Akamai

WHITE PAPER

8 cosas que se deben hacer y evitar con respecto a la seguridad de las API

Factores esenciales de una estrategia de seguridad de API sólida

¿Por qué es tan complicado proteger las API?

La seguridad de las API encabeza la lista de prioridades de muchos ejecutivos de TI y por una buena razón. Tenga en cuenta lo siguiente:

"El aumento del número de API se traduce en atractivas superficies de ataque. Por su parte, los responsables de la seguridad siguen desconcertados al respecto".

— The Eight Components of API Security, Forrester Research, Inc., 28 de septiembre de 2023

Factores que influyen en el aumento del riesgo de las API

Para poder hacer frente a estos riesgos, las empresas deben ser conscientes de los siguientes aspectos antes de comenzar a implementar una estrategia de seguridad de API eficaz:

Las API son un objetivo móvil	
Conocimiento de las API internas	**Exposición externa de las API**
Los procesos de DevOps en constante cambio están permanentemente creando y retirando API, por lo que nunca se cuenta con un inventario de API completo.	Unas prácticas de API poco consolidadas ponen, de manera no intencionada, API confidenciales, incluidas muchas API en la sombra, a la vista de terceros.

Las API son vulnerables a dos tipos distintos de amenazas	
Vulnerabilidades técnicas	**Uso indebido y abuso**
Los atacantes pueden aprovechar las vulnerabilidades de software y las configuraciones incorrectas, incluidos los Eliminación de las barreras empresariales	El abuso de la lógica empresarial y otros comportamientos, como el scraping agresivo de datos, pueden producirse de forma independiente a una vulnerabilidad técnica.

Para abordar el desafío complejo de la seguridad de las API, es necesario contar con un enfoque muy estudiado que incluya:

Incorporación de los últimos avances tecnológicos

Eliminación de las barreras empresariales

Gestión del panorama completo de amenazas de API

A continuación se indican algunas estrategias básicas que se deben seguir, y problemas que evitar, en su proceso de creación de una estrategia de seguridad de API más sofisticada en su empresa.

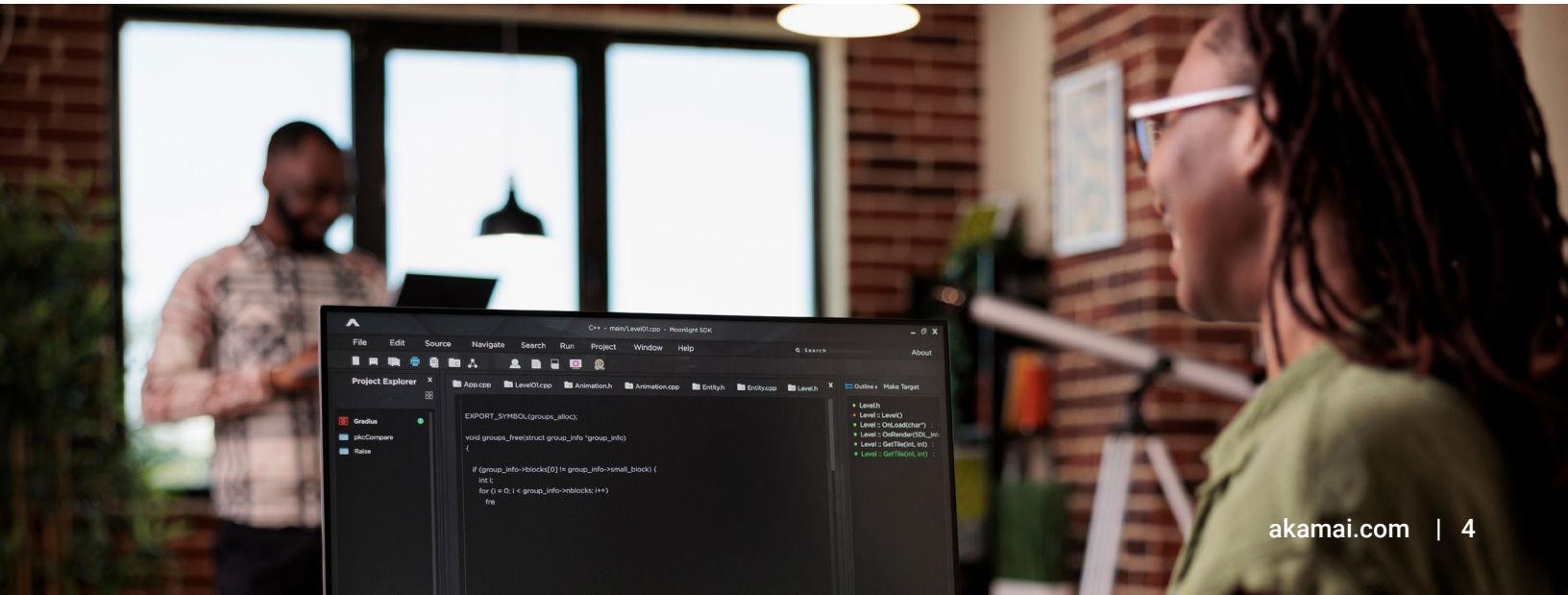
Las 8 cosas que se deben hacer y evitar con respecto a una seguridad de API eficaz

