ESTUDIO SOBRE EL IMPACTO DE LA SEGURIDAD DE API DE 2024

Sector de servicios financieros

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

El año pasado, el 88,7 % de las empresas de servicios financieros sufrieron un ataque a las API que gestionan sus datos y conectan a clientes y partners con servicios esenciales. Mediante el uso de métodos cada vez más innovadores, los atacantes pueden acceder a los datos de las API desprotegidas para robar información personal y financiera, como los saldos de las cuentas y los historiales de transacciones.

Los equipos de seguridad están al tanto de estos ataques y sus consecuencias, por lo que buscan constantemente formas de mejorar la protección. Afrontar otro vector de ataque puede antojarse desalentador, especialmente en el caso de las API, cuya mala configuración o cuyos fallos en la lógica empresarial pueden descubrirse y explotarse con facilidad.

¿Cómo disponemos de esta información? Akamai ha encuestado a más de 1200 profesionales de TI y seguridad, desde directores de seguridad de la información hasta personal de seguridad de las aplicaciones, para conocer sus experiencias con las amenazas relacionadas con las API.

En esta publicación, hemos filtrado nuestros resultados para los encuestados pertenecientes al sector de los servicios financieros, que afirmaron que las principales consecuencias de sus incidentes de seguridad de API fueron las "sanciones por parte de los reguladores" y el "aumento del estrés o la presión para mi equipo o departamento". Estas repercusiones interrelacionadas se entienden fácilmente, dado que sus homólogos han estimado el coste de afrontar los incidentes de las API en 832 800 dólares, un 40 % más que el promedio de los ocho sectores encuestados y la mayor cifra en comparación con cualquier otro sector.

Siga leyendo para obtener información sobre el sector en el Estudio sobre el impacto de la seguridad de API de 2024.

La visibilidad disminuye conforme aumentan los ataques

Aunque el 84 % de las organizaciones de todos los sectores sufrieron incidentes de seguridad de API, las empresas de servicios financieros fueron objeto de ataques con más frecuencia que la media, con un 88,7 %. Sus homólogos identificaron dos vulnerabilidades clave que impulsaron estos ataques: los firewalls de red que no detectan las amenazas (26,5 %) y las vulnerabilidades dentro de las API en herramientas de IA generativa, como los modelos de lenguaje de gran tamaño (LLM) (23,2 %).

A pesar de las crecientes pruebas de amenazas a las API, desde incidentes frecuentes hasta altos costes de corrección y multas normativas, nuestros resultados sugieren que muchos equipos de servicios financieros aún no han priorizado la seguridad de las API. De hecho, la seguridad de API ocupa el noveno lugar entre las prioridades de ciberseguridad para el próximo año, con un 18,5 %.

La distinción entre actividad de API genuina y maliciosa o fraudulenta sigue siendo un reto para el sector financiero, especialmente cuando se trata de tener visibilidad de los muchos riesgos de las API. Si bien el 73,5 % de sus homólogos afirma que tiene un inventario completo de sus API, solo el 28,5 % de este subconjunto sabe cuáles devuelven datos confidenciales, lo que incluye información de identificación personal (PII) y datos que abarcan desde los historiales de crédito de los titulares de tarjetas hasta los registros financieros de los grandes clientes de banca comercial.

88,7 % de las empresas de servicios financieros sufrió algún incidente de seguridad de API en los últimos 12 meses

Tan solo el 28,5 % de las empresas de servicios financieros con inventarios de API completos saben cuáles devuelven datos confidenciales

832 800 USD = impacto financiero medio de un incidente de seguridad de API para las empresas de servicios financieros en los últimos 12 meses

3 consecuencias principales

1. **Aumento del estrés** o la presión para el equipo de seguridad
2. **Sanciones** por parte de los reguladores
3. **Pérdida de la confianza** y la reputación

