ESTUDIO SOBRE EL IMPACTO DE LA SEGURIDAD DE API 2024

Cómo le afectan los incidentes relacionados con las API a usted y a su equipo

Akamai

Una publicación afiliada a los
informes sobre el estado de Internet (SOTI) de Akamai

Contenido

Resumen ejecutivo

Para esta tercera edición del estudio sobre el impacto que tienen las API en la seguridad (conocido anteriormente como el informe "API Security Disconnect") se encuestaron 1207 expertos y responsables de EE. UU., Reino Unido y (nuevo en 2024) Alemania. El estudio examina cómo experimentan las empresas los eventos de seguridad de API (su frecuencia, causas e impactos) y cómo abordan los departamentos de seguridad las API como vector de ataque.

Para obtener una visión más completa, hemos realizado una encuesta a un grupo representativo de:

- directores de seguridad de la información (CISO), directores de TI (CIO), directores de tecnología (CTO), profesionales sénior de la seguridad y miembros del equipo de seguridad de las aplicaciones de organizaciones de menos de 500 a más de 1000 personas;
- ocho sectores: servicios financieros, e-commerce y retail, atención sanitaria, sector gubernamental y público, fabricación, energía y servicios públicos, y (nuevo en 2024) automoción y seguros

Introducción

A menudo, las API se consideran un vector de ataque *emergente*, incluso habiendo datos que demuestran que los ataques contra esas API son frecuentes y muy perjudiciales. Tenga en cuenta estas estadísticas:

- De enero de 2023 a junio de 2024 se registraron 108 000 millones de ataques a API, según un reciente informe sobre el estado de Internet (SOTI) de Akamai.
- Así lo expone el informe Gartner® Market Guide for API Protection de mayo de 2024*: "Según datos actuales, se estima que cada vez que se ataca una API, se filtran de media 10 veces más datos confidenciales que con cualquier otro tipo de vulneración".
- Los ataques también están aumentando. El informe SOTI también afirma que los ataques a API y aplicaciones web aumentaron conjuntamente un 49 % entre el primer trimestre de 2023 y el de 2024.

Muchas API no están lo suficientemente protegidas, lo que las convierte en un vector de ataque atractivo y rentable para los ciberdelincuentes.

Estos aumentos no son ninguna sorpresa. Entre bastidores, las API facilitan la comunicación y el intercambio de datos entre casi todas las tecnologías que impulsan sus iniciativas digitales: herramientas de IA generativa, aplicaciones que interactúan con los clientes, servicios en la nube y muchas otras más. Sin embargo, muchas API no están lo suficientemente protegidas, ya sea porque se han creado sin autenticación, tienen errores de configuración o están totalmente olvidadas, lo que las convierte en un vector de ataque atractivo y rentable para los ciberdelincuentes. Solo necesitan encontrar una API vulnerable y, *zas*, obtienen acceso directo a todos los datos que transfiere cuando recibe una llamada, que pueden ser miles de registros.

En un nivel general, nuestra investigación demostró que la seguridad de API aún no se ha convertido en un elemento clave en el marco de una estrategia de seguridad integral. Las empresas suelen tratar las amenazas a las API como un problema emergente, a pesar de que los datos de los ataques, así como el impacto financiero y la carga que suponen para los equipos y que se detectaron en nuestro estudio, demostraron que cada vez son más numerosos y que, a menudo, se llevan a cabo con éxito. Nuestros resultados de 2024 ofrecen una visión de cómo afectan los incidentes de seguridad de API a sus homólogos y a sus organizaciones. Esperamos que estos datos le ayuden a posicionar a su propio equipo para que pueda evaluar mejor sus medidas para proteger a las API y reforzar sus puntos débiles.

Conclusiones a nivel general: Los incidentes relacionados con las API afectan a los equipos empresariales y los estresan

Los resultados de nuestro estudio de 2024 demostraron que las API son un vector de ataque que está creciendo y creando considerables dificultades en materia de seguridad para los equipos. Nuestros encuestados mostraron un consenso significativo sobre lo siguiente:

- Observan que los incidentes de seguridad de API han aumentado durante tres años consecutivos.
- Gastan más de medio millón de dólares de media para gestionar los incidentes relacionados con las API y recuperarse de ellos (según los encuestados que son directivos de EE. UU., el impacto financiero medio es de 943 162 dólares).
- Sienten el coste humano que llevan aparejados los incidentes relacionados con las API, por el impacto del estrés y el daño a la reputación que sufren sus equipos (especialmente el escrutinio interno que amplifica esta presión); el coste humano es aún más importante que los costes de reparación de los incidentes.

Los encuestados ofrecieron puntos de vista mixtos sobre la integridad de sus inventarios de API, y esta variabilidad fue aún más pronunciada cuando se desglosó por cargo (consulte la página 11). Sorprendentemente, es menor el número de empresas con inventarios de API completos que también saben cuáles transfieren datos confidenciales. Esta cifra, ya de por sí baja en 2023, ha pasado del 40 % a tan solo el 27 % en 2024.

Los encuestados también indicaron que las herramientas tradicionales en las que han confiado para proteger las API no cubren completamente todos los riesgos. Esas herramientas, como los firewalls de aplicaciones web (WAF), las puertas de enlace de API y los firewalls de red, son a menudo las primeras en ser señaladas como culpables cuando un ataque se lleva a cabo con éxito (consulte la lista completa de causas en la página 17 y una nota sobre WAF y WAAP en la página 12).

Los profesionales de la seguridad sienten el coste humano que llevan aparejados los incidentes relacionados con las API, por el impacto del estrés y el daño a la reputación que sufren sus equipos; el coste humano tiene una importancia aún mayor que los costes de reparación de los incidentes.

Los resultados de nuestro estudio también nos permiten deducir algunos de los motivos principales por los que las estrategias de seguridad de API aún no se han priorizado más, a pesar de las pruebas que evidencian que merecen mucha más atención. Uno de los factores clave es que los cargos de seguridad clave no se ponen de acuerdo en cuanto al número, la ubicación y los atributos de riesgo de las API que necesitan protección, probablemente debido a la escasa visibilidad de las API y a que falta una única fuente de información fiable.