1 Esfuércese por tener una visión completa de las API

Merece la pena insistir: no puede proteger las API si no sabe que las tiene. Cuanto más tiempo pase una API sin identificación ni supervisión, más probabilidades habrá de que se convierta en un objetivo de un atacante. La mejor manera de tener una visión completa es garantizar que su plataforma de seguridad de API pueda incorporar información de la gama más amplia posible de fuentes de datos, entre las que se incluyen puertas de enlace de API, dispositivos de red, soluciones de coordinación de microservicios, proveedores de nube, etc. En concreto, su solución de seguridad de API debería poder hacer lo siguiente:

Tiempo	Lugar
• Detectar las API de forma continua • Supervisar las llamadas a las distintas API • Registrar la actividad de la sesión a corto plazo • Analizar el comportamiento de las API a lo largo del tiempo	• Detectar las API de toda la empresa • Detectar las API heredadas • Identificar las API en la sombra

La visión completa de las API le ayudará a evitar filtraciones de datos en las API, sobre todo porque en la técnica de filtración de datos más reciente los atacantes utilizan la actividad baja y lenta para extraer datos de las API. Saber dónde están todas sus API es el primer paso necesario para evitar este nuevo tipo de ataque.



2 Evite el miedo a la nube

Los firewalls de aplicaciones web (WAF) se valen de técnicas basadas en firmas para evitar que API no autorizadas lleguen a su empresa. Los ataques a las API siguen evolucionando, lo que hace que necesite una capa adicional para defenderlas totalmente frente a toda la gama de posibles riesgos mediante el análisis de comportamiento. Ahora resulta esencial supervisar el comportamiento de las API en su empresa, y no solo de aquellas que quedan expuestas externamente.

Para sacar el máximo partido al análisis de comportamiento, debe analizarse el tráfico de las API en la nube. En ocasiones, los equipos de seguridad se muestran reacios a enviar a la nube información confidencial sobre la actividad de sus empresas. Sin embargo, realizar análisis de comportamiento reales con técnicas de detección y respuesta extendidas sobre el volumen de datos de las API que generan la mayoría de las empresas resulta muy poco práctico sin las posibilidades de ampliación y la flexibilidad que ofrece la nube.

Además, dado que los equipos de seguridad se ven desbordados por la falta de recursos, las implementaciones de productos que impliquen mucho tiempo y que sean complejas supondrán un importante obstáculo para el progreso. Teniendo en cuenta el creciente riesgo que supone un uso cada vez más extendido de las API, los equipos de seguridad no se pueden permitir quedarse atrás. Es por este motivo que necesita migrar a la nube como parte de su estrategia de seguridad de API.

3 Convierta el contexto empresarial en un elemento central de su estrategia

Detectar API e identificar los riesgos de seguridad son solo los primeros pasos para conseguir una superficie de ataque de API menor. Plantéese las tres preguntas siguientes:

1. ¿Cómo podría saber si las credenciales de API de un partner concreto han sido vulneradas?

2. ¿Cómo podría saber si se está produciendo espionaje corporativo como scraping de datos en una API?

3. ¿Cómo podría saber si su API de facturación está sufriendo un ataque por parte de un usuario que itera números de factura para robar datos de cuentas?

En el primer caso, la actividad parece originarse en un usuario legítimo, por lo que la única forma de detectar intenciones maliciosas es observando un cambio en el comportamiento esperado de la API en cuestión. El segundo y tercer caso también representan ejemplos de comportamiento no autorizado que se vale de modelos de acceso de API legítimos. Estos son otros casos en los que resulta fundamental conocer el contexto empresarial, además de lo que ocurre a nivel técnico.

