos confidenciales.

625 634 \$ es el impacto financiero que han representado los incidentes de seguridad de las API para las empresas de seguros en los últimos 12 meses.

3 consecuencias principales

1. **Pérdida de la confianza de los clientes y pérdida de cuentas (28 %)**
2. **Daños a la reputación del departamento ante los altos puestos (25,3 %).**
3. **Costes asumidos para solucionar los problemas (24,7 %).**

Fuente:
Akamai, [Estudio sobre el impacto de la seguridad de API de 2024](#)



Hemos observado **varias tendencias** que dificultan la protección de las API:

- **Proliferación continua de API:** Con cada una de las iniciativas digitales, las API se multiplican y evolucionan constantemente, lo que dificulta el poder contar con un inventario preciso.
- **Una gran variedad de estándares:** Muchas aseguradoras cuentan con varios equipos de desarrollo que trabajan de forma autónoma en las distintas unidades de negocio sin utilizar una estrategia unificada para favorecer un diseño seguro.
- **Riesgos que pasan desapercibidos:** Las API transmiten datos confidenciales de los asegurados, pero la mayoría de las organizaciones no pueden identificar qué API concretas son las que devuelven información confidencial.

Piense en lo que puede suceder con una API que implemente un departamento sin una supervisión adecuada por parte de un equipo de seguridad. Tal vez la API se haya diseñado con el objetivo de compartir registros, pero sin los controles adecuados, o que se haya dejado activa después de llevar a cabo actualizaciones en el sistema, lo que podría haber dejado expuestos los datos confidenciales de los clientes en algunos lugares.

Impacto de los incidentes de API en el cumplimiento, la confianza del cliente y el estrés del equipo

No es de extrañar que las empresas de seguros son plenamente conscientes de las consecuencias financieras que tienen las amenazas de las API. En nuestra encuesta, solicitamos a los encuestados que divulgaran los costes estimados de los incidentes de seguridad de las API que han experimentado en los últimos 12 meses:

	Sector de los seguros	Media de todos los sectores
 Estados Unidos	625 633,70 \$	591 404,01 \$
 Reino Unido	493 000,50 £	420 103,18 £
 Alemania	373 918,72 €	403 453,26 €

Si bien las repercusiones financieras son significativas, los participantes del estudio afirmaron con rotundidad que del análisis de los costes se puede deducir una combinación de inquietudes relativas a los ingresos y la reputación. Cuando se les pidió que enumeraran el impacto principal del incidente de seguridad de API que hubieran experimentado:

- El 28 % mencionó "la pérdida de la confianza de los clientes y la pérdida de cuentas".
- El 25,3 % mencionó "los daños a la reputación del equipo ante los altos puestos y la junta directiva".
- El 24,7 % mencionó los "costes asumidos para solucionar los problemas".

Reducción del riesgo y el estrés mediante la seguridad proactiva de API

Los ataques a las API dirigidos a empresas de seguros están aumentando de alcance, escala, sofisticación y coste. Esto incluye los ataques de bots impulsados por IA generativa, que se adaptan rápidamente para eludir las herramientas de seguridad de API tradicionales y otras defensas perimetrales. Muchos equipos de seguridad de su sector están experimentando estas amenazas de primera mano y padecen las consecuencias, tanto en términos financieros como humanos. Con todo, incluso cuando las organizaciones comprenden la importancia de las amenazas de API, se plantean la siguiente pregunta: ¿Qué podemos hacer?

Tomar medidas ya para proteger mejor sus API, así como los datos que intercambian, puede permitir a su organización proteger sus ingresos y aliviar la carga de los equipos de seguridad; todo ello al tiempo que se mantiene la confianza que tanto les ha costado ganarse de las juntas directivas y los clientes. Entre estos pasos se incluye el desarrollo de los conocimientos de su equipo sobre las amenazas de API avanzadas y las capacidades necesarias para defenderse ante ellas.



Para leer el informe completo y obtener más información sobre las prácticas recomendadas en materia de visibilidad y protección de API, descargue el **Estudio sobre el impacto de la seguridad de API de 2024**.

¿Todo listo para hablar sobre sus retos y descubrir cómo puede ayudarle Akamai?

Solicite una demostración personalizada de la solución Akamai API Security

Akamai ofrece soluciones diseñadas para ayudar a las organizaciones a reducir los riesgos relacionados con las amenazas que se tratan en este artículo:

- **Akamai API Security:** Detecta las API, comprende su situación de riesgo, analiza sus comportamientos y evita que las amenazas se infiltren en su empresa.
- **Akamai Account Protector:** Ayuda a prevenir el abuso en la apertura de cuentas mediante la supervisión del comportamiento de los usuarios en tiempo real y la adaptación a los perfiles de riesgo cambiantes.



La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Aprovechando la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en [X](#), antes conocido como Twitter, y [LinkedIn](#). Publicado el 25 de mayo.