También observamos una falta de consenso entre los expertos y los responsables de seguridad en cuanto a las causas de los ataques a las API. ¿Se deben a las herramientas que utilizan, los errores que cometieron sus codificadores en el proceso de desarrollo o los ataques a defectos en las innovaciones de IA generativa? Depende de a quién se le pregunte.

Por supuesto, el otro motivo por el que la seguridad de API no ha adquirido mayor importancia estratégica es que los equipos ya están más que apretados para cubrir otras amenazas apremiantes, las cuales probablemente también estén recibiendo la mayor parte del presupuesto, la atención del equipo y el esfuerzo. Profundicemos en los resultados.

Estudio del impacto de la seguridad de API: 2024
Resumen de conclusiones clave

84 % Porcentaje de encuestados que sufrió algún incidente de seguridad de API en los últimos 12 meses

Coste medio para gestionar los incidentes relacionados con las API en los últimos 12 meses:

EE. UU.	Reino Unido	Alemania
591 404 $	420 103 £	403 453 €

Baja visibilidad

Tan solo el 27 % de las empresas con inventarios de API completos conocen cuáles transfieren datos confidenciales, en comparación con el 40 % en 2023.

Nivel de estrés alto

Impacto n. 1 de los incidentes relacionados con las API *CISO*: Daños a la reputación de nuestro departamento ante los altos puestos y la junta directiva. *CIO*: Aumento del estrés o la presión para mi equipo o departamento.

Pruebas escasas

Solo el 13 % y el 18 % de los encuestados prueban sus API en tiempo real y a diario, respectivamente, desde la fase de desarrollo hasta el entorno de producción.

El coste financiero de los incidentes de seguridad de API agrava el impacto en los equipos y sus responsables. Las costosas vulneraciones de seguridad atraen el escrutinio y pueden hacer pensar a las partes interesadas influyentes, como la junta directiva, que los equipos no están haciendo su trabajo correctamente. Eso es muy estresante. De hecho, los participantes de todas las regiones mencionaron el estrés en sus equipos como el principal impacto de un incidente de seguridad de API.

El estado actual de la seguridad de API

Durante los últimos tres años, el número de organizaciones que afirman haber sufrido incidentes de seguridad de API ha aumentado constantemente, alcanzando un máximo de 84 % en 2024 (véase a continuación). ¿Cómo afectan estos ataques a las API a las organizaciones? ¿Qué es lo que están haciendo, o no están haciendo aún, para reducir el riesgo que corren? Hemos estructurado nuestros resultados como respuestas a estas preguntas.

¿Los ataques de API están teniendo un impacto significativo en las organizaciones y sus equipos de seguridad?

La respuesta corta es que sí. Este ha sido el primer año que recopilamos datos sobre el impacto financiero de un incidente de seguridad de API y ha resultado ser significativo: el coste medio que conlleva corregir incidentes relacionados con las API (incluidos el tiempo de inactividad, las reparaciones del sistema, los honorarios legales, las sanciones y cualquier otro gasto asociado) para el 84 % de las organizaciones que los han experimentado en los últimos 12 meses fue de:

- **591 404 $** en EE. UU.
- **420 103 £** en el Reino Unido
- **403 453 €** en Alemania

Algunos cargos indicaron que los costes eran mucho más altos, especialmente los encuestados que son directivos de EE. UU., que afirmaron que ascienden a un total de 943 162 $, casi un 60 % más que la media del total de encuestados de EE. UU.

¿Ha sufrido algún incidente de seguridad de API en los últimos 12 meses?

Año	Total	EE. UU.	Reino Unido	Alemania
2022	76 %	75 %	77 %	—
2023	78 %	85 %	69 %	—
2024	84 %	83 %	83 %	84 %

Independientemente del número exacto, el coste financiero de los incidentes de seguridad de API agrava el coste humano. Las costosas vulneraciones de seguridad atraen el escrutinio y pueden hacer pensar a las partes interesadas influyentes, como la junta directiva, que los equipos no están haciendo su trabajo correctamente. Eso es muy estresante. De hecho, los participantes de todas las zonas geográficas mencionaron el "estrés" (en concreto, el estrés en sus equipos) como el principal impacto de un incidente de seguridad de API, seguido de "daños a la reputación de nuestro departamento ante los altos puestos y la junta directiva" y los "costes de reparación" en tercer lugar. Notablemente, los impactos internos que más afectan a la moral reaparecen y dominan los tres impactos inferiores, que están casi empatados (véase a continuación).

Los resultados fueron similares cuando se desglosaron por sector: El "aumento del estrés o la presión para el equipo después de una vulneración de API" también fue el principal impacto en cuatro de los ocho sectores encuestados (consulte el cuadro de la página 9). Esto incluye al sector de los servicios financieros, que registraron el mayor impacto económico de todos los sectores, con 832 801 dólares.

Impactos más citados de los incidentes de seguridad de API

1. Aumento del estrés o la presión para el equipo o departamento: **27,0 %**
2. Daños a la reputación de nuestro departamento ante los altos puestos y la junta directiva: **26,6 %**
3. Costes para intentar solucionar el problema **25,8 %**
4. Sanciones por parte de los reguladores: **25,4 %**
5. Pérdida de la confianza de los clientes y pérdida de cuentas: **25,0 %**
6. Pérdida de productividad: **24,1 %**
7. Pérdida de la confianza y la reputación: **23,8 %**
8. Pérdida de la confianza de los empleados: **23,8 %**
9. Mayor escrutinio interno de nuestro equipo o departamento por parte de la empresa: **23,5 %**

Información basada en la pregunta: ¿Qué costes o impactos han tenido en su empresa los incidentes de seguridad de API? (Seleccione un máximo de 3); n=1207