4 Evite que los datos sean una calle de sentido único

Una de las funciones esenciales de un enfoque de seguridad de API eficaz es la capacidad de enviar alertas y eventos a las herramientas de flujo de trabajo de TI y supervisión de seguridad preferidas. Un error que cometen habitualmente los proveedores de seguridad, y los equipos que envían las alertas, es considerar las alertas de seguridad y las respuestas automatizadas como un flujo de comunicación de sentido único.

Al igual que ocurre con otros muchos procesos empresariales legítimos, los ataques pueden producirse durante mucho tiempo. Para conseguir su objetivo previsto, el análisis de comportamiento del uso de las API debe llevarse a cabo durante un periodo de 30 días como mínimo. Esto permite tener una imagen más completa y precisa del comportamiento previsto de referencia. También permite detectar ataques que se ejecutan de forma lenta durante varios días o semanas, así como numerosas sesiones de API. Piense en un ataque de scraping de datos de actividad baja y lenta que se encuentre por debajo de una limitación de velocidad definida: este comportamiento solo se detectaría si se examinara el comportamiento histórico y se tuviera en cuenta cualquier cambio.

Una alerta sin detalles de apoyo posiblemente tendría más desventajas que ventajas. Sin embargo, una alerta con mucho contexto sobre la causa y el efecto sería mucho más útil. No obstante, la verdadera ventaja se consigue al proporcionar una alerta útil con mucho contexto y ofrecer al que la recibe la posibilidad de consultar un conjunto de datos más amplio a la hora de analizar el incidente. Tras esto, puede usar las protecciones de los WAF para bloquear de forma inmediata el tráfico que suponga una posible amenaza para su empresa.

5 Priorice la colaboración interdepartamental

Algunas de las mayores ventajas de la seguridad de API pueden provenir de una prevención proactiva de vulnerabilidades durante las fases de diseño, desarrollo e implementación. Para lograr esto de forma eficaz, necesita que sus equipos colaboren.

Para que empiecen a colaborar, proporcione a los equipos encargados de las API visibilidad sobre cómo se utilizan estas (ya sea de de forma correcta o indebida) en condiciones reales. Con el tiempo, esta exposición fomentará una cultura que lleve a plantearse la seguridad en las primeras fases de los procesos de desarrollo e implementación de API. Además, asegúrese de:

- Que existen ventajas no específicas de la seguridad, además de las características de seguridad principales de su enfoque, que ayuden a los equipos de API a trabajar de forma más eficaz.
- Que resulte sencillo para los usuarios no familiarizados con la seguridad, como el caso de los desarrolladores, ver y consultar el inventario y la información de la actividad de las API.
- Utilizar respuestas contextuales, como integraciones en herramientas de desarrollo, por ejemplo, Jira, que abran de forma proactiva tickets para que se lleven a cabo las correcciones de seguridad que los desarrolladores necesiten realizar.

Considerar que la seguridad de las API es una tarea de todos y facilitar la participación de las partes interesadas externas al equipo de seguridad permite que nos olvidemos de la necesidad de buscar culpables y que los equipos de desarrollo, operaciones y seguridad trabajen juntos de formas beneficiosas para todas las partes.

6 Evite perder de vista las API de terceros

Otro problema habitual que hay que evitar con la estrategia de seguridad de API es asumir que solo tiene que preocuparse por sus propias API. Por más deseable que sea creer que el WAF o la puerta de enlace de API que ha adquirido consolida toda su estrategia de seguridad de API, esto no es siempre así.

Por ejemplo, simplemente por el hecho de que haya una estrategia de puerta de enlace de API centralizada en vigor, no asuma que las API en la sombra no vayan a eludir el enfoque principal de control de API. Si su empresa depende de API de terceros, su puerta de enlace considerará que dichas API están autenticadas, incluso aunque hayan sufrido ataques antes de conectarse a su entorno.

Su estrategia de protección de API debe estar vinculada a sus tecnologías de API principales, como las puertas de enlace de API, pero también debe recopilar toda la información posible de otras fuentes, como dispositivos de red, plataformas en la nube y herramientas de orquestación de microservicios. Esta es la única forma de contar con una imagen completa de su superficie de ataque de las API y de que su estrategia de seguridad tenga garantía de futuro, ya que inevitablemente se producirán cambios tecnológicos y de infraestructuras.