Fuente:
Akamai, "Estudio sobre el impacto de la seguridad de API", 2024

Akamai

Piense en lo que puede suceder con una API en la sombra que implemente un departamento o una filial de un proveedor de servicios financieros sin colaboración ni supervisión por parte de los equipos centrales de seguridad o TI de la empresa. Esta API podría:

- Haberse creado para devolver datos de transacciones de clientes sin unos controles de autorización adecuados y sin las pruebas oportunas para detectar errores de configuración.
- Haberse sustituido por una nueva versión sin desactivarse previamente la anterior, la cual sigue expuesta a Internet.
- Haber pasado desapercibida ante las herramientas tradicionales, que no pueden detectar las API no administradas.
- Haberse visto explotada por ciberdelincuentes que acceden a cuentas de clientes reales para robar sus activos.

Esto no es una mera hipótesis. Según el estudio True Cost of Fraud™ (El verdadero coste del fraude) de 2023 de LexisNexis® Risk Solutions, el 50 % de las pérdidas por fraude pueden atribuirse al abuso en la apertura de nuevas cuentas, para lo cual los estafadores abusan de las API con el propósito de abrir cuentas a gran escala. Además, nuestro escenario refleja lo que los equipos de TI y seguridad reales citan como las principales causas de sus incidentes de API.

Impacto de los incidentes de API en el cumplimiento, los costes empresariales y el estrés del equipo

El informe Gartner® Market Guide for API Protection* de mayo de 2024 expone lo siguiente: "Según datos actuales, se estima que cada vez que se vulnera una API, se filtran de media 10 veces más datos confidenciales que con cualquier otro tipo de incidente". No es de extrañar que la normativa PCI DSS v4.0, ampliamente seguida, haya añadido requisitos en torno a la seguridad de las API. El estándar ahora requiere que las organizaciones validen su código de API antes de su lanzamiento, realicen pruebas periódicas para detectar vulnerabilidades y confirmen el uso seguro de los componentes basados en API, algo especialmente importante en un sector en el que las API facilitan millones de transacciones financieras a diario.

La pérdida de la confianza de los reguladores puede resultar en un mayor escrutinio, lo que a su vez supondría más trabajo para los equipos, que ya atraviesan dificultades para satisfacer las exigencias en materia de cumplimiento. Además, esto podría acarrear la imposición de multas cuantiosas.

Teniendo estos datos en cuenta, no cabe duda de que las empresas de servicios financieros son plenamente conscientes de las consecuencias de las amenazas de API. Por primera vez, solicitamos a los encuestados de los tres países participantes que divulgaran el impacto financiero estimado de los incidentes de seguridad de las API que han experimentado en los últimos 12 meses.

	Sector de servicios financieros	Media de todos los sectores
EE. UU.	832 800 USD	591 404 USD
Reino Unido	297 189 GBP	420 103 GBP
Alemania	604 405 EUR	403 453 EUR

P3. Si ha sufrido algún incidente de seguridad de API, ¿cuál ha sido el impacto financiero total estimado de estos incidentes combinados? Incluya todos los costes relacionados, como reparaciones del sistema, tiempo de inactividad, honorarios legales, multas y cualquier otro gasto asociado.

* Gartner, Market Guide for API Protection, 29 de mayo de 2024. GARTNER es una marca comercial registrada y una marca de servicio de Gartner, Inc. o sus filiales en EE. UU. y otros países, y se usa aquí con permiso. Todos los derechos reservados.

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

Los ataques a las API dirigidos a empresas de servicios financieros están aumentando en 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. Estos pasos, junto con el desarrollo de los conocimientos de su equipo sobre las amenazas de API avanzadas y las capacidades necesarias para defenderse ante ellas, pueden contribuir a preservar la confianza que tanto ha costado ganarse de las juntas directivas y los clientes.

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, que detecta las API, comprende su situación de riesgo, analiza sus comportamientos y evita que las amenazas se infiltren en su empresa.
- Akamai Account Protector, que previene 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.

Akamai

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 en marzo de 2025.