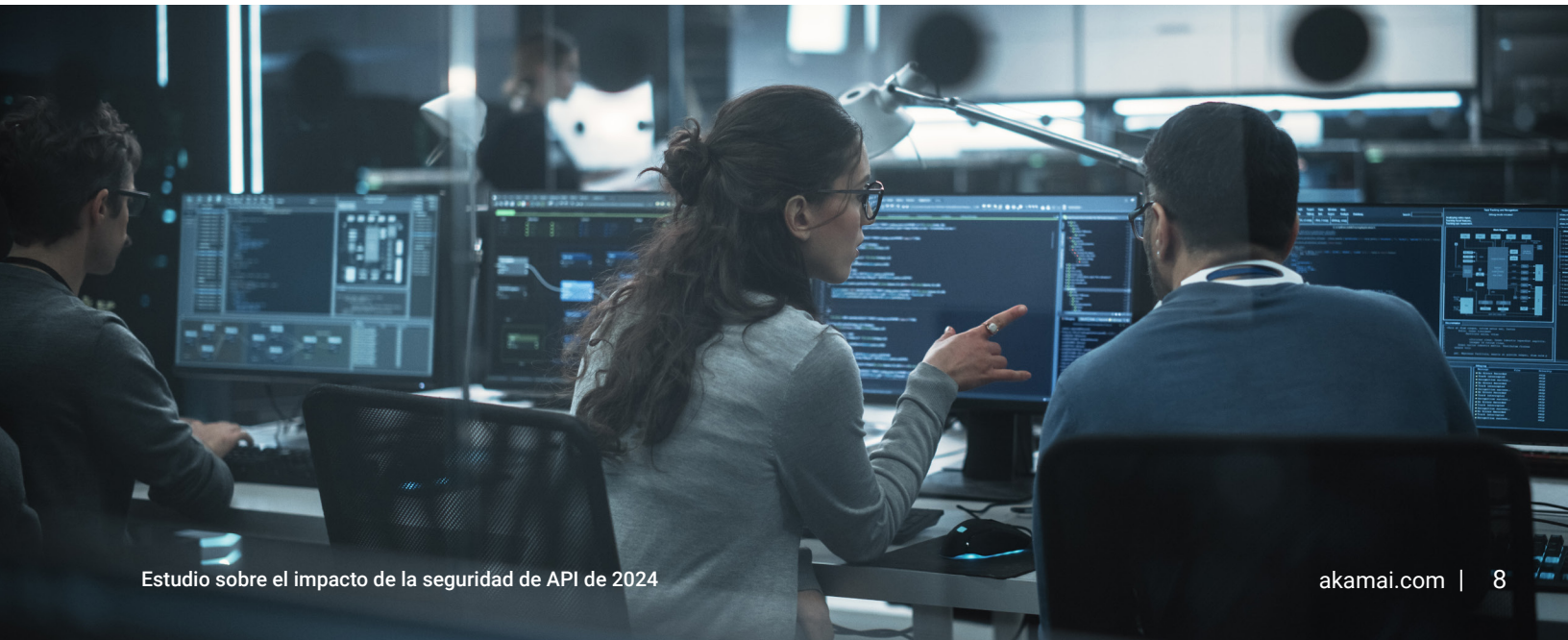
La relación entre los costes financieros y humanos de los ataques de API también quedó clara en las respuestas de los responsables de TI y seguridad sobre los impactos de los incidentes (se permitió a cada encuestado elegir hasta tres). En general, todos los cargos de todas las regiones creen que los incidentes de seguridad de API afectan especialmente al personal.

- Los dos impactos principales para los directores de seguridad de la información (CISO), que son "los daños a la reputación de nuestro departamento ante los altos puestos y la junta directiva" y "la pérdida de la confianza de los clientes y la pérdida de cuentas", revelaron un empate exacto entre el impacto a nivel humano y a nivel financiero, con un 31 %.
- Del mismo modo, los principales impactos para los directores de TI mostraron un empate entre el "aumento del estrés o la presión para mi equipo o departamento" y los "costes de reparación", con un 34 %.

Estos resultados tienen sentido para los directores de seguridad de la información y los directores de TI: ¿y si los equipos a los que dirigen siguen estando desbordados por los incidentes de seguridad que crean malas condiciones laborales, disparan los presupuestos e incomodan a los clientes? Estos líderes no quieren que el talento de calidad se vaya o que la reputación de su departamento se desplome. Si a esto le sumamos las presiones financieras, como los costes de corrección o el abandono de los clientes, el estrés sobre los directores de seguridad de la información y los directores de TI aumenta considerablemente. De hecho, la "pérdida de la confianza de los clientes y la pérdida de cuentas" fue el principal impacto de un incidente de seguridad de API para los encuestados de los sectores de seguros y automoción (consulte el cuadro de la página siguiente para obtener más resultados por sectores).

Las respuestas principales para los cargos restantes fueron las siguientes:

- Director de tecnología, 30 %: "Pérdida de la confianza de los empleados»
- Profesional sénior de seguridad, 27 %: "Daños a la reputación de nuestro departamento ante nuestros altos puestos y la junta directiva"
- El equipo de seguridad de las aplicaciones, 31 %: "Aumento del estrés o la presión para mi equipo o departamento"



Impactos más citados de los incidentes de seguridad de API por sector	
Automoción	Pérdida de la confianza de los clientes y pérdida de cuentas: **33 %**
Energía y servicios públicos	Daños a la reputación de nuestro departamento ante los altos puestos y la junta directiva: **36 %**
Servicios financieros	Empate: Aumento del estrés o la presión para mi equipo o departamento + sanciones normativas, ambos un **29 %**
Sector guberna-mental y público	Aumento del estrés o la presión para mi equipo o departamento: **29 %**
Atención sanitaria	Empate: Pérdida de la confianza y la reputación + pérdida de productividad: ambas un **29 %**
Seguros	Pérdida de la confianza de los clientes y pérdida de cuentas: **28 %**
Fabricación	Aumento del estrés o la presión para mi equipo o departamento: **34 %**
E-commerce y retail	Aumento del estrés o la presión para mi equipo o departamento: **29 %**

Información basada en la pregunta: ¿Qué costes o impactos han tenido en su empresa los incidentes de seguridad de API? (Seleccione un máximo de 3); n=1207

¿Hay una visibilidad adecuada de las API y los posibles riesgos?