7 Evite responder y pasar a otra cosa

Aunque responder de forma rápida y eficaz a las alertas es algo bueno, si solo se centra en mitigarlas cuando se producen, habrá perdido la oportunidad de evitarlas la próxima vez. Es mejor que se plantee llevar a cabo una búsqueda proactiva de amenazas. Si su partner de seguridad de API le permite realizar consultas de datos, podrá demostrar sus propias hipótesis, conocer las relaciones implicadas e identificar las posibles amenazas antes de que se conviertan en un incidente de seguridad. Por ejemplo, si identifica un comportamiento incorrecto de uso de API por parte de un partner específico, podrá buscar un comportamiento similar por parte de otros partners o proveedores con unos pocos clics.

Cualquier partner de seguridad de API debe almacenar los datos históricos en un lago de datos y permitir el acceso a esos datos para favorecer las investigaciones y la búsqueda de amenazas.

Lo ideal es que este tipo de funciones de consulta completas se ofrezca de dos formas:

1. Como interfaz web de usuario sencilla e intuitiva.

2. Como conjunto de interfaces de API en los propios proveedores de seguridad de API para permitir su uso durante el desarrollo de flujos de trabajo más sofisticados.

8 Plantéese la seguridad de las API como un proceso continuo

La mejor forma de integrar la seguridad de las API directamente en su empresa es a través de las pruebas de API. Al añadir esta herramienta al ciclo de vida de las API, puede limitar las posibilidades de que una API vulnerable o mal configurada llegue a la fase de producción. Estas pruebas y correcciones en las primeras fases del ciclo de desarrollo provocan menos dolores de cabeza, ahorran tiempo y reducen los gastos.

A continuación, los equipos de seguridad deben comenzar a trabajar para proteger sus API mediante la creación de un inventario de aquellas que se están usando en sus empresas. Como se añaden y retiran API de forma constante, es fundamental que los equipos de seguridad mantengan un inventario actualizado de las interfaces de API en sus repositorios de datos y aplicaciones confidenciales. Cuando la detección continua de API se realiza de forma eficaz, las API en la sombra, no autorizadas, olvidadas, zombis, huérfanas y obsoletas se convierten en problemas del pasado.

Los equipos de seguridad deben contar con la visibilidad que necesitan para detectar y mitigar una amplia gama de nuevas amenazas de seguridad de API. Pero esto no impide que deba llevarse a cabo la detección de amenazas durante el tiempo de ejecución. El abuso de la lógica empresarial solo se encuentra en las API en producción. La comparación del comportamiento en tiempo de ejecución con los patrones de uso normales de referencia ayuda a revelar un comportamiento abusivo.

Por último, es importante detener realmente las amenazas que podrían atacar sus API en cualquier momento durante el tiempo de ejecución. El bloqueo automático por parte del WAF resulta fundamental para este paso, ya que tener simplemente alertas para todo no será suficiente para proteger su empresa a nivel general. Otras respuestas automatizadas se pueden modificar y personalizar, por ejemplo, al reducir la limitación de velocidad en la puerta de enlace de API, abrir un ticket de Jira para que un desarrollador lo investigue o enviar un correo electrónico al equipo de seguridad. Solo se puede responder de la forma adecuada a cada una de las amenazas detectadas cuando se conoce el contexto y se puede adaptar el mecanismo de respuesta.

Resumen

Qué hacer	Qué evitar
✓ Esfuércese por tener una visión completa de las API	✗ Evite el miedo a la nube
✓ Convierta el contexto empresarial en un elemento central de su estrategia	✗ Evite que los datos sean una calle de sentido único
✓ Priorice la colaboración interdepartamental	✗ Evite perder de vista las API de terceros
✓ Plantéese la seguridad de las API como un proceso continuo	✗ Evite responder y pasar a otra cosa

Comience hoy mismo

¿Está preparado para dar el primer paso hacia un enfoque moderno y sistemático de la seguridad de las API?

Más información sobre Akamai API Security.

El planteamiento en materia de seguridad de Akamai basado en la nube permite comenzar en minutos. En cuestión de horas, podrá disfrutar de una visión general del uso de las API en toda su empresa y tener una idea clara de las relaciones entre su lógica empresarial y sus API.