No. Es más, en realidad ha empeorado. Este año, son menos los encuestados que tienen un inventario completo de sus API y también saben cuáles transfieren datos confidenciales. Esta cifra, ya de por sí baja en 2023, ha pasado del 40 % a tan solo el 27 % en 2024. (Este resultado podría tener un valor positivo si deducimos que más organizaciones están intentando tener un inventario completo, pero carecen de las herramientas necesarias para localizar cada API e identificar la actividad que se produce en cada una).

Son menos los encuestados que tienen un inventario completo de sus API y también saben cuáles transfieren datos confidenciales. Esta cifra, **ya de por sí baja en 2023, ha pasado del 40 %** a tan solo el **27 % en 2024**.

Estado actual de los inventarios de API y la concienciación, todos los encuestados

	2024	2023
Sí, **y sabemos** cuáles transfieren datos confidenciales	27 %	40 %
Sí, **pero no sabemos** cuáles transfieren datos confidenciales	43 %	32 %
Tenemos un inventario parcial de nuestras API **y sabemos** cuáles transfieren datos confidenciales	23 %	24 %
Tenemos un inventario parcial, **pero no sabemos** cuáles transfieren datos confidenciales	6 %	4 %
No, **no** tenemos ningún inventario	1 %	—

Información basada en la pregunta: ¿Tiene un inventario completo de sus API y sabe cuáles transfieren datos confidenciales? (Seleccione entre cinco opciones); n=1207

Si observamos a los líderes de los tres países y los ocho sectores encuestados, los directores de TI tienden a creer, en mayor medida con respecto a los directores de seguridad de la información, que sus organizaciones cuentan con inventarios de API completos. A nivel experto, tanto los profesionales sénior de seguridad como los miembros del equipo de seguridad de aplicaciones están en gran medida de acuerdo con la visión común los directores de TI de que hay un inventario completo de todas las API.

¿Cómo se comparan de media los cinco cargos en lo que se refiere a conocer (o no conocer) qué API transfieren datos confidenciales cuando reciben una llamada? La respuesta es importante, ya que muchas de estas llamadas provienen de fuentes maliciosas y tienen como objetivo aprovechar las vulnerabilidades comunes de las API.

Cuatro tipos de API no gestionadas que reciben ataques para acceder a los datos

1. Las **API en la sombra** (también conocidas como "API no documentadas") existen y operan fuera de los canales supervisados oficiales de una organización.
2. Las **API no aprobadas** son API maliciosas o no autorizadas que suponen un riesgo para la seguridad de un sistema o una red.
3. Las **API zombis** incluyen cualquier API que permanezca en ejecución incluso después de que se haya sustituido por nuevas versiones u otras API por completo.
4. Las **API obsoletas** son API que ya no se recomiendan para su uso debido a cambios en las mismas.

Estos resultados ofrecen algunas conclusiones curiosas sobre la visibilidad del riesgo de las API. La mayoría de los directores de seguridad de la información y los directores de tecnología respondieron que tenían un inventario completo *sin* saber qué API transfieren información confidencial (llamemos a esta circunstancia "conocimiento de datos confidenciales") o que tenían un inventario parcial *con* conocimiento de datos confidenciales.

La mayoría de los directores de TI afirmaron tener un inventario completo de API, y de esos directores de TI, el 42,9 % también contaba con un conocimiento completo de datos confidenciales, mientras que el 36,3 % afirmó que no tenía ese conocimiento. Los profesionales sénior de seguridad estaban de acuerdo con los directores de TI (el 75 % afirmó que tenía un inventario completo), pero se *invertía* la situación en lo que respecta al conocimiento de datos confidenciales: el 32,5 % de los profesionales sénior de seguridad afirmó que tenía conocimientos de datos confidenciales y el 42,5 % dijo que no lo tenía.

Por último, los miembros del personal de seguridad de las aplicaciones, probablemente los más prácticos de todos los encuestados, registraron la mayoría más amplia entre los cinco cargos. Casi la mitad afirmó tener un inventario completo sin conocimiento de datos confidenciales; la otra mitad se dividió aproximadamente entre:

- Inventario completo con pleno conocimiento de los datos confidenciales
- Inventario parcial con conocimiento completo de datos confidenciales de esas API

Podemos ver que la medición de los inventarios aún no se ha estandarizado lo suficiente como para producir un recuento de API de una sola fuente. Dada la variabilidad, también es probable que más empresas con inventarios completos *no* tengan conocimiento completo de datos confidenciales. Saber qué API transfieren datos confidenciales siempre es importante. Sin embargo, tener un inventario parcial puede resultar la situación más peligrosa, ya que las API ocultas, no aprobadas, zombis y obsoletas son objetivos muy golosos, tienen una protección deficiente y, por lo general, eluden las herramientas de seguridad tradicionales.

Estado actual de los inventarios de API y la concienciación, desglosados por cargo

	Director de seguridad de la información (CISO)	Director de TI	Director de tecnología	Profesional sénior de la seguridad	Seguridad de las aplicaciones
Tenemos un inventario completo **y sabemos** cuáles transfieren datos confidenciales	17,2 %	42,9 %	16,5 %	32,5 %	26,4 %
Tenemos un inventario completo, **pero no sabemos** cuáles transfieren datos confidenciales	41,4 %	36,3 %	34,8 %	42,5 %	47,4 %
Tenemos un inventario parcial de nuestras API **y sabemos** cuáles transfieren datos confidenciales	32,5 %	15,4 %	39,9 %	18,3 %	20,4 %
Tenemos un inventario parcial, **pero no sabemos** cuáles transfieren datos confidenciales	8,3 %	5,5 %	8,2 %	5,8 %	5,2 %

Información basada en la pregunta: ¿Tiene un inventario completo de sus API y sabe cuáles transfieren datos confidenciales? (Seleccione entre cinco opciones); n=1207

En un momento en el que las API no gestionadas se han disparado y han demostrado ser capaces de eludir las herramientas de seguridad tradicionales, estos resultados revelan una brecha de seguridad común que hace que el vector de ataque de las API sea más atractivo para los atacantes.

Por supuesto, las API no gestionadas son solo uno de los atributos (de al menos cinco) de las API que un equipo de seguridad necesita ver y evaluar. La gama incluye:

- **API con vulnerabilidades conocidas** a las que aún no se han aplicado parches
- **API que no se gestionan o que se han olvidado** (en la sombra, no aprobadas, zombis, obsoletas)
- **API expuestas a riesgos externos** (como credenciales, claves y variables fuera de su control)
- **API con errores de los operadores** (configuraciones de seguridad incorrectas en infraestructura y servicios)
- **API con vulnerabilidades no detectadas** y errores que los atacantes identifican y aprovechan

Como mínimo, la variedad de respuestas entre los cargos en relación con los inventarios de API y la visibilidad de las vulnerabilidades de API sugiere que:

- Las empresas siguen confiando en productos de seguridad que no están diseñados específicamente para detectar y proteger las API, especialmente las de alto riesgo y no gestionadas.
- Los departamentos de seguridad aún tienen que definir los atributos de riesgo de una API que deben visualizarse y evaluarse, o bien crear consenso entre sus numerosas unidades de negocio, equipos de desarrolladores y proveedores sobre su estrategia para detectar todas las API y crear un inventario.

Resolver estas discrepancias puede ser un primer paso importante para justificar la inversión en capacidades más sólidas para salvaguardar y proteger todas las API (consulte el apartado "Cómo avanzar hacia una estrategia más madura para la seguridad de API" en la página 18). En la situación actual, la seguridad de las API no suele contar con la atención e interés necesarios para recibir una asignación presupuestaria, lo que dificulta priorizar y financiar iniciativas encaminadas a mejorar no solo la protección de las API y las aplicaciones web, sino también la estrategia de seguridad general de una organización.

Mejor juntas: WAAP + protecciones específicas de API

Diseñada para identificar y mitigar rápidamente las amenazas procedentes de diversos vectores de ataque, la protección de API y aplicaciones web (WAAP) amplía las protecciones tradicionales de un WAF. **Una solución de seguridad de API, que funciona conjuntamente, amplía las protecciones incluso más allá del firewall para crear la defensa más sólida posible**.

¿Se prueban las API con la frecuencia suficiente como para reducir el riesgo de uso malintencionado o vulneraciones?

No, no con la suficiente frecuencia. Las API públicas que tienen errores de configuración, carecen de controles de autenticación, contienen errores de codificación o albergan otros riesgos evitables son exactamente las que los atacantes están buscando, y esos atacantes son cada vez mejores encontrándolas.

Por lo tanto, cada vez que su equipo de desarrollo envía API como estas a producción, sin someterlas a pruebas exhaustivas primero, es como colocar involuntariamente una carga de trabajo futura para su equipo de seguridad (una carga de trabajo que sin duda es urgente y contribuye a lo que nuestros resultados revelaron sobre el estrés).

Pero observe que hemos dicho que son riesgos *evitables*.

Si prueba las API en la fase de desarrollo, con frecuencia y de forma eficiente mediante la automatización, *antes* de lanzarlas al entorno de producción, su organización, sus desarrolladores y su equipo de seguridad jugarán con una ventaja. Y esa ventaja es inmediata, porque esto permite reducir el estrés causado por vulnerabilidades desconocidas y saber que no se encontrarán errores en la fase de producción, que es cuando son exponencialmente más difíciles y costosos de corregir.

Si prueba las API en la fase de desarrollo, con frecuencia y de forma eficiente mediante la automatización, *antes* de lanzarlas al entorno de producción, su organización, sus desarrolladores y su equipo de seguridad jugarán con una ventaja.

Sin embargo, por ahora, el hecho de hacer pruebas no está ganando terreno, según nuestros encuestados. Las frecuencia de las pruebas de API, tanto en tiempo real como a diario, se redujó con respecto al año pasado a lo largo del ciclo de vida de las API, incluso en la fase de producción.

- En 2023, el 18 % de los encuestados en EE. UU. y Reino Unido afirmaron haber realizado pruebas en tiempo real. Esta cifra ha descendido **hasta el 13 % en 2024**.
- En 2023, el 37 % de los encuestados en EE. UU. y Reino Unido afirmaron haber realizado pruebas al menos una vez al día. **En 2024, solo el 13 % realizó pruebas con esta frecuencia**, aunque el 26 % de los encuestados en Alemania realizaron pruebas una vez al día.

Las pruebas semanales de API son más comunes para los participantes de todas las zonas geográficas, pero no alcanzaron el 50 % en ninguna de ellas. Además, la frecuencia de las pruebas de API varió ampliamente entre estas zonas geográficas, desde hacer las pruebas en *tiempo real* hasta *no hacerlas en absoluto*. Sorprendentemente, solo el 6 % de los encuestados respondió que "solo probamos la seguridad de las API antes de enviarlas al entorno de producción". Lo ideal es que los equipos pasen a pruebas continuas a lo largo del ciclo de vida de las API.

¿Qué significa probar continuamente las API?

Las vulnerabilidades se pueden introducir en las API en cualquier momento de su ciclo de vida, desde los errores de codificación que se producen en la fase de desarrollo hasta las brechas de seguridad que surgen cuando los usuarios comienzan a interactuar con la API. Por eso, idealmente, las pruebas de API se realizan en la fase de desarrollo ("shift-left") y también de forma continua mientras están en la fase de producción ("shift-right").

Ejemplos de pruebas de API en la fase de desarrollo:

- Ejecutar pruebas automatizadas que simulan tráfico malicioso.
- Analizar las especificaciones de las API con respecto a las políticas de control establecidas.
- Probar las API bajo demanda o como parte de un proceso de integración e implementación continuas (CI/CD).

Ejemplos de pruebas de API en la fase de producción:

- Supervisar continuamente el tráfico de API y evaluar los metadatos del tráfico.
- Identificar los cambios en las API mediante análisis automatizado.
- Detectar los problemas en tiempo real y corregirlos antes de que los atacantes se den cuenta.

¿Satisfacen sus protocolos de seguridad de API los requisitos de cumplimiento?

En muchas normativas de protección de datos, las API no se mencionan por su nombre, pero los requisitos se centran claramente en proteger las aplicaciones y la infraestructura dentro de las cuales operan las API. Las normativas de cumplimiento están en constante evolución y hay normativas adicionales en curso con implicaciones para las API, incluida la Ley Estadounidense de Derechos de Privacidad (actualmente en modo borrador) y la Ley de Resiliencia Cibernética de la UE.

Las normativas y los marcos de trabajo con implicaciones actuales y directas para la seguridad de API incluyen:

- PCI DSS (actualmente v4.0.1)
- Reglamento General de Protección de Datos (RGPD)
- Ley de Resiliencia Operativa Digital (DORA)
- Ley de Transferibilidad y Responsabilidad de Seguros Médicos (HIPAA)
- Directiva relativa a la seguridad de las redes y sistemas de información (NIS2)

La seguridad de API recibe atención, pero sigue estando en segundo plano

Si los ataques a las API son costosos y suponen sanciones, si contribuyen a la pérdida de confianza de los clientes, si causan un aumento de la presión sobre el personal y la pérdida de credibilidad ante las juntas directivas de las empresas, ¿por qué los equipos no están tomando medidas más decisivas? Las respuestas a las siguientes preguntas nos pueden ayudar a entenderlo.

¿De qué manera están priorizando los distintos cargos empresariales la seguridad de las API?

Pedimos a nuestros encuestados que identificaran sus principales prioridades de ciberseguridad para los próximos 12 meses, y les permitimos seleccionar hasta tres prioridades de una amplia lista (consulte el cuadro). Las seis prioridades principales diferían solo en un 2 % y las seis inferiores solo en un 1 %, lo que sugiere que las prioridades son similares en todas las zonas geográficas y sectores, y que los equipos a menudo se ven obligados a hacer malabarismos con todas ellas.

En algunos sectores, sin embargo, las diferencias de clasificación fundamentales para las API cuentan una historia diferente. Por ejemplo, el sector de energía y servicios públicos asigna a la seguridad de API la prioridad más baja de entre todos los sectores, con un 13,2 % (y por debajo de la media de todos los participantes de la encuesta, con un 18 %). Al mismo tiempo, el sector de energía y servicios públicos también registró el mayor número de incidentes de seguridad de API, con un 91 %, el más alto de todos los ocho sectores y por encima de la media del 84 %. ¿Qué se deduce de estos datos? La baja prioridad dada a la seguridad de API y la alta tasa de ataques.

Prioridades de seguridad más citadas en los próximos 12 meses

1. Defensa contra ataques impulsados por la IA generativa: **21,2 %**
2. Defensa contra el ransomware: **20,5 %**
3. Protección de la autenticación para los usuarios de la plantilla: **19,7 %**
4. Gestión y protección de los secretos de los desarrolladores: **19,6 %**
5. Protección de los terminales: **19,2 %**
6. Soluciones de seguridad en la nube: **19,1 %**
7. Protección del acceso con privilegios a TI: **18,6 %**
8. Prevención de pérdida de datos: **18,6 %**
9. Protección de las API frente a los atacantes: **17,9 %.**
10. Protección de las aplicaciones: **17,7 %**
11. Gestión de información y eventos de seguridad: **17,6 %**
12. Gestión y respuesta a incidentes: **17,6 %**

Información basada en la pregunta: ¿Cuáles son las principales prioridades de ciberseguridad de su empresa en los próximos 12 meses? (Seleccione un máximo de 3); n=1207

Al desglosar las respuestas por cargos, surgieron datos más reveladores:

- Los directores de seguridad de la información mencionaron las amenazas asistidas por la IA generativa y la protección de las API como las principales preocupaciones, con un porcentaje del **25,5 %** y el **24,8 %**, respectivamente.
- El personal de seguridad de las aplicaciones se alineó con los directores de seguridad de la información, citando los ataques asistidos por la IA generativa como su máxima prioridad, con un **22,5 %**.
- Tanto los directores de TI como los directores de tecnología se centraron en el acceso con privilegios, y los directores de tecnología agregaron la respuesta a incidentes en un empate.
- Solo los profesionales sénior de seguridad asignaron al ransomware la máxima prioridad.

Estas diferencias nos llevan de nuevo a formular preguntas como las siguientes: ¿Por qué las distintas capas de la organización de seguridad de TI trabajan aparentemente con distintos manuales de estrategia? ¿Y por qué los principales responsables de seguridad y los empleados de primera línea parecen estar de acuerdo sobre el importante papel que desempeñan las API (y sus riesgos) en los ataques asistidos por IA generativa, mientras que otros cargos no lo están?

Tal vez sea porque los directores de seguridad de la información ven a sus unidades de negocio implementar rápidamente innovaciones como aplicaciones impulsadas por IA generativa para satisfacer la demanda, mientras que los miembros del equipo de seguridad de las aplicaciones opinan igual; solo *ellos* conocen el alcance de las incógnitas con respecto a las vulnerabilidades de los componentes de IA (como los LLM) que acceden a los datos confidenciales. Además, este equipo tiene un asiento en primera fila para las numerosas señales de advertencia que indican que los atacantes están incorporando la IA generativa a sus métodos de ataque.

Pero el motivo principal podría ser el más simple: las comunicaciones entre los altos cargos y los equipos de empleados, tanto en una dirección como en la otra, no se producen con la frecuencia suficiente, especialmente en las grandes empresas, lo que provoca una desconexión entre las prioridades de los directivos frente a lo que los equipos *deben* gestionar en el día a día.

Por último, comparemos las principales prioridades en materia de ciberseguridad de los encuestados con las causas que mencionaron con respecto a sus incidentes de seguridad de API. Como se muestra en la página 17, tres de las causas más citadas se refieren a herramientas de seguridad de aplicaciones tradicionales que no fueron capaces de detectar problemas de API. La comparación ofrece una buena oportunidad para iniciar un debate sobre cómo las soluciones de detección y pruebas de API podrían mejorar no solo su seguridad de API, sino casi todas sus prioridades de seguridad principales.

En otras palabras, si las herramientas de seguridad de API adecuadas pueden proteger no solo las API, sino también mejorar la seguridad de campos como los de los datos, la nube y las aplicaciones, esto hace que la seguridad de API no parezca tanto un campo aislado y un nicho para las partes interesadas. Si hablamos de mejoras para el panorama en general, puede que sea más fácil obtener la aprobación para que las API ocupen un lugar más elevado en la lista de prioridades.

Si las herramientas de seguridad de API adecuadas pueden proteger no solo las API, sino también mejorar la seguridad de campos como los de los datos, la nube y las aplicaciones, esto hace que la seguridad de API no parezca tanto un campo aislado y un nicho para las partes interesadas.

¿La falta de convergencia con respecto a los incidentes de seguridad de API indica que no hay una única fuente de información?

Hemos resaltado las diferencias entre los directivos y el personal de primera línea en sus prioridades generales de seguridad, y esas diferencias persisten en temas más específicos relacionados con las amenazas de API. Por ejemplo, los directores de TI están en sintonía con el equipo de seguridad de las aplicaciones en lo que respecta a la concienciación sobre los ataques a las API (aproximadamente el 88 % de cada cargo afirma haber sufrido incidentes). Mientras tanto, el director de seguridad de la información, el director de tecnología y el profesional sénior de seguridad tienen ocho puntos porcentuales menos: aproximadamente el 80 % afirmó haber sufrido incidentes.

La causa más citada de los incidentes de seguridad de API también varió según el cargo, y la mayoría de los directores de seguridad de la información y profesionales sénior de seguridad afirmaron que la puerta de enlace de API no lo detectó, mientras que los otros tres cargos nombraron a un culpable diferente:

- CISO: La puerta de enlace de API no lo detectó: **26,8 %**
- CIO: Exposición no intencionada a Internet: **28,6 %**
- CTO: El WAF no lo detectó: **25,9 %**
- Profesional sénior de seguridad: La puerta de enlace de API no lo detectó: **23,3 %**
- Equipo de seguridad de las aplicaciones: Configuración incorrecta de API: **23,2 %**

Causas más citadas de los incidentes de seguridad de API, todos los encuestados

1. Las API tuvieron una exposición no intencionada a Internet: **21,8 %**
2. El firewall de aplicaciones web (WAF) no lo detectó: **21,8 %**
3. La puerta de enlace de API no lo detectó: **20,2 %**
4. Las API en herramientas y tecnologías de IA generativa, por ejemplo, LLM: **20,0 %**
5. Configuración incorrecta de API: **19,9 %**
6. El firewall de red no lo detectó: **19,6 %**
7. Herramienta y servicio técnico conocidos, por ejemplo, Microsoft: **19,2 %**
8. Vulnerabilidad debida a errores de codificación de API: **19,1 %**
9. API no gestionadas, por ejemplo, API inactivas o zombis: **18,9 %**
10. Falta de controles de autenticación de API: **18,8 %**
11. Vulnerabilidades de autorización: **18,7 %**
12. Solución de software descargada de Internet: **17,6 %**
13. Solución de software de nivel medio, por ejemplo, Slack: **16,3 %**

Información basada en la pregunta: ¿Cuáles cree que son las causas de los incidentes de seguridad de API que ha experimentado su organización? (Seleccione un máximo de 3); n=1207

El coste indicado de los incidentes de seguridad de API también mostró una falta de consenso entre los cargos más altos y los más bajos, aunque es importante tener en cuenta que al dividir los datos por cargo *y* región da como resultado, naturalmente, un tamaño de muestra menor. Sin embargo, cabe destacar las diferencias en estos subconjuntos, especialmente en EE. UU., donde los directores de TI y los directores de tecnología afirmaron que el coste de los incidentes era de aproximadamente 1 millón de dólares y los directores de seguridad de la información indicaron que era de unos 737 000 dólares, mientras que los profesionales sénior de seguridad y el personal de seguridad de las aplicaciones afirmaron que el coste era de unos 375 000 dólares y 444 000 dólares, respectivamente.

En el Reino Unido, los costes se ajustaron más a los subconjuntos específicos de cargos, aunque los miembros del equipo de seguridad de las aplicaciones de ese país registraron la cifra más alta, con 749 000 libras esterlinas, y los directores de seguridad de la información la cifra más baja, con 190 000 libras esterlinas. Los cargos intermedios variaron desde 374 000 £ hasta 222 000 £. La disparidad de Alemania en cuanto a las afirmaciones sobre costes fue similar a la del Reino Unido, con la estimación más alta procedente del personal con mayor rango y más práctico, 345 000 €, y el coste más bajo de los directores de seguridad de la información con mayor rango, 197 000 €, (resultados opuestos a los de EE. UU.). En general, todos los cargos de todas las regiones creen que los incidentes de seguridad de API afectan especialmente al personal (ver Impactos, página 7).

Cómo avanzar hacia una estrategia más madura para la seguridad de API

Como ya hemos mencionado, nuestros resultados dejan claro que los miembros de los equipos de seguridad de los distintos estratos de la organización no ven la seguridad de API desde el mismo punto de vista. Por otro lado, lo que también está claro es que tienen un terreno común sobre el que construir. Conocen los costes (financieros y humanos) y reconocen que las herramientas en las que han confiado no son suficientes.

Dado que la seguridad de API tiene un impacto tan grande en las organizaciones, los siguientes pasos podrían ser decidir en qué basarse, qué cambiar y mostrar a los líderes cómo proteger las API puede tener un impacto positivo en los resultados. Un buen punto de partida es conseguir un consenso en su departamento de seguridad, desde el director de seguridad de la información hasta el equipo de seguridad de las aplicaciones, sobre cómo priorizar la seguridad de API, seguido de promover una comunicación abierta entre los miembros del equipo de seguridad de las aplicaciones de primera línea y los niveles de gestión intermedios.

Pasos que puede dar

Para cerrar nuestro estudio, hemos reunido una serie de pasos que su equipo de seguridad puede seguir para poner en marcha o desarrollar su estrategia de seguridad de API y avanzar hacia una protección de API madura.

1 Comience con la detección y visibilidad de API

Para llevar a cabo un inventario completo de todo el conjunto de API, busque herramientas con un enfoque automatizado para descubrir las API y los microservicios que admiten. La amplitud de la cobertura es fundamental, ya que las API no gestionadas (consulte el cuadro de la página 10) son un objetivo principal para los atacantes.

2 Invierta en pruebas

Seleccione una solución de seguridad de API que le permita comprobar fácilmente si las API están codificadas correctamente para realizar su función prevista. Idealmente, las pruebas se realizan antes de la implementación, pero también es importante probar todas las API que ya están en producción con análisis en tiempo real del tráfico y las posibles vulnerabilidades.

3 Prosiga con una documentación completa de las API

Auditar constantemente todo su entorno de API para identificar problemas de configuración u otros errores es esencial. Sus capacidades de auditoría también deben garantizar que todas las API cuentan con la documentación adecuada y determinar si contienen datos confidenciales o si carecen de los controles de seguridad adecuados. Esto también le ayuda a prepararse para las normativas de cumplimiento relacionadas con la seguridad de API, tanto implícita como explícitamente (consulte la página 14).

4 Utilice la detección en tiempo de ejecución

Una solución de seguridad de API con detección automatizada en tiempo de ejecución le permite diferenciar entre actividad de API "normal" y "anómala". Gracias a esta forma de supervisar las interacciones de las API, puede detectar aquellos comportamientos que supongan una amenaza en tiempo real y tomar medidas.

5 Responda a los comportamientos sospechosos

Al integrar una solución de seguridad de API con su pila de seguridad existente (por ejemplo, WAF o WAAP), podrá detectar comportamientos de alto riesgo y bloquear el tráfico sospechoso antes de que pueda acceder a los recursos críticos.

6 Investigue y busque amenazas

En la etapa más madura de la seguridad de API, realice análisis forenses a partir de datos de amenazas anteriores para saber si se identificaron correctamente los riesgos y si han surgido patrones que permiten la búsqueda proactiva de amenazas mediante una combinación de herramientas sofisticadas e inteligencia humana.

Conclusión

El informe de este año dejó claro que la seguridad, en este caso, la seguridad de API, no gira solo en torno a las listas de amenazas o herramientas: hay que enfocarse en las personas.

Nuestro estudio confirma que los equipos de seguridad están sobrecargados y que la idea de añadir un nuevo vector de ataque a la carga de trabajo de su equipo puede parecer desalentadora. Sin embargo, la proliferación de API no va a disminuir, y tomar medidas para proteger sus API tiene un fuerte efecto dominó en otras muchas prioridades importantes, como las vulnerabilidades relacionadas con la IA generativa (para proteger las API que intercambian datos con los LLM) y la seguridad en la nube (para reducir el riesgo en todas las API incluidas en las cargas de trabajo que migra).

Creemos firmemente que ser proactivo con respecto a la seguridad de API no solo protege su empresa, sino que también posiciona a su equipo para que sea mucho más creíble y fiable en su visión de este vector de ataque crítico, entre sus homólogos, líderes y la junta directiva. Esto tiene la enorme ventaja de reducir los niveles de estrés en su equipo: nuestro estudio demostró que se ven muy afectados por los incidentes de seguridad de API y el escrutinio y la pérdida de reputación que generan, tanto frente a los compañeros de trabajo como frente a los clientes.

Tomar medidas ahora también facilita de forma preventiva la planificación y la elaboración de informes de cumplimiento, por no hablar de la prevención oportuna de sanciones normativas. ¿Por qué no empezamos ya?

- Si está preparado para considerar los siguientes pasos en su camino hacia una estrategia de seguridad de API madura, le recomendamos que comience echándole un vistazo a nuestro white paper, Fundamentos de seguridad de API.
- Si está listo para hablar sobre sus retos y cómo podemos ayudarle, es muy fácil solicitar una demostración personalizada de Akamai API Security.

Acerca del Estudio sobre el impacto de la seguridad de API

Opinion Matters realizó la encuesta para el Estudio sobre el impacto de la seguridad de API de 2024 entre el 12 de junio de 2023 y el 7 de julio de 2024. Su equipo encuestó a un total de 1207 participantes con el siguiente desglose por domicilio de la empresa: 404 del Reino Unido, 402 de EE. UU. y 401 de Alemania. Un tercio de los encuestados eran directores de TI o directores de seguridad de la información; un tercio eran profesionales sénior de la seguridad; y un tercio pertenecían a equipos de seguridad de aplicaciones que trabajaban en empresas de menos de 500 personas a más de 1000 personas de ocho sectores clave: automoción, servicios financieros, e-commerce y retail, atención sanitaria, seguros, sector gubernamental y público, fabricación y energía y servicios públicos.

Opinion Matters emplea a miembros de The Market Research Society, y sigue el código de conducta de la MRS y los principios de ESOMAR. Opinion Matters también forma parte del British Polling Council.

Créditos

Redactora principal
Annie Brunholzl

Editor jefe
John Natale

Director de investigación
Mitch Mayne

Editora de textos
Randi Kravitz

Promociones
Barney Beal

Marketing y publicación
Georgina Morales Hampe

Revisión y expertos en la materia
Pam Cobb
Jim Lubinskas
Kimberly Gomez
Stas Neyman

Estado de Internet en materia de seguridad

Lea números anteriores del aclamado informe sobre el estado de Internet en materia de seguridad de Akamai y entérese de cuándo se publican los siguientes números. **akamai.com/soti**

Investigación de Akamai sobre amenazas

Conozca los últimos análisis de inteligencia frente a amenazas, informes de seguridad e investigación sobre ciberseguridad. **akamai.com/security-research**

Akamai API Security

Descubra cómo Akamai protege las API a lo largo de todo su ciclo de vida, desde el desarrollo hasta la producción, con capacidades esenciales para la detección de API, la gestión de la estrategia, la protección en tiempo de ejecución y las pruebas de seguridad de API. https://www.akamai.com/products/api-security

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. Gracias a 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 noviembre de 